Configura le notifiche

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

Sommario

Configura le notifiche . . . 1
- Configura Active IQ Unified Manager per inviare notifiche di avviso . . . 1
- Configura le impostazioni di notifica degli eventi in Active IQ Unified Manager . . . 1
- Abilita l’autenticazione remota in Active IQ Unified Manager . . . 2
- Disabilita i gruppi nidificati dall’autenticazione remota in Active IQ Unified Manager . . . 4
- Configura i servizi di autenticazione in Active IQ Unified Manager . . . 4
- Aggiungi i server di autenticazione ad Active IQ Unified Manager . . . 5
- Verifica la configurazione dei server di autenticazione in Active IQ Unified Manager . . . 7
- Aggiungi avvisi in Active IQ Unified Manager . . . 7
  - Esempio di aggiunta di un avviso . . . 8

Configura le notifiche

Configura Active IQ Unified Manager per inviare notifiche di avviso

Puoi configurare Unified Manager per inviare notifiche che ti avvisano degli eventi nel tuo ambiente. Prima di poter inviare le notifiche, devi configurare diverse altre opzioni di Unified Manager.

Prima di iniziare

Devi avere il ruolo di Amministratore dell'applicazione.

Dopo aver distribuito Unified Manager e completato la configurazione iniziale, dovresti prendere in considerazione la configurazione del tuo ambiente per attivare avvisi e generare notifiche via email o trap SNMP in base alla ricezione di eventi.

Passaggi

1. "Configura le impostazioni di notifica degli eventi".

   Se desideri ricevere notifiche di avviso quando si verificano determinati eventi nel tuo ambiente, devi configurare un server SMTP e fornire un indirizzo e-mail da cui inviare le notifiche di avviso. Se preferisci utilizzare le trap SNMP, puoi selezionare questa opzione e fornire le informazioni necessarie.

2. "Abilita l'autenticazione remota".

   Se vuoi che gli utenti remoti di LDAP o Active Directory accedano all'istanza di Unified Manager e ricevano notifiche di avviso, devi abilitare l'autenticazione remota.

3. "Aggiungi server di autenticazione".

   Puoi aggiungere server di autenticazione in modo che gli utenti remoti nel server di autenticazione possano accedere a Unified Manager.

4. "Aggiungi utenti".

   Puoi aggiungere diversi tipi di utenti locali o remoti e assegnare ruoli specifici. Quando crei un avviso, assegni un utente per ricevere le notifiche dell'avviso.

5. "Aggiungi avvisi".

   Dopo aver aggiunto l'indirizzo email per l'invio delle notifiche, aver aggiunto gli utenti che le riceveranno, aver configurato le impostazioni di rete e le opzioni SMTP e SNMP necessarie per il tuo ambiente, puoi assegnare gli avvisi.

Configura le impostazioni di notifica degli eventi in Active IQ Unified Manager

Puoi configurare Unified Manager per inviare notifiche di avviso quando viene generato un evento o quando un evento viene assegnato a un utente. Puoi configurare il server SMTP utilizzato per inviare l'avviso e impostare diversi meccanismi di notifica; ad

esempio, le notifiche di avviso possono essere inviate come email o trap SNMP.

Prima di iniziare

Devi avere le seguenti informazioni:

- Indirizzo e-mail da cui viene inviata la notifica di avviso

  L'indirizzo email compare nel campo "From" nelle notifiche di avviso inviate. Se l'email non può essere recapitata per qualsiasi motivo, questo indirizzo email viene utilizzato anche come destinatario della posta non recapitabile.

- host name del server SMTP e nome utente e password per accedere al server
- host name o indirizzo IP dell'host di destinazione del trap che riceverà il trap SNMP, insieme alla versione SNMP, alla porta del trap outbound, alla community e ad altri valori di configurazione SNMP richiesti

  Per specificare più destinazioni trap, separa ciascun host con una virgola. In questo caso, tutte le altre impostazioni SNMP, come la versione e la porta trap outbound, devono essere uguali per tutti gli host nell'elenco.

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

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Generale** > **Notifiche**.
2. Nella pagina Notifiche, configura le impostazioni appropriate.

   Note:

   - Se il campo "Da" è precompilato con l'indirizzo "ActiveIQUnifiedManager@localhost.com", devi modificarlo con un indirizzo email reale e funzionante per assicurarti che tutte le notifiche email vengano recapitate correttamente.
   - Se non è possibile risolvere l'host name del server SMTP, puoi specificare l'indirizzo IP (IPv4 o IPv6) del server SMTP al posto dell'host name.
3. Fare clic su **Save**.
4. Se hai selezionato l'opzione **Usa STARTTLS** o **Usa SSL**, dopo aver cliccato sul pulsante **Salva** verrà visualizzata una pagina relativa al certificato. Verifica i dettagli del certificato e accettalo per salvare le impostazioni di notifica.

   Puoi fare clic sul pulsante **Visualizza dettagli certificato** per visualizzare i dettagli del certificato. Se il certificato esistente è scaduto, deseleziona la casella **Usa STARTTLS** o **Usa SSL**, salva le impostazioni di notifica e seleziona nuovamente la casella **Usa STARTTLS** o **Usa SSL** per visualizzare un nuovo certificato.

Abilita l'autenticazione remota in Active IQ Unified Manager

Puoi abilitare l'autenticazione remota in modo che il server Unified Manager possa comunicare con i tuoi server di autenticazione. Gli utenti del server di autenticazione possono accedere all'interfaccia grafica di Unified Manager per gestire oggetti e dati di storage.

Prima di iniziare

Devi avere il ruolo di Amministratore dell'applicazione.

Il server Unified Manager deve essere connesso direttamente al server di autenticazione. Devi disabilitare tutti i client LDAP locali, come SSSD (System Security Services Daemon) o NSLCD (Name Service LDAP Caching Daemon).

Puoi abilitare l'autenticazione remota usando Open LDAP o Active Directory. Se l'autenticazione remota è disabilitata, gli utenti remoti non possono accedere a Unified Manager.

L'autenticazione remota è supportata tramite LDAP e LDAPS (LDAP sicuro). Unified Manager utilizza la porta 389 come porta predefinita per le comunicazioni non sicure e la porta 636 come porta predefinita per le comunicazioni sicure.

Il certificato utilizzato per autenticare gli utenti deve essere conforme al formato X.509.

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Generale** > **Autenticazione remota**.
2. Seleziona la casella **Abilita l'autenticazione remota…**.
3. Nel campo Servizio di autenticazione, seleziona il tipo di servizio e configura il servizio di autenticazione.

Per il tipo di autenticazione…	Inserisci le seguenti informazioni…
Active Directory	• Nome dell'amministratore del server di autenticazione in uno dei seguenti formati: ◦ `domainname\username` ◦ `username@domainname` ◦ `Bind Distinguished Name` (utilizzando la notazione LDAP appropriata) • Password di amministratore • Nome distinto di base (utilizzando la notazione LDAP appropriata)
Open LDAP	• Nome distinto di bind (nella notazione LDAP appropriata) • Password di bind • Nome distinto di base

Se l'autenticazione di un utente di Active Directory richiede molto tempo o va in timeout, è probabile che il server di autenticazione impieghi molto tempo a rispondere. Disabilitare il supporto per i gruppi nidificati in Unified Manager potrebbe ridurre il tempo di autenticazione.

Se selezioni l'opzione "Usa connessione sicura" per il server di autenticazione, Unified Manager comunica con il server di autenticazione utilizzando il protocollo Secure Sockets Layer (SSL).

4. **Facoltativo:** Aggiungi server di autenticazione e verifica l'autenticazione.
5. Fare clic su **Save**.

Disabilita i gruppi nidificati dall'autenticazione remota in Active IQ Unified Manager

Se hai abilitato l'autenticazione remota, puoi disabilitare l'autenticazione dei gruppi nidificati in modo che solo i singoli utenti, e non i membri dei gruppi, possano autenticarsi in remoto a Unified Manager. Puoi disabilitare i gruppi nidificati quando vuoi migliorare i tempi di risposta dell'autenticazione di Active Directory.

Prima di iniziare

- Devi avere il ruolo di Amministratore dell'applicazione.
- La disabilitazione dei gruppi nidificati si applica solo quando utilizzi Active Directory.

Disabilitare il supporto per i gruppi nidificati in Unified Manager potrebbe ridurre il tempo di autenticazione. Se il supporto per i gruppi nidificati è disabilitato e aggiungi un gruppo remoto a Unified Manager, i singoli utenti devono essere membri del gruppo remoto per autenticarsi in Unified Manager.

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Generale** > **Autenticazione remota**.
2. Seleziona la casella **Disabilita la ricerca di gruppi nidificati**.
3. Fare clic su **Save**.

Configura i servizi di autenticazione in Active IQ Unified Manager

I servizi di autenticazione consentono di autenticare utenti o gruppi remoti in un server di autenticazione prima di concedere loro l'accesso a Unified Manager. Puoi autenticare gli utenti utilizzando servizi di autenticazione predefiniti (come Active Directory o OpenLDAP) oppure configurando un meccanismo di autenticazione personalizzato.

Prima di iniziare

- Devi aver abilitato l'autenticazione remota.
- Devi avere il ruolo di Amministratore dell'applicazione.

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Generale** > **Autenticazione remota**.
2. Seleziona uno dei seguenti servizi di autenticazione:

Se selezioni…	Poi fai così…
Active Directory	a. Inserisci il nome e la password dell'amministratore. b. Specifica il nome distinto di base del 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**.

Se selezioni…	Poi fai così…
OpenLDAP	a. Inserisci il nome distinto di bind e la password di bind. b. Specifica il nome distinto di base del 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**.
Altri	a. Inserisci il nome distinto di bind e la password di bind. b. Specifica il nome distinto di base del 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**. c. Specifica la versione del protocollo LDAP supportata dal server di autenticazione. d. Inserisci il nome utente, l'appartenenza al gruppo, il gruppo utente e gli attributi del membro.

Se vuoi modificare il servizio di autenticazione, devi eliminare tutti i server di autenticazione esistenti e quindi aggiungere nuovi server di autenticazione.

3. Fare clic su **Save**.

Aggiungi i server di autenticazione ad Active IQ Unified Manager

Puoi aggiungere server di autenticazione e abilitare l'autenticazione remota sul server di gestione in modo che gli utenti remoti all'interno del server di autenticazione possano accedere a Unified Manager.

Prima di iniziare

- Devono essere disponibili le seguenti informazioni:
  - host name o indirizzo IP del server di autenticazione
  - Numero di porta del server di autenticazione
- Devi aver abilitato l'autenticazione remota e configurato il servizio di autenticazione in modo che il server di gestione possa autenticare utenti o gruppi remoti nel server di autenticazione.
- Devi avere il ruolo di Amministratore dell'applicazione.

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

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Generale** > **Autenticazione remota**.
2. Attiva o disattiva l'opzione **Utilizza connessione sicura**:

Se vuoi…	Poi fai così…
Abilitalo	a. Seleziona l'opzione **Usa connessione sicura**. b. Nell'area Server di autenticazione, fai clic su **Aggiungi**. c. Nella finestra di dialogo Aggiungi server di autenticazione, immetti il nome di autenticazione o l'indirizzo IP (IPv4 o IPv6) del server. d. Nella finestra di dialogo Autorizza host, fai clic su Visualizza certificato. e. Nella finestra di dialogo Visualizza certificato, verifica le informazioni del certificato e poi fai clic su **Chiudi**. f. Nella finestra di dialogo Autorizza host, fai clic su **Sì**. Quando abiliti l'opzione **Utilizza l'autenticazione tramite connessione sicura**, Unified Manager comunica con il server di autenticazione e visualizza il certificato. Unified Manager utilizza la porta 636 come porta predefinita per la comunicazione sicura e la porta 389 per la comunicazione non sicura.
Disabilitalo	a. Deseleziona l'opzione **Use Secure Connection**. b. Nell'area Server di autenticazione, fai clic su **Aggiungi**. c. Nella finestra di dialogo Aggiungi server di autenticazione, specifica l'host name o l'indirizzo IP (IPv4 o IPv6) del server e i dettagli della porta. d. Fai clic su **Add**.

   Il server di autenticazione che hai aggiunto viene visualizzato nell'area Servers.

3. Esegui un'autenticazione di prova per verificare di poter autenticare gli utenti nel server di autenticazione che hai aggiunto.

Verifica la configurazione dei server di autenticazione in Active IQ Unified Manager

Puoi convalidare la configurazione dei server di autenticazione per assicurarti che il server di gestione sia in grado di comunicare con essi. Puoi convalidare la configurazione cercando un utente o un gruppo remoto nei tuoi server di autenticazione e autenticandoli utilizzando le impostazioni configurate.

Prima di iniziare

- Devi aver abilitato l'autenticazione remota e configurato il servizio di autenticazione in modo che il server Unified Manager possa autenticare l'utente remoto o il gruppo remoto.
- Devi aver aggiunto i server di autenticazione affinché il server di gestione possa cercare l'utente remoto o il gruppo remoto su questi server e autenticarli.
- Devi avere il ruolo di Amministratore dell'applicazione.

Se il servizio di autenticazione è impostato su Active Directory e stai convalidando l'autenticazione di utenti remoti che appartengono al gruppo principale del server di autenticazione, le informazioni sul gruppo principale non vengono visualizzate nei risultati dell'autenticazione.

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Generale** > **Autenticazione remota**.
2. Fai clic su **Test Authentication**.
3. Nella finestra di dialogo Test User, specifica il nome utente e la password dell'utente remoto o il nome utente del gruppo remoto, quindi fai clic su **Test**.

   Se stai autenticando un gruppo remoto, non devi inserire la password.

Aggiungi avvisi in Active IQ Unified Manager

Puoi configurare gli avvisi per ricevere una notifica quando viene generato un evento specifico. Puoi configurare gli avvisi per una singola risorsa, per un gruppo di risorse o per eventi di un particolare tipo di severità. Puoi specificare la frequenza con cui vuoi ricevere le notifiche e associare uno script all'avviso.

Prima di iniziare

- Devi aver configurato le impostazioni di notifica, come l'indirizzo email dell'utente, il server SMTP e l'host delle trap SNMP, affinché il server Active IQ Unified Manager possa utilizzare tali impostazioni per inviare notifiche agli utenti quando viene generato un evento.
- Devi conoscere le risorse e gli eventi per i quali vuoi attivare l'avviso, nonché i nomi utente o gli indirizzi e-mail degli utenti che vuoi avvisare.
- Se vuoi che uno script venga eseguito in base all'evento, devi aver aggiunto lo script a Unified Manager usando la pagina Script.
- Devi disporre del ruolo di Amministratore dell'applicazione o di Amministratore dello storage.

Puoi creare un avviso direttamente dalla pagina Dettagli evento dopo aver ricevuto un evento, oltre a crearlo dalla pagina Configurazione avvisi, come descritto qui.

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Storage Management** > **Alert Setup**.
2. Nella pagina Configurazione avvisi, fai clic su **Aggiungi**.
3. Nella finestra di dialogo Aggiungi avviso, fai clic su **Nome** e inserisci un nome e una descrizione per l'avviso.
4. Fai clic su **Risorse** e seleziona le risorse da includere o da escludere dall'avviso.

   Puoi impostare un filtro specificando una stringa di testo nel campo **Il nome contiene** per selezionare un gruppo di risorse. In base alla stringa di testo che specifichi, l'elenco delle risorse disponibili mostra solo quelle che corrispondono alla regola di filtro. La stringa di testo che specifichi fa distinzione tra maiuscole e minuscole.

   Se una risorsa soddisfa sia le regole di inclusione sia quelle di esclusione che hai specificato, la regola di esclusione ha la precedenza su quella di inclusione e non viene generato alcun avviso per gli eventi correlati alla risorsa esclusa.

5. Fai clic su **Eventi** e seleziona gli eventi in base al nome dell'evento o al tipo di severità per i quali vuoi attivare un avviso.

   Per selezionare più di un evento, tieni premuto il tasto Ctrl mentre fai le tue selezioni.

6. Fai clic su **Azioni**, seleziona gli utenti che vuoi notificare, scegli la frequenza di notifica, scegli se inviare una trap SNMP al ricevitore trap e assegna uno script da eseguire quando si genera un avviso.

   Se modifichi l'indirizzo email specificato per l'utente e riapri l'avviso per modificarlo, il campo Nome appare vuoto perché l'indirizzo email modificato non è più associato all'utente selezionato in precedenza. Inoltre, se modifichi l'indirizzo email dell'utente selezionato dalla pagina Users, l'indirizzo email modificato non viene aggiornato per l'utente selezionato.

   Puoi anche scegliere di notificare gli utenti tramite trap SNMP.

7. Fare clic su **Save**.

Esempio di aggiunta di un avviso

Questo esempio mostra come creare un avviso che soddisfi i seguenti requisiti:

- Nome dell'avviso: HealthTest
- Risorse: include tutti i volumi il cui nome contiene "abc" ed esclude tutti i volumi il cui nome contiene "xyz"
- Eventi: include tutti gli eventi critici relativi all'integrità
- Azioni: include "sample@domain.com", uno script "Test" e l'utente deve essere avvisato ogni 15 minuti

Esegui i seguenti passaggi nella finestra di dialogo Aggiungi avviso:

Passaggi

1. Fai clic su **Nome** e inserisci **HealthTest** nel campo **Nome avviso**.
2. Fai clic su **Risorse**, e nella scheda Includi seleziona **Volumi** dall'elenco a discesa.
   a. Inserisci **abc** nel campo **Il nome contiene** per visualizzare i volumi il cui nome contiene "abc".
   b. Seleziona **<<All Volumes whose name contains 'abc'>>** dall'area Risorse disponibili e spostalo

nell’area Risorse selezionate.

c. Fai clic su **Escludi**, inserisci **xyz** nel campo **Il nome contiene** e poi fai clic su **Aggiungi**.

3. Fai clic su **Eventi** e seleziona **Critico** dal campo **Gravità evento**.
4. Seleziona **Tutti gli eventi critici** dall’area Eventi corrispondenti e spostalo nell’area Eventi selezionati.
5. Fai clic su **Azioni** e inserisci **sample@domain.com** nel campo Avvisa questi utenti.
6. Seleziona **Ricorda ogni 15 minuti** per inviare una notifica all’utente ogni 15 minuti.

   Puoi configurare un avviso in modo che invii ripetutamente notifiche ai destinatari per un periodo di tempo specificato. Devi determinare l’ora a partire dalla quale la notifica dell’evento è attiva per l’avviso.

7. Nel menu Seleziona script da eseguire, seleziona lo script **Test**.
8. Fare clic su **Save**.

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.