Audit-Protokollierung

Active IQ Unified Manager 9.13

NetApp
December 18, 2023

Inhalt

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.

Mit dem **Audit Log: File View** können Sie alle in Ihrem Active IQ Unified Manager verfügbaren Audit-Log-Dateien anzeigen und darauf zugreifen. 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:

Status	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.

Die Audit-Log-Dateien werden regelmäßig archiviert und zur Referenz in der Datenbank gespeichert. Vor der Archivierung werden die Audit-Protokolle digital signiert, um die Sicherheit und Integrität zu gewährleisten.

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.

> Der Wert **Connection Timeout** kann sich auf die Konfiguration auswirken. Wenn die Konfiguration länger als der definierte Wert reagiert, kann dies zu einem Konfigurationsfehler aufgrund eines Verbindungsfehlers führen. Um eine erfolgreiche Verbindung herzustellen, erhöhen Sie den Wert **Connection Timeout** und versuchen Sie die Konfiguration erneut.