Modifica l'host name di 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/task_change_unified_manager_host_name_on_vmware.html on November 13, 2026. Always check docs.netapp.com for the latest.

Sommario

Modifica l’host name di Unified Manager 1
Cambia l’host name della virtual appliance Active IQ Unified Manager 1
Genera un certificato di sicurezza HTTPS in Active IQ Unified Manager 1
Riavvia la macchina virtuale Active IQ Unified Manager 4
Cambia l’host name di Active IQ Unified Manager sui sistemi Linux 4

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
   ```

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.