Verwalten des OnCommand Workflow Automation-SSL-Zertifikats

OnCommand Workflow Automation 5.1

NetApp
April 19, 2024

Inhalt

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
   ```