管理 OnCommand Workflow Automation SSL 证书

OnCommand Workflow Automation 5.0

NetApp
April 19, 2024

目录

管理 OnCommand Workflow Automation SSL 证书

您可以将默认 OnCommand Workflow Automation （ WFA ） SSL 证书替换为自签名证书或由证书颁发机构（ CA ）签名的证书。

默认的自签名 WFA SSL 证书是在 WFA 安装期间生成的。升级时，先前安装的证书将替换为新证书。如果您使用的是非默认自签名证书或由 CA 签名的证书，则必须将默认 WFA SSL 证书替换为您的证书。

替换默认的 Workflow Automation SSL 证书

如果证书已过期或要延长证书的有效期，则可以替换默认的 Workflow Automation （ WFA ） SSL 证书。

您需要的内容

您必须对安装了 WFA 的 Linux 系统具有 root 权限。

关于此任务

此操作步骤 将使用默认 WFA 安装路径。如果您在安装期间更改了默认位置，则必须使用自定义 WFA 安装路径。

步骤

1. 以 root 用户身份登录到 WFA 主机。
2. 在 Shell 提示符处，导航到 WFA 服务器上的以下目录：

   ```
   wfa_install_location/wfa/bin
   ```

3. 停止 WFA 数据库和服务器服务：

   ` 。 /WFA -stop=WFA`

   ` 。 /WFA -stop=DB`

4. 从以下位置删除 `wfa.keystore` 文件： `wfa_install_location/wfa/jboss/standalone` 或 `configuration/keystore` 。
5. 在 WFA 服务器上打开 Shell 提示符，然后将目录更改为以下位置：

   ```
   wfa_install_location/wfa/jre/bin
   ```

6. 获取数据库密钥：

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

   `xxxx` 是新证书有效期的天数。

7. 出现提示时，请提供密码（默认密码或新密码）。

   默认密码为 `changeit` 。如果不想使用默认密码，则必须从以下位置更改 `standalis-full.xml` 文件中 SSL 元素的密码属性： `WFA_INSTALL_location/WFA/jboss/standalon/configuration`

   - 示例 *

```
<ssl name="ssl" password="new_password" certificate-key-
file="${jboss.server.config.dir}/keystore/wfa.keystore"
```

8. 输入证书的所需详细信息。
9. 查看显示的信息，然后输入 是 。
10. 出现以下消息时按 * 输入 * ： 输入 `<ssl keystore>` 的密钥密码 `<` 如果与密钥库密码相同，则返回 `>` 。
11. 重新启动 WFA 服务：

    ` 。 /WFA -start=DB`

    ` 。 /WFA -start=WFA`

为 Workflow Automation 创建证书签名请求

您可以在 Linux 中创建证书签名请求（ CSR ），以便使用由证书颁发机构（ CA ）签名的 SSL 证书，而不是 Workflow Automation （ WFA ）的默认 SSL 证书。

您需要的内容

- 您必须对安装了 WFA 的 Linux 系统具有 root 权限。
- 您必须已替换 WFA 提供的默认 SSL 证书。

关于此任务

此操作步骤 将使用默认 WFA 安装路径。如果在安装期间更改了默认路径，则必须使用自定义 WFA 安装路径。

步骤

1. 以 root 用户身份登录到 WFA 主机。
2. 在 WFA 服务器上打开 Shell 提示符，然后将目录更改为以下位置：

   ```
   wfa_install_location/wfa/jre/bin
   ```

3. 创建 CSR 文件：

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

   file_name 是 CSR 文件的名称。

4. 出现提示时，请提供密码（默认密码或新密码）。

   默认密码为 * 更改 IT* 。如果您不想使用默认密码，则必须从 `WFA_INSTALL_location/WFA/jboss/standalon/configuration` 位置更改 `standalone full.xml` 文件中 SSL 元素的密码属性。

   - 示例 *

```
<ssl name="ssl" password="new_password" certificate-key-
file="${jboss.server.config.dir}/keystore/wfa.keystore"
```

5. 将 _file_name.csr 文件发送到 CA 以获取签名证书。

   有关详细信息，请参见 CA 网站。

6. 从 CA 下载链证书，然后将链证书导入到密钥库：

   `keytool -import -alias "ssl keystore CA certificate" -keystore wfa_install_location/wfa/jboss/standalstandal/configuration/keystore/wfa.keystore" -trustcacers -file C ： \chain_cert.cer`

   `C ： \chain_cert.cer` 是从 CA 收到的链证书文件。此文件必须采用 X.509 格式。

7. 导入从 CA 收到的签名证书： `keytool -import -alias "ssl keystore" -keystore wfa_install_location/wfa/jboss/standalstandal/configuration/keystore/wfa.keystore" -trustcacers -file C ： \certificate.cer`

   `C ： \certification.cer` 是从 CA 收到的链证书文件。

8. 启动 WFA 服务：

   ` 。 /WFA -start=DB`

   ` 。 /WFA -start=WFA`