



# **Verwalten des OnCommand Workflow Automation-SSL-Zertifikats**

OnCommand Workflow Automation 5.1

NetApp  
April 19, 2024

# Inhalt

- Verwalten des OnCommand Workflow Automation-SSL-Zertifikats. . . . . 1
  - Ersetzen Sie das Standard-SSL-Zertifikat der Workflow Automation . . . . . 1
  - Erstellen Sie eine Anfrage zum Signieren eines Zertifikats für Workflow Automation . . . . . 2

# Verwalten des OnCommand Workflow Automation-SSL-Zertifikats

Sie können das WFA OnCommand Workflow Automation SSL-Standardzertifikat durch ein selbstsigniertes Zertifikat oder ein Zertifikat ersetzen, das von einer Zertifizierungsstelle (CA) signiert ist.

Bei der Installation von WFA wird das selbstsignierte WFA SSL-Zertifikat generiert. Wenn Sie ein Upgrade durchführen, wird das Zertifikat für die vorherige Installation durch das neue Zertifikat ersetzt. Wenn Sie ein nicht standardmäßiges selbstsigniertes Zertifikat oder ein von einer CA signiertes Zertifikat verwenden, müssen Sie das Standard-WFA SSL-Zertifikat durch Ihr Zertifikat ersetzen.

## Ersetzen Sie das Standard-SSL-Zertifikat der Workflow Automation

Sie können das Standard-SSL-Zertifikat der Workflow Automation (WFA) ersetzen, wenn das Zertifikat abgelaufen ist oder Sie die Gültigkeitsdauer des Zertifikats erhöhen möchten.

Sie müssen Root-Rechte für das Linux-System besitzen, auf dem WFA installiert ist.

In diesem Verfahren wird der WFA Standardinstallationspfad verwendet. Wenn Sie während der Installation den Standardspeicherort geändert haben, müssen Sie auch den benutzerdefinierten WFA Installationspfad verwenden.

### Schritte

1. Melden Sie sich als Root-Benutzer auf der WFA Host Machine an.
2. Navigieren Sie an der Shell-Eingabeaufforderung zum folgenden Verzeichnis auf dem WFA Server:  
WFA\_install\_location/wfa/bin
3. Stoppen Sie die WFA Datenbank- und Serverdienste:

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

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

4. Löschen Sie die datei wfa.keystore aus dem folgenden Verzeichnis:  
WFA\_install\_location/wfa/jboss/Standalone/Configuration/keystore.
5. Öffnen Sie eine Shell-Eingabeaufforderung auf dem WFA-Server, und ändern Sie dann das Verzeichnis in den folgenden Speicherort: <OpenJDK\_install\_Location>/bin
6. Erhalten Sie den Datenbankschlüssel:

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

Xxxx ist die Anzahl der Tage für die Gültigkeit des neuen Zertifikats.

7. Geben Sie bei der entsprechenden Aufforderung das Kennwort ein (Standard oder neu).

Das Standardpasswort ist ein zufällig generiertes verschlüsseltes Passwort.

Um das Standardpasswort zu erhalten und zu entschlüsseln, befolgen Sie die Schritte im Knowledge Base-Artikel ["Verlängern des selbstsignierten Zertifikats bei WFA 5.1.1.0.4"](#)

Um ein neues Passwort zu verwenden, befolgen Sie die Schritte im Knowledge Base-Artikel ["So aktualisieren Sie ein neues Passwort für den Schlüsselspeicher in WFA."](#)

8. Geben Sie die erforderlichen Details für das Zertifikat ein.
9. Überprüfen Sie die angezeigten Informationen, und geben Sie dann ein `Yes`.
10. Drücken Sie **Enter**, wenn Sie dazu aufgefordert werden: Geben Sie das Schlüsselpasswort für <SSL keystore> <ZURÜCK, wenn das gleiche wie das Schlüsselspeicherkennwort> ein.
11. Starten Sie die WFA Services neu:

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

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

## Erstellen Sie eine Anfrage zum Signieren eines Zertifikats für Workflow Automation

Sie können eine Zertifikatsignierungsanforderung (CSR) in Linux erstellen, sodass Sie das SSL-Zertifikat, das von einer Zertifizierungsstelle (CA) signiert ist, anstelle des Standard-SSL-Zertifikats für Workflow Automation (WFA) verwenden können.

- Sie müssen Root-Rechte für das Linux-System besitzen, auf dem WFA installiert ist.
- Sie müssen das von WFA bereitgestellte Standard-SSL-Zertifikat ersetzt haben.

In diesem Verfahren wird der WFA Standardinstallationspfad verwendet. Wenn Sie während der Installation den Standardpfad geändert haben, müssen Sie den benutzerdefinierten WFA Installationspfad verwenden.

### Schritte

1. Melden Sie sich als Root-Benutzer auf der WFA Host Machine an.
2. Öffnen Sie eine Shell-Eingabeaufforderung auf dem WFA-Server, und ändern Sie dann das Verzeichnis in den folgenden Speicherort: <OpenJDK\_install\_Location>/bin
3. CSR-Datei erstellen:

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

File\_Name ist der Name der CSR-Datei.

4. Geben Sie bei der entsprechenden Aufforderung das Kennwort ein (Standard oder neu).

Das Standardpasswort ist ein zufällig generiertes verschlüsseltes Passwort.

Um das Standardpasswort zu erhalten und zu entschlüsseln, befolgen Sie die Schritte im Knowledge Base-Artikel ["Verlängern des selbstsignierten Zertifikats bei WFA 5.1.1.0.4"](#)

Um ein neues Passwort zu verwenden, befolgen Sie die Schritte im Knowledge Base-Artikel ["So aktualisieren Sie ein neues Passwort für den Schlüsselspeicher in WFA."](#)

5. Senden Sie die Datei file\_Name.csr an die CA, um ein signiertes Zertifikat zu erhalten.

Weitere Informationen finden Sie auf der CA-Website.

6. Laden Sie ein Kettenzertifikat von der CA herunter, und importieren Sie dann das Kettenzertifikat in Ihren Schlüsselspeicher:

```
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 Ist die von der Zertifizierungsstelle empfangene Datei für die Kette. Die Datei muss im X.509-Format vorliegen.

7. Importieren Sie das signierte Zertifikat, das Sie von der CA erhalten haben:

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

certificate.cer Ist die von der Zertifizierungsstelle empfangene Datei für die Kette.

8. Starten Sie die WFA Services:

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

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

## Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

## Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.