Gestion du certificat SSL OnCommand Workflow Automation

OnCommand Workflow Automation 5.1

NetApp
April 19, 2024

Sommaire

Gestion du certificat SSL OnCommand Workflow Automation

Vous pouvez remplacer le certificat SSL OnCommand Workflow Automation (WFA) par défaut par un certificat auto-signé ou un certificat signé par une autorité de certification (CA).

Le certificat SSL WFA auto-signé par défaut est généré au cours de l'installation de WFA. Lorsque vous effectuez une mise à niveau, le certificat de l'installation précédente est remplacé par le nouveau certificat. Si vous utilisez un certificat auto-signé non par défaut ou un certificat signé par une autorité de certification, vous devez remplacer le certificat SSL WFA par défaut par votre certificat.

Remplacez le certificat SSL par défaut de Workflow Automation

Vous pouvez remplacer le certificat SSL par défaut de Workflow Automation (WFA) si le certificat a expiré ou si vous souhaitez augmenter la période de validité du certificat.

Vous devez disposer de privilèges root pour le système Linux sur lequel vous avez installé WFA.

Le chemin d'installation par défaut de WFA est utilisé dans cette procédure. Si vous avez modifié l'emplacement par défaut lors de l'installation, vous devez utiliser le chemin d'installation personnalisé de WFA.

Étapes

1. Connectez-vous en tant qu'utilisateur root sur la machine hôte WFA.
2. À l'invite du shell, accédez au répertoire suivant sur le serveur WFA : WFA_install_location/wfa/bin
3. Arrêter les services serveur et base de données WFA :

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

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

4. Supprimez le fichier wfa.keystore à l'emplacement suivant : WFA_install_location/wfa/jboss/autonome/configuration/keystore.
5. Ouvrez une invite de shell sur le serveur WFA, puis modifiez les répertoires à l'emplacement suivant : <OpenJDK_install_location>/bin
6. Obtenez la clé de base de données :

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

   xxxx correspond au nombre de jours de validité du nouveau certificat.

7. Lorsque vous y êtes invité, indiquez le mot de passe (par défaut ou nouveau).

   Le mot de passe par défaut est un mot de passe chiffré généré de manière aléatoire.

Pour obtenir et décrypter le mot de passe par défaut, suivez les étapes de l'article de la base de connaissances "Comment renouveler le certificat auto-signé sur WFA 5.1.1.0.4"

Pour utiliser un nouveau mot de passe, suivez les étapes de l'article de la base de connaissances "Comment mettre à jour un nouveau mot de passe pour le magasin de clés dans WFA."

8. Entrez les détails requis pour le certificat.
9. Vérifiez les informations affichées, puis entrez `Yes`.
10. Appuyez sur **entrée** lorsque le message suivant s'affiche : saisissez le mot de passe de la clé pour <magasin de clés SSL> <RETURN si le mot de passe du magasin de clés est identique à celui du magasin de clés>.
11. Redémarrez les services WFA:

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

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

Créer une demande de signature de certificat pour Workflow Automation

Vous pouvez créer une demande de signature de certificat (CSR) dans Linux de sorte que vous puissiez utiliser le certificat SSL signé par une autorité de certification (CA) au lieu du certificat SSL par défaut pour Workflow Automation (WFA).

- Vous devez disposer de privilèges root pour le système Linux sur lequel vous avez installé WFA.
- Vous devez avoir remplacé le certificat SSL par défaut fourni par WFA.

Le chemin d'installation par défaut de WFA est utilisé dans cette procédure. Si vous avez modifié le chemin par défaut lors de l'installation, vous devez utiliser le chemin d'installation personnalisé de WFA.

Étapes

1. Connectez-vous en tant qu'utilisateur root sur la machine hôte WFA.
2. Ouvrez une invite de shell sur le serveur WFA, puis modifiez les répertoires à l'emplacement suivant : <OpenJDK_install_location>/bin
3. Créer un fichier CSR :

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

    Nom_fichier est le nom du fichier CSR.

4. Lorsque vous y êtes invité, indiquez le mot de passe (par défaut ou nouveau).

    Le mot de passe par défaut est un mot de passe chiffré généré de manière aléatoire.

    Pour obtenir et décrypter le mot de passe par défaut, suivez les étapes de l'article de la base de connaissances "Comment renouveler le certificat auto-signé sur WFA 5.1.1.0.4"

Pour utiliser un nouveau mot de passe, suivez les étapes de l'article de la base de connaissances "Comment mettre à jour un nouveau mot de passe pour le magasin de clés dans WFA."

5. Envoyez le fichier file_name.csr à l'autorité de certification pour obtenir un certificat signé.

   Consultez le site Web de l'AC pour plus de détails.

6. Téléchargez un certificat de chaîne à partir de l'autorité de certification, puis importez le certificat de chaîne dans votre magasin de clés :

   ```
   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` Est le fichier de certificat de chaîne reçu de l'autorité de certification. Le fichier doit être au format X.509.

7. Importez le certificat signé que vous avez reçu de l'autorité de certification :

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

   `certificate.cer` Est le fichier de certificat de chaîne reçu de l'autorité de certification.

8. Démarrer les services WFA :

   ```
   ./wfa --start=DB

   ./wfa --start=WFA
   ```