OnCommand Workflow Automation SSL 証明書の管理

OnCommand Workflow Automation 5.1

NetApp
April 19, 2024

目次

OnCommand Workflow Automation SSL 証明書の管理 1
Workflow Automation のデフォルトの SSL 証明書を置き換えます 1
Workflow Automation の証明書署名要求を作成します 2

OnCommand Workflow Automation SSL 証明書の管理

デフォルトの OnCommand Workflow Automation （ WFA ） SSL 証明書を自己署名証明書または認証局（ CA ）が署名した証明書に置き換えることができます。

デフォルトの自己署名 WFA SSL 証明書は WFA のインストール時に生成されます。アップグレードすると、以前のインストールの証明書が新しい証明書に置き換えられます。デフォルト以外の自己署名証明書または CA によって署名された証明書を使用している場合は、デフォルトの WFA SSL 証明書を証明書に置き換える必要があります。

Workflow Automation のデフォルトの SSL 証明書を置き換えます

証明書の有効期限が切れている場合や証明書の有効期間を延長する場合は、 Workflow Automation （ WFA ）のデフォルトの SSL 証明書を置き換えることができます。

WFA をインストールした Linux システムに対する root 権限が必要です。

WFA のデフォルトのインストールパスは、この手順 で使用されます。インストール時にデフォルトの場所を変更した場合は、カスタムの WFA インストールパスを使用する必要があります。

手順

1. WFA ホストマシンに root ユーザとしてログインします。
2. シェルプロンプトで、 WFA サーバの次のディレクトリに移動します。 wfa_install_location /wfa/bin
3. WFA データベースと WFA サーバのサービスを停止します。

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

   ```
   ./wfa－stop=DB
   ```

4. wfa_install_location /wfa/jboss/standalone/configuration/keystore にある wfa_keystore ファイルを削除します。
5. WFA サーバでシェルプロンプトを開き、 <OpenJDK のインストール先 >/bin にディレクトリを変更します
6. データベースキーを取得します。

   keytool -keysize 2048 -genkey -alias "ssl keystore" -keyalg RSA -keystore "wfa_install_location /wfa/standalone/configuration /keystore.keystore" -dValidity xxxx`

   xxxx は、新しい証明書の有効期間を示す日数です。

7. プロンプトが表示されたら、パスワードを入力します（デフォルトまたは新規）。

   デフォルトのパスワードは、ランダムに生成された暗号化パスワードです。

   デフォルトのパスワードを取得して復号化するには、ナレッジベースの記事の手順に従います "WFA

5.1.1.0.4の自己署名証明書を更新する方法"

新しいパスワードを使用するには、Knowledge Base記事の手順に従います "WFAでキーストアの新しいパスワードを更新する方法"

8. 証明書に必要な詳細情報を入力します。
9. 表示された情報を確認し、「 Yes 」と入力します。
10. 次のメッセージが表示されたら、 * Enter * を押します。 Enter key password for <SSL keystore><return if same as keystore password>
11. WFA のサービスを再起動します。

    ```
    ./wfa－start=db
    ```

    `./wfa — start=wfa

Workflow Automation の証明書署名要求を作成します

Linux で証明書署名要求（ CSR ）を作成すると、 Workflow Automation （ WFA ）のデフォルトの SSL 証明書ではなく、認証局（ CA ）が署名した SSL 証明書を使用できるようになります。

- WFA をインストールした Linux システムに対する root 権限が必要です。
- WFA のデフォルトの SSL 証明書を置き換えておく必要があります。

WFA のデフォルトのインストールパスは、この手順 で使用されます。インストール時にデフォルトパスを変更した場合は、カスタムの WFA インストールパスを使用する必要があります。

手順

1. WFA ホストマシンに root ユーザとしてログインします。
2. WFA サーバでシェルプロンプトを開き、 <OpenJDK のインストール先 >/bin にディレクトリを変更します
3. CSR ファイルを作成します。

    keytool -certreq -keystore wfa_install_location WFA/jboss/standalone/configuration /keystore/wfa_keystore -alias "ssl keystore" -file /root/file_name .csr`

    file_name は CSR ファイル名です。

4. プロンプトが表示されたら、パスワードを入力します（デフォルトまたは新規）。

    デフォルトのパスワードは、ランダムに生成された暗号化パスワードです。

    デフォルトのパスワードを取得して復号化するには、ナレッジベースの記事の手順に従います "WFA 5.1.1.0.4の自己署名証明書を更新する方法"

    新しいパスワードを使用するには、Knowledge Base記事の手順に従います "WFAでキーストアの新しいパスワードを更新する方法"

5. file_name .CSR ファイルを CA に送信して署名済み証明書を取得します。

   詳細については、 CA の Web サイトを参照してください。

6. CA からチェーン証明書をダウンロードし、チェーン証明書をキーストアにインポートします。

   keytool -import -alias "ssl keystore wfa_install_location /wfa/standalone/configuration /keystore.keystore"-trustcacerts -file chain_cert.cer

   「chain_cert.cer」は、CAから受信したチェーン証明書ファイルです。ファイルは X.509 形式である必要があります。

7. CA から受け取った署名済み証明書をインポートします。

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

   「certificate.cer」は、CAから受信したチェーン証明書ファイルです。

8. WFA のサービスを開始します。

   ```
   ./wfa－start=db
   ```

   `./wfa — start=wfa