# Registrazione di audit

## Active IQ Unified Manager

NetApp
November 13, 2026

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

# Sommario

Registrazione di audit . . . . . 1
Scopri i registri di controllo in Active IQ Unified Manager . . . . . 1
Configura i registri di controllo di Active IQ Unified Manager . . . . . 2
Abilita la registrazione remota dei log di controllo in Active IQ Unified Manager . . . . . 2

# Registrazione di audit

## Scopri i registri di controllo in Active IQ Unified Manager

Puoi rilevare se i log di audit sono stati compromessi utilizzando Audit Logs. Tutte le attività eseguite da un utente vengono monitorate e registrate in Audit Logs. Gli audit vengono eseguiti per tutte le funzionalità dell'interfaccia utente e delle API esposte pubblicamente di Active IQ Unified Manager.

Puoi usare **Audit Log: File View** per visualizzare e accedere a tutti i file di audit log disponibili in Active IQ Unified Manager. I file in Audit Log: File View sono elencati in base alla data di creazione. Questa vista mostra le informazioni di tutti gli audit log acquisiti dall'installazione o dall'aggiornamento fino al presente nel sistema. Ogni volta che esegui un'azione in Unified Manager, le informazioni vengono aggiornate e sono disponibili nei log. Lo stato di ciascun file di log viene acquisito usando l'attributo "File Integrity Status", che viene monitorato attivamente per rilevare manomissioni o eliminazioni del file di log. Gli audit log possono avere uno dei seguenti stati quando sono disponibili nel sistema:

| Stato | Descrizione |
|---|---|
| ATTIVO | File in cui sono attualmente registrati i log. |
| NORMALE | File inattivo, compresso e memorizzato nel sistema. |
| MANOMESSO | File compromesso da un utente che lo ha modificato manualmente. |
| MANUAL_DELETE | File eliminato da un utente autorizzato. |
| ROLLOVER_DELETE | File eliminato a causa della rimozione in base al criterio di configurazione Rolling. |
| UNEXPECTED_DELETE | File eliminato per motivi sconosciuti. |

La pagina Audit Log include i seguenti pulsanti di comando:

- Configurare
- Elimina
- Scarica

Il pulsante **DELETE** ti consente di eliminare uno qualsiasi dei log di controllo elencati nella vista Audit Logs. Puoi eliminare un log di controllo e, facoltativamente, specificare un motivo per eliminare il file, il che ti aiuterà in futuro a determinare se l'eliminazione è valida. La colonna REASON elenca il motivo insieme al nome dell'utente che ha eseguito l'operazione di eliminazione.

Se elimini un file di log, il file verrà rimosso dal sistema, ma la relativa voce nella tabella DB non verrà eliminata.

Puoi scaricare i log di audit da Active IQ Unified Manager utilizzando il pulsante **DOWNLOAD** nella sezione Log di audit ed esportare i file di log di audit. I file contrassegnati come "NORMAL" o "TAMPERED" vengono scaricati in formato `.gzip` compresso.

I file di log di audit vengono archiviati periodicamente e salvati nel database per consultazione. Prima dell'archiviazione, i file di log di audit vengono firmati digitalmente per garantirne la sicurezza e l'integrità.

Quando viene generato un bundle AutoSupport completo, il bundle di supporto include sia i file di log di audit archiviati che quelli attivi. Ma quando viene generato un bundle di supporto leggero, include solo i file di log di audit attivi. I file di log di audit archiviati non sono inclusi.

# Configura i registri di controllo di Active IQ Unified Manager

Puoi usare il pulsante **Configure** nella sezione Audit Logs per configurare i criteri di rotazione per i file Audit Log e anche per abilitare la registrazione remota per gli Audit Logs.

Puoi impostare i valori di **MAX FILE SIZE** e **AUDIT LOG RETENTION DAYS** in base alla quantità e alla frequenza dei dati che vuoi archiviare nel sistema. Il valore nel campo **TOTAL AUDIT LOG SIZE** rappresenta la dimensione totale dei dati dell'audit log presenti nel sistema. La policy di rollover è determinata dai valori nei campi **AUDIT LOG RETENTION DAYS**, **MAX FILE SIZE** e **TOTAL AUDIT LOG SIZE**. Quando la dimensione del backup dell'audit log raggiunge il valore configurato in **TOTAL AUDIT LOG SIZE**, il file archiviato per primo viene eliminato. Questo significa che il file meno recente viene eliminato. Tuttavia, la voce del file continua a essere disponibile nel database ed è contrassegnata come "Rollover Delete". Il valore di **AUDIT LOG RETENTION DAYS** indica il numero di giorni per cui i file dell'audit log vengono conservati. Qualsiasi file più vecchio del valore impostato in questo campo viene sottoposto a rollover.

**Passaggi**

1. Fai clic su **Registri di controllo** > > **Configura**.
2. Inserisci i valori in **DIMENSIONE MASSIMA DEL FILE**, **DIMENSIONE TOTALE DEL LOG DI AUDIT** e **GIORNI DI CONSERVAZIONE DEL LOG DI AUDIT**.

   Per abilitare la registrazione remota, seleziona **Abilita registrazione remota**.

# Abilita la registrazione remota dei log di controllo in Active IQ Unified Manager

Puoi selezionare la casella di controllo **Enable Remote Logging** nella finestra di dialogo Configure Audit Logs per abilitare la registrazione remota dei log di controllo. Puoi usare questa funzionalità per trasferire i log di controllo a un server Syslog remoto. In questo modo puoi gestire i log di controllo quando lo spazio è limitato.

La registrazione remota dei log di controllo fornisce un backup a prova di manomissione nel caso in cui i file di log di controllo sul server Active IQ Unified Manager vengano manomessi.

**Passaggi**

1. Nella finestra di dialogo **Configura log di audit**, seleziona la casella di controllo **Abilita registrazione remota**.

   Vengono visualizzati campi aggiuntivi per configurare la registrazione remota.

2. Inserisci il **HOSTNAME** e **PORT** del server remoto a cui vuoi connetterti.
3. Nel campo **CERTIFICATO CA DEL SERVER**, fai clic su **SFOGLIA** per selezionare un certificato pubblico del server di destinazione.

   Il certificato deve essere caricato in `.pem` formato. Questo certificato deve essere ottenuto dal server Syslog di destinazione e non deve essere scaduto. Il certificato deve contenere "hostname" selezionato

come parte dell'attributo `SubjectAltName` (SAN).

4. Inserisci i valori per i seguenti campi: **CHARSET**, **CONNECTION TIMEOUT**, **RECONNECTION DELAY**.

   I valori per questi campi devono essere espressi in millisecondi.

5. Seleziona il formato Syslog e la versione del protocollo richiesti nei campi **FORMATO** e **PROTOCOLLO**.
6. Seleziona la casella di controllo **Abilita autenticazione del client** se il server Syslog di destinazione richiede l'autenticazione basata su certificati.

   Dovrai scaricare il certificato di autenticazione del client e caricarlo sul server Syslog prima di salvare la configurazione di Audit Log, altrimenti la connessione non riuscirà. A seconda del tipo di server Syslog, potresti dover creare un hash del certificato di autenticazione del client.

   Esempio: syslog-ng richiede che venga creato <hash> del certificato utilizzando il comando `openssl x509 -noout -hash -in cert.pem`, quindi dovresti creare un collegamento simbolico dal certificato di autenticazione del client a un file denominato in base a <hash> .0.

7. Fai clic su **Salva** per configurare la connessione con il tuo server e abilitare la registrazione remota.

   Sarai reindirizzato alla pagina dei log di audit.



Il valore di **Timeout di connessione** può influire sulla configurazione. Se la configurazione impiega più tempo a rispondere rispetto al valore definito, può causare un errore della configurazione dovuto a un errore di connessione. Per stabilire una connessione corretta, aumenta il valore di **Timeout di connessione** e riprova la configurazione.

## Informazioni sul copyright

Copyright © 2026 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

## Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina http://www.netapp.com/TM sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.