



Cambiare il nome host di Unified Manager

Active IQ Unified Manager

NetApp
October 15, 2025

This PDF was generated from https://docs.netapp.com/it-it/active-iq-unified-manager-916/config/task_generate_an_https_security_certificate_ocf.html on October 15, 2025. Always check docs.netapp.com for the latest.

Sommario

- Cambiare il nome host di Unified Manager 1
 - Modificare il nome host dell'appliance virtuale Unified Manager 1
 - Genera un certificato di sicurezza HTTPS 2
 - Riavviare la macchina virtuale Unified Manager 4
 - Modificare il nome host di Unified Manager sui sistemi Linux 4

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 **Si** 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
```

Informazioni sul copyright

Copyright © 2025 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 COMMERCIALIZZABILITÀ 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 CONSEGUENZIALE (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.