Configura Active IQ Unified Manager

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

Sommario

Configura Active IQ Unified Manager . . . 1
- Scopri come configurare Active IQ Unified Manager . . . 1
- Scopri la sequenza di configurazione in Active IQ Unified Manager . . . 1
- Accedi all'interfaccia utente web in Active IQ Unified Manager . . . 1
- Esegui la configurazione iniziale dell'interfaccia utente web di Active IQ Unified Manager . . . 2
- Aggiungi cluster ad Active IQ Unified Manager . . . 4
- Configura le notifiche . . . 6
  - Configura Active IQ Unified Manager per inviare notifiche di avviso . . . 6
  - Configura le impostazioni di notifica degli eventi in Active IQ Unified Manager . . . 7
  - Abilita l'autenticazione remota in Active IQ Unified Manager . . . 8
  - Disabilita i gruppi nidificati dall'autenticazione remota in Active IQ Unified Manager . . . 9
  - Configura i servizi di autenticazione in Active IQ Unified Manager . . . 10
  - Aggiungi i server di autenticazione ad Active IQ Unified Manager . . . 11
  - Verifica la configurazione dei server di autenticazione in Active IQ Unified Manager . . . 12
  - Aggiungi avvisi in Active IQ Unified Manager . . . 13
- Cambia la password dell'utente locale in Active IQ Unified Manager . . . 15
- Imposta il timeout di inattività della sessione in Active IQ Unified Manager . . . 15
- Imposta il timeout della sessione tramite la CLI in Active IQ Unified Manager . . . 16
- Modifica l'host name di Unified Manager . . . 16
  - Cambia l'host name della virtual appliance Active IQ Unified Manager . . . 16
  - Genera un certificato di sicurezza HTTPS in Active IQ Unified Manager . . . 17
  - Riavvia la macchina virtuale Active IQ Unified Manager . . . 19
  - Cambia l'host name di Active IQ Unified Manager sui sistemi Linux . . . 19
- Abilita e disabilita la gestione dello storage basata su policy in Active IQ Unified Manager . . . 20

Configura Active IQ Unified Manager

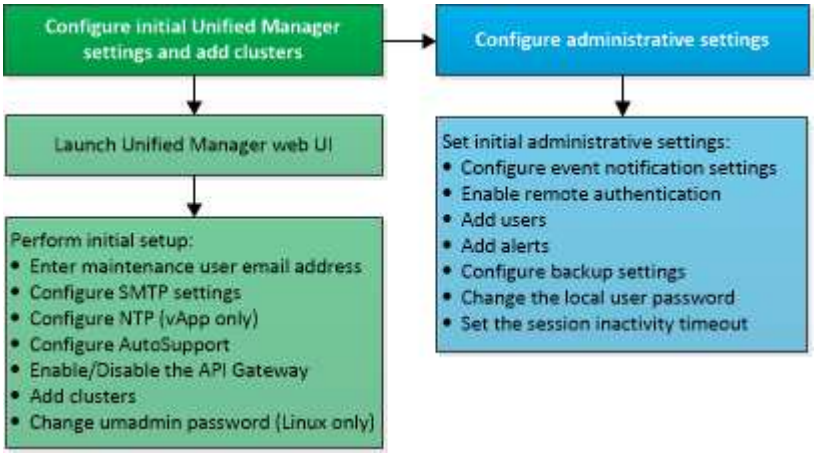
Scopri come configurare Active IQ Unified Manager

Dopo aver installato Active IQ Unified Manager (precedentemente OnCommand Unified Manager) devi completare la configurazione iniziale (chiamata anche procedura guidata della prima esperienza) per accedere all'interfaccia utente web. Quindi puoi eseguire ulteriori attività di configurazione, come aggiungere cluster, configurare l'autenticazione remota, aggiungere utenti e aggiungere avvisi.

Alcune delle procedure descritte in questo manuale sono necessarie per completare la configurazione iniziale della tua istanza di Unified Manager. Altre procedure sono impostazioni di configurazione consigliate, utili da impostare sulla tua nuova istanza o da conoscere prima di iniziare il monitoraggio regolare dei tuoi sistemi ONTAP.

Scopri la sequenza di configurazione in Active IQ Unified Manager

Il flusso di configurazione descrive le attività che devi eseguire prima di poter utilizzare Unified Manager.



Accedi all'interfaccia utente web in Active IQ Unified Manager

Dopo aver installato Unified Manager, puoi accedere all'interfaccia web per configurare Unified Manager e iniziare a monitorare i tuoi sistemi ONTAP.

Prima di iniziare

- Se è la prima volta che accedi all'interfaccia utente web, devi accedere come utente di manutenzione (o come utente umadmin per le installazioni Linux).
- Se intendi consentire agli utenti di accedere a Unified Manager utilizzando il nome breve anziché il fully qualified domain name (FQDN) o l'indirizzo IP, la configurazione di rete deve risolvere questo nome breve in un FQDN valido.

- Se il server utilizza un certificato digitale autofirmato, il browser potrebbe visualizzare un avviso che indica che il certificato non è attendibile. Puoi accettare il rischio per continuare l'accesso oppure installare un certificato digitale firmato da un'Autorità di Certificazione (CA) per l'autenticazione del server.

Passaggi

1. Avvia l'interfaccia utente web di Unified Manager dal browser utilizzando l'URL visualizzato al termine dell'installazione. L'URL corrisponde all'indirizzo IP o al fully qualified domain name (FQDN) del server Unified Manager.

   Il collegamento è nel seguente formato: `https://URL`.

2. Accedi all'interfaccia utente web di Unified Manager utilizzando le credenziali del tuo utente di manutenzione.

> Se effettui tre tentativi consecutivi di accesso all'interfaccia web senza successo entro un'ora, verrai bloccato fuori dal sistema e dovrai contattare il tuo system administrator. Questa procedura si applica solo agli utenti locali.

Esegui la configurazione iniziale dell'interfaccia utente web di Active IQ Unified Manager

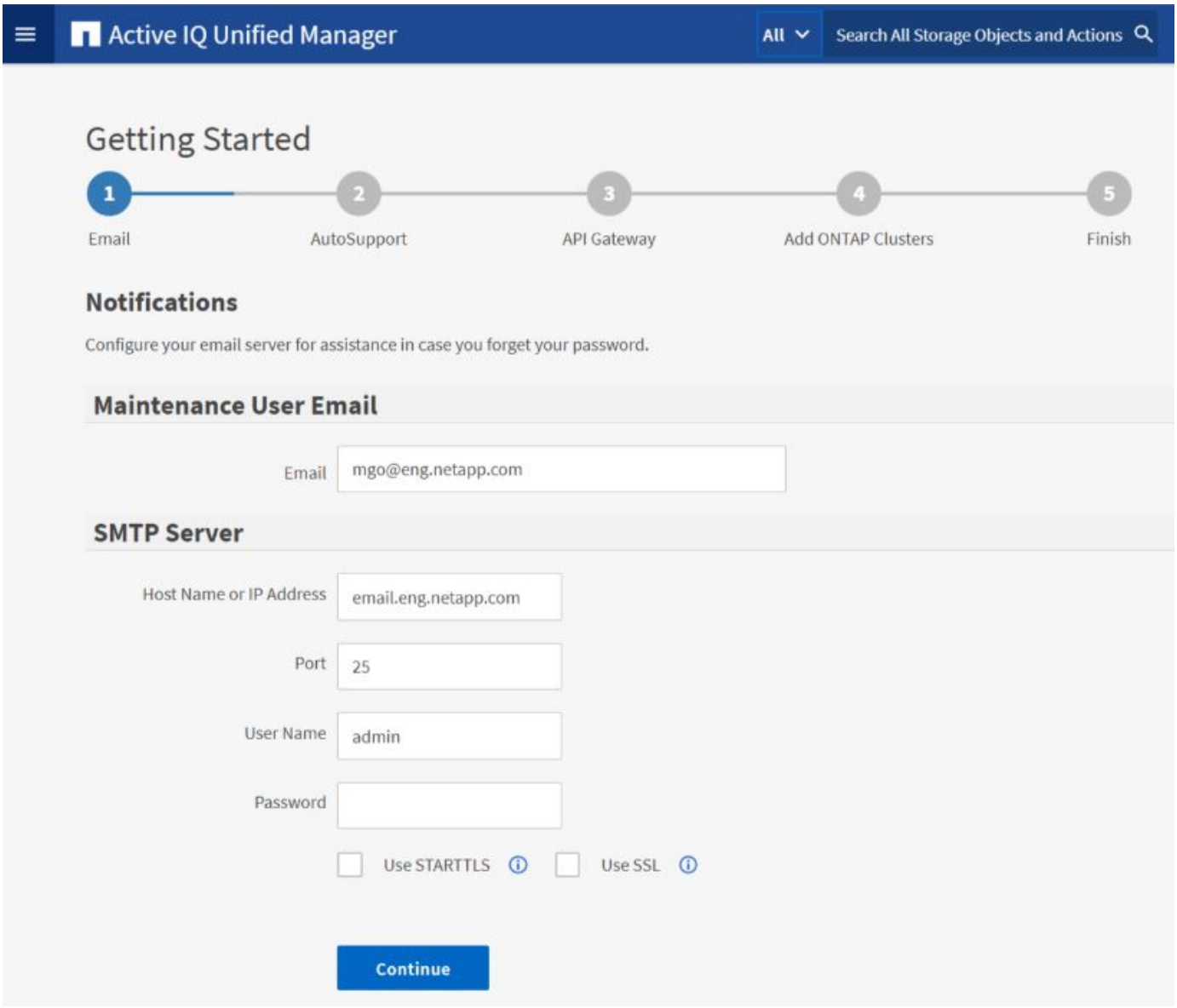
Per utilizzare Unified Manager, devi prima configurare le opzioni di configurazione iniziale, tra cui il server NTP, l'indirizzo email dell'utente di manutenzione, l'host del server SMTP e l'aggiunta dei cluster ONTAP.

Prima di iniziare

Devi aver eseguito le seguenti operazioni:

- Avviata l'interfaccia utente web di Unified Manager utilizzando l'URL fornito dopo l'installazione
- Hai effettuato l'accesso utilizzando il nome utente e la password di manutenzione (utente umadmin per le installazioni Linux) creati durante l'installazione

La pagina Getting Started di Active IQ Unified ManagerGetting viene visualizzata solo quando accedi per la prima volta all'interfaccia utente web. La pagina seguente proviene da un'installazione su VMware.



Se vuoi modificare una di queste opzioni in seguito, puoi selezionare la tua scelta dalle opzioni generali nel riquadro di navigazione sinistro di Unified Manager. Tieni presente che l'impostazione NTP è valida solo per le installazioni VMware e può essere modificata in seguito tramite la console di manutenzione di Unified Manager.

Passaggi

1. Nella pagina Initial Setup di Active IQ Unified Manager, inserisci l'indirizzo email dell'utente di manutenzione, l'host name del server SMTP ed eventuali opzioni SMTP aggiuntive, nonché il server NTP (solo per le installazioni VMware). Quindi fai clic su **Continue**.

   Se hai selezionato l'opzione **Usa STARTTLS** o **Usa SSL**, dopo aver cliccato sul pulsante **Continua** verrà visualizzata una pagina relativa al certificato. Verifica i dettagli del certificato e accettalo per proseguire con le impostazioni di configurazione iniziali dell'interfaccia web.

2. Nella pagina AutoSupport, fai clic su **Accetta e continua** per abilitare l'invio di messaggi AutoSupport da Unified Manager a NetAppActive IQ.

   Se devi designare un proxy per fornire l'accesso a Internet e inviare contenuti di AutoSupport, oppure se vuoi disabilitare AutoSupport, usa l'opzione **General** > **AutoSupport** dall'interfaccia web.

3. Sui sistemi Red Hat, modifica la password dell'utente umadmin dalla stringa predefinita "admin" a una stringa personalizzata.
4. Nella pagina Configura API Gateway, seleziona se vuoi utilizzare la funzionalità API Gateway che consente a Unified Manager di gestire i cluster ONTAP che intendi monitorare tramite le API REST di ONTAP. Quindi fai clic su **Continua**.

   In seguito puoi abilitare o disabilitare questa impostazione nell'interfaccia utente web da **Generale** > **Impostazioni funzionalità** > **API Gateway**. Per ulteriori informazioni sulle API, consulta "Guida introduttiva alle API REST di Active IQ Unified Manager".

5. Aggiungi i cluster che vuoi far gestire a Unified Manager, quindi fai clic su **Avanti**. Per ogni cluster che prevedi di gestire, devi disporre dell'host name o dell'indirizzo IP di gestione del cluster (IPv4 o IPv6), oltre alle credenziali di nome utente e password; l'utente deve avere il ruolo "admin".

   Questo passaggio è facoltativo. Puoi aggiungere i cluster in un secondo momento nell'interfaccia web da **Storage Management** > **Cluster Setup**.

6. Nella pagina Riepilogo, verifica che tutte le impostazioni siano corrette e fai clic su **Finish**.

La pagina "Per iniziare" si chiude e viene visualizzata la pagina "Dashboard di Unified Manager".

Aggiungi cluster ad Active IQ Unified Manager

Puoi aggiungere un cluster ad Active IQ Unified Manager per monitorare il cluster. Ciò include la possibilità di ottenere informazioni sul cluster, come lo stato di salute, la capacità, le prestazioni e la configurazione del cluster, in modo da poter individuare e risolvere eventuali problemi.

Prima di iniziare

- Devi disporre del ruolo di Amministratore dell'applicazione o di Amministratore dello storage.
- Devi avere le seguenti informazioni:
  - Unified Manager supporta cluster ONTAP on-premises, ONTAP Select, Cloud Volumes ONTAP.
  - host name o indirizzo IP di gestione del cluster

    L'host name è il nome di dominio completo (FQDN) o il nome breve che Unified Manager utilizza per connettersi al cluster. L'host name deve risolversi nell'indirizzo IP di gestione del cluster.

    L'indirizzo IP di gestione del cluster deve corrispondere alla LIF di gestione del cluster della storage virtual machine (SVM) amministrativa. Se usi una LIF di gestione dei nodi, l'operazione non riesce.

  - Il cluster deve eseguire il software versione di ONTAP 9.1 o successiva.
  - Nome utente e password dell'amministratore di ONTAP

    Questo account deve avere il ruolo *admin* con l'accesso all'applicazione impostato su *ontapi*, *amqp*, *console* e *http*.

  - Il numero di porta per connetterti al cluster utilizzando il protocollo HTTPS (in genere la porta 443)
  - Possiedi i certificati richiesti:

    Certificato SSL (HTTPS): questo certificato appartiene a Unified Manager. Un certificato SSL (HTTPS)

autofirmato predefinito viene generato con una nuova installazione di Unified Manager. NetApp consiglia di aggiornarlo a un certificato firmato da una CA per una maggiore sicurezza. Se il certificato del server scade, devi rigenerarlo e riavviare Unified Manager perché i servizi incorporino il nuovo certificato. Per ulteriori informazioni sulla rigenerazione del certificato SSL, vedi "Generazione di un certificato di sicurezza HTTPS".

Certificato EMS: Questo certificato appartiene a Unified Manager. Lo usi durante l'autenticazione per le notifiche EMS ricevute da ONTAP.

Certificati per la comunicazione TLS reciproca: Utilizzati durante la comunicazione TLS reciproca tra Unified Manager e ONTAP. L'autenticazione basata su certificati è abilitata per un cluster, in base alla versione di ONTAP. Se il cluster che esegue la versione di ONTAP è inferiore alla 9.5, l'autenticazione basata su certificati non è abilitata.

L'autenticazione basata su certificato non viene abilitata automaticamente per un cluster se stai aggiornando una versione precedente di Unified Manager. Tuttavia, puoi abilitarla modificando e salvando i dettagli del cluster. Se il certificato scade, devi rigenerarlo per incorporare il nuovo certificato. Per ulteriori informazioni su come visualizzare e rigenerare il certificato, consulta "Modifica dei cluster".



- Puoi aggiungere un cluster dall'interfaccia utente web e l'autenticazione basata su certificati viene abilitata automaticamente.
- Puoi aggiungere un cluster tramite la CLI di Unified Manager; l'autenticazione basata su certificati non è abilitata per impostazione predefinita. Se aggiungi un cluster utilizzando la CLI di Unified Manager, devi modificare il cluster utilizzando l'interfaccia utente di Unified Manager. Puoi consultare "Comandi CLI di Unified Manager supportati" per aggiungere un cluster utilizzando la CLI di Unified Manager.
- Se per un cluster è abilitata l'autenticazione basata su certificato e esegui il backup di Unified Manager da un server e lo ripristini su un altro server Unified Manager in cui il nome host o l'indirizzo IP sono cambiati, il monitoraggio del cluster potrebbe non riuscire. Per evitare il problema, modifica e salva i dettagli del cluster. Per ulteriori informazioni su come modificare i dettagli del cluster, consulta "Modifica dei cluster".

+ **Certificati del cluster**: Questo certificato è di proprietà di ONTAP. Non puoi aggiungere un cluster a Unified Manager con un certificato scaduto e, se il certificato è già scaduto, devi rigenerarlo prima di aggiungere il cluster. Per informazioni sulla generazione dei certificati, consulta l'articolo della knowledge base (KB) "Come rinnovare un certificato autofirmato di ONTAP nell'interfaccia utente di System Manager".

- Devi disporre di spazio sufficiente sul server Unified Manager. Non puoi aggiungere un cluster al server se oltre il 90% dello spazio nella directory del database è già occupato.

Per una configurazione MetroCluster, devi aggiungere sia il cluster locale che quello remoto e i cluster devono essere configurati correttamente.

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Gestione dello storage** > **Configurazione del cluster**.
2. Nella pagina Configurazione cluster, fai clic su **Aggiungi**.
3. Nella finestra di dialogo Aggiungi cluster, specifica i valori richiesti, come l'host name o l'indirizzo IP del cluster, il nome utente, la password e il numero di porta.

   Puoi modificare l'indirizzo IP di gestione del cluster da IPv6 a IPv4 o da IPv4 a IPv6. Il nuovo indirizzo IP viene visualizzato nella griglia del cluster e nella pagina di configurazione del cluster al termine del

successivo ciclo di monitoraggio.

4. Fai clic su **Submit**.
5. Nella finestra di dialogo Authorize Host, fai clic su **View Certificate** per visualizzare le informazioni sul certificato del cluster.
6. Fai clic su **Yes**.

   Dopo aver salvato i dettagli del cluster, puoi visualizzare il certificato per la comunicazione TLS reciproca di un cluster.

   Se l'autenticazione basata su certificati non è abilitata, Unified Manager verifica il certificato solo quando il cluster viene aggiunto inizialmente. Unified Manager non verifica il certificato per ogni chiamata API a ONTAP.

Una volta individuati tutti gli oggetti per un nuovo cluster, Unified Manager inizia a raccogliere i dati storici sulle prestazioni relativi ai 15 giorni precedenti. Queste statistiche vengono raccolte utilizzando la funzionalità di raccolta della continuità dei dati. Questa funzionalità ti fornisce oltre due settimane di informazioni sulle prestazioni di un cluster immediatamente dopo che è stato aggiunto. Al termine del ciclo di raccolta della continuità dei dati, i dati real-time sulle prestazioni del cluster vengono raccolti, per impostazione predefinita, ogni cinque minuti.

Poiché la raccolta di 15 giorni di dati sulle prestazioni richiede un elevato utilizzo della CPU, ti consigliamo di scaglionare l'aggiunta di nuovi cluster in modo che i processi di raccolta della continuità dei dati non vengano eseguiti contemporaneamente su troppi cluster. Inoltre, se riavvii Unified Manager durante il periodo di raccolta della continuità dei dati, la raccolta verrà interrotta e vedrai delle lacune nei grafici delle prestazioni per l'intervallo di tempo mancante.

Se ricevi un messaggio di errore che indica che non puoi aggiungere il cluster, verifica se gli orologi dei due sistemi non sono sincronizzati e se la data di inizio del certificato HTTPS di Unified Manager è successiva alla data del cluster. Devi assicurarti che gli orologi siano sincronizzati tramite NTP o un servizio simile.

Informazioni correlate

"Installazione di un certificato HTTPS firmato e restituito da una CA"

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**.
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**.

Cambia la password dell'utente locale in Active IQ Unified Manager

Puoi modificare la password di accesso dell'utente locale per prevenire potenziali rischi per la sicurezza.

Prima di iniziare

Devi aver effettuato l'accesso come utente locale.

Le password dell'utente di manutenzione e degli utenti remoti non possono essere modificate seguendo questi passaggi. Per modificare la password di un utente remoto, contatta l'amministratore delle password. Per modificare la password dell'utente di manutenzione, consulta "Utilizzo della console di manutenzione".

Passaggi

1. Accedi a Unified Manager.
2. Dalla barra dei menu in alto, fai clic sull'icona dell'utente e poi su **Cambia password**.

   L'opzione **Cambia password** non compare se sei un utente remoto.

3. Nella finestra di dialogo Cambia password, immetti la password corrente e la nuova password.
4. Fare clic su **Save**.

Se Unified Manager è configurato in una configurazione ad alta disponibilità, devi modificare la password sul secondo nodo della configurazione. Entrambe le istanze devono avere la stessa password.

Imposta il timeout di inattività della sessione in Active IQ Unified Manager

Puoi specificare il valore del timeout di inattività per Unified Manager in modo che la sessione termini automaticamente dopo un determinato periodo di inattività. Per impostazione predefinita, il timeout è impostato su 4.320 minuti (72 ore).

Prima di iniziare

Devi avere il ruolo di Amministratore dell'applicazione.

Questa impostazione influisce su tutte le sessioni utente attualmente connesse.

Questa opzione non è disponibile se hai abilitato l'autenticazione Security Assertion Markup Language (SAML).

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Generale** > **Impostazioni funzionalità**.
2. Nella pagina **Impostazioni funzionalità**, specifica il timeout di inattività scegliendo una delle seguenti opzioni:

Se vuoi…	Poi fai così…
Non impostare alcun timeout in modo che la sessione non si chiuda mai automaticamente	Nel pannello **Timeout di inattività**, sposta il cursore verso sinistra (disattivato) e fai clic su **Applica**.
Imposta un numero specifico di minuti come valore di timeout	Nel pannello **Timeout di inattività**, sposta il cursore verso destra (attivo), specifica il valore del timeout di inattività in minuti e fai clic su **Applica**.

Imposta il timeout della sessione tramite la CLI in Active IQ Unified Manager

Puoi impostare un valore massimo di timeout della sessione per Unified Manager utilizzando la CLI, in modo che la sessione termini automaticamente dopo un determinato periodo di tempo. Per impostazione predefinita, il timeout della sessione è impostato sul valore massimo, ovvero 4,320 minuti (72 ore). Ciò significa che la sessione termina automaticamente dopo 72 ore, anche se hai effettuato l'accesso e stai utilizzando attivamente Unified Manager.

Informazioni su questa attività

Devi avere il ruolo di Amministratore dell'applicazione.

L'impostazione del timeout di sessione influisce su tutte le sessioni degli utenti che hanno effettuato l'accesso.

Passaggi

1. Accedi alla CLI di Unified Manager inserendo il comando `um cli login`. Usa un nome utente e una password validi per l'autenticazione.
2. Inserisci il `um option set max.session.timeout.value=<in mins>` comando per modificare il valore di timeout della sessione.

Modifica l'host name di Unified Manager

Cambia l'host name della virtual appliance Active IQ Unified Manager

All'host di rete viene assegnato un nome quando l'appliance virtuale Unified Manager viene distribuita per la prima volta. Puoi modificare l'host name dopo la distribuzione. Se modifichi l'host name, devi anche rigenerare il certificato HTTPS.

Prima di iniziare

Per eseguire queste attività, devi aver effettuato l'accesso a Unified Manager come utente di manutenzione oppure disporre del ruolo Application Administrator.

Puoi utilizzare l'host name (o l'indirizzo IP dell'host) per accedere all'interfaccia utente web di Unified Manager. Se durante la distribuzione hai configurato un indirizzo IP statico per la rete, allora hai assegnato un nome all'host di rete. Se hai configurato la rete tramite DHCP, l'host name dovrebbe essere ricavato dal DNS. Se DHCP o DNS non sono configurati correttamente, l'host name "Unified Manager" viene assegnato automaticamente e associato al certificato di sicurezza.

Indipendentemente da come è stato assegnato l'host name, se cambi l'host name e intendi utilizzare il nuovo host name per accedere all'interfaccia utente web di Unified Manager, devi generare un nuovo certificato di

sicurezza.

Se accedi all'interfaccia utente web utilizzando l'indirizzo IP del server anziché l'host name, non è necessario generare un nuovo certificato se modifichi l'host name. Tuttavia, è best practice aggiornare il certificato in modo che l'host name nel certificato corrisponda all'host name effettivo.

Se cambi l'host name in Unified Manager, devi aggiornare manualmente l'host name in OnCommand Workflow Automation (WFA). L'host name non viene aggiornato automaticamente in WFA.

Il nuovo certificato non entra in vigore finché la macchina virtuale Unified Manager non viene riavviata.

Passaggi

1. Genera un certificato di sicurezza HTTPS

   Se vuoi utilizzare il nuovo host name per accedere all'interfaccia utente web di Unified Manager, devi rigenerare il certificato HTTPS per associarlo al nuovo host name.

2. Riavvia la macchina virtuale di Unified Manager

   Dopo aver rigenerato il certificato HTTPS, devi riavviare la macchina virtuale Unified Manager.

Genera un certificato di sicurezza HTTPS in Active IQ Unified Manager

Quando installi Active IQ Unified Manager per la prima volta, viene installato un certificato HTTPS predefinito. Puoi generare un nuovo certificato di sicurezza HTTPS che sostituisce quello esistente.

Prima di iniziare

Devi avere il ruolo di Amministratore dell'applicazione.

Esistono diversi motivi per rigenerare il certificato, ad esempio per ottenere valori migliori per il Distinguished Name (DN), per avere una chiave di dimensioni maggiori, un periodo di scadenza più lungo o se il certificato corrente è scaduto.

Se non hai accesso all'interfaccia utente web di Unified Manager, puoi rigenerare il certificato HTTPS con gli stessi valori utilizzando la console di manutenzione. Durante la rigenerazione dei certificati, puoi definire la dimensione della chiave e la durata di validità della chiave. Se usi l' `Reset Server Certificate` opzione dalla console di manutenzione, viene creato un nuovo certificato HTTPS valido per 397 giorni. Questo certificato avrà una chiave RSA di 2048 bit.

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Generale** > **Certificato HTTPS**.
2. Fai clic su **Rigenera certificato HTTPS**.

   Viene visualizzata la finestra di dialogo Rigenera certificato HTTPS.

3. Seleziona una delle seguenti opzioni a seconda di come vuoi generare il certificato:

Se vuoi…	Fai così…
Rigenera il certificato con i valori correnti	Fai clic sull'opzione **Rigenera utilizzando gli attributi del certificato corrente**.

Se vuoi…	Fai così…
Genera il certificato utilizzando valori diversi	Fai clic sull'opzione **Aggiorna gli attributi del certificato corrente**. I campi Common Name e Alternative Names useranno i valori del certificato esistente se non inserisci nuovi valori. Il campo "Common Name" deve essere impostato sul FQDN dell'host. Gli altri campi non richiedono valori, ma puoi inserirli, ad esempio, per EMAIL, COMPANY, DEPARTMENT, Città, Stato e Paese, se vuoi che questi valori vengano popolati nel certificato. Puoi anche selezionare tra i valori disponibili di KEY SIZE (l'algoritmo della chiave è "RSA".) e VALIDITY PERIOD. • I valori consentiti per la dimensione della chiave sono `2048`, `3072` e `4096`. • I periodi di validità vanno da un minimo di 1 giorno a un massimo di 36500 giorni. Sebbene sia consentito un periodo di validità di 36500 giorni, ti consigliamo di usare un periodo di validità non superiore a 397 giorni o 13 mesi. Questo perché, se selezioni un periodo di validità superiore a 397 giorni e prevedi di esportare un CSR per questo certificato e di farlo firmare da una CA nota, la validità del certificato firmato che la CA ti restituisce verrà ridotta a 397 giorni. • Puoi selezionare la casella di controllo "Escludi informazioni di identificazione locali (ad es. localhost)" se vuoi rimuovere le informazioni di identificazione locali dal campo Nomi alternativi del certificato. Quando questa casella di controllo è selezionata, nel campo Nomi alternativi viene usato solo ciò che inserisci nel campo. Se lasciato vuoto, il certificato risultante non avrà alcun campo Nomi alternativi.

4. Fai clic su **Sì** per rigenerare il certificato.

5. Riavvia il server Unified Manager affinché il nuovo certificato diventi effettivo.
6. Verifica le informazioni del nuovo certificato visualizzando il certificato HTTPS.

Riavvia la macchina virtuale Active IQ Unified Manager

Puoi riavviare la macchina virtuale dalla console di manutenzione di Unified Manager. Devi riavviare dopo aver generato un nuovo certificato di sicurezza o se si verifica un problema con la macchina virtuale.

Prima di iniziare

L'appliance virtuale è accesa.

Hai effettuato l'accesso alla console di manutenzione come utente di manutenzione.

Puoi anche riavviare la macchina virtuale da vSphere utilizzando l'opzione **Restart Guest**. Per ulteriori informazioni, consulta la documentazione VMware.

Passaggi

1. Accedi alla console di manutenzione.
2. Seleziona **Configurazione di sistema** > **Riavvia macchina virtuale**.

Cambia l'host name di Active IQ Unified Manager sui sistemi Linux

A un certo punto, potresti voler modificare l'host name della macchina Red Hat Enterprise Linux su cui hai installato Unified Manager. Ad esempio, potresti voler rinominare l'host per identificare più facilmente i server Unified Manager in base al tipo, al gruppo di lavoro o al gruppo di cluster monitorato quando elenchi le tue macchine Linux.

Prima di iniziare

Devi avere accesso come utente root al sistema Linux su cui è installato Unified Manager.

Puoi utilizzare l'host name (o l'indirizzo IP dell'host) per accedere all'interfaccia utente web di Unified Manager. Se durante la distribuzione hai configurato un indirizzo IP statico per la tua rete, avrai assegnato un nome all'host di rete. Se hai configurato la rete tramite DHCP, l'host name dovrebbe essere ricavato dal DNS server.

Indipendentemente da come è stato assegnato l'host name, se cambi l'host name e intendi utilizzare il nuovo host name per accedere all'interfaccia utente web di Unified Manager, devi generare un nuovo certificato di sicurezza.

Se accedi all'interfaccia web utilizzando l'indirizzo IP del server anziché l'host name, non devi generare un nuovo certificato se modifichi l'host name. Tuttavia, è best practice aggiornare il certificato, in modo che l'host name nel certificato corrisponda all'host name effettivo. Il nuovo certificato non ha effetto finché non riavvii la macchina Linux.

Se cambi l'host name in Unified Manager, devi aggiornare manualmente l'host name in OnCommand Workflow Automation (WFA). L'host name non viene aggiornato automaticamente in WFA.

Passaggi

1. Accedi come utente root al sistema Unified Manager che desideri modificare.
2. Arresta il software Unified Manager e il relativo software MySQL immettendo il seguente comando:

```
systemctl stop ocieau ocie mysqld
```

3. Modifica l'host name usando il comando Linux `hostnamectl`:

```
hostnamectl set-hostname new_FQDN
```

```
hostnamectl set-hostname nuhost.corp.widget.com
```

4. Rigenera il certificato HTTPS per il server:

```
/opt/netapp/essentials/bin/cert.sh create
```

5. Riavvia il servizio di rete:

```
systemctl restart NetworkManager.service
```

6. Dopo il riavvio del servizio, verifica se il nuovo host name riesce a eseguire un ping verso se stesso:

```
ping new_hostname
```

```
ping nuhost
```

Questo comando dovrebbe restituire lo stesso indirizzo IP impostato in precedenza per l'host name originale.

7. Dopo aver completato e verificato la modifica dell'host name, riavvia Unified Manager immettendo il seguente comando:

```
systemctl start mysqld ocie ocieau
```

Abilita e disabilita la gestione dello storage basata su policy in Active IQ Unified Manager

A partire da Unified Manager 9.7, puoi eseguire il provisioning dei carichi di lavoro dello storage (volumi e LUN) sui cluster ONTAP e gestire questi carichi di lavoro in base ai livelli di servizio delle prestazioni assegnati. Questa funzionalità è simile alla creazione di carichi di lavoro in ONTAP System Manager e all'associazione di policy QoS, ma se la applichi tramite Unified Manager puoi eseguire il provisioning e gestire i carichi di lavoro in tutti i cluster monitorati dalla tua istanza di Unified Manager.

Devi avere il ruolo di Amministratore dell'applicazione.

Questa opzione è abilitata per impostazione predefinita, ma puoi disabilitarla se non vuoi eseguire il provisioning e gestire i carichi di lavoro tramite Unified Manager.

Quando attivata, questa opzione fornisce molti nuovi elementi nell'interfaccia utente:

Nuovi contenuti	Posizione
Una pagina per il provisioning di nuovi carichi di lavoro	Disponibile da **Attività comuni** > **Provisioning**

Nuovi contenuti	Posizione
Una pagina per creare policy dei livelli di servizio delle prestazioni	Disponibile in **Impostazioni** > **Policy** > **Livelli di servizio delle prestazioni**
Una pagina per creare criteri di efficienza dello storage per le prestazioni	Disponibile in **Impostazioni** > **Criteri** > **Efficienza di archiviazione**
Pannelli che descrivono le prestazioni correnti del workload e gli IOPS del workload	Disponibile dalla Dashboard

Per ulteriori informazioni su queste pagine e su questa funzionalità, consulta la guida online nel prodotto.

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Generale** > **Impostazioni funzionalità**.
2. Nella pagina **Impostazioni funzionalità**, abilita o disabilita la gestione dello storage basata su policy scegliendo una delle seguenti opzioni:

Se vuoi…	Poi fai così…
Disabilita la gestione dello storage basata su policy	Nel pannello **Gestione dello storage basata su policy**, sposta il cursore verso sinistra.
Abilita la gestione dello storage basata su policy	Nel pannello **Gestione dello storage basata su policy**, sposta il cursore verso destra.

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.