



Gestione del certificato SSL OnCommand Workflow Automation

OnCommand Workflow Automation 5.1

NetApp
April 19, 2024

This PDF was generated from <https://docs.netapp.com/it-it/workflow-automation/rhel-install/task-replace-the-default-workflow-automation-ssl-certificate-linux.html> on April 19, 2024. Always check docs.netapp.com for the latest.

Sommario

- Gestione del certificato SSL OnCommand Workflow Automation 1
 - Sostituire il certificato SSL predefinito di Workflow Automation 1
 - Creare una richiesta di firma del certificato per Workflow Automation. 2

Gestione del certificato SSL OnCommand Workflow Automation

È possibile sostituire il certificato SSL predefinito di OnCommand Workflow Automation (Wfa) con un certificato autofirmato o firmato da un'autorità di certificazione (CA).

Il certificato SSL WFA autofirmato predefinito viene generato durante l'installazione di WFA. Quando si esegue l'aggiornamento, il certificato per l'installazione precedente viene sostituito con il nuovo certificato. Se si utilizza un certificato autofirmato non predefinito o un certificato firmato da una CA, è necessario sostituire il certificato SSL Wfa predefinito con il certificato.

Sostituire il certificato SSL predefinito di Workflow Automation

È possibile sostituire il certificato SSL predefinito di Workflow Automation (WFA) se il certificato è scaduto o se si desidera aumentare il periodo di validità del certificato.

È necessario disporre dei privilegi di root per il sistema Linux su cui è stato installato WFA.

In questa procedura viene utilizzato il percorso di installazione predefinito di WFA. Se è stata modificata la posizione predefinita durante l'installazione, è necessario utilizzare il percorso di installazione WFA personalizzato.

Fasi

1. Accedere come utente root sul computer host WFA.
2. Al prompt della shell, accedere alla seguente directory sul server WFA: WFA_install_location/wfa/bin
3. Arrestare i servizi del server e del database WFA:

```
./wfa --stop=WFA
```

```
./wfa --stop=DB
```

4. Eliminare il file wfa.keystore dalla seguente posizione:
WFA_install_location/wfa/jboss/standalone/Configuration/keystore.
5. Aprire un prompt della shell sul server WFA e modificare le directory nel percorso seguente:
<OpenJDK_install_location>/bin
6. Ottenere la chiave del database:

```
keytool -keysize 2048 -genkey -alias "ssl keystore" -keyalg RSA -keystore  
"WFA_install_location/wfa/jboss/standalone/configuration/keystore/wfa.keystore"  
-validity xxxx
```

xxxx indica il numero di giorni di validità del nuovo certificato.

7. Quando richiesto, inserire la password (predefinita o nuova).

La password predefinita è una password crittografata generata in modo casuale.

Per ottenere e decrittare la password predefinita, seguire la procedura descritta nell'articolo della

Knowledge base ["Come rinnovare il certificato autofirmato su WFA 5.1.1.0.4"](#)

Per utilizzare una nuova password, seguire la procedura descritta nell'articolo della Knowledge base ["Come aggiornare una nuova password per il keystore in WFA."](#)

8. Inserire i dettagli richiesti per il certificato.
9. Esaminare le informazioni visualizzate, quindi immettere `Yes`.
10. Premere **Invio** quando richiesto dal seguente messaggio: Inserire la password della chiave per <SSL keystore> <RETURN if same as keystore password>.
11. Riavviare i servizi WFA:

```
./wfa --start=DB
```

```
./wfa --start=WFA
```

Creare una richiesta di firma del certificato per Workflow Automation

È possibile creare una richiesta di firma del certificato (CSR) in Linux in modo da poter utilizzare il certificato SSL firmato da un'autorità di certificazione (CA) invece del certificato SSL predefinito per Workflow Automation (Wfa).

- È necessario disporre dei privilegi di root per il sistema Linux su cui è stato installato WFA.
- È necessario sostituire il certificato SSL predefinito fornito da WFA.

In questa procedura viene utilizzato il percorso di installazione predefinito di WFA. Se il percorso predefinito è stato modificato durante l'installazione, è necessario utilizzare il percorso di installazione WFA personalizzato.

Fasi

1. Accedere come utente root sul computer host WFA.
2. Aprire un prompt della shell sul server WFA e modificare le directory nel percorso seguente:
<OpenJDK_install_location>/bin
3. Creare un file CSR:

```
keytool -certreq -keystore  
WFA_install_location/wfa/jboss/standalone/configuration/keystore/wfa.keystore  
-alias "ssl keystore" -file /root/file_name.csr
```

File_name è il nome del file CSR.

4. Quando richiesto, inserire la password (predefinita o nuova).

La password predefinita è una password crittografata generata in modo casuale.

Per ottenere e decrittare la password predefinita, seguire la procedura descritta nell'articolo della Knowledge base ["Come rinnovare il certificato autofirmato su WFA 5.1.1.0.4"](#)

Per utilizzare una nuova password, seguire la procedura descritta nell'articolo della Knowledge base ["Come aggiornare una nuova password per il keystore in WFA."](#)

5. Inviare il file nome_file.csr alla CA per ottenere un certificato firmato.

Per ulteriori informazioni, visitare il sito Web della CA.

6. Scarica un certificato di catena dalla CA, quindi importa il certificato di catena nel keystore:

```
keytool -import -alias "ssl keystore CA certificate" -keystore  
WFA_install_location/wfa/jboss/standalone/configuration/keystore/wfa.keystore"  
-trustcacerts -file chain_cert.cer
```

chain_cert.cer È il file di certificato di catena ricevuto dalla CA. Il file deve essere in formato X.509.

7. Importare il certificato firmato ricevuto dalla CA:

```
keytool -import -alias "ssl keystore" -keystore  
WFA_install_location/wfa/jboss/standalone/configuration/keystore/wfa.keystore"  
-trustcacerts -file certificate.cer
```

certificate.cer È il file di certificato di catena ricevuto dalla CA.

8. Avviare i servizi WFA:

```
./wfa --start=DB
```

```
./wfa --start=WFA
```

Informazioni sul copyright

Copyright © 2024 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.