Configura Active IQ Unified Manager

Active IQ Unified Manager

NetApp
October 15, 2025

Sommario

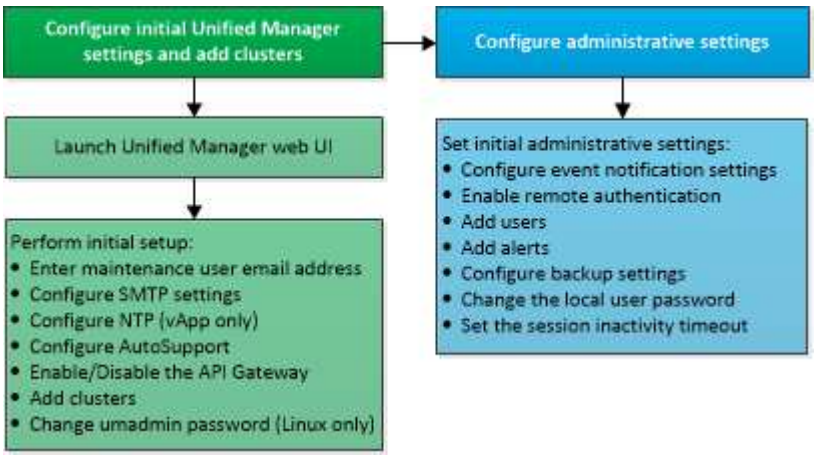
Configura Active IQ Unified Manager

Dopo aver installato Active IQ Unified Manager (in precedenza OnCommand Unified Manager), è necessario completare la configurazione iniziale (chiamata anche procedura guidata per la prima esperienza) per accedere all'interfaccia utente Web. È quindi possibile eseguire ulteriori attività di configurazione, come l'aggiunta di cluster, la configurazione dell'autenticazione remota, l'aggiunta di utenti e l'aggiunta di avvisi.

Alcune delle procedure descritte in questo manuale sono necessarie per completare la configurazione iniziale dell'istanza di Unified Manager. Altre procedure sono impostazioni di configurazione consigliate che è utile impostare sulla nuova istanza o che è bene conoscere prima di iniziare il monitoraggio regolare dei sistemi ONTAP .

Panoramica della sequenza di configurazione

Il flusso di lavoro di configurazione descrive le attività che è necessario eseguire prima di poter utilizzare Unified Manager.



Accedi all'interfaccia utente web di Unified Manager

Dopo aver installato Unified Manager, puoi accedere all'interfaccia utente 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 effettuare l'accesso come utente di manutenzione (o utente umadmin per le installazioni Linux).
- Se si prevede di consentire agli utenti di accedere a Unified Manager utilizzando il nome breve anziché il nome di dominio completo (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. È possibile accettare il rischio di continuare l'accesso oppure installare un certificato digitale firmato da un'autorità di certificazione (CA) per l'autenticazione del server.

Passi

1. Avviare l'interfaccia utente Web di Unified Manager dal browser utilizzando l'URL visualizzato al termine

dell'installazione. L'URL è l'indirizzo IP o il nome di dominio completo (FQDN) del server Unified Manager.

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

2. Accedi all'interfaccia utente Web di Unified Manager utilizzando le tue credenziali utente di manutenzione.

Se effettui tre tentativi consecutivi di accesso all'interfaccia utente web senza successo nell'arco di un'ora, verrai bloccato fuori dal sistema e dovrai contattare l'amministratore di sistema. Questa opzione è valida solo per gli utenti locali.

Eseguire la configurazione iniziale dell'interfaccia utente Web di Unified Manager

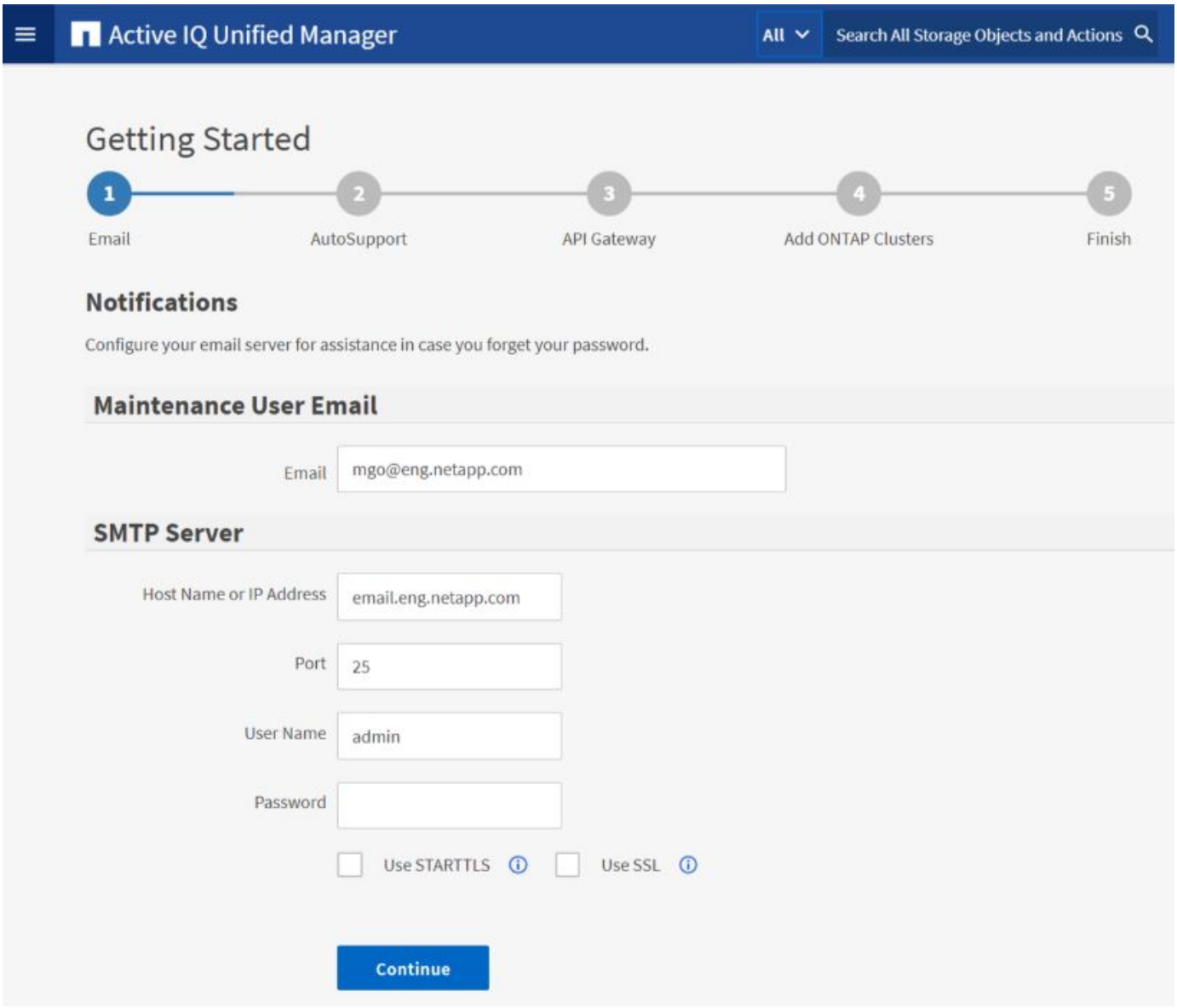
Per utilizzare Unified Manager, è necessario innanzitutto configurare le opzioni di configurazione iniziale, tra cui il server NTP, l'indirizzo e-mail dell'utente addetto alla manutenzione, l'host del server SMTP e l'aggiunta di cluster ONTAP .

Prima di iniziare

Devi aver eseguito le seguenti operazioni:

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

La pagina introduttiva di Active IQ Unified Manager viene visualizzata solo quando si accede per la prima volta all'interfaccia utente Web. La pagina seguente è tratta da un'installazione su VMware.



Se in seguito desideri modificare una di queste opzioni, puoi selezionarla dalle opzioni Generali nel riquadro di navigazione a sinistra di Unified Manager. Si noti 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.

Passi

1. Nella pagina Configurazione iniziale Active IQ Unified Manager , immettere l'indirizzo e-mail dell'utente addetto alla manutenzione, il nome host del server SMTP e tutte le opzioni SMTP aggiuntive, nonché il server NTP (solo installazioni VMware). Quindi fare clic su **Continua**.

   Se hai selezionato l'opzione **Usa STARTTLS** o **Usa SSL**, dopo aver cliccato sul pulsante **Continua** verrà visualizzata una pagina del certificato. Verificare i dettagli del certificato e accettare il certificato per continuare con le impostazioni di configurazione iniziale dell'interfaccia utente Web.

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

   Se è necessario designare un proxy per fornire l'accesso a Internet per inviare contenuti AutoSupport , oppure se si desidera disattivare AutoSupport, utilizzare l'opzione **Generale** > * AutoSupport*

dall'interfaccia utente Web.

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

   È possibile abilitare o disabilitare questa impostazione in un secondo momento nell'interfaccia utente Web da **Generale** > **Impostazioni funzionalità** > **API Gateway**. Per ulteriori informazioni sulle API, vedere"Introduzione alle API REST Active IQ Unified Manager" .

5. Aggiungere i cluster che si desidera vengano gestiti da Unified Manager, quindi fare clic su **Avanti**. Per ogni cluster che intendi gestire, devi disporre del nome host o dell'indirizzo IP di gestione del cluster (IPv4 o IPv6) insieme alle credenziali di nome utente e password; l'utente deve avere il ruolo "admin".

   Questo passaggio è facoltativo. È possibile aggiungere cluster in un secondo momento nell'interfaccia utente Web da **Gestione archiviazione** > **Configurazione cluster**.

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

La pagina Introduzione si chiude e viene visualizzata la pagina Dashboard di Unified Manager.

Aggiungi cluster

È possibile aggiungere un cluster ad Active IQ Unified Manager in modo da poterlo monitorare. Ciò include la possibilità di ottenere informazioni sul cluster, quali integrità, capacità, prestazioni e configurazione del cluster, in modo da poter individuare e risolvere eventuali problemi che potrebbero verificarsi.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario disporre delle seguenti informazioni:
  - Unified Manager supporta cluster ONTAP on-premise, ONTAP Select Cloud Volumes ONTAP.
  - Nome host o indirizzo IP di gestione del cluster

    Il nome host è il nome FQDN o nome breve utilizzato da Unified Manager per connettersi al cluster. Il nome host deve essere risolto nell'indirizzo IP di gestione del cluster.

    L'indirizzo IP di gestione del cluster deve essere il LIF di gestione del cluster della macchina virtuale di archiviazione amministrativa (SVM). Se si utilizza un LIF di gestione dei nodi, l'operazione fallisce.

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

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

  - Il numero di porta per connettersi al cluster tramite il protocollo HTTPS (in genere la porta 443)
  - Hai i certificati richiesti:

Certificato SSL (HTTPS): Questo certificato è di proprietà di Unified Manager. Con una nuova installazione di Unified Manager viene generato un certificato SSL autofirmato predefinito (HTTPS). NetApp consiglia di aggiornarlo al certificato firmato da una CA per una maggiore sicurezza. Se il certificato del server scade, è necessario rigenerarlo e riavviare Unified Manager affinché i servizi incorporino il nuovo certificato. Per ulteriori informazioni sulla rigenerazione del certificato SSL, vedere"Generazione di un certificato di sicurezza HTTPS" .

Certificato EMS: Questo certificato è di proprietà di Unified Manager. Viene utilizzato 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 certificato è abilitata per un cluster, in base alla versione ONTAP . Se il cluster che esegue la versione ONTAP è precedente alla 9.5, l'autenticazione basata su certificato non è abilitata.

L'autenticazione basata su certificato non viene abilitata automaticamente per un cluster se si aggiorna una versione precedente di Unified Manager. Tuttavia, è possibile abilitarlo modificando e salvando i dettagli del cluster. Se il certificato scade, è necessario rigenerarlo per incorporare il nuovo certificato. Per ulteriori informazioni sulla visualizzazione e la rigenerazione del certificato, vedere"Modifica dei cluster" .

- È possibile aggiungere un cluster dall'interfaccia utente Web e l'autenticazione basata su certificato verrà abilitata automaticamente.
- È possibile aggiungere un cluster tramite Unified Manager CLI; l'autenticazione basata su certificato non è abilitata per impostazione predefinita. Se si aggiunge un cluster tramite Unified Manager CLI, è necessario modificare il cluster tramite l'interfaccia utente di Unified Manager. Puoi vedere"Comandi CLI di Unified Manager supportati" per aggiungere un cluster utilizzando Unified Manager CLI.
- Se per un cluster è abilitata l'autenticazione basata su certificato e si esegue il backup di Unified Manager da un server e lo si ripristina su un altro server Unified Manager in cui il nome host o l'indirizzo IP è stato modificato, il monitoraggio del cluster potrebbe non riuscire. Per evitare il fallimento, modificare e salvare i dettagli del cluster. Per ulteriori informazioni sulla modifica dei dettagli del cluster, vedere"Modifica dei cluster" .

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

- È necessario disporre di spazio adeguato sul server Unified Manager. Non è possibile aggiungere un cluster al server quando è già stato utilizzato più del 90% dello spazio nella directory del database.

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

Passi

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

È possibile 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 ciclo di monitoraggio successivo.

4. Fare clic su **Invia**.
5. Nella finestra di dialogo Autorizza host, fare clic su **Visualizza certificato** per visualizzare le informazioni sul certificato del cluster.
6. Fare clic su **Sì**.

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

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

Dopo aver individuato tutti gli oggetti per un nuovo cluster, Unified Manager inizia a raccogliere dati storici sulle prestazioni dei 15 giorni precedenti. Queste statistiche vengono raccolte utilizzando la funzionalità di raccolta della continuità dei dati. Questa funzionalità fornisce informazioni sulle prestazioni di un cluster per oltre due settimane, subito dopo la sua aggiunta. Una volta completato il ciclo di raccolta della continuità dei dati, i dati sulle prestazioni del cluster in tempo reale vengono raccolti, per impostazione predefinita, ogni cinque minuti.

Poiché la raccolta di 15 giorni di dati sulle prestazioni richiede un uso intensivo della CPU, si consiglia di scaglionare l'aggiunta di nuovi cluster in modo che i sondaggi sulla raccolta della continuità dei dati non vengano eseguiti su troppi cluster contemporaneamente. Inoltre, se si riavvia Unified Manager durante il periodo di raccolta della continuità dei dati, la raccolta verrà interrotta e si vedranno delle lacune nei grafici delle prestazioni per il periodo di tempo mancante.

Se viene visualizzato un messaggio di errore che indica che non è possibile aggiungere il cluster, verificare che gli orologi sui due sistemi non siano sincronizzati e che la data di inizio del certificato HTTPS di Unified Manager sia successiva alla data sul cluster. È necessario assicurarsi che gli orologi siano sincronizzati tramite NTP o un servizio simile.

Informazioni correlate

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

Configurare Unified Manager per inviare notifiche di avviso

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

Prima di iniziare

È necessario disporre del ruolo di amministratore dell'applicazione.

Dopo aver distribuito Unified Manager e completato la configurazione iniziale, dovresti prendere in considerazione la possibilità di configurare l'ambiente in modo da attivare avvisi e generare e-mail di notifica o trap SNMP in base alla ricezione di eventi.

Passi

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

   Se si desidera che vengano inviate notifiche di avviso quando si verificano determinati eventi nel proprio ambiente, è necessario configurare un server SMTP e fornire un indirizzo e-mail da cui verrà inviata la notifica di avviso. Se si desidera utilizzare trap SNMP, è possibile selezionare tale opzione e fornire le informazioni necessarie.

2. "Abilita 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 abilitare l'autenticazione remota.

3. "Aggiungi 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. "Aggiungi utenti".

   È possibile aggiungere diversi tipi di utenti locali o remoti e assegnare ruoli specifici. Quando si crea un avviso, si assegna un utente che riceverà le notifiche di avviso.

5. "Aggiungi avvisi".

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

Configurare le impostazioni di notifica degli eventi

È possibile configurare Unified Manager in modo che invii notifiche di avviso quando viene generato un evento o quando un evento viene assegnato 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.

Prima di iniziare

È necessario disporre delle seguenti informazioni:

- Indirizzo email da cui viene inviata la notifica di avviso

  L'indirizzo email appare nel campo "Da" nelle notifiche di avviso inviate. Se per qualsiasi motivo l'e-mail non può essere recapitata, questo indirizzo e-mail viene utilizzato anche come destinatario per la posta non recapitata.

- Nome host del server SMTP e nome utente e password per accedere al server
- Nome host o indirizzo IP per l'host di destinazione della trappola che riceverà la trappola SNMP, insieme alla versione SNMP, alla porta della trappola in uscita, alla community e ad altri valori di configurazione SNMP richiesti

  Per specificare più destinazioni trap, separare ogni host con una virgola. In questo caso, tutte le altre impostazioni SNMP, come la versione e la porta trap in uscita, devono essere le stesse per tutti gli host

nell'elenco.

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Passi

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

   Note:

   - Se l'indirizzo del mittente è precompilato con l'indirizzo "ActiveIQUnifiedManager@localhost.com", dovresti modificarlo con un indirizzo email reale e funzionante per assicurarti che tutte le notifiche email vengano recapitate correttamente.
   - Se non è possibile risolvere il nome host del server SMTP, è possibile specificare l'indirizzo IP (IPv4 o IPv6) del server SMTP anziché il nome host.
3. Fare clic su **Salva**.
4. Se hai selezionato l'opzione **Usa STARTTLS** o **Usa SSL**, dopo aver fatto clic sul pulsante **Salva** verrà visualizzata una pagina del certificato. Verificare i dettagli del certificato e accettare il certificato per salvare le impostazioni di notifica.

   È possibile 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

È possibile abilitare 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 gli oggetti di archiviazione e i dati.

Prima di iniziare

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, ad esempio SSSD (System Security Services Daemon) o NSLCD (Name Service LDAP Caching Daemon).

È possibile abilitare l'autenticazione remota utilizzando 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 (Secure LDAP). Unified Manager utilizza 389 come porta predefinita per le comunicazioni non sicure e 636 come porta predefinita per le comunicazioni sicure.

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

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale** > **Autenticazione remota**.
2. Seleziona la casella **Abilita 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…
Directory attiva	• 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)
Apri LDAP	• Associa nome distinto (nella notazione LDAP appropriata) • Password di collegamento • Nome distinto di base

Se l'autenticazione di un utente di Active Directory richiede molto tempo o scade, è probabile che il server di autenticazione stia impiegando molto tempo a 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 tramite il protocollo Secure Sockets Layer (SSL).

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

Disabilita i gruppi nidificati dall'autenticazione remota

Se è abilitata l'autenticazione remota, è possibile disabilitare l'autenticazione di gruppo nidificata in modo che solo i singoli utenti, e non i membri del gruppo, possano autenticarsi in remoto su Unified Manager. È possibile disabilitare i gruppi nidificati quando si desidera migliorare il tempo di risposta dell'autenticazione di Active Directory.

Prima di iniziare

- È necessario disporre del ruolo di amministratore dell'applicazione.
- La disabilitazione 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 per i gruppi nidificati è disabilitato e se un gruppo remoto viene aggiunto a Unified Manager, i singoli utenti devono essere membri del gruppo remoto per autenticarsi in Unified Manager.

Passi

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

Impostare i servizi di autenticazione

I servizi di autenticazione consentono l'autenticazione di utenti 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) oppure configurando un proprio meccanismo di autenticazione.

Prima di iniziare

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

Passi

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

Se selezioni…	Allora fai così…
Directory attiva	a. Inserisci 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 associazione. 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 selezioni…	Allora fai così…
Altri	a. Immettere il nome distinto e la password di associazione. 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 utente e gli attributi del membro.

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

3. Fare clic su **Salva**.

Aggiungi 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.

Prima di iniziare

- 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 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.
- 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) (che utilizza 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.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale** > **Autenticazione remota**.
2. Abilita o disabilita l'opzione **Usa connessione sicura**:

Se lo desidera…	Allora fai così…
Abilitalo	a. Selezionare l'opzione **Usa connessione protetta**. b. Nell'area Server di autenticazione, fare clic su **Aggiungi**. c. Nella finestra di dialogo 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 sul certificato, quindi fare clic su **Chiudi**. f. Nella finestra di dialogo Autorizza host, fare clic su **Sì**. Quando si abilita l'opzione **Usa autenticazione connessione protetta**, Unified Manager comunica con il server di autenticazione e visualizza il certificato. Unified Manager utilizza la porta 636 come porta predefinita per le comunicazioni protette e la porta 389 per le comunicazioni non protette.
Disabilitarlo	a. Deselezionare l'opzione **Usa connessione protetta**. b. Nell'area Server di autenticazione, fare clic su **Aggiungi**. c. Nella finestra di dialogo 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. Esegui un'autenticazione di prova per confermare che puoi autenticare gli utenti nel server di autenticazione che hai aggiunto.

Testare la 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 cercando un utente o un gruppo remoto dai server di autenticazione e autenticandolo tramite le impostazioni configurate.

Prima di iniziare

- È necessario 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.
- È necessario aver aggiunto i server di autenticazione affinché il server di gestione possa cercare l'utente 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 di utenti remoti che appartengono al gruppo primario del server di autenticazione, le informazioni sul gruppo primario non vengono visualizzate nei risultati dell'autenticazione.

Passi

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

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

Aggiungi avvisi

È possibile configurare degli avvisi per essere avvisati quando viene generato un evento specifico. È possibile configurare gli avvisi per una singola risorsa, per un gruppo di risorse o per eventi di un tipo di gravità specifico. È possibile specificare la frequenza con cui si desidera ricevere la notifica e associare uno script all'avviso.

Prima di iniziare

- È necessario aver configurato le impostazioni di notifica, quali l'indirizzo e-mail dell'utente, il server SMTP e l'host trap SNMP, per consentire al server Active IQ Unified Manager di utilizzare queste impostazioni per inviare notifiche agli utenti quando viene generato un evento.
- 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 a cui si desidera inviare la notifica.
- Se si desidera che uno script venga eseguito in base all'evento, è necessario aver aggiunto lo script a Unified Manager tramite la pagina Script.
- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

È possibile creare un avviso direttamente dalla pagina Dettagli evento dopo aver ricevuto un evento, oltre a creare un avviso dalla pagina Impostazione avviso, come descritto qui.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione** > **Configurazione avvisi**.
2. Nella pagina Impostazione avvisi, fare clic su **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 **Il nome contiene** per selezionare un gruppo di risorse. In base alla stringa di testo specificata, l'elenco delle risorse disponibili visualizza solo le risorse che corrispondono alla regola del filtro. La stringa di testo specificata è sensibile alla distinzione tra maiuscole e minuscole.

   Se una risorsa è conforme sia alle regole di inclusione che a quelle di 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 gravità dell'evento per cui si desidera attivare un avviso.

   Per selezionare più di un evento, premere il tasto Ctrl mentre si effettuano le selezioni.

6. Fare clic su **Azioni** e selezionare gli utenti a cui si desidera inviare la notifica, scegliere la frequenza della 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 email specificato per l'utente e si riapre l'avviso per modificarlo, il campo Nome appare vuoto perché l'indirizzo email modificato non è più associato all'utente precedentemente selezionato. Inoltre, se hai modificato l'indirizzo email dell'utente selezionato dalla pagina Utenti, l'indirizzo email modificato non verrà aggiornato per l'utente selezionato.

   È anche possibile scegliere di avvisare gli utenti tramite trap SNMP.

7. Fare clic su **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 essere avvisato ogni 15 minuti

Eseguire i seguenti passaggi nella finestra di dialogo Aggiungi avviso:

Passi

1. Fare clic su **Nome** e immettere **HealthTest** nel campo **Nome avviso**.
2. Fare clic su **Risorse** e, nella scheda Includi, selezionare **Volumi** dall'elenco a discesa.
   a. Immettere **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 spostarlo nell'area Risorse selezionate.
   c. Fare clic su **Escludi** e immettere **xyz** nel campo **Il nome contiene**, quindi fare clic su **Aggiungi**.
3. Fare clic su **Eventi** e selezionare **Critico** dal campo Gravità evento.

4. Seleziona **Tutti gli eventi critici** dall'area Eventi corrispondenti e spostalo nell'area Eventi selezionati.
5. Fare clic su **Azioni** e immettere **sample@domain.com** nel campo Avvisa questi utenti.
6. Seleziona **Ricorda ogni 15 minuti** per avvisare l'utente ogni 15 minuti.

   È possibile configurare un avviso in modo che invii ripetutamente notifiche ai destinatari per un periodo di tempo specificato. È necessario stabilire l'orario a partire dal quale la notifica dell'evento è attiva per l'avviso.

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

Cambia la password dell'utente locale

È possibile 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 per l'utente addetto alla manutenzione e per gli utenti remoti non possono essere modificate seguendo questi passaggi. Per modificare la password di un utente remoto, contattare l'amministratore delle password. Per modificare la password dell'utente addetto alla manutenzione, vedere"Utilizzo della console di manutenzione" .

Passi

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

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

3. Nella finestra di dialogo Cambia password, immettere la password corrente e quella nuova.
4. Fare clic su **Salva**.

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

Imposta il timeout di inattività della sessione

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

Prima di iniziare

È necessario disporre del ruolo di amministratore dell'applicazione.

Questa impostazione ha effetto su tutte le sessioni utente registrate.

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

Passi

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

Se lo desidera…	Allora fai così…
Non impostare alcun timeout in modo che la sessione non venga mai chiusa automaticamente	Nel pannello **Timeout di inattività**, spostare il cursore verso sinistra (off) e fare clic su **Applica**.
Imposta un numero specifico di minuti come valore di timeout	Nel pannello **Timeout di inattività**, spostare il cursore verso destra (on), specificare il valore del timeout di inattività in minuti e fare clic su **Applica**.

Imposta il timeout della sessione tramite CLI

È possibile impostare un valore massimo di timeout della sessione per Unified Manager tramite la CLI, in modo che la sessione venga terminata 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 questo compito

È necessario disporre del ruolo di amministratore dell'applicazione.

L'impostazione del timeout della sessione ha effetto su tutte le sessioni degli utenti registrati.

Passi

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

Cambiare il nome host di Unified Manager

A un certo punto, potresti voler modificare il nome host del sistema 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 monitorati.

I passaggi necessari per modificare il nome host sono diversi a seconda che Unified Manager sia in esecuzione su un server VMware ESXi, su un server Red Hat Linux o su un server Microsoft Windows.

Modificare il nome host dell'appliance virtuale Unified Manager

All'host di rete viene assegnato un nome quando l'appliance virtuale Unified Manager

viene distribuita per la prima volta. È possibile modificare il nome host dopo la distribuzione. Se si modifica il nome host, è necessario rigenerare anche il certificato HTTPS.

Prima di iniziare

Per eseguire queste attività, è necessario aver effettuato l'accesso a Unified Manager come utente addetto alla manutenzione oppure avere il ruolo di amministratore dell'applicazione assegnato.

È possibile utilizzare il nome host (o l'indirizzo IP host) per accedere all'interfaccia utente Web di Unified Manager. Se hai configurato un indirizzo IP statico per la tua rete durante la distribuzione, allora avrai designato un nome per l'host di rete. Se hai configurato la rete tramite DHCP, il nome host dovrebbe essere preso dal DNS. Se DHCP o DNS non sono configurati correttamente, il nome host "Unified Manager" viene assegnato automaticamente e associato al certificato di sicurezza.

Indipendentemente da come è stato assegnato il nome host, se si modifica il nome host e si intende utilizzare il nuovo nome host per accedere all'interfaccia utente Web di Unified Manager, è necessario generare un nuovo certificato di sicurezza.

Se si accede all'interfaccia utente Web utilizzando l'indirizzo IP del server anziché il nome host, non è necessario generare un nuovo certificato se si modifica il nome host. Tuttavia, è consigliabile aggiornare il certificato in modo che il nome host nel certificato corrisponda al nome host effettivo.

Se si modifica il nome host in Unified Manager, è necessario aggiornare manualmente il nome host in OnCommand Workflow Automation (WFA). Il nome host non viene aggiornato automaticamente in WFA.

Il nuovo certificato non avrà effetto finché non verrà riavviata la macchina virtuale Unified Manager.

Passi

1. Genera un certificato di sicurezza HTTPS

   Se si desidera utilizzare il nuovo nome host per accedere all'interfaccia utente Web di Unified Manager, è necessario rigenerare il certificato HTTPS per associarlo al nuovo nome host.

2. Riavviare la macchina virtuale Unified Manager

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

Genera un certificato di sicurezza HTTPS

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

Prima di iniziare

È necessario disporre del ruolo di amministratore dell'applicazione.

Possono esserci molteplici motivi per rigenerare il certificato, ad esempio se si desiderano valori migliori per il Nome distinto (DN), se si desidera una dimensione della chiave maggiore, un periodo di scadenza più lungo o se il certificato corrente è scaduto.

Se non si ha accesso all'interfaccia utente Web di Unified Manager, è possibile rigenerare il certificato HTTPS con gli stessi valori utilizzando la console di manutenzione. Durante la rigenerazione dei certificati, è possibile definire la dimensione della chiave e la durata di validità della chiave. Se usi il `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 dimensione 2048 bit.

Passi

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

   Viene visualizzata la finestra di dialogo Rigenera certificato HTTPS.

3. Selezionare una delle seguenti opzioni a seconda di come si desidera generare il certificato:

Se lo desidera…	Fai questo…
Rigenera il certificato con i valori correnti	Fare clic sull'opzione **Rigenera utilizzando gli attributi del certificato corrente**.

Se lo desidera…	Fai questo…
Generare il certificato utilizzando valori diversi	Fare clic sull'opzione **Aggiorna gli attributi del certificato corrente**. Se non si immettono nuovi valori, i campi Nome comune e Nomi alternativi utilizzeranno i valori del certificato esistente. Il ``Nome comune' dovrebbe essere impostato sul nome di dominio completo (FQDN) dell'host. Gli altri campi non richiedono valori, ma è possibile immettere valori, ad esempio, per EMAIL, AZIENDA, REPARTO, Città, Stato e Paese se si desidera che tali valori vengano compilati nel certificato. È anche possibile selezionare tra le DIMENSIONI DELLA CHIAVE disponibili (l'algoritmo della chiave è "RSA") e il PERIODO DI VALIDITÀ. • 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 36.500 giorni, si consiglia di utilizzare un periodo di validità non superiore a 397 giorni o 13 mesi. Poiché se selezioni un periodo di validità superiore a 397 giorni e intendi esportare una CSR per questo certificato e farla firmare da una CA nota, la validità del certificato firmato restituito dalla CA verrà ridotta a 397 giorni. • È possibile selezionare la casella di controllo "Escludi informazioni di identificazione locali (ad esempio localhost)" se si desidera rimuovere le informazioni di identificazione locali dal campo Nomi alternativi nel certificato. Quando questa casella di controllo è selezionata, nel campo Nomi alternativi verrà utilizzato solo ciò che inserisci nel campo. Se lasciato vuoto, il certificato risultante non avrà alcun campo Nomi alternativi.

4. Fare clic su **Sì** per rigenerare il certificato.
5. Riavviare il server Unified Manager affinché il nuovo certificato abbia effetto.
6. Verificare le informazioni del nuovo certificato visualizzando il certificato HTTPS.

Riavviare la macchina virtuale Unified Manager

È possibile riavviare la macchina virtuale dalla console di manutenzione di Unified Manager. È necessario 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 addetto alla manutenzione.

È anche possibile riavviare la macchina virtuale da vSphere utilizzando l'opzione **Riavvia Guest**. Per ulteriori informazioni, consultare la documentazione VMware.

Passi

1. Accedere alla console di manutenzione.
2. Selezionare **Configurazione di sistema** > **Riavvia macchina virtuale**.

Modificare il nome host di Unified Manager sui sistemi Linux

A un certo punto, potresti voler modificare il nome host del computer 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 monitorati quando elenchi i tuoi computer Linux.

Prima di iniziare

È necessario disporre dell'accesso come utente root al sistema Linux su cui è installato Unified Manager.

È possibile utilizzare il nome host (o l'indirizzo IP host) per accedere all'interfaccia utente Web di Unified Manager. Se hai configurato un indirizzo IP statico per la tua rete durante la distribuzione, allora avrai designato un nome per l'host di rete. Se hai configurato la rete tramite DHCP, il nome host dovrebbe essere preso dal server DNS.

Indipendentemente da come è stato assegnato il nome host, se si modifica il nome host e si intende utilizzare il nuovo nome host per accedere all'interfaccia utente Web di Unified Manager, è necessario generare un nuovo certificato di sicurezza.

Se si accede all'interfaccia utente Web utilizzando l'indirizzo IP del server anziché il nome host, non è necessario generare un nuovo certificato se si modifica il nome host. Tuttavia, è consigliabile aggiornare il certificato in modo che il nome host nel certificato corrisponda al nome host effettivo. Il nuovo certificato non avrà effetto finché non verrà riavviato il computer Linux.

Se si modifica il nome host in Unified Manager, è necessario aggiornare manualmente il nome host in OnCommand Workflow Automation (WFA). Il nome host non viene aggiornato automaticamente in WFA.

Passi

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

   ```
   systemctl stop ocieau ocie mysqld
   ```

3. Cambia il nome host usando Linux `hostnamectl` comando:

   ```
   hostnamectl set-hostname new_FQDN
   ```

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

4. Rigenerare il certificato HTTPS per il server:

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

5. Riavviare il servizio di rete:

   ```
   systemctl restart NetworkManager.service
   ```

6. Dopo aver riavviato il servizio, verificare se il nuovo nome host è in grado di eseguire il ping su se stesso:

   ```
   ping new_hostname
   ```

   ```
   ping nuhost
   ```

   Questo comando dovrebbe restituire lo stesso indirizzo IP impostato in precedenza per il nome host originale.

7. Dopo aver completato e verificato la modifica del nome host, riavviare Unified Manager immettendo il seguente comando:

   ```
   systemctl start mysqld ocie ocieau
   ```

Abilitare e disabilitare la gestione dell'archiviazione basata su policy

A partire da Unified Manager 9.7, è possibile eseguire il provisioning di carichi di lavoro di archiviazione (volumi e LUN) sui cluster ONTAP e gestire tali 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 quando applicata tramite Unified Manager è possibile eseguire il provisioning e gestire i carichi di lavoro su tutti i cluster monitorati dall'istanza di Unified Manager.

È necessario disporre del ruolo di amministratore dell'applicazione.

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

Se abilitata, 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**
Una pagina per creare policy di livello di servizio delle prestazioni	Disponibile da **Impostazioni** > **Criteri** > **Livelli di servizio delle prestazioni**
Una pagina per creare policy di efficienza di archiviazione delle prestazioni	Disponibile da **Impostazioni** > **Criteri** > **Efficienza di archiviazione**
Pannelli che descrivono le prestazioni del carico di lavoro e gli IOPS del carico di lavoro attuali	Disponibile dalla Dashboard

Per maggiori informazioni su queste pagine e su questa funzionalità, consultare la guida in linea del prodotto.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale** > **Impostazioni funzionalità**.
2. Nella pagina **Impostazioni funzionalità**, disabilita o abilita la gestione dell'archiviazione basata su criteri scegliendo una delle seguenti opzioni:

Se lo desidera…	Allora fai così…
Disabilitare la gestione dell'archiviazione basata su policy	Nel pannello **Gestione dell'archiviazione basata su criteri**, spostare il cursore verso sinistra.
Abilita la gestione dell'archiviazione basata su policy	Nel pannello **Gestione dell'archiviazione basata su criteri**, spostare il cursore verso destra.