How to Reset SSL Certificates in an Upgraded 7.5.0 Domain Back to Using the SSL Certificates From an Old Version Domain

How to Reset SSL Certificates in an Upgraded 7.5.0 Domain Back to Using the SSL Certificates From an Old Version Domain

Overview

In 7.5.0, we always regenerate the SSL certificates used for management traffic between Node Managers and API Gateways. This is safer during upgrade, as it means that the old and new version Node Managers cannot mistakenly communicate with each other. This section describes the manual steps that may be carried out after a successful upgrade to get the newly upgraded 7.5.0 domain to use the certificates from an old installation. In most cases this will not be a required as the new certificates generated during sysupgrade may be used. Some customers may wish to revert to using the old version certificates if they are custom certificates. **Note that it is not possible to revert back to using certificates from an old version if the old version is older than 7.3.0.**

Previously, SSL certificates were only regenerated at upgrade time when upgrading from versions older than 7.3.0, and upgrades of newer versions reused the old version system SSL certificates in the new version system.

The following steps give an overview of the procedure to reset the SSL certificates to use the certificates from an old version system in a newly upgraded 7.5.0 system. Follow the more detailed examples below when performing the steps.

- On the main Admin Node Manager node:
    - Using the old version Policy Studio edit the old version Node Manager entity store configuration.
        - Export the Domain CA certificate to a PEM file.
        - Export the Node Manager "topology-cert” certificate and key to a P12 file.
    - Using the 7.5.0 Policy Studio create a project using the "From existing configuration” option. Point the project at the 7.5.0 Admin Node Manager configuration.
        - Edit the "Management HTTPS Interface”. Remove references to the "topology-cert” certificate and the "CN=Domain” CA certificate from the listener. These certificates are the new certificates generated via sysupgrade that we no longer wish to use if we are reverting to the certificates from the old version.
        - Remove the "topology-cert”.
        - Remove the "CN=Domain” CA certificate.
        - Import the exported Domain CA certificate from the PEM file created using the old version Policy Studio.

        - Import the exported "topology-cert" from the P12 file created using the old version Policy Studio.
        - Set the Issuer on the imported "topology-cert" to the Domain CA.
        - If there is a duplicate Node Manager certificate, Remove it.
        - Edit the "Management HTTPS Interface", point it at the imported "topology-cert" and the imported Domain CA certificate.
        - Copy the project contents to the `~/7.5.0/apigateway/conf/fed` directory.
        - Restart the Admin Node Manager
    - For each API Gateway instance on the current node, edit the `mgmt.xml` to contain the correct Domain CA dname.
    - For each API Gateway instance on the main Admin Node Manager host, copy the certs.xml from the old version to the 7.5.0 install, e.g. `cp ~/7.3.1/apigateway/group-2/instance-1/conf/certs.xml ~/7.5.0/apigateway/group-2/instance-1/conf/certs.xml`.
    - Restart each API Gateway instance.
    - Check out https://anm-host:8090. The API Gateway instances on the main Admin Node Manager host should have a live status. The Admin Node Manager will not be able to communicate with other nodes in the domain yet. There will be SSL errors in the Admin Node Manager trace file at this point.
    - If the old version used system generated SSL certificates then copy the `apigateway/groups/certs` directory from the old version installation into the new version installation. This will ensure that new API Gateways added to the 7.5.0 topology in future are signed using the same Domain CA key.
- On each subsequent node in the domain, do the following:-
    - Using the old version Policy Studio, edit the old version Node Manager entity store configuration for that node.
        - Export the Node Manager "topology-cert" certificate and key to a P12 file.
        - (No need to export the Domain CA certificate again).
    - Use the 7.5.0 Policy Studio as above, but point it at the current node's Node Manager configuration.
        - Edit the "Management HTTPS Interface" as above.
        - Import the exported Domain CA certificate as above.
        - Import the exported "topology-cert" for this node as above.
        - Set the Issuer on the imported "topology-cert" as above.
        - If there is a duplicate Node Manager certificate, Remove it.
        - Edit the "Management HTTPS Interface", to use imported certificates as above.
        - Copy the project contents to the `~/7.5.0/apigateway/conf/fed` directory.
        - Restart the Node Manager on the current node.
    - For each API Gateway instance on the current node, edit the `mgmt.xml` to contain the correct Domain CA dname.
    - For each API Gateway instance on the current node, copy the certs.xml from the old version to the 7.5.0 install, e.g. `cp ~/7.3.1/apigateway/group-`

`2/instance-1/conf/certs.xml ~/7.5.0/apigateway/group-2/instance-1/conf/certs.xml`.

- Restart each API Gateway instance.
- There is no need to copy the `apigateway/groups/certs` directory on subsequent nodes.
- Check out https://anm-host:8090, all API Gateways running on this node should have a live status.

The following sections give more concrete examples of the procedure to revert the SSL certificates, for a single node 7.3.1 system, and a multi-node 7.3.1 system.

Example 7.3.1 -> 7.5.0 Single Node Upgrade

Create 7.3.1 Single Node System

If an API Gateway domain is using the default SSL management certificate option, (i.e. system generated keys and certificates), the default dname for the Domain CA certificate is `CN=Domain`. Create a 7.3.1 single node system with a single API Gateway instance with a non-default dname for the Domain CA certificate so that we can see more clearly when we are using the old version certificates, Vs the new default certificates in the 7.5.0 upgraded installation. This is not a requirement, i.e. the Domain CA certificate dname may be the same in the old and new version installations if required. For the purposes of this guide, the dname of the Domain CA in the 7.3.1 domain is `CN=7.3.1-Domain`. After upgrade, the dname of the Domain CA in the 7.5.0 domain will always be `CN=Domain`, there is no way to change during sysupgrade. It may be changed post upgrade via a complete regeneration of all SSL certificates, certificate regeneation is not covered here.

Create a 7.3.1 Node Manager using a non-default Domain CA dname as follows:-

```
cd 7.3.1-install-dir/posix/bin
./managedomain -i --domain_name 7.3.1-Domain
```

Start the Node Manager.

Create an API Gateway instance.

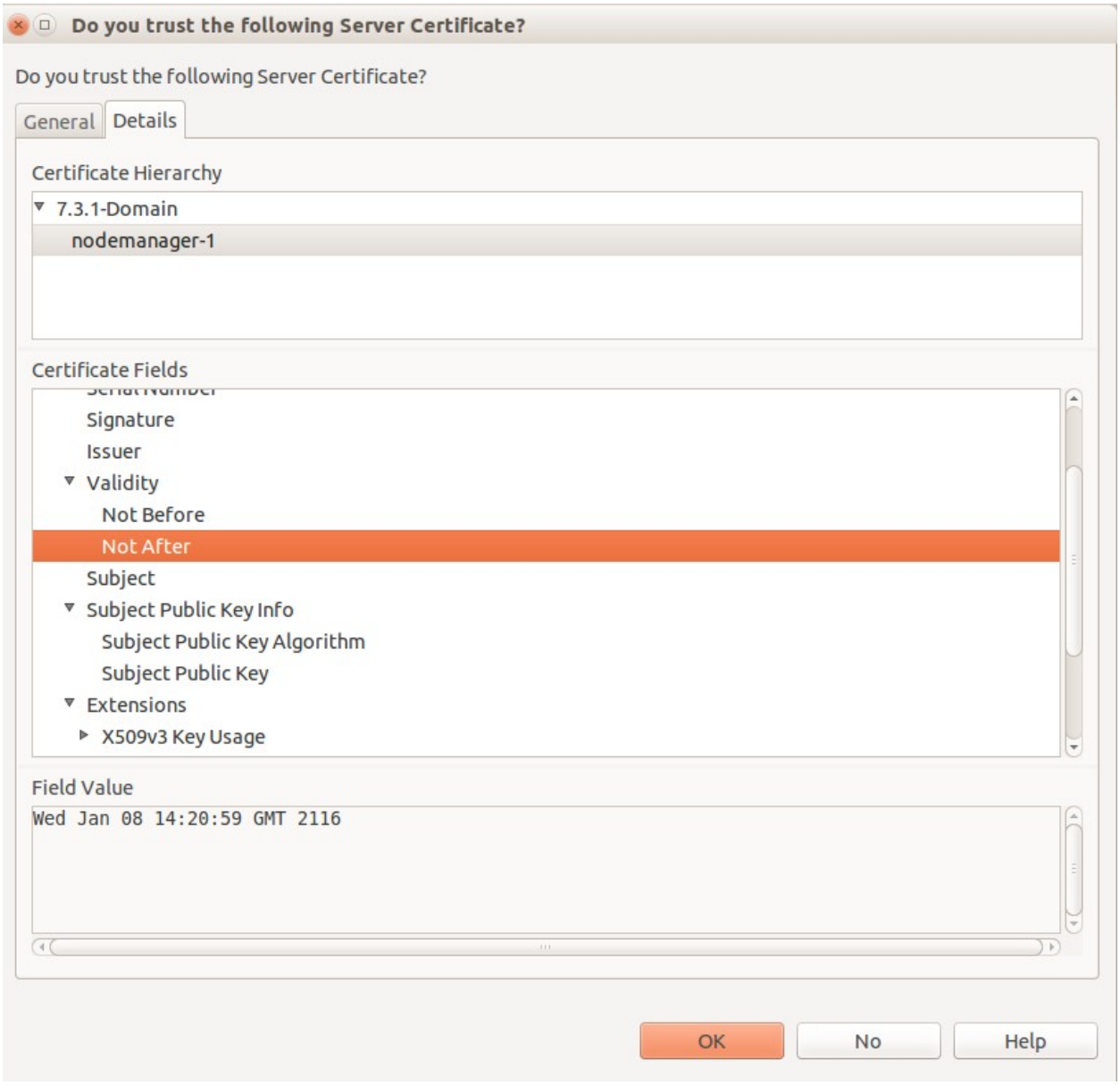
```
./managedomain -c -n APIGateway1 -g Group1
```

Start API Gateway instance.

If upgrading a pre-existing old version with a default Domain CA dname, use the validity times to determine whether you are viewing the old version certificate, or the new version certificate generated during sysupgrade.

View the 7.3.1 Admin Node Manager Certificate

This is an optional step. Start **7.3.1 Policy Studio** and view the certificate details when connecting to the Admin Node Manager.



Note the CN of the certificate that signs the Node Manager certificate is set to "7.3.1-Domain".

Run Sysupgrade

Run sysupgrade in 7.5.0 installation, pointing it at the 7.3.1 installation and follow normal procedure, bringing down the old version processes when prompted.

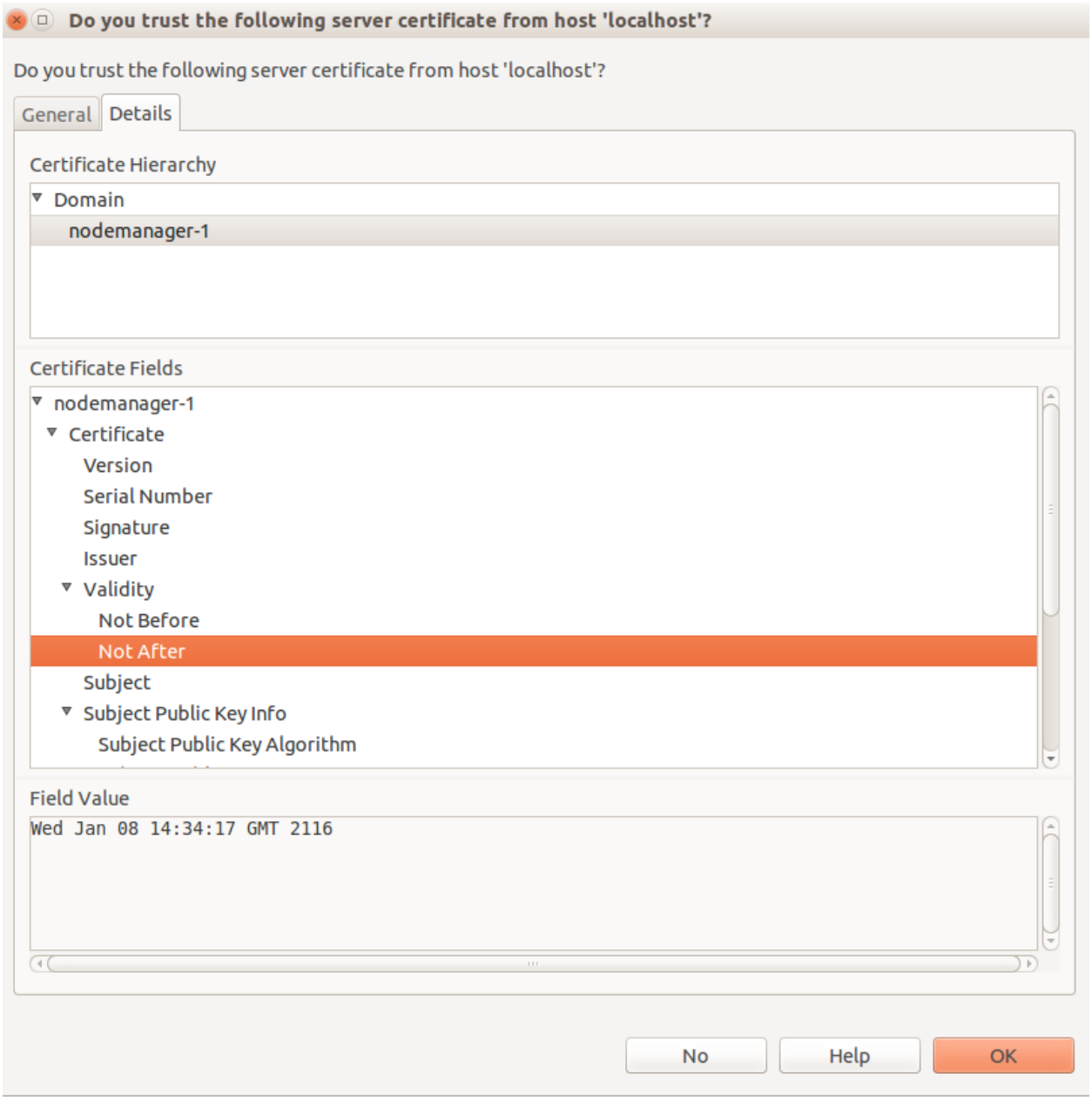
```
cd 7.5.0-install-dir/apigateway/upgrade/bin
./sysupgrade /home/mcollins/AxwayInstalls/GOLD/7.3.1/apigateway
```

When sysupgrade completes, we should now have a 7.5.0 Admin Node Manager and API Gateway running.

Verify that the domain looks OK in the API Gateway Manager UI, i.e. https://localhost:8090.

View the 7.5.0 Admin Node Manager Certificate

This is an optional step. Start the 7.5.0 Policy Studio.
Click "New Project from an API Gateway instance”.

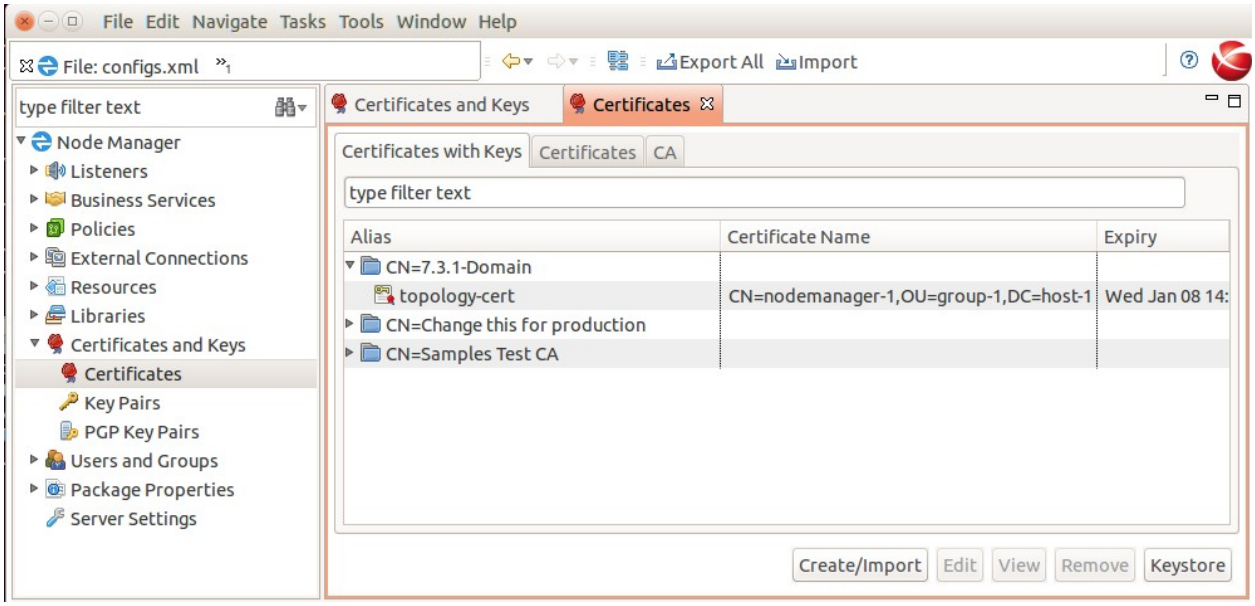


We see that a different Validity period and the CN of the Domain CA certificate is "Domain" as opposed to "7.3.1-Domain". We will now start to revert the SSL certificates for the 7.5.0 installation back to those used in the 7.3.1 domain.

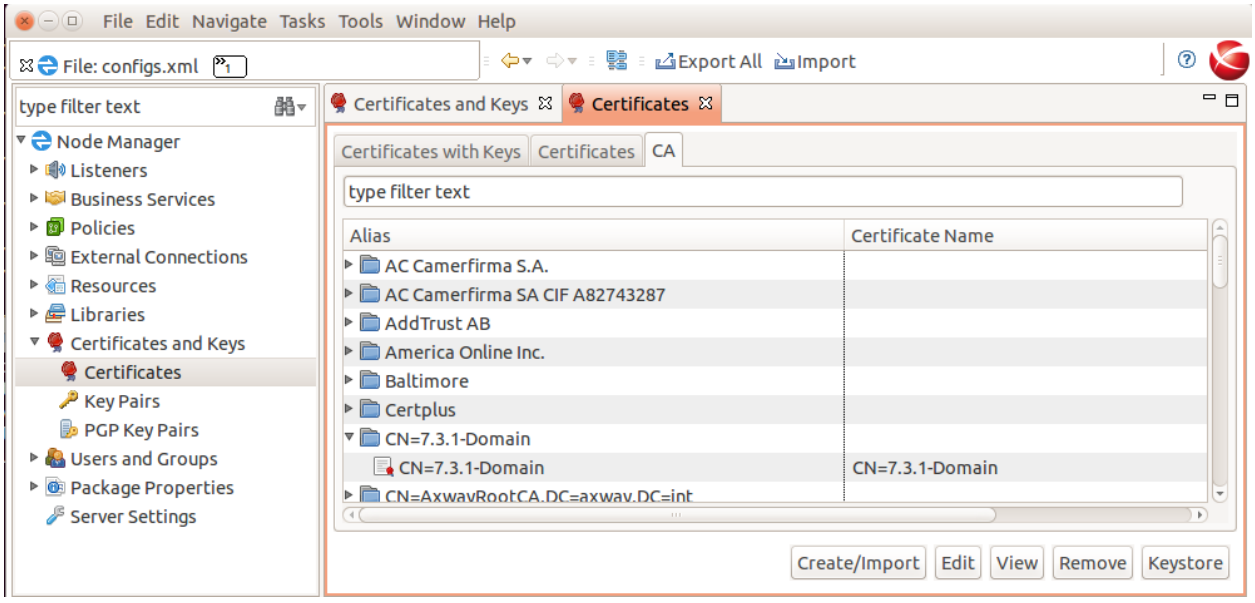
Extract the 7.3.1 Certificate Details for the Domain CA and the Admin Node Manager

Use the **7.3.1 Policy Studio**.

Choose the "Open File" option and point at the `7.3.1-install-dir/apigateway/conf/fed/configs.xml` file.
Browse to "Certificates and Keys".



Under the "Certificates with Key" tab, find the "topology-cert", click "Edit"
Then click "Export Certificate and Key" and save the key and cert to a file on disk, e.g. `7.3.1.p12`.



Under the "CA" tab, find the Domain CA certificate with alias "CN=7.3.1-Domain", click "Edit".

Then click "Export Certificate" and save the certificate to a file on disk, e.g. `7.3.1-domain-cert.pem`.

Close 7.3.1 Policy Studio.

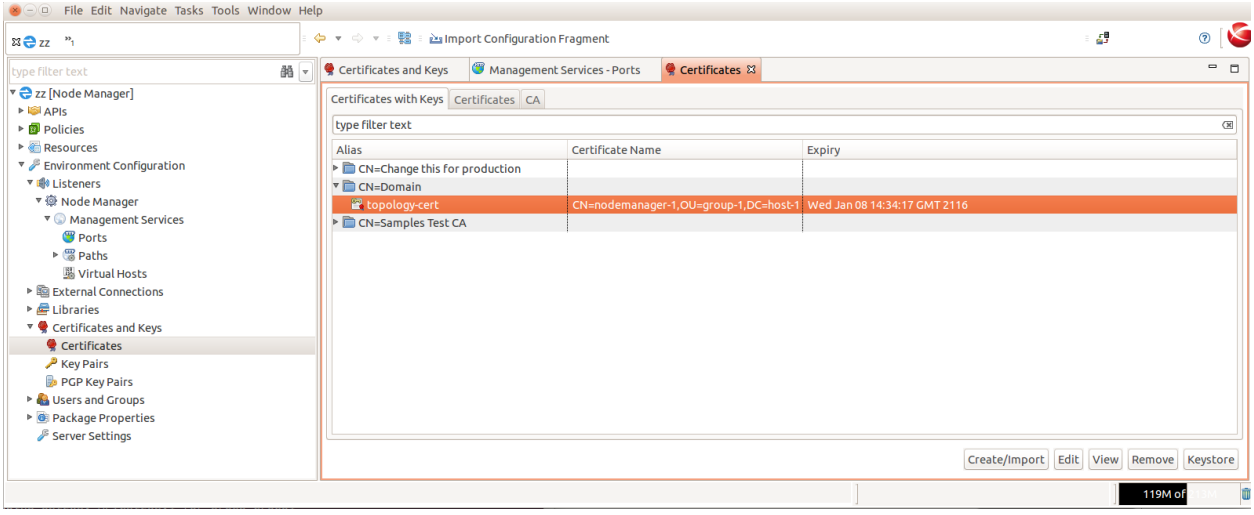
Revert the SSL Certificate for the 7.5.0 Admin Node Manager

Run **7.5.0 Policy Studio**.

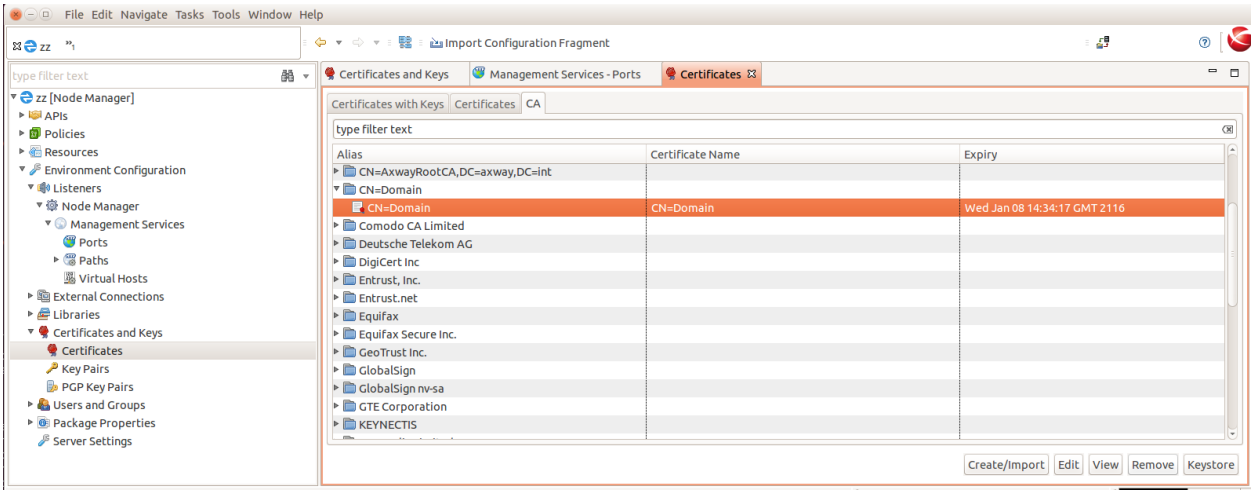
Create a new project based on the 7.5.0 Node Manager configuration, use the "From existing configuration" option and point at the `7.5.0-install-dir/apigateway/conf/fed` directory.

Browse to "Listeners/Node Manager/Management Services/Ports" and edit the "Management HTTPS Interface".
Update it temporarily so that it does not use the "topology-cert" certificate on the "Network" tab, select any other certificate.
Click on the "Mutual Authentication" tab and ensure that the "CN=Domain" certificate is not selected as a trusted certificate.
Click OK.

Browse to "Certificates and Keys".
On the "Certificates with Keys" tab, find the "topology-cert". Select it and click "Remove".



Under the "CA" tab, find the Domain CA key, ie. "CN=Domain", that signed the "topology-cert", select it and click "Remove".



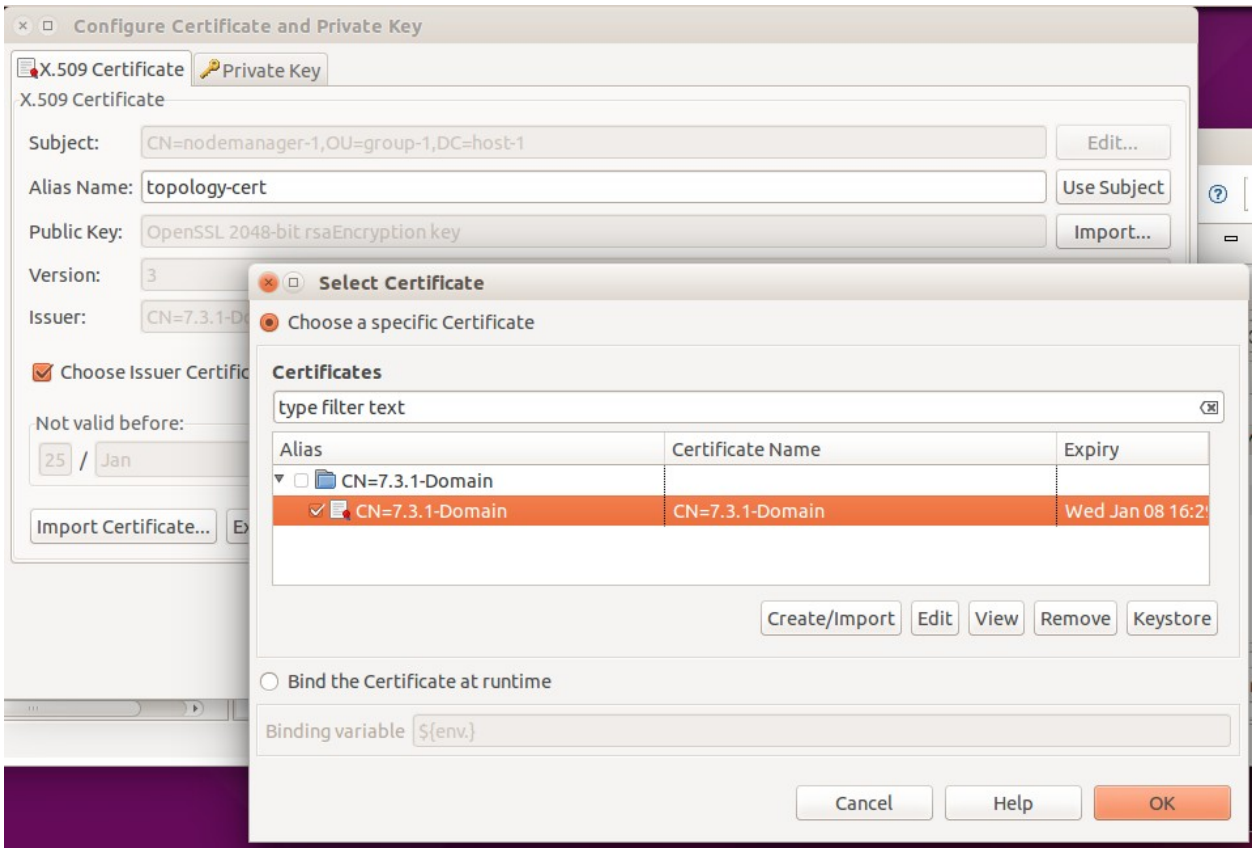
Under the "CA" tab, you will also find the "CN=7.3.1-Domain" certificate. This remains in the Node Manager configuration after upgrade. Remove this also.

Click "Create/Import".
Click "Import Certificate". Select the domain CA certificate file, e.g. `7.3.1-domain-cert.pem`.
Select "Use Subject" for alias.
Click OK.

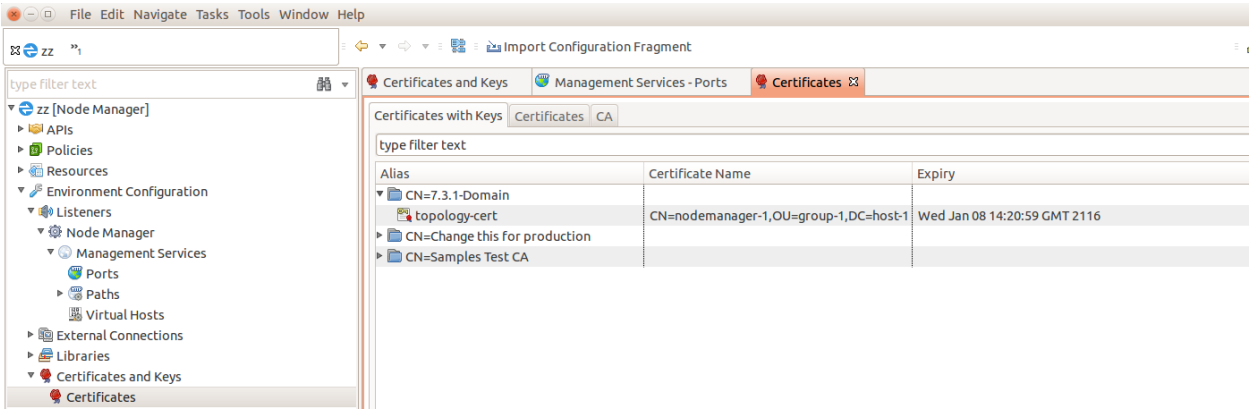
Click "Create/Import" again.
Click "Import Certificate + Key". Select the p12 file exported from 7.3.1, e.g. `7.3.1.p12`.
Enter "topology-cert" as the "Alias Name".
Click OK.

Select the "Certificates" tab, select the CN=nodemanager-1, OU=group-1..." certificate.
Click "Remove".

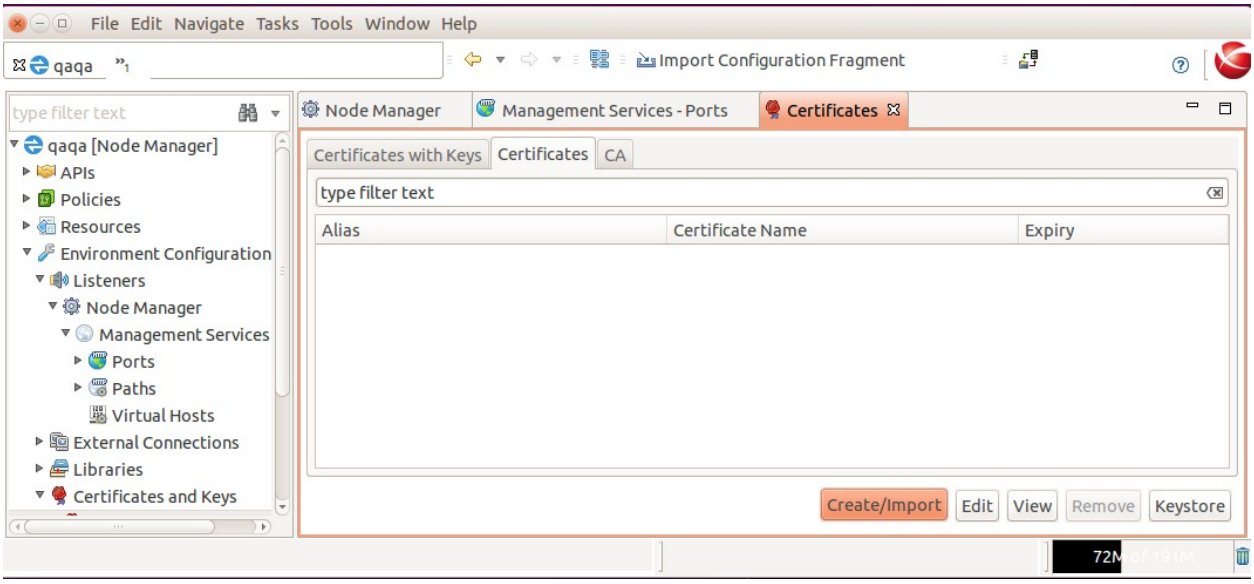
Select the "topology-cert" again.
Edit and select "Choose Issuer Certificate" and set it to "CN=7.3.1-Domain".
Click OK.



The following should now be seen on the "Certificates" screen tabs:-
Tab "Certificates with Keys":

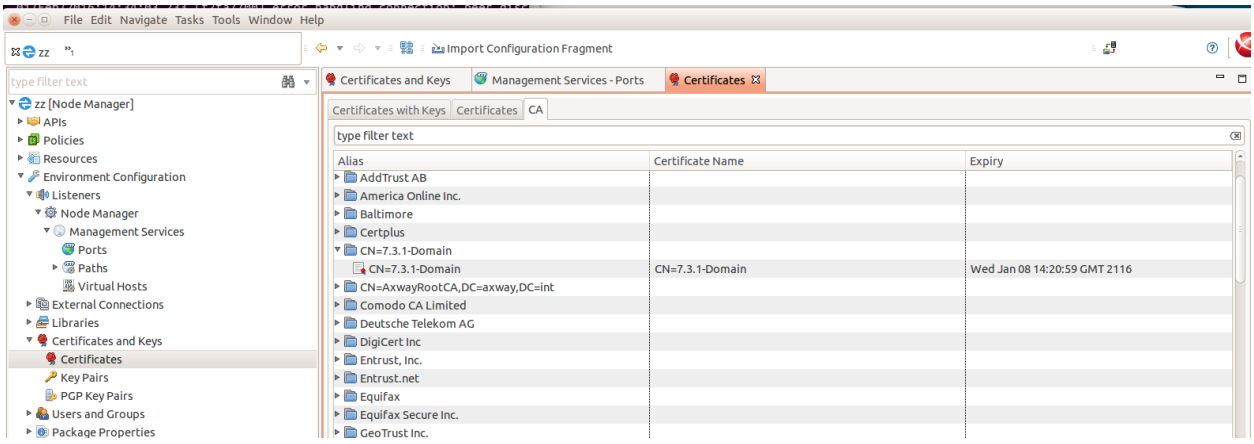


Tab "Certificates”:



Ensure <u>no</u> nodemanager certificate is listed on the tab above.

Tab "CA”:



Browse to "Listeners/Node Manager/Management Services/Ports" and edit the "Management HTTPS Interface”.
Update it to use the "topology-cert” certificate on the "Network” tab.
Click on the "Mutual Authentication” tab and ensure that the Domain CA certificate from the old version, i.e. "CN=7.3.1-Domain”, is selected as a trusted certificate.
Click OK.
Close the project.

Take a backup of `7.5.0-install-dir/apigateway/conf/fed`.
Go to the project directory on disk that you used above in the 7.5.0 Policy Studio.
Copy all files in the project directory to `7.5.0-install-dir/apigateway/conf/fed`.
Restart the Admin Node Manager.

At this point only the Admin Node Manager has been reset to use the SSL certificates from 7.3.1. It cannot talk to the local API Gateway instance yet. Verify the trace for the Admin Node Manager is using the old 7.3.1 certificate, search for this trace statement:-

```
INFO    01/Feb/2016:14:56:41.738 [5537:00000000000000000000000]     Topology certificate:
dname=CN=nodemanager-1,OU=group-1,DC=host-1, issuer=CN=7.3.1-Domain, expiry=Wed Jan 08 14:20:59
GMT 2116
```

There will be lots of SSL errors in the Admin Node Manager trace file as it it trying to communicate with the local API Gateway, which is still using the default 7.5.0 SSL certificate signed by Domain CA with dname `CN=Domain`.

Revert the SSL Certificate for the 7.5.0 API Gateway

Edit the `7.5.0-install-dir/apigateway/groups/group-2/instance-1/conf/mgmt.xml`, change the TrustedCA to be the dname of the 7.3.1 domain CA certificate. If the dname of the Domian CA in the old version was "CN=Domain", this step may be skipped.

```
<HTTP monitoringEnabled="false" name="Management Services" provider="HTTP">
    <SSLInterface activetimeout="60000" address="localhost" auditConn="1" backlog="64"
ciphers="FIPS:!SSLv3:!aNULL" clientAuth="required" depth="1"
dhParams="MEYCQQDaWDwW2YUiidDkr3VvTMqS3UvlM7gE+w/tlO+cikQD7VdGUNNpmdsp13Yna6LT1BLiGPTdHghM9tgAPnx
HdOgzAgEC" enabled="1" idletimeout="60000" inputEncodings=".inherit" maxRequestMemory="16777216"
name="Internal Management HTTPS Interface" opsSettingsUsage="PORT" outputEncodings=".inherit"
port="${env.PORT.MANAGEMENT}" protocol="any" recordCircuitPath="0" recordInboundTxns="0"
recordOutboundTxns="0" recordTrace="0" resolveSubjectCNtoNetAddr="0" reuseAddress="false"
ssloptions="nosslv2 nosslv3" tracelevel="INHERIT" transparentProxy="false">
        <include file="certs.xml" />
        <Identity cert="topology-cert" />
        <VerifyHasTrustedSigner />
        <VerifyIsLocalNodeManager />
    <TrustedCA cert="CN=7.3.1-Domain" /></SSLInterface>
    <MetricsFeedServer httpMethod="*" uriprefix="/metrics" />
    <OPDbViewer httpMethod="*" provider="HTTPops" uriprefix="/ops/" />
    <Application httpMethod="*" sessiontimeoutSeconds="300" uriprefix="/">
        <Servlet class="org.glassfish.jersey.servlet.ServletContainer" name="api" uri="api">
            <Property name="jersey.config.server.provider.classnames"
value="org.glassfish.jersey.media.multipart.MultiPartFeature" />
            <Property name="jersey.config.server.provider.packages"
value="com.vordel.api.monitoring;com.vordel.api.management;com.vordel.api.configuration;com.vorde
l.dwe.file;com.vordel.kps.rest;com.vordel.api.domainaudit;com.vordel.ama.rest;com.vordel.api.disc
overy" />
        </Servlet>
    </Application>
</HTTP>
```

Take a backup of the `certs.xml` file for the API Gateway instance in the 7.5.0 installation, i.e. `7.5.0-install-dir/apigateway/groups/group-2/instance-1/conf/certs`.

Copy the `7.3.1-install-dir/apigateway/groups/group-2/instance-1/conf/certs.xml` to the equivalent 7.5.0 directory.

Restart the local API Gateway.

Verify the 7.5.0 Domain is Operational

Open the API Gateway Manager UI and ensure that the API Gateway status is OK.

Copy Domain CA Key and Certificate from Old Version to 7.5.0

Make a backup of directory `7.5.0-install-dir/groups/certs`.

Copy the content of directory `7.3.1-install-dir/groups/certs` into the 7.5.0 equivalent.

This step is required if the old version was using system generated certificates. No processes need to be restarted after carrying out this step.

Create a New API Gateway Instance in the 7.5.0 Domain

```
./managedomain -c -n APIGateway2 -g Group2 --instance_management_port 6085 --instance_services_port 6086
```

Note: Choose two unused port numbers for the management port and services ports.
Start the API Gateway and ensure the status of it is OK on the API Gateway Manager UI.

Example 7.3.1 -> 7.5.0 Multi-Node Upgrade

Create 7.3.1 Multi-Node System

We use a non-default Domain CA dname in this example, this is not a requirement, see the single node example for more information on this topic.

We will revert the SSL certificates of a 2 node 7.3.1 system with the following topology:-

- **NodeA**: ANM, APIGateway1 in Group1
- **NodeB**: NM, APIGateway2 in Group1

On NodeA:-

- Create a 7.3.1 Admin Node Manager on NodeA using a non-default Domain CA dname as follows:-
  `cd 7.3.1-install-dir/posix/bin`

```
./managedomain -i --domain_name 7.3.1-Domain --anm_host NodeA
```

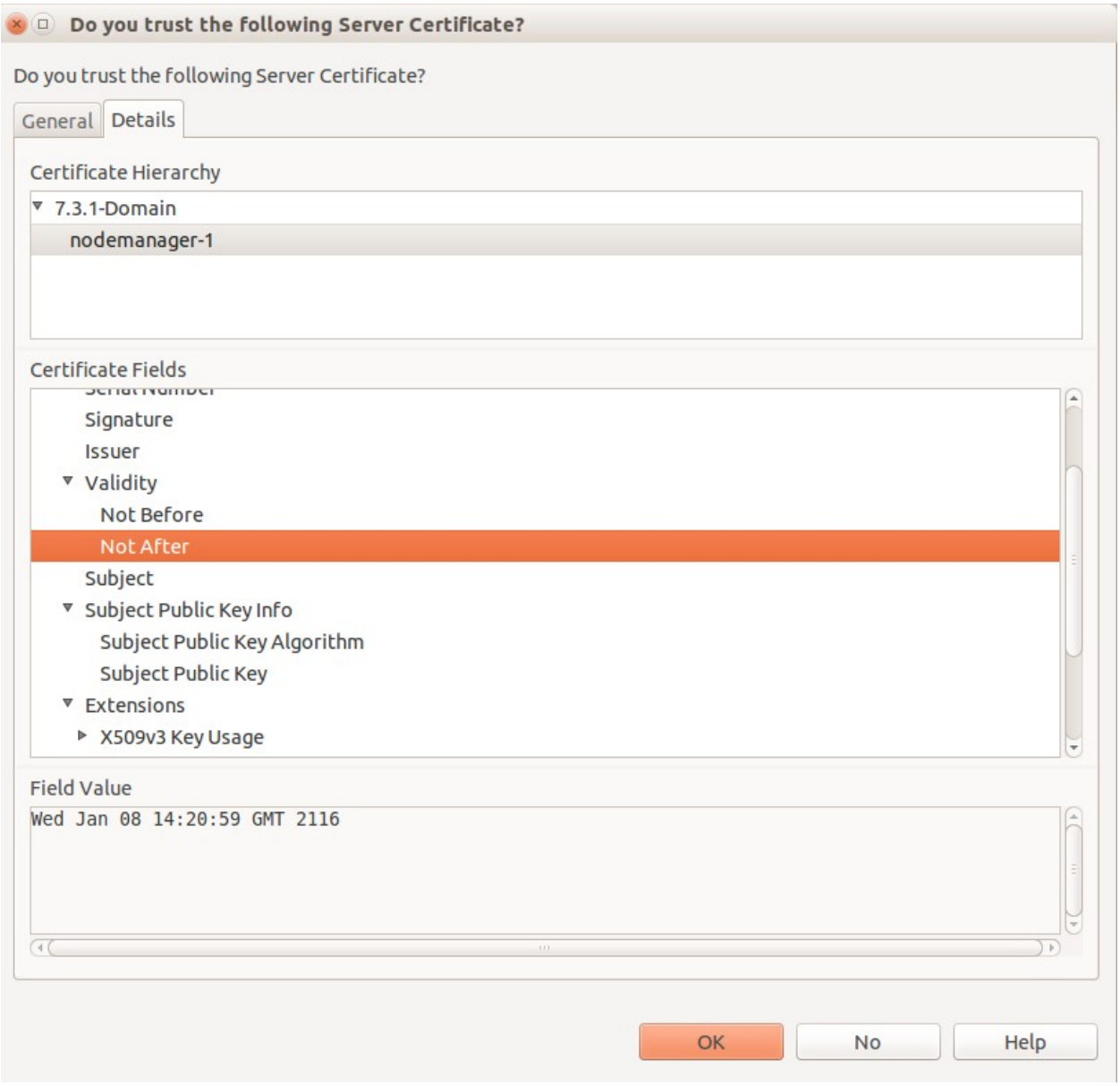
- Start the Admin Node Manager on NodeA.
- Create an API Gateway instance on NodeA.
  ```
  ./managedomain -c -n APIGateway1 -g Group1
  ```
- Start API Gateway instance.

On NodeB:-

- Create the Node Manager:-
  ```
  cd 7.3.1-install-dir/posix/bin
  ./managedomain -a --anm_host NodeA --anm_host NodeB
  ```
- Start the Node Manager on NodeB.
- Create an API Gateway instance on NodeB.
  ```
  ./managedomain -c -n APIGateway2 -g Group1
  ```
- Start API Gateway instance.

View the 7.3.1 Admin Node Manager Certificate

This is an optional step. Start **7.3.1 Policy Studio** and view the certificate details when connecting to the Admin Node Manager.



Note the CN of the certificate that signs the Admin Node Manager certificate is set to "7.3.1-Domain".

Run Sysupgrade on NodeA and NodeB

Run sysupgrade in 7.5.0 installation, pointing it at the 7.3.1 installation and follow normal procedure, bringing down the old version processes when prompted.

On **NodeA**:

```
cd 7.5.0-install-dir/apigateway/upgrade/bin
./sysupgrade /home/mcollins/AxwayInstalls/GOLD/7.3.1/apigateway
```

Run the export, preupgrade, upgrade, applydb steps on NodeA, then goto NodeB

On **NodeB**:

```
cd 7.5.0-install-dir/apigateway/upgrade/bin
./sysupgrade /home/mcollins/AxwayInstalls/GOLD/7.3.1/apigateway
--anm_host NodeA
```

Run the export, preupgrade, upgrade, applydb steps on NodeB, then stop all old version processes on NodeA and NodeB.

Return to **NodeA** and run the apply step.

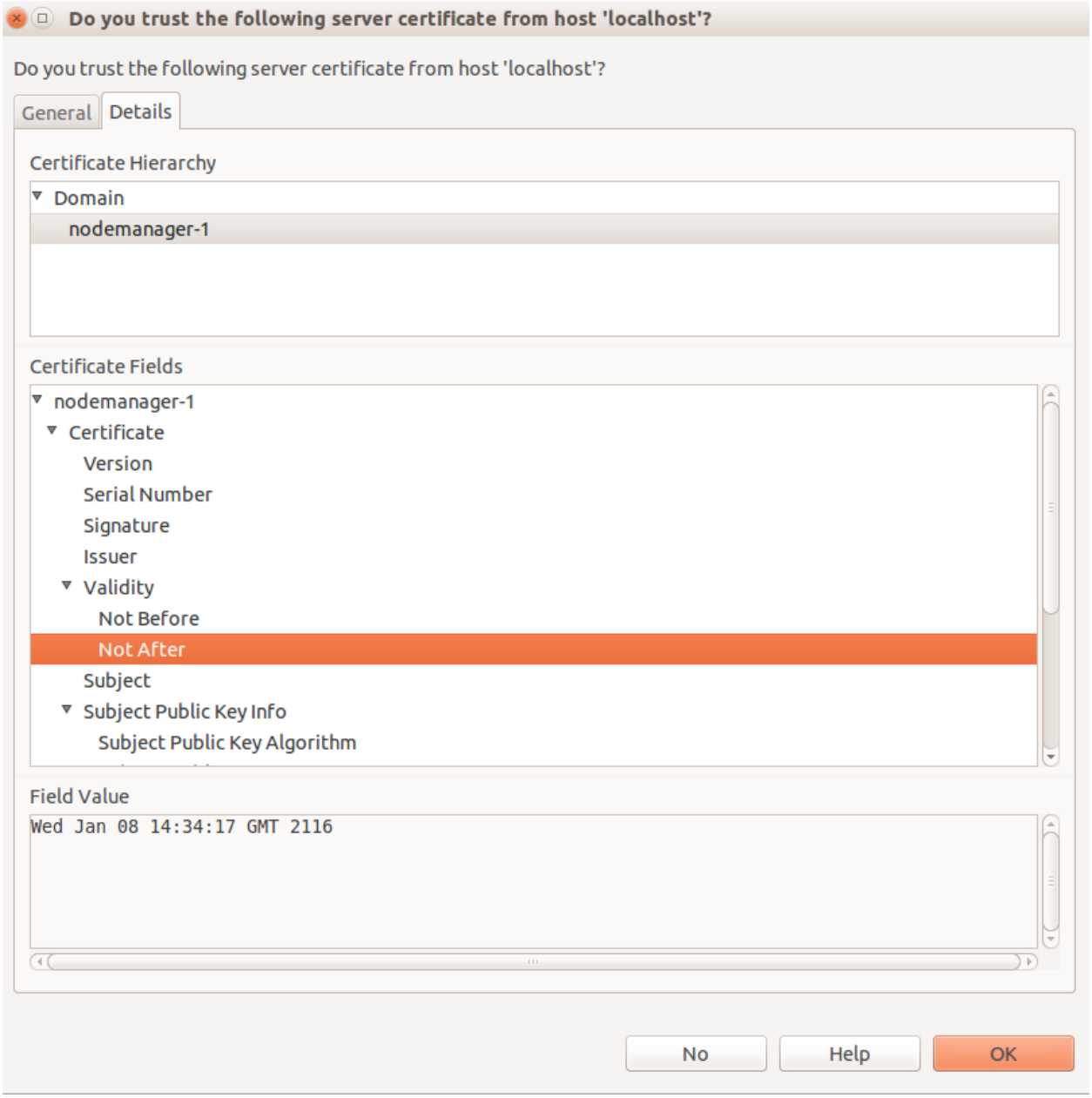
Return to **NodeB** and run the apply step.

When sysupgrade completes, we should now have an equivalent 7.5.0 domain running on NodeA and NodeB.

Verify that the domain looks OK in the API Gateway Manager UI.

View the 7.5.0 Admin Node Manager Certificate

This is an optional step. Start the 7.5.0 Policy Studio
Click "New Project from an API Gateway instance”.

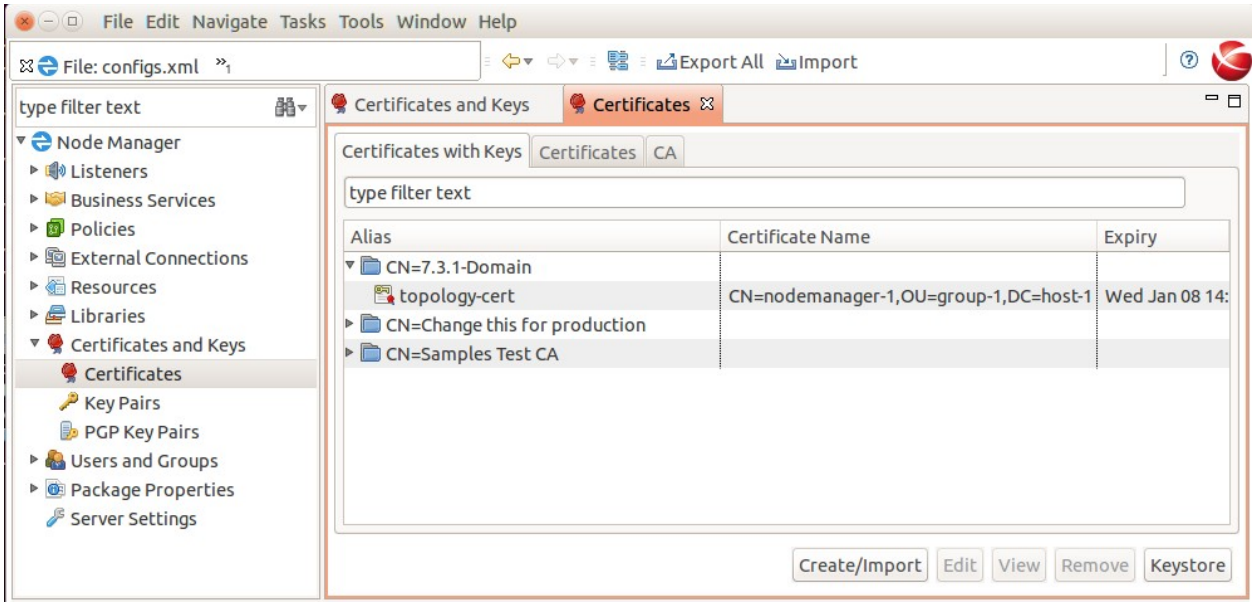


We see that a different Validity period and the CN of the Domain CA certificate is "Domain" as opposed to "7.3.1-Domain". We will now start to revert the SSL certificates for the 7.5.0 domain back to those used in the 7.3.1 domain.

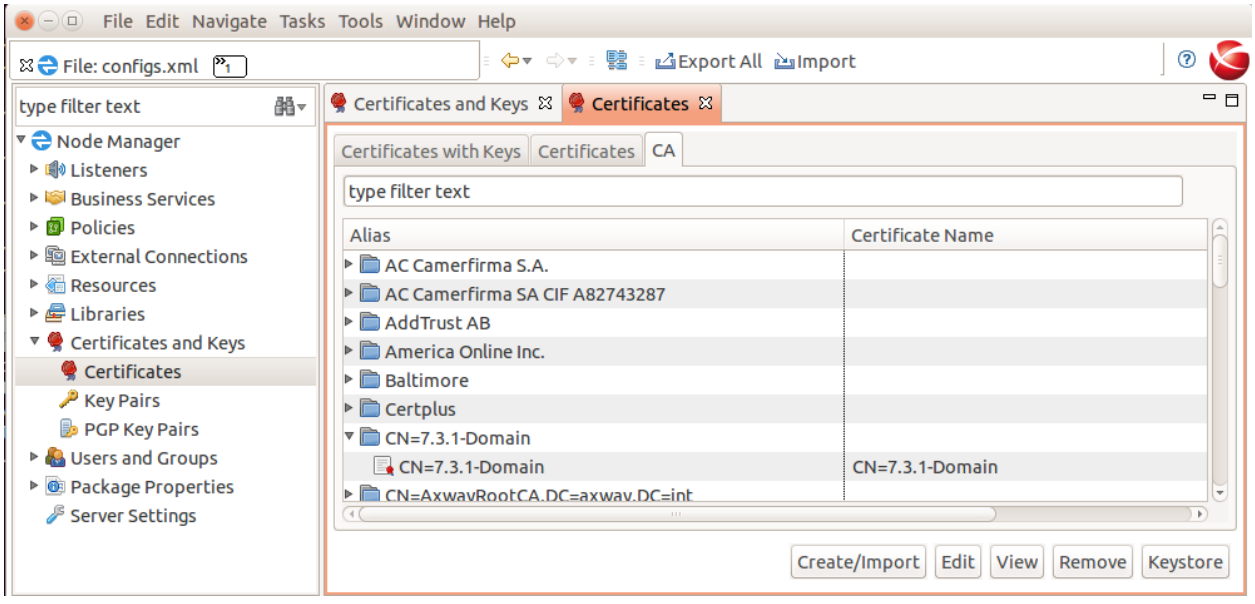
Extract the 7.3.1 Certificate Details for the Domain CA and the Admin Node Manager on Node A

Use the **7.3.1 Policy Studio**.

Choose the "Open File" option and point at the `7.3.1-install-dir/apigateway/conf/fed/configs.xml` file on **NodeA**.
Browse to "Certificates and Keys".



Under the "Certificates with Key" tab, find the "topology-cert., click "Edit"
Then click "Export Certificate and Key" and save the key and cert to a file on disk, e.g. `7.3.1-NodeA.p12`.

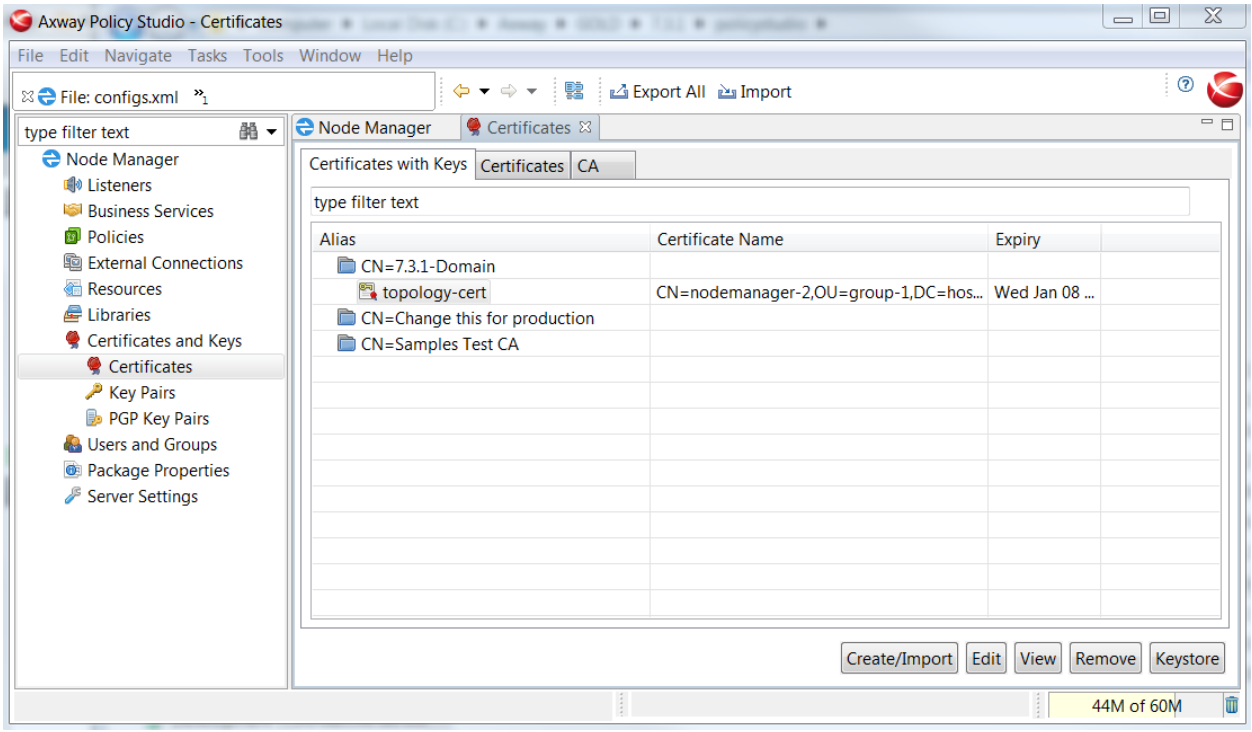


Under the "CA" tab, find the Domain CA certificate with alias "CN=7.3.1-Domain", click "Edit".

Then click "Export Certificate" and save the key and cert to a file on disk, e.g. `7.3.1-domain-cert.pem`.

Extract the 7.3.1 Certificate Details for the Node Manager on NodeB

Use the **7.3.1 Policy Studio**.
Choose the "Open File" option and point at the `7.3.1-install-dir/apigateway/conf/fed/configs.xml` file on **NodeB**.
Browse to "Certificates and Keys".



Under the "Certificates with Key" tab, find the "topology-cert., click "Edit"
Then click "Export Certificate and Key" and save the key and cert to a file on disk, e.g. `7.3.1-NodeB.p12`.

Close 7.3.1 Policy Studio.

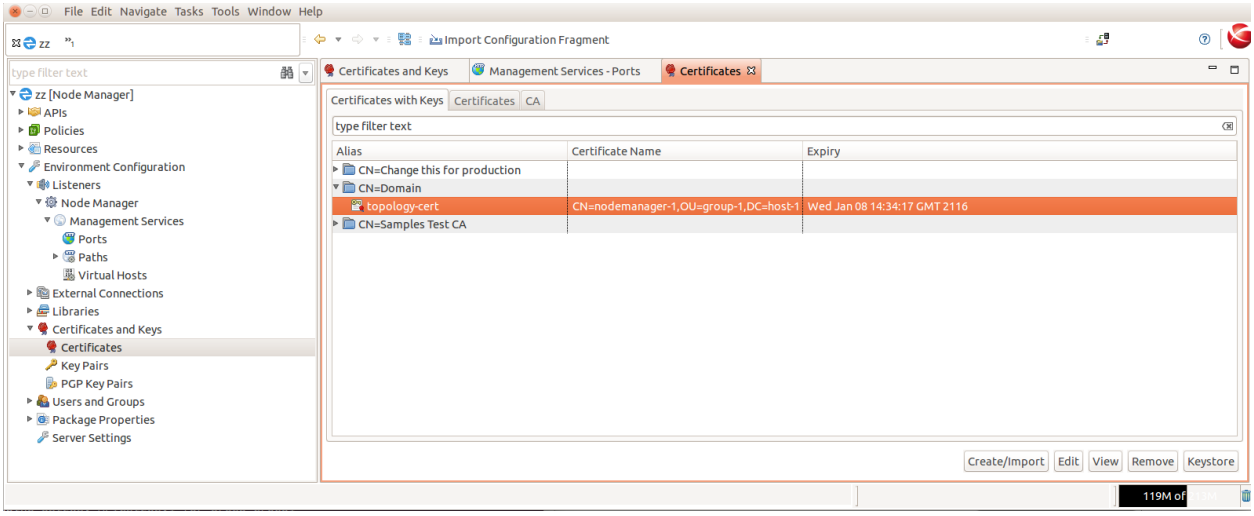
Revert the SSL Certificate for the 7.5.0 Admin Node Manager on NodeA

Run **7.5.0 Policy Studio**.

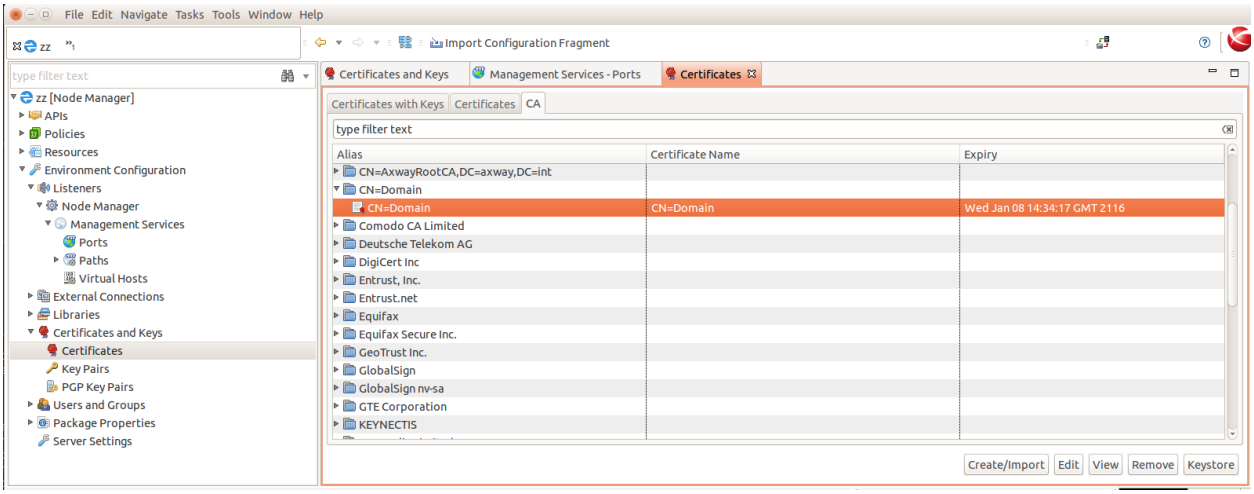
Create a new project based on the 7.5.0 Node Manager configuration, use the "From existing configuration" option and point at the `7.5.0-install-dir/apigateway/conf/fed` directory on **NodeA**.

Browse to "Listeners/Node Manager/Management Services/Ports" and edit the "Management HTTPS Interface".
Update it temporarily so that it does not use the "topology-cert" certificate on the "Network" tab.
Click on the "Mutual Authentication" tab and ensure that the "CN=Domain" certificate is not selected as a trusted certificate.
Click OK.

Browse to "Certificates and Keys".
On the "Certificates with Keys" tab, find the "topology-cert".
Select it and click "Remove".



Under the "CA" tab, find the Domain CA key ("CN=Domain") that signed the "topology-cert".
Select it and click "Remove".



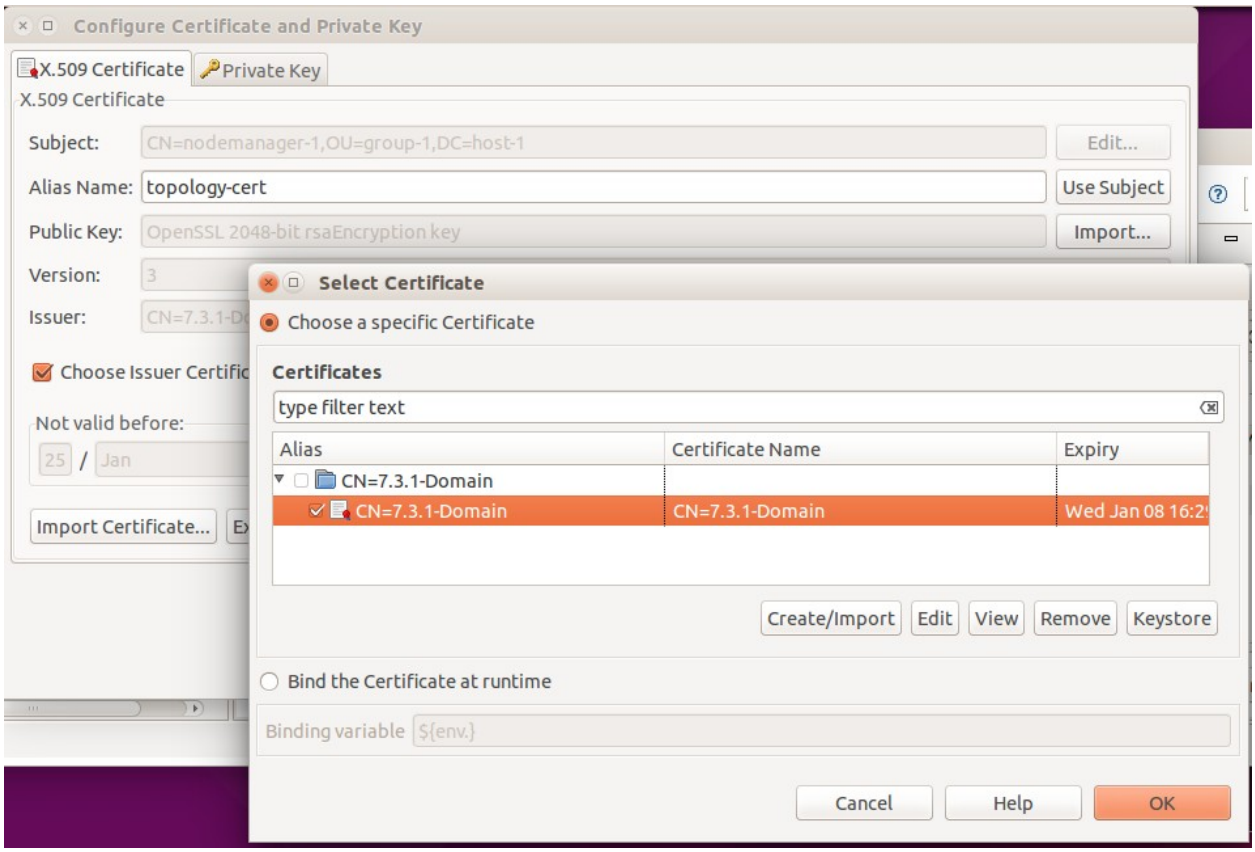
Under the "CA" tab, you will also find the "CN=7.3.1-Domain" certificate. This remains in the Node Manager configuration after upgrade. Remove this also.

Click "Create/Import".
Click "Import Certificate". Select the domain CA certificate file, e.g. `7.3.1-domain-cert.pem`.
Select "Use Subject" for alias.
Click OK.

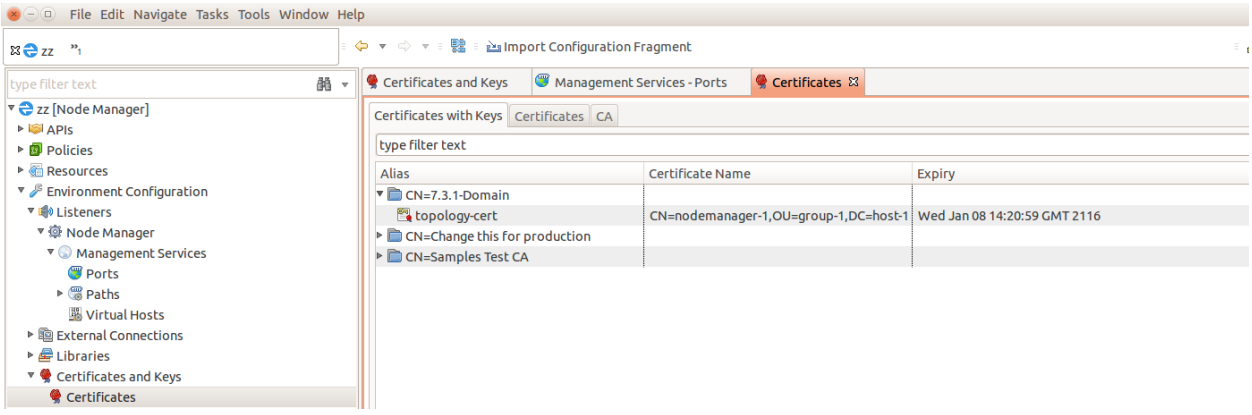
Click "Create/Import" again.
Click "Import Certificate + Key".
Select the p12 file exported from 7.3.1, e.g. `7.3.1-NodeA.p12`.
Enter "topology-cert" as the "Alias Name".
Click OK.

Select the "Certificates" tab, select the CN=nodemanager-1, OU=group-1..." certificate.
Click "Remove".

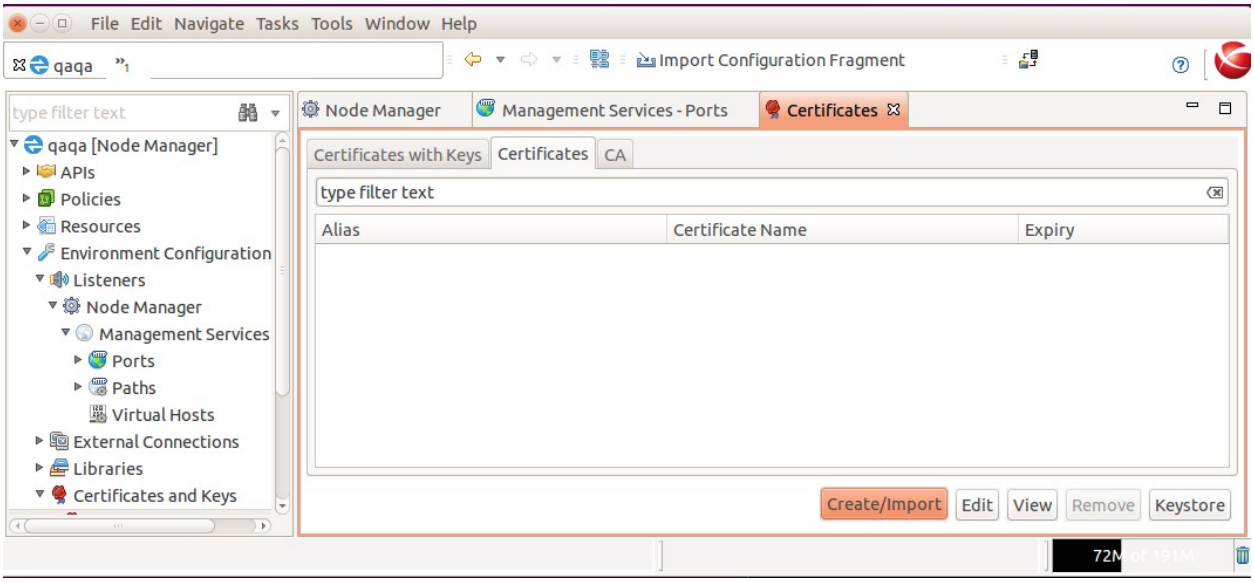
Select the "topology-cert" again.
Select "Choose Issuer Certificate" and set it to "CN=7.3.1-Domain".
Click OK.



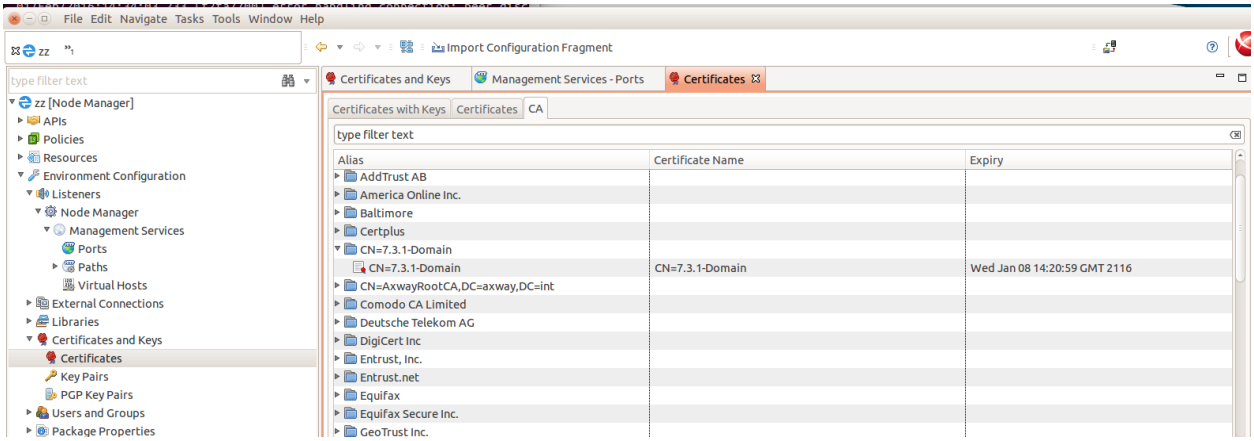
The following should now be seen on the "Certificates" screen for each tab:-
Tab "Certificates with Keys":



Tab "Certificates":



Ensure no nodemanager certificate is listed on the tab above.



Browse to "Listeners/Node Manager/Management Services/Ports" and edit the "Management HTTPS Interface".
Update it to use the "topology-cert" certificate on the "Network" tab.
Click on the "Mutual Authentication" tab and ensure that the Domain CA certificate from the old version, i.e. "CN=7.3.1-Domain", is selected as a trusted certificate.
Click OK.
Close the project.

Take a backup of `7.5.0-install-dir/apigateway/conf/fed`.
Go to the project directory on disk that you used above in the 7.5.0 Policy Studio.
Copy all files in the project directory to `7.5.0-install-dir/apigateway/conf/fed`.

Restart the Admin Node Manager on NodeA.

At this point only the Admin Node Manager on NodeA has been reset to use the SSL certificates from 7.3.1. It cannot talk to the local API Gateway instance yet, or the remote Node Manager on NodeB. SSL errors will be visible in the trace. Verify the trace for the Admin Node Manager on NodeA is using the old 7.3.1 certificate, search for this trace statement:-

```
INFO    01/Feb/2016:14:56:41.738 [5537:00000000000000000000000]     Topology certificate:
dname=CN=nodemanager-1,OU=group-1,DC=host-1, issuer=CN=7.3.1-Domain, expiry=Wed Jan 08 14:20:59
GMT 2116
```

Revert the SSL Certificate for the 7.5.0 API Gateway on NodeA

Edit the `7.5.0-install-dir/apigateway/groups/group-2/instance-1/conf/mgmt.xml`, change the TrustedCA to be the dname of the 7.3.1 domain CA certificate.

```
<HTTP monitoringEnabled="false" name="Management Services" provider="HTTP">
    <SSLInterface activetimeout="60000" address="localhost" auditConn="1" backlog="64"
ciphers="FIPS:!SSLv3:!aNULL" clientAuth="required" depth="1"
dhParams="MEYCQQDaWDwW2YUiidDkr3VvTMqS3UvlM7gE+w/tlO+cikQD7VdGUNNpmdsp13Yna6LT1BLiGPTdHghM9tgAPnx
HdOgzAgEC" enabled="1" idletimeout="60000" inputEncodings=".inherit" maxRequestMemory="16777216"
name="Internal Management HTTPS Interface" opsSettingsUsage="PORT" outputEncodings=".inherit"
port="${env.PORT.MANAGEMENT}" protocol="any" recordCircuitPath="0" recordInboundTxns="0"
recordOutboundTxns="0" recordTrace="0" resolveSubjectCNtoNetAddr="0" reuseAddress="false"
ssloptions="nosslv2 nosslv3" tracelevel="INHERIT" transparentProxy="false">
        <include file="certs.xml" />
        <Identity cert="topology-cert" />
        <VerifyHasTrustedSigner />
        <VerifyIsLocalNodeManager />
    <TrustedCA cert="CN=7.3.1-Domain" /></SSLInterface>
    <MetricsFeedServer httpMethod="*" uriprefix="/metrics" />
    <OPDbViewer httpMethod="*" provider="HTTPops" uriprefix="/ops/" />
    <Application httpMethod="*" sessiontimeoutSeconds="300" uriprefix="/">
        <Servlet class="org.glassfish.jersey.servlet.ServletContainer" name="api" uri="api">
            <Property name="jersey.config.server.provider.classnames"
value="org.glassfish.jersey.media.multipart.MultiPartFeature" />
            <Property name="jersey.config.server.provider.packages"
value="com.vordel.api.monitoring;com.vordel.api.management;com.vordel.api.configuration;com.vorde
l.dwe.file;com.vordel.kps.rest;com.vordel.api.domainaudit;com.vordel.ama.rest;com.vordel.api.disc
overy" />
        </Servlet>
    </Application>
</HTTP>
```

Take a backup of the certs.xml file for the API Gateway instance, i.e. `7.5.0-install-dir/apigateway/groups/group-2/instance-1/conf/certs.xml`

Copy the `7.3.1-install-dir/apigateway/groups/group-x/instance-x/conf/certs.xml` to the equivalent 7.5.0 directory.

Restart the local API Gateway on NodeA.

Revert the SSL Certificate for the 7.5.0 Admin Node Manager on NodeB

Repeat the same steps as described for NodeA. Ensure that `7.3.1-NodeB.p12` file is imported, i.e. the file specific to NodeB.

Revert the SSL Certificate for the 7.5.0 API Gateway on NodeB

Repeat the same steps as described for NodeA.

Verify the 7.5.0 Domain is Operational

Open the API Gateway Manager and ensure that the API Gateway status is OK. All API Gateway instances should have a live status.

Copy Domain CA Key and Certificate from Old Version to 7.5.0

On **NodeA** only, make a backup of directory `7.5.0-install-dir/groups/certs.`

Copy the content of directory `7.3.1-install-dir/groups/certs` into the 7.5.0 equivalent.

This step is required if the old version was using system generated certificates. No processes need to be restarted after carrying out this step.

Create a New API Gateway Instance in the 7.5.0 Domain

On NodeA or NodeB:-

```
./managedomain -c -n APIGateway2 -g Group2 --instance_management_port
6085 --instance_services_port 6086
```

Note: Choose two unused port numbers for the management port and services port.
Start the API Gateway and ensure the status of it is OK on the API Gateway Manager UI.