Audit-Protokollierung

Active IQ Unified Manager 9.11

NetApp
October 16, 2025

This PDF was generated from https://docs.netapp.com/de-de/active-iq-unified-manager-911/config/task_configure_audit_logs.html on October 16, 2025. Always check docs.netapp.com for the latest.

Inhalt

Audit-Protokollierung 1
Audit-Protokolle werden konfiguriert 2
Aktivieren der Fernprotokollierung von Audit-Protokollen 2

Audit-Protokollierung

Sie können erkennen, ob die Audit-Protokolle unter Verwendung von Audit-Protokollen kompromittiert wurden. Alle von einem Benutzer durchgeführten Aktivitäten werden überwacht und in den Audit-Protokollen protokolliert. Die Audits werden für alle Benutzerschnittstellen und öffentlich exponierte APIs' Funktionalitäten von Active IQ Unified Manager durchgeführt.

Sie können die Ansicht Überwachungsprotokoll: Dateiansicht verwenden, um alle in Ihrem Active IQ Unified Manager verfügbaren Audit-Log-Dateien anzuzeigen und darauf zuzugreifen. Die Dateien im Audit Log: File View werden basierend auf ihrem Erstellungsdatum aufgelistet. In dieser Ansicht werden Informationen über das gesamte Überwachungsprotokoll angezeigt, das von der Installation oder dem Upgrade auf die im System vorhandenen Protokolle erfasst wird. Wenn Sie in Unified Manager eine Aktion ausführen, werden die Informationen aktualisiert und stehen in den Protokollen zur Verfügung. Der Status jeder Protokolldatei wird mit dem Attribut „`File Integrity Status`“ erfasst, das aktiv überwacht wird, um Manipulation oder Löschung der Protokolldatei zu erkennen. Die Audit-Protokolle können einen der folgenden Status haben, wenn die Audit-Protokolle im System verfügbar sind:

Bundesland	Beschreibung
AKTIV	Datei, in der Protokolle aktuell protokolliert werden.
NORMAL	Datei, die inaktiv, komprimiert und im System gespeichert ist.
MANIPULIERT	Datei, die von einem Benutzer kompromittiert wurde, der die Datei manuell bearbeitet hat.
MANUELL_LÖSCHEN	Datei, die von einem autorisierten Benutzer gelöscht wurde.
ROLLOVER_DELETE	Datei, die aufgrund von Rolling Off auf der Grundlage Rolling Configuration Policy gelöscht wurde.
UNEXPECTED_DELETE	Datei, die aus unbekannten Gründen gelöscht wurde.

Die Seite „Prüfprotokoll“ enthält die folgenden Befehlsschaltflächen:

- Konfigurieren
- Löschen
- Download

Mit der Schaltfläche **DELETE** können Sie alle in der Ansicht Audit Logs aufgeführten Audit-Protokolle löschen. Sie können ein Audit-Protokoll löschen und optional einen Grund angeben, die Datei zu löschen, was in Zukunft hilft, ein gültiges Löschen zu bestimmen. Die SPALTE GRUND enthält den Grund und den Namen des Benutzers, der den Löschvorgang durchgeführt hat.

Das Löschen einer Protokolldatei führt zum Löschen der Datei aus dem System, der Eintrag in der DB-Tabelle wird jedoch nicht gelöscht.

Sie können die Audit-Protokolle von Active IQ Unified Manager mit der Schaltfläche **DOWNLOAD** im Bereich Audit-Protokolle herunterladen und die Audit-Log-Dateien exportieren. Die Dateien, die als „`NORMAL`“ oder „`MANIPULIERT`“ markiert sind, werden komprimiert heruntergeladen `.gzip` Formatieren.

Wenn ein komplettes AutoSupport Bundle generiert wird, enthält das Support Bundle sowohl archivierte als auch aktive Audit-Log-Dateien. Wenn aber ein Light Support Bundle erzeugt wird, enthält es nur die aktiven Audit-Protokolle. Die archivierten Prüfprotokolle sind nicht enthalten.

Audit-Protokolle werden konfiguriert

Sie können die Schaltfläche **Konfigurieren** im Bereich Audit Logs verwenden, um die Rolling Policy für Audit Log-Dateien zu konfigurieren und auch die Remote-Protokollierung für die Audit-Protokolle zu aktivieren.

Sie können die Werte in den AUFBEWAHRUNGSTAGEN **MAX-DATEIGRÖSSE** und **AUDIT-LOGBUCH** entsprechend der gewünschten Menge und Häufigkeit der Daten festlegen, die Sie im System speichern möchten. Der Wert im Feld **GESAMTE LOGGRÖSSE DES AUDITS** ist die Größe der gesamten Audit-Log-Daten im System. Die Roll-Over-Richtlinie wird durch die Werte im Feld **AUDIT LOG RETENTION DAYS**, **MAX FILE SIZE** und **TOTAL AUDIT LOG SIZE** bestimmt. Wenn die Größe des Backups des Revisionsprotokolls den in **GESAMT-AUDIT-LOG-GRÖSSE** konfigurierten Wert erreicht, wird die zuerst archivierte Datei gelöscht. Das bedeutet, dass die älteste Datei gelöscht wird. Der Dateieintrag ist jedoch weiterhin in der Datenbank verfügbar und wird als „`Rollover Delete`“ markiert. Der **AUDIT LOG RETENTION DAYS**-Wert gilt für die Anzahl der Tage, an denen die Audit Log-Dateien aufbewahrt werden. Jede Datei, die älter als der in diesem Feld eingestellte Wert ist, wird über gerollt.

Schritte

1. Klicken Sie Auf **Prüfprotokolle** > **Konfigurieren**.
2. Geben Sie die Werte in den * MAX-DATEIGRÖSSEN*, **GESAMT-AUDIT-LOG-GRÖSSE** und **AUDIT-LOG-AUFBEWAHRUNGSTAGE** ein.

   Wenn Sie die Fernprotokollierung aktivieren möchten, wählen Sie die Option **Remote Logging aktivieren**.

Aktivieren der Fernprotokollierung von Audit-Protokollen

Aktivieren Sie das Kontrollkästchen **Remote-Protokollierung aktivieren** im Dialogfeld Audit-Protokolle konfigurieren, um die Remote-Audit-Protokollierung zu aktivieren. Mit dieser Funktion können Sie Überwachungsprotokolle an einen Remote Syslog-Server übertragen. Auf diese Weise können Sie Ihre Audit-Protokolle verwalten, wenn es Platzbeschränkungen gibt.

Die Remote-Protokollierung von Audit-Protokollen bietet ein manipulationssicheres Backup, falls die Audit-Log-Dateien auf dem Active IQ Unified Manager Server manipuliert werden.

Schritte

1. Aktivieren Sie im Dialogfeld **Audit Logs konfigurieren** das Kontrollkästchen **Remote Logging aktivieren**.

Zusätzliche Felder zum Konfigurieren der Remote-Protokollierung werden angezeigt.

2. Geben Sie den **HOSTNAME** und den **PORT** des Remoteserver ein, mit dem Sie eine Verbindung herstellen möchten.
3. Klicken Sie im Feld **SERVER CA ZERTIFIKAT** auf **DURCHSUCHEN**, um ein öffentliches Zertifikat des Zielservers auszuwählen.

   Das Zertifikat sollte in hochgeladen werden `.pem` Formatieren. Dieses Zertifikat sollte vom Ziel-Syslog-Server abgerufen werden und sollte nicht abgelaufen sein. Das Zertifikat sollte den ausgewählten „`hostname`“ als Teil des enthalten `SubjectAltName` (SAN)-Attribut.

4. Geben Sie die Werte für die folgenden Felder ein: **CHARSET**, **VERBINDUNGS-TIMEOUT**, **VERBINDUNGSVERZÖGERUNG**.

   Für diese Felder sollten die Werte in Millisekunden angegeben werden.

5. Wählen Sie das erforderliche Syslog-Format und die TLS-Protokollversion in den Feldern **FORMAT** und **PROTOKOLL** aus.
6. Aktivieren Sie das Kontrollkästchen **Client Authentication** aktivieren, wenn für den Ziel-Syslog-Server eine zertifikatbasierte Authentifizierung erforderlich ist.

   Sie müssen das Clientauthentifizierungszertifikat herunterladen und auf den Syslog-Server hochladen, bevor Sie die Konfiguration des Überwachungsprotokolls speichern. Andernfalls schlägt die Verbindung fehl. Je nach Typ des Syslog-Servers müssen Sie möglicherweise einen Hash des Client-Authentifizierungszertifikats erstellen.

   Beispiel: Syslog-ng erfordert, dass mit dem Befehl ein <Hash> des Zertifikats erstellt wird `openssl x509 -noout -hash -in cert.pem`, Und dann sollten Sie symbolisch das Clientauthentifizierungszertifikat mit einer Datei verknüpfen, die nach dem <Hash> .0 benannt ist.

7. Klicken Sie auf **Speichern**, um die Verbindung mit Ihrem Server zu konfigurieren und die Fernprotokollierung zu aktivieren.

   Sie werden zur Seite Audit Logs weitergeleitet.

Copyright-Informationen

Copyright © 2025 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.