Managing OnCommand Workflow Automation SSL certificate

OnCommand Workflow Automation 5.1

NetApp
August 30, 2024

Table of Contents

Managing OnCommand Workflow Automation SSL certificate

You can replace the default OnCommand Workflow Automation (WFA) SSL certificate with a self-signed certificate or a certificate signed by a Certificate Authority (CA).

The default self-signed WFA SSL certificate is generated during the installation of WFA. When you are upgrading, the certificate for the previous installation is replaced with the new certificate. If you are using a non-default self-signed certificate or a certificate signed by a CA, you must replace the default WFA SSL certificate with your certificate.

Replace the default Workflow Automation SSL certificate

You can replace the default Workflow Automation (WFA) SSL certificate if the certificate has expired or if you want to increase the validity period of the certificate.

You must have root privileges for the Linux system on which you have installed WFA.

The default WFA installation path is used in this procedure. If you changed the default location during installation, you must use the custom WFA installation path.

Steps

1. Log in as a root user on the WFA host machine.
2. At the shell prompt, navigate to the following directory on the WFA server: WFA_install_location/wfa/bin
3. Stop the WFA database and server services:

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

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

4. Delete the wfa.keystore file from the following location: WFA_install_location/wfa/jboss/standalone/configuration/keystore.
5. Open a shell prompt on the WFA server, and then change directories to the following location: <OpenJDK_install_location>/bin
6. Obtain the database key:

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

   xxxx is the number of days for the validity of the new certificate.

7. When prompted, provide the password (default or new).

   The default password is a randomly generated encrypted password.

   To obtain and decrypt the default password, follow the steps in the Knowledge Base article How to renew the self-signed certificate on WFA 5.1.1.0.4

To use a new password, follow the steps in the Knowledge Base article How to update a new password for the keystore in WFA.

8. Enter the required details for the certificate.
9. Review the displayed information, and then enter `Yes`.
10. Press **Enter** when prompted by the following message: Enter key password for <SSL keystore> <RETURN if same as keystore password>.
11. Restart the WFA services:

```
./wfa --start=DB

./wfa --start=WFA
```

Create a certificate signing request for Workflow Automation

You can create a certificate signing request (CSR) in Linux so that you can use the SSL certificate that is signed by a Certificate Authority (CA) instead of the default SSL certificate for Workflow Automation (WFA).

- You must have root privileges for the Linux system on which you have installed WFA.
- You must have replaced the default SSL certificate that is provided by WFA.

The default WFA installation path is used in this procedure. If you have changed the default path during installation, then you must use the custom WFA installation path.

Steps

1. Log in as a root user on the WFA host machine.
2. Open a shell prompt on the WFA server, and then change directories to the following location: <OpenJDK_install_location>/bin
3. Create a CSR file:

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

   file_name is the name of the CSR file.

4. When prompted, provide the password (default or new).

   The default password is a randomly generated encrypted password.

   To obtain and decrypt the default password, follow the steps in the Knowledge Base article How to renew the self-signed certificate on WFA 5.1.1.0.4

   To use a new password, follow the steps in the Knowledge Base article How to update a new password for the keystore in WFA.

5. Send the file_name.csr file to the CA to obtain a signed certificate.

See the CA web site for details.

6. Download a chain certificate from the CA, and then import the chain certificate to your 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` is the chain certificate file that is received from the CA. The file must be in the X.509 format.

7. Import the signed certificate that you received from the CA:

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

   `certificate.cer` is the chain certificate file that is received from the CA.

8. Start the WFA services:

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

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

Copyright information

Trademark information