Configurazione di Unified Manager per l'invio di notifiche di avviso

Active IQ Unified Manager 9.11

NetApp
December 18, 2023

Sommario

Configurazione di Unified Manager per l'invio di notifiche di avviso

È possibile configurare Unified Manager in modo che invii notifiche che avvisano l'utente in merito a eventi nel proprio ambiente. Prima di poter inviare le notifiche, è necessario configurare diverse altre opzioni di Unified Manager.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione.

Dopo aver implementato Unified Manager e aver completato la configurazione iniziale, è necessario configurare l'ambiente in modo da attivare avvisi e generare messaggi e-mail di notifica o trap SNMP in base alla ricezione degli eventi.

Fasi

1. "Configurare le impostazioni di notifica degli eventi"

   Se si desidera inviare notifiche di avviso quando si verificano determinati eventi nell'ambiente, è necessario configurare un server SMTP e fornire un indirizzo e-mail da cui inviare la notifica di avviso. Se si desidera utilizzare i trap SNMP, è possibile selezionare tale opzione e fornire le informazioni necessarie.

2. "Abilitare l'autenticazione remota"

   Se si desidera che gli utenti LDAP o Active Directory remoti accedano all'istanza di Unified Manager e ricevano notifiche di avviso, è necessario attivare l'autenticazione remota.

3. "Aggiungere server di autenticazione"

   È possibile aggiungere server di autenticazione in modo che gli utenti remoti all'interno del server di autenticazione possano accedere a Unified Manager.

4. "Aggiungere utenti"

   È possibile aggiungere diversi tipi di utenti locali o remoti e assegnare ruoli specifici. Quando si crea un avviso, si assegna a un utente la ricezione delle notifiche.

5. "Aggiungere avvisi"

   Dopo aver aggiunto l'indirizzo e-mail per l'invio delle notifiche, aver aggiunto gli utenti per la ricezione delle notifiche, aver configurato le impostazioni di rete e configurato le opzioni SMTP e SNMP necessarie per l'ambiente, è possibile assegnare gli avvisi.

Configurazione delle impostazioni di notifica degli eventi

È possibile configurare Unified Manager in modo che invii notifiche di avviso quando viene generato un evento o quando viene assegnato un evento a un utente. È possibile configurare il server SMTP utilizzato per inviare l'avviso e impostare vari meccanismi di notifica, ad esempio le notifiche di avviso possono essere inviate come e-mail o trap SNMP.

Cosa ti serve

È necessario disporre delle seguenti informazioni:

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

  L'indirizzo e-mail viene visualizzato nel campo "da" nelle notifiche di avviso inviate. Se non è possibile recapitarlo per qualsiasi motivo, questo indirizzo e-mail viene utilizzato anche come destinatario per la posta non recapitabile.

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

  Per specificare più destinazioni di trap, separare ciascun host con una virgola. In questo caso, tutte le altre impostazioni SNMP, ad esempio versione e porta trap in uscita, devono essere le stesse per tutti gli host dell'elenco.

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale** > **Notifiche**.
2. Nella pagina Notifiche, configurare le impostazioni appropriate e fare clic su **Salva**.

   Note:

   - Se l'indirizzo da è pre-compilato con l'indirizzo "ActiveIQUnifiedManager@localhost.com", devi cambiarlo in un indirizzo e-mail reale e funzionante per assicurarti che tutte le notifiche e-mail siano inviate correttamente.
   - Se il nome host del server SMTP non può essere risolto, è possibile specificare l'indirizzo IP (IPv4 o IPv6) del server SMTP invece del nome host.

Attivazione dell'autenticazione remota

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

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione.

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

È possibile attivare l'autenticazione remota utilizzando Open LDAP o Active Directory. Se l'autenticazione remota è disattivata, gli utenti remoti non possono accedere a Unified Manager.

L'autenticazione remota è supportata su LDAP e LDAPS (Secure LDAP). Unified Manager utilizza 389 come

porta predefinita per le comunicazioni non protette e 636 come porta predefinita per le comunicazioni protette.

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

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Generale** > **autenticazione remota**.
2. Selezionare la casella **Enable remote Authentication…** (attiva autenticazione remota…).
3. Nel campo Servizio di autenticazione, selezionare il tipo di servizio e configurare il servizio di autenticazione.

Per tipo di autenticazione…	Inserire 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 dell'amministratore • Nome distinto di base (utilizzando la notazione LDAP appropriata)
Aprire LDAP	• Nome distinto di binding (nella notazione LDAP appropriata) • Associare la password • Nome distinto di base

   Se l'autenticazione di un utente di Active Directory richiede molto tempo o si verifica un timeout, il server di autenticazione probabilmente impiega molto tempo per rispondere. La disattivazione del supporto per i gruppi nidificati in Unified Manager potrebbe ridurre il tempo di autenticazione.

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

4. **Opzionale:** aggiungere server di autenticazione e verificare l'autenticazione.
5. Fare clic su **Save** (Salva).

Disattivazione dei gruppi nidificati dall'autenticazione remota

Se l'autenticazione remota è attivata, è possibile disattivare l'autenticazione dei gruppi nidificati in modo che solo i singoli utenti e non i membri del gruppo possano autenticarsi in remoto in Unified Manager. È possibile disattivare i gruppi nidificati quando si desidera migliorare i tempi di risposta per l'autenticazione di Active Directory.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione.
- La disattivazione dei gruppi nidificati è applicabile solo quando si utilizza Active Directory.

La disattivazione del supporto per i gruppi nidificati in Unified Manager potrebbe ridurre il tempo di autenticazione. Se il supporto di gruppi nidificati è disattivato e se un gruppo remoto viene aggiunto a Unified Manager, i singoli utenti devono essere membri del gruppo remoto per autenticarsi in Unified Manager.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Generale** > **autenticazione remota**.
2. Selezionare la casella **Disable Nested Group Lookup** (Disattiva ricerca gruppi nidificati).
3. Fare clic su **Save** (Salva).

Impostazione dei servizi di autenticazione

I servizi di autenticazione consentono l'autenticazione di utenti remoti o gruppi remoti in un server di autenticazione prima di fornire loro l'accesso a Unified Manager. È possibile autenticare gli utenti utilizzando servizi di autenticazione predefiniti (ad esempio Active Directory o OpenLDAP) o configurando il proprio meccanismo di autenticazione.

Cosa ti serve

- È necessario aver attivato l'autenticazione remota.
- È necessario disporre del ruolo di amministratore dell'applicazione.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Generale** > **autenticazione remota**.
2. Selezionare uno dei seguenti servizi di autenticazione:

Se si seleziona…	Quindi…
Active Directory	a. Immettere il nome e la password dell'amministratore. b. Specificare il nome distinto di base del server di autenticazione. Ad esempio, se il nome di dominio del server di autenticazione è ou@domain.com, il nome distinto di base è **cn=ou,DC=domain,DC=com**.
OpenLDAP	a. Immettere il nome distinto e la password di bind. b. Specificare il nome distinto di base del server di autenticazione. Ad esempio, se il nome di dominio del server di autenticazione è ou@domain.com, il nome distinto di base è **cn=ou,DC=domain,DC=com**.

Se si seleziona…	Quindi…
Altri	a. Immettere il nome distinto e la password di bind. b. Specificare il nome distinto di base del server di autenticazione. Ad esempio, se il nome di dominio del server di autenticazione è ou@domain.com, il nome distinto di base è **cn=ou,DC=domain,DC=com**. c. Specificare la versione del protocollo LDAP supportata dal server di autenticazione. d. Immettere il nome utente, l'appartenenza al gruppo, il gruppo di utenti e gli attributi del membro.

Se si desidera modificare il servizio di autenticazione, è necessario eliminare tutti i server di autenticazione esistenti e aggiungere nuovi server di autenticazione.

3. Fare clic su **Save** (Salva).

Aggiunta di server di autenticazione

È possibile 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.

Cosa ti serve

- Devono essere disponibili le seguenti informazioni:
  - Nome host o indirizzo IP del server di autenticazione
  - Numero di porta del server di autenticazione
- È necessario aver attivato 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.
- È necessario disporre del ruolo di amministratore dell'applicazione.

Se il server di autenticazione che si sta aggiungendo fa parte di una coppia ad alta disponibilità (ha) (utilizzando lo stesso database), è possibile 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.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Generale** > **autenticazione remota**.
2. Attivare o disattivare l'opzione **Usa connessione protetta**:

Se si desidera…	Quindi…
Abilitarlo	a. Selezionare l'opzione **Usa connessione protetta**. b. Nella sezione Authentication Servers (Server di autenticazione), fare clic su **Add** (Aggiungi) c. Nella finestra di dialogo Add Authentication Server (Aggiungi server di autenticazione), immettere il nome di autenticazione o l'indirizzo IP (IPv4 o IPv6) del server. d. Nella finestra di dialogo autorizza host, fare clic su Visualizza certificato. e. Nella finestra di dialogo Visualizza certificato, verificare le informazioni del certificato, quindi fare clic su **Chiudi**. f. Nella finestra di dialogo autorizza host, fare clic su **Sì**. Quando si attiva l'opzione **Usa autenticazione connessione sicura**, Unified Manager comunica con il server di autenticazione e visualizza il certificato. Unified Manager utilizza 636 come porta predefinita per comunicazioni sicure e il numero di porta 389 per comunicazioni non sicure.
Disattivarlo	a. Deselezionare l'opzione **Usa connessione protetta**. b. Nella sezione Authentication Servers (Server di autenticazione), fare clic su **Add** (Aggiungi) c. Nella finestra di dialogo Add Authentication Server (Aggiungi server di autenticazione), specificare il nome host o l'indirizzo IP (IPv4 o IPv6) del server e i dettagli della porta. d. Fare clic su **Aggiungi**.

Il server di autenticazione aggiunto viene visualizzato nell'area Server.

3. Eseguire un'autenticazione di prova per confermare che è possibile autenticare gli utenti nel server di autenticazione aggiunto.

Verifica della configurazione dei server di autenticazione

È possibile convalidare la configurazione dei server di autenticazione per garantire che il

server di gestione sia in grado di comunicare con essi. È possibile convalidare la configurazione ricercando un utente remoto o un gruppo remoto dai server di autenticazione e autenticandoli utilizzando le impostazioni configurate.

Cosa ti serve

- È necessario aver attivato 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.
- È necessario aggiungere i server di autenticazione in modo che il server di gestione possa cercare l'utente remoto o il gruppo remoto da questi server e autenticarli.
- È necessario disporre del ruolo di amministratore dell'applicazione.

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

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Generale** > **autenticazione remota**.
2. Fare clic su **Test Authentication**.
3. Nella finestra di dialogo Test User, specificare il nome utente e la password dell'utente remoto o il nome utente del gruppo remoto, quindi fare clic su **Test**.

   Se si sta autenticando un gruppo remoto, non è necessario immettere la password.

Aggiunta di avvisi

È possibile configurare gli avvisi in modo che notifichino quando viene generato un determinato evento. È possibile configurare gli avvisi per una singola risorsa, per un gruppo di risorse o per eventi di un particolare tipo di severità. È possibile specificare la frequenza con cui si desidera ricevere una notifica e associare uno script all'avviso.

Cosa ti serve

- Per consentire al server Active IQ Unified Manager di utilizzare queste impostazioni per inviare notifiche agli utenti quando viene generato un evento, è necessario aver configurato le impostazioni di notifica, ad esempio l'indirizzo e-mail dell'utente, il server SMTP e l'host trap SNMP.
- È necessario conoscere le risorse e gli eventi per i quali si desidera attivare l'avviso, nonché i nomi utente o gli indirizzi e-mail degli utenti che si desidera notificare.
- Se si desidera eseguire uno script in base all'evento, è necessario aggiungere lo script a Unified Manager utilizzando la pagina script.
- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

È possibile creare un avviso direttamente dalla pagina Dettagli evento dopo aver ricevuto un evento, oltre a creare un avviso dalla pagina Configurazione avviso, come descritto di seguito.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Alert Setup**.
2. Nella pagina Alert Setup, fare clic su **Add** (Aggiungi).

3. Nella finestra di dialogo Aggiungi avviso, fare clic su **Nome** e immettere un nome e una descrizione per l'avviso.
4. Fare clic su **risorse** e selezionare le risorse da includere o escludere dall'avviso.

   È possibile impostare un filtro specificando una stringa di testo nel campo **Nome contiene** per selezionare un gruppo di risorse. In base alla stringa di testo specificata, l'elenco delle risorse disponibili visualizza solo le risorse corrispondenti alla regola di filtro. La stringa di testo specificata fa distinzione tra maiuscole e minuscole.

   Se una risorsa è conforme alle regole di inclusione ed esclusione specificate, la regola di esclusione ha la precedenza sulla regola di inclusione e l'avviso non viene generato per gli eventi correlati alla risorsa esclusa.

5. Fare clic su **Eventi** e selezionare gli eventi in base al nome dell'evento o al tipo di severità per cui si desidera attivare un avviso.

   Per selezionare più eventi, premere il tasto Ctrl mentre si effettuano le selezioni.

6. Fare clic su **azioni**, selezionare gli utenti che si desidera notificare, scegliere la frequenza di notifica, scegliere se inviare una trap SNMP al ricevitore della trap e assegnare uno script da eseguire quando viene generato un avviso.

   Se si modifica l'indirizzo di posta elettronica specificato per l'utente e si riapre l'avviso per la modifica, il campo Nome appare vuoto perché l'indirizzo di posta elettronica modificato non è più associato all'utente precedentemente selezionato. Inoltre, se l'indirizzo e-mail dell'utente selezionato è stato modificato dalla pagina utenti, l'indirizzo e-mail modificato non viene aggiornato per l'utente selezionato.

   È inoltre possibile scegliere di inviare una notifica agli utenti tramite trap SNMP.

7. Fare clic su **Save** (Salva).

Esempio di aggiunta di un avviso

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

- Nome 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 sanitari critici
- Azioni: Include "sample@domain.com", uno script "Test" e l'utente deve ricevere una notifica ogni 15 minuti

Nella finestra di dialogo Aggiungi avviso, attenersi alla seguente procedura:

Fasi

1. Fare clic su **Nome** e immettere **HealthTest** nel campo **Nome avviso**.
2. Fare clic su **Resources** (risorse) e nella scheda include (Includi) selezionare **Volumes** (volumi) dall'elenco a discesa.
   a. Immettere **abc** nel campo **Nome contiene** per visualizzare i volumi il cui nome contiene "abc".
   b. Selezionare **<<All Volumes whose name contains 'abc'>>** dall'area risorse disponibili e spostarla nell'area risorse selezionate.

   c. Fare clic su **Escludi**, immettere **xyz** nel campo **Nome contiene**, quindi fare clic su **Aggiungi**.

3. Fare clic su **Eventi** e selezionare **critico** dal campo gravità evento.
4. Selezionare **All Critical Events** (tutti gli eventi critici) dall'area Matching Events (Eventi corrispondenti) e spostarla nell'area Selected Events (Eventi selezionati).
5. Fare clic su **azioni** e digitare **sample@domain.com** nel campo Avvisa questi utenti.
6. Selezionare **promemoria ogni 15 minuti** per avvisare l'utente ogni 15 minuti.

   È possibile configurare un avviso per inviare ripetutamente notifiche ai destinatari per un periodo di tempo specificato. È necessario determinare l'ora in cui la notifica dell'evento è attiva per l'avviso.

7. Nel menu Select script to Execute (Seleziona script da eseguire), selezionare **Test** script.
8. Fare clic su **Save** (Salva).