Gestisci l'autenticazione

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/task_edit_authentication_servers.html on November 13, 2026. Always check docs.netapp.com for the latest.

Sommario

Gestisci l'autenticazione . . . 1
- Modifica i server di autenticazione in Active IQ Unified Manager . . . 1
- Elimina i server di autenticazione in Active IQ Unified Manager . . . 1
- Autenticati con Active Directory o OpenLDAP in Active IQ Unified Manager . . . 1
- Registrazione di audit . . . 2
  - Scopri i registri di controllo in Active IQ Unified Manager . . . 2
  - Configura i registri di controllo di Active IQ Unified Manager . . . 3
  - Abilita la registrazione remota dei log di controllo in Active IQ Unified Manager . . . 3
- Usa la pagina di autenticazione remota in Active IQ Unified Manager . . . 4
  - Area dei server di autenticazione . . . 7

Gestisci l’autenticazione

Modifica i server di autenticazione in Active IQ Unified Manager

Puoi cambiare la porta che il server Unified Manager usa per comunicare con il tuo server di autenticazione.

Prima di iniziare

Devi avere il ruolo di Amministratore dell’applicazione.

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Generale** > **Autenticazione remota**.
2. Seleziona la casella **Disable Nested Group Lookup**.
3. Nell’area **Server di autenticazione**, seleziona il server di autenticazione che vuoi modificare, quindi fai clic su **Modifica**.
4. Nella finestra di dialogo **Modifica server di autenticazione**, modifica i dettagli della porta.
5. Fare clic su **Save**.

Elimina i server di autenticazione in Active IQ Unified Manager

Puoi eliminare un server di autenticazione se vuoi impedire al server Unified Manager di comunicare con il server di autenticazione. Ad esempio, se vuoi cambiare un server di autenticazione con cui comunica il server di gestione, puoi eliminare il server di autenticazione e aggiungerne uno nuovo.

Prima di iniziare

Devi avere il ruolo di Amministratore dell’applicazione.

Quando elimini un server di autenticazione, gli utenti o i gruppi remoti di tale server non potranno più accedere a Unified Manager.

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Generale** > **Autenticazione remota**.
2. Seleziona uno o più server di autenticazione che desideri eliminare, quindi fai clic su **Elimina**.
3. Fai clic su **Sì** per confermare la richiesta di eliminazione.

   Se l’opzione **Usa connessione sicura** è abilitata, i certificati associati al server di autenticazione vengono eliminati insieme al server di autenticazione.

Autenticati con Active Directory o OpenLDAP in Active IQ Unified Manager

Puoi abilitare l’autenticazione remota sul server di gestione e configurarlo in modo che

comunichi con i server di autenticazione, così gli utenti presenti in tali server possono accedere a Unified Manager.

Puoi utilizzare uno dei seguenti servizi di autenticazione predefiniti oppure specificare un servizio di autenticazione personalizzato:

- Microsoft Active Directory

  Non puoi utilizzare Microsoft Lightweight Directory Services.

- OpenLDAP

Puoi selezionare il servizio di autenticazione richiesto e aggiungere i server di autenticazione appropriati per consentire agli utenti remoti presenti nel server di autenticazione di accedere a Unified Manager. Le credenziali per gli utenti o i gruppi remoti vengono gestite dal server di autenticazione. Il server di gestione utilizza il protocollo LDAP (Lightweight Directory Access Protocol) per autenticare gli utenti remoti all'interno del server di autenticazione configurato.

Per gli utenti locali creati in Unified Manager, il server di gestione mantiene un proprio database di nomi utente e password. Il server di gestione esegue l'autenticazione e non utilizza Active Directory o OpenLDAP per l'autenticazione.

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.

Usa la pagina di autenticazione remota in Active IQ Unified Manager

Puoi usare la pagina Autenticazione remota per configurare Unified Manager in modo che comunichi con il server di autenticazione per autenticare gli utenti remoti che tentano

di accedere alla web UI di Unified Manager.

Devi disporre del ruolo di Amministratore dell'applicazione o di Amministratore dello storage.

Dopo aver selezionato la casella di controllo "Enable remote authentication", puoi abilitare l'autenticazione remota usando un server di autenticazione.

- **Servizio di autenticazione**

  Ti consente di configurare il server di gestione per autenticare gli utenti nei provider di servizi directory, come Active Directory e OpenLDAP, oppure di specificare un tuo meccanismo di autenticazione. Puoi specificare un servizio di autenticazione solo se hai abilitato l'autenticazione remota.

  - **Active Directory**
    - Nome dell'amministratore

      Specifica il nome dell'amministratore del server di autenticazione.

    - Password

      Specifica la password per accedere al server di autenticazione.

    - Nome distinto di base

      Specifica la posizione degli utenti remoti nel server di autenticazione. Ad esempio, se il domain name del server di autenticazione è ou@domain.com, il nome distinto di base è **cn=ou,dc=domain,dc=com**.

    - Disabilita la ricerca di gruppi nidificati

      Specifica se abilitare o disabilitare l'opzione di ricerca dei gruppi nidificati. Per impostazione predefinita, questa opzione è disabilitata. Se usi Active Directory, puoi velocizzare l'autenticazione disabilitando il supporto per i gruppi nidificati.

    - Usa una connessione sicura

      Specifica il servizio di autenticazione utilizzato per comunicare con i server di autenticazione.

  - **OpenLDAP**
    - Distinguished Name di bind

      Specifica il nome distinto di bind utilizzato insieme al nome distinto di base per trovare gli utenti remoti nel server di autenticazione.

    - Password di bind

      Specifica la password per accedere al server di autenticazione.

    - Nome distinto di base

      Specifica la posizione degli utenti remoti nel server di autenticazione. Ad esempio, se il domain name del server di autenticazione è ou@domain.com, il nome distinto di base è **cn=ou,dc=domain,dc=com**.

- Usa una connessione sicura

  Specifica che Secure LDAP viene usato per comunicare con i server di autenticazione LDAP.

- **Altri**

  - Distinguished Name di bind

    Specifica il nome distinto di bind utilizzato insieme al nome distinto di base per trovare gli utenti remoti nel server di autenticazione che hai configurato.

  - Password di bind

    Specifica la password per accedere al server di autenticazione.

  - Nome distinto di base

    Specifica la posizione degli utenti remoti nel server di autenticazione. Ad esempio, se il domain name del server di autenticazione è ou@domain.com, il nome distinto di base è **cn=ou,dc=domain,dc=com**.

  - Versione del protocollo

    Specifica la versione del protocollo LDAP (Lightweight Directory Access Protocol) supportata dal tuo server di autenticazione. Puoi specificare se la versione del protocollo deve essere rilevata automaticamente oppure impostarla su 2 o 3.

  - Attributo nome utente

    Specifica il nome dell'attributo nel server di autenticazione che contiene i nomi di accesso degli utenti da autenticare nel server di gestione.

  - Attributo di appartenenza al gruppo

    Specifica un valore che assegna l'appartenenza al gruppo del server di gestione agli utenti remoti in base a un attributo e a un valore specificati nel server di autenticazione dell'utente.

  - UGID

    Se gli utenti remoti sono inclusi come membri di un oggetto GroupOfUniqueNames nel server di autenticazione, questa opzione ti consente di assegnare l'appartenenza al gruppo del server di gestione agli utenti remoti in base a un attributo specificato in tale oggetto GroupOfUniqueNames.

  - Disabilita la ricerca di gruppi nidificati

    Specifica se abilitare o disabilitare l'opzione di ricerca dei gruppi nidificati. Per impostazione predefinita, questa opzione è disabilitata. Se usi Active Directory, puoi velocizzare l'autenticazione disabilitando il supporto per i gruppi nidificati.

  - Membro

    Specifica il nome dell'attributo che il server di autenticazione utilizza per memorizzare le informazioni sui singoli membri di un gruppo.

  - Classe oggetto utente

Specifica la classe di oggetti di un utente nel server di autenticazione remoto.

- Classe oggetto di gruppo

  Specifica la classe di oggetti di tutti i gruppi nel server di autenticazione remoto.

  I valori che inserisci per gli attributi *Member*, *User Object Class* e *Group Object Class* devono essere gli stessi di quelli aggiunti nelle configurazioni di Active Directory, OpenLDAP e LDAP. In caso contrario, l'autenticazione potrebbe non riuscire.

- Usa una connessione sicura

  Specifica il servizio di autenticazione utilizzato per comunicare con i server di autenticazione.

  Se vuoi modificare il servizio di autenticazione, assicurati di eliminare tutti i server di autenticazione esistenti e di aggiungerne di nuovi.

Area dei server di autenticazione

L'area Server di autenticazione visualizza i server di autenticazione con cui il server di gestione comunica per individuare e autenticare gli utenti remoti. Le credenziali per gli utenti o i gruppi remoti vengono gestite dal server di autenticazione.

- **Pulsanti di comando**

  Ti consente di aggiungere, modificare o eliminare i server di autenticazione.

  - Aggiungi

    Consente di aggiungere un server di autenticazione.

  Se il server di autenticazione che stai aggiungendo fa parte di una coppia ad alta disponibilità (che utilizza lo stesso database), puoi aggiungere anche il server di autenticazione partner. Questo consente al server di gestione di comunicare con il partner quando uno dei server di autenticazione non è raggiungibile.

  - Modifica

    Ti consente di modificare le impostazioni di un server di autenticazione selezionato.

  - Elimina

    Elimina i server di autenticazione selezionati.

- **Nome o indirizzo IP**

  Visualizza l'host name o l'indirizzo IP del server di autenticazione utilizzato per autenticare l'utente sul server di gestione.

- **Porta**

  Visualizza il numero della porta del server di autenticazione.

- **Test di autenticazione**

  Questo pulsante convalida la configurazione del tuo server di autenticazione autenticando un utente o un gruppo remoto.

Durante la fase di test, se specifichi solo il nome utente, il server di gestione cerca l'utente remoto nel server di autenticazione, ma non lo autentica. Se specifichi sia il nome utente che la password, il server di gestione cerca e autentica l'utente remoto.

Non puoi testare l'autenticazione se l'autenticazione remota è disabilitata.

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.