Audit-Logging

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/de-de/active-iq-unified-manager-918/config/concept_audit_logging.html on November 13, 2026. Always check docs.netapp.com for the latest.

Inhalt

Audit-Logging 1
Informationen zu Audit-Protokollen in Active IQ Unified Manager 1
Konfiguration der Audit-Protokolle von Active IQ Unified Manager 2
Die Remote-Protokollierung von Audit-Protokollen in Active IQ Unified Manager kann aktiviert werden 2

Audit-Logging

Informationen zu Audit-Protokollen in Active IQ Unified Manager

Mithilfe von Revisionsprotokollen lässt sich feststellen, ob die Revisionsprotokolle manipuliert wurden. Alle von einem Benutzer durchgeführten Aktivitäten werden überwacht und in den Revisionsprotokollen protokolliert. Die Audits werden für alle Funktionen der Benutzeroberfläche und der öffentlich zugänglichen APIs von Active IQ Unified Manager durchgeführt.

Mit der **Audit Log: File View** können Sie alle in Ihrem Active IQ Unified Manager verfügbaren Revisionsprotokolldateien anzeigen und darauf zugreifen. Die Dateien in der **Audit Log: File View** sind nach ihrem Erstellungsdatum aufgelistet. Diese Ansicht zeigt Informationen zu allen Revisionsprotokollen an, die seit der Installation oder dem Upgrade bis zum aktuellen Zeitpunkt im System erfasst wurden. Wenn Sie im Unified Manager eine Aktion ausführen, werden die Informationen aktualisiert und sind in den Protokollen verfügbar. Der Status jeder Protokolldatei wird mithilfe des Attributs “File Integrity Status” erfasst, das aktiv überwacht wird, um Manipulationen oder das Löschen der Protokolldatei zu erkennen. Die Revisionsprotokolle können einen der folgenden Status aufweisen, wenn sie im System verfügbar sind:

Status	Beschreibung
AKTIV	Datei, in der Protokolle derzeit protokolliert werden.
NORMAL	Eine inaktive, komprimierte und im System gespeicherte Datei.
MANIPULIERT	Datei, die von einem Benutzer kompromittiert wurde, der die Datei manuell bearbeitet hat.
MANUAL_DELETE	Datei, die ein autorisierter Benutzer gelöscht hat.
ROLLOVER_DELETE	Datei, die aufgrund des auf der Rolling Configuration Policy basierenden Entfernens gelöscht wurde.
UNEXPECTED_DELETE	Datei, die aus unbekannten Gründen gelöscht wurde.

Die Seite „Revisionsprotokoll“ enthält die folgenden Befehlsschaltflächen:

- Konfigurieren
- Löschen
- Download

Mit der Schaltfläche **DELETE** können Sie alle in der Ansicht „Audit Logs“ aufgeführten Revisionsprotokolle löschen. Sie können ein Revisionsprotokoll löschen und optional einen Grund für das Löschen der Datei angeben, was künftig dabei hilft, eine gültige Löschung nachzuvollziehen. In der Spalte REASON werden der Grund zusammen mit dem Namen des Benutzers aufgeführt, der den Löschvorgang durchgeführt hat.



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

Sie können die Revisionsprotokolle aus Active IQ Unified Manager über die Schaltfläche **HERUNTERLADEN** im Bereich „Audit Logs“ herunterladen und die Revisionsprotokolldateien exportieren. Die Dateien, die als

„NORMAL“ oder „TAMPERED“ gekennzeichnet sind, werden in einem komprimierten `.gzip` Format heruntergeladen.

Die Revisionsprotokoll-Dateien werden regelmäßig archiviert und zur späteren Referenz in der Datenbank gespeichert. Vor der Archivierung werden die Revisionsprotokolle digital signiert, um die Sicherheit und Integrität zu wahren.

Wenn ein vollständiges AutoSupport Bundle generiert wird, enthält das Support Bundle sowohl archivierte als auch aktive Revisionsprotokolldateien. Wenn jedoch ein kompaktes Support Bundle generiert wird, enthält es nur die aktiven Revisionsprotokolle. Die archivierten Revisionsprotokolle sind nicht enthalten.

Konfiguration der Audit-Protokolle von Active IQ Unified Manager

Mit der Schaltfläche **Configure** im Abschnitt „Revisionsprotokolle“ lässt sich die Rotationsrichtlinie für Revisionsprotokolldateien konfigurieren und außerdem die Remote Protokollierung für die Revisionsprotokolle aktivieren.

Sie können die Werte in **MAX FILE SIZE** und **AUDIT LOG RETENTION DAYS** entsprechend der gewünschten Datenmenge und -häufigkeit festlegen, die Sie im System speichern möchten. Der Wert im Feld **TOTAL AUDIT LOG SIZE** ist die Größe der gesamten im System vorhandenen Revisionsprotokolldaten. Die Rotationsrichtlinie wird durch die Werte im Feld **AUDIT LOG RETENTION DAYS**, **MAX FILE SIZE** und **TOTAL AUDIT LOG SIZE** bestimmt. Wenn die Größe der Revisionsprotokoll-Sicherung den in **TOTAL AUDIT LOG SIZE** konfigurierten Wert erreicht, wird die Datei gelöscht, die zuerst archiviert wurde. Das bedeutet, dass die älteste Datei gelöscht wird. Der Dateieintrag bleibt jedoch weiterhin in der Datenbank verfügbar und ist als “Rollover Delete” gekennzeichnet. Der Wert **AUDIT LOG RETENTION DAYS** steht für die Anzahl der Tage, für die die Revisionsprotokolldateien aufbewahrt werden. Jede Datei, die älter ist als der in diesem Feld festgelegte Wert, wird rotiert.

Schritte

1. **Revisionsprotokolle** > > **Konfigurieren** auswählen.
2. Werte für **MAXIMALE DATEIGRÖSSE**, **GESAMTGRÖSSE DES REVISIONSPROTOKOLLS** und **AUFBEWAHRUNGSTAGE DES REVISIONSPROTOKOLLS** werden eingegeben.

   Die Aktivierung der Remote-Protokollierung erfolgt über **Enable Remote Logging**.

Die Remote-Protokollierung von Audit-Protokollen in Active IQ Unified Manager kann aktiviert werden

Sie können im Dialogfeld „Revisionsprotokolle konfigurieren“ das Kontrollkästchen „Remote-Protokollierung aktivieren“ auswählen, um die Remote-Revisionsprotokollierung zu aktivieren. Mit dieser Funktion können Sie Revisionsprotokolle an einen Remote-Syslog-Server übertragen. Dies ermöglicht Ihnen, Ihre Revisionsprotokolle auch bei begrenztem Speicherplatz zu managen.

Die Remote-Protokollierung von Revisionsprotokollen bietet eine manipulationssichere Sicherung für den Fall, dass die Revisionsprotokoll-Dateien auf dem Active IQ Unified Manager Server manipuliert werden.

Schritte

1. Im Dialogfeld **Revisionsprotokolle konfigurieren** kann das Kontrollkästchen **Remote-Protokollierung aktivieren** ausgewählt werden.

   Es werden zusätzliche Felder zum Konfigurieren der Remote-Protokollierung angezeigt.

2. Für die Verbindung mit dem gewünschten Remote-Server werden **HOSTNAME** und **PORT** eingegeben.
3. Im Feld **SERVER CA CERTIFICATE** erfolgt die Auswahl eines öffentlichen Zertifikats des Zielservers über **BROWSE**.

   Das Zertifikat sollte im `.pem` Format hochgeladen werden. Dieses Zertifikat sollte vom Ziel Syslog-Server bezogen werden und darf nicht abgelaufen sein. Das Zertifikat sollte den ausgewählten “hostname” als Teil des `SubjectAltName`(SAN)-Attributs enthalten.

4. Einzugeben sind die Werte für die folgenden Felder: **CHARSET**, **CONNECTION TIMEOUT**, **RECONNECTION DELAY**.

   Die Werte sollten für diese Felder in Millisekunden angegeben werden.

5. Die Auswahl des gewünschten Syslog-Formats und der TLS Protokollversion erfolgt in den Feldern **FORMAT** und **PROTOCOL**.
6. Wenn der Ziel-Syslog-Server eine zertifikatbasierte Authentifizierung erfordert, ist das Kontrollkästchen **Client-Authentifizierung aktivieren** auszuwählen.

   Sie müssen das Zertifikat für die Client-Authentifizierung herunterladen und vor dem Speichern der Konfiguration des Revisionsprotokolls auf den Syslog-Server hochladen, andernfalls schlägt die Verbindung fehl. Je nach Typ des Syslog-Servers müssen Sie möglicherweise einen Hash des Zertifikats für die Client-Authentifizierung erstellen.

   Beispiel: syslog-ng erfordert, dass ein <hash> des Zertifikats mit dem Befehl `openssl x509 -noout -hash -in cert.pem` erstellt wird. Anschließend sollten Sie das Client-Authentifizierungs-Zertifikat symbolisch mit einer Datei verknüpfen, die nach dem <hash> .0 benannt ist.

7. **Speichern** konfiguriert die Verbindung mit Ihrem Server und aktiviert die Remote-Protokollierung.

   Sie werden zur Seite „Revisionsprotokolle“ weitergeleitet.

> Der Wert für **Verbindungs-Zeitüberschreitung** kann sich auf die Konfiguration auswirken. Wenn die Konfiguration länger für eine Antwort benötigt als der definierte Wert, kann dies aufgrund eines Verbindungsfehlers zu einem Konfigurationsfehler führen. Für den Aufbau einer erfolgreichen Verbindung sollte der Wert für **Verbindungs-Zeitüberschreitung** erhöht und die Konfiguration erneut versucht werden.

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.