OnCommand Workflow Automation SSL 証明書の管理

OnCommand Workflow Automation

NetApp
October 09, 2025

This PDF was generated from https://docs.netapp.com/ja-jp/workflow-automation/rhel-install/task-replace-the-default-workflow-automation-ssl-certificate-linux.html on October 09, 2025. Always check docs.netapp.com for the latest.

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`

著作権に関する情報

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、http://www.netapp.com/TMに記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。