How to configure secure https connection to Matroos

Background

The MATROOS web service from the Dutch Rijkswaterstaat changes to a secure SSL connection. That means that the address in the url changes from http://matroos.rws.nl to https://matroos.rws.nl.

This article describes how you can configure FEWS to use the https method. This applies to any import from Matroos, so for importypes like noos_timeseries.

Why?

Delft-FEWS is based on JAVA and JAVA does not have by default the PKI Overheid certificate in it's distribution. Unlike popular browsers like Firefox, Chrome or IE. Therefore the PKI Overheid certificate should be made known to JAVA using the below approach.

Be aware: in May 2018, the Matroos server required the StaatDerNederlanden-Root-GA3 certificate, while LMW-SIP and AQUALARM required the StaatDerNederlanden-Root-GA2 certificate.

Step-by-step guide

1. Change the URL in the import config files from
   <serverUrl>http://matroos.rws.nl/direct</serverUrl>
   to
   <serverUrl>https://matroos.rws.nl/direct</serverUrl>

2. Add the attached file client.truststore to the root of your region folder. Note that this file has been generated as a combination of the Staat der Nederlanden - RootGA3 and RootGA2 certificates, due to expire in 2028.

   In case you have already an existing truststore, the certificate StaatderNederlandenRootCA-G3.cer should be added for Matroos (or StaatderNederlandenRootCA-G2.crt for LMW-SIP) to that existing file. Attached generate_certificate.cmd provides an example script.

3. Note that you have a FEWS version 2014.01 or higher (or patch) with at least build number 57691 in case you use only a client.truststore. Older versions need a set of both client.keystore and client.truststore. Alternative is to add just a dummy client.keystore.

4. In case you have still a FEWS version with Java 7, you need to ensure that Java uses the correct TLS protocol v1.2. This is already correct in Java 8. To use TLSv1.2 with Java 7, you should define the next argument in the mc proxy conf or jpif/ini file: -Dhttps.protocols=TLSv1.2

MC Proxy Configuration

On a FSS the client truststore should be configured in the fews.master.mcproxy.conf explicitly by passing the -Djavax.net.ssl.trustStore parameter in the jvm section of the master.conf. An example configuration looks as follows:

```
<jvm path="D:\fews\jre-8u73\bin\java">
        <arg id="0" value="-Xmx1536M"/>
        <arg id="1" value="-Djava.library.path=D:/fews/fss/nlknmc00/FSS00/FewsShell/bin"/>
        <arg id="2" value="-Djava.awt.headless=true"/>
        <arg id="3" value="-Djavax.net.ssl.trustStore=D:\fews\fss\truststores\rws.truststore"/>
</jvm>
```

Related articles

See also the general information on the generation of client truststores at

https://publicwiki.deltares.nl/display/FEWSDOC/Import+data+using+OPeNDAP#ImportdatausingOPeNDAP-ImportdatafromaserverthatusesSSL

ClientConfig XML File for Operator Client and Forecasting Shell Servers - 2018.02 - 2021.01
#08RootConfigurationFilesforOperatorClientandForecastingShellServers-truststore

Here is described how you can generate your own client truststore file, for example using a private password.

- How to Import data
- How to configure secure https connection to Matroos