HTTPS Certificate Rotation

Alex Clemons - 2022-04-21 - Comments (0) - Autoform DM FAQs

The process for rotating your expired, expiring or temporary certificate for both standalone and clustered servers is detailed below:

Pre-requisites

- A PFX Keystore containing a new, valid certificate and private key along with the alias and password for the Keystore.

Installation

The process of rotating your HTTPS certificate is straightforward and should not take more than a few minutes. As noted in the pre-requisites you will need your new Keystore and access to the node.properties file for your server installation. This Keystore should contain both the new certificate and the private key and can be either in JKS format or PFX format (typically a certificate exported from a Windows environment will be in PFX format).

For standalone and clustered installations, both the Keystore and node.properties are located alongside each other.

With a clustered installation, the certificate rotation must be carried out on the load balancer.

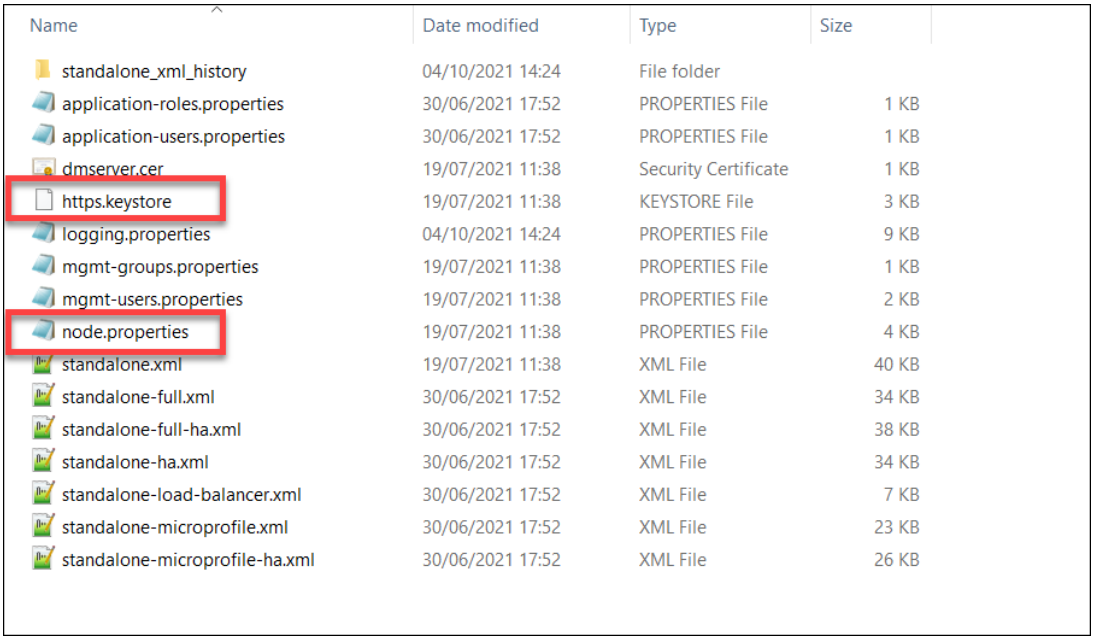
Example:

Standalone Installation

```
C:\Program Files\Formpipe Software\Autoform DM\Server_10.0\wildfly-x.x.x.Final\standalone\configuration\
```

Cluster Installation (Load Balancer Path)

`C:\Program Files\Formpipe Software\Autoform DM\Server_10 - Cluster_<cluster name> - **Role_LB** - <node name>\wildfly-x.x.x.Final\domain\configuration\`



Keystore

Autoform DM is set to look for a Keystore called `https.keystore` in the above folder. To carry out the rotation, follow these steps:

1. Rename the existing (old) file (`https.expired`).

2. Locate your new Keystore and copy it into the appropriate directory, depending on your installation type.

3. Rename your new certificate to `https.keystore`.

node.properties

Once you have copied and renamed your Keystore, you need to update the existing Keystore alias and password to match those to your new Keystore. These credentials are stored in the `node.properties` file which is located in the same directory.

1. Open the file with a txt editor and update the values for `https.keystore.alias=` and `https.keystore.password=` (see example below):

These values should be updated if switching to use your own certificates/keystore from an auto-generated one.

Example:

https.keystore.alias=examplealias

https.keystore.password=Securepassword

2. Save your file, then restart the Autoform DM service for the changes to take effect.

For a clustered deployment, you only need to restart the Load Balancer service.

Your new certificate should now be active for your standalone / clustered deployment.

[Optional] Validate Keystore

If you have forgotten your Keystore alias or if you want to validate the Keystore, then use the command below which will prompt for your password:

```
\jdk-11.0.4_11\bin\keytool.exe -list -keystore \path\to\keystore
```

This will list the alias for the certificate and verify the Keystore format. The listed certificate entry should be of type `PrivateKeyEntry`.