IBM OMNIbus 8.1 and Netcool/Impact 7.1

SSL Configuration: A step by step example

Author: Gheorghe Mihaela, IBM NSA L2 Software Engineer | IBM Clouds Lab
Mihaela.Gheorghe1@ibm.com

Description

This guide has the purpose to illustrate a complete step by step example for SSL configuration for OMNIbus 8.1 and Netcool/Impact 7.1. Impact UI and Server are installed on the same server.

The versions used within this document to illustrate the steps required were OMNIbus 8.1 FP17 and Netcool/Impact 7.1 FP 15 but they can be used with any other fixpack versions if further changes to the products won't state something different due to code changes.

Configure OMNIbus 8.1 in SSL mode

1. Create object server and add SSL port

For this step edit omni.dat file and set SSL port for the object server definition.

```
#
# omni.dat file as prototype for interfaces file
#
# Ident: $Id: omni.dat 1.5 1999/07/13 09:34:20 chris Development $
#
[NCOMS]
{
        Primary: unmeet1.castle.fyre.ibm.com 4100 ssl 5100
}
[NCO_GATE]
{
        Primary: unmeet1.castle.fyre.ibm.com 4300
}
[NCO_PA]
{
        Primary: unmeet1.castle.fyre.ibm.com 4200
}
[NCO_PROXY]
{
        Primary: unmeet1.castle.fyre.ibm.com 4400
}
```

2. Run nco_igen script to generate the interfaces and afterwards start the object server

cd /Miha/opt/IBM/Tivoli/netcool/bin
./nco_igen

```
[root@unmeet1 tmpIM]# /Miha/opt/IBM/tivoli/netcool/bin/nco_igen
```

cd /Miha/opt/IBM/Tivoli/netcool/omnibus/bin
./nco_objserv -name NCOMS &

```
[root@unmeet1 tmpIM]# /Miha/opt/IBM/tivoli/netcool/omnibus/bin/nco_objserv -name
 NCOMS &
[1] 14685
[root@unmeet1 tmpIM]#
Netcool/OMNIbus Object Server - Version 8.1.0 64-bit

(C) Copyright IBM Corp. 1994, 2012

Server 'NCOMS' initialised - entering RUN state.

[root@unmeet1 tmpIM]#
```

3. Create OMNIbus certificate for SSL

3.1. Create CMS key database (Acting as Issuing CA):

./nc_gskcmd -keydb -create -db "/Miha/opt/IBM/tivoli/netcool/etc/security/keys/omni.kdb" -pw netcool -stash -expire 3660

```
[root@unmeet1 bin]# ./nc_gskcmd -keydb -create -db "/Miha/opt/IBM/tivoli/netcool
/etc/security/keys/omni.kdb" -pw netcool -stash -expire 3660
```

3.2. Create self-signed CA certificate:

./nc_gskcmd -cert -create -db "/Miha/opt/IBM/tivoli/netcool/etc/security/keys/omni.kdb" -pw netcool -label "CA" -size 1024 -ca true -dn "CN=CA,O=IBM,OU=Support,L=IBMRO,ST=Bucharest" -expire 3660 -x509version 3

```
[root@unmeet1 bin]# ./nc_gskcmd -cert -create -db "/Miha/opt/IBM/tivoli/netcool/
etc/security/keys/omni.kdb" -pw netcool -label "CA" -size 1024 -ca true -dn "CN=
CA,O=IBM,OU=Support,L=IBMRO,ST=Bucharest" -expire 3660 -x509version 3
[root@unmeet1 bin]#
```

3.3. Export the CA Certificate for distribution:

./nc_gskcmd -cert -extract -db "/Miha/opt/IBM/tivoli/netcool/etc/security/keys/omni.kdb" -pw netcool -label "CA" -target "/Miha/opt/IBM/tivoli/netcool/etc/security/keys/cacert.arm"

```
[root@unmeet1 bin]# ./nc_gskcmd -cert -extract -db "/Miha/opt/IBM/tivoli/netcool
/etc/security/keys/omni.kdb" -pw netcool -label "CA" -target "/Miha/opt/IBM/tivo
li/netcool/etc/security/keys/cacert.arm"
```

3.4. Create certificate request for primary ObjectServer:

Note: Label is same as the server name in omni.dat file as is the Common Name (CN)

./nc_gskcmd -certreq -create -db "/Miha/opt/IBM/tivoli/netcool/etc/security/keys/omni.kdb" -pw netcool -label "NCOMS" -size 2048 -dn

"CN=NCOMS,O=IBM,OU=Support,L=IBMRO,ST=Bucharest" -file "/Miha/opt/IBM/tivoli/netcool/etc/security/keys/NCOMS_req.arm"

```
[root@unmeet1 bin]# ./nc_gskcmd -certreq -create -db "/Miha/opt/IBM/tivoli/netco
ol/etc/security/keys/omni.kdb" -pw netcool -label "NCOMS" -size 2048 -dn "CN=NCO
MS,O=IBM,OU=Support,L=IBMRO,ST=Bucharest" -file "/Miha/opt/IBM/tivoli/netcool/et
c/security/keys/NCOMS_req.arm"
```

3.5. Sign the certificate requests using above created signer certificate label CA:

./nc_gskcmd -cert -sign -db "/Miha/opt/IBM/tivoli/netcool/etc/security/keys/omni.kdb" -pw netcool -label "CA" -target "/Miha/opt/IBM/tivoli/netcool/etc/security/keys/NCOMS_req.arm" -expire 3660 -file "/Miha/opt/IBM/tivoli/netcool/etc/security/keys/NCOMS_req.arm"

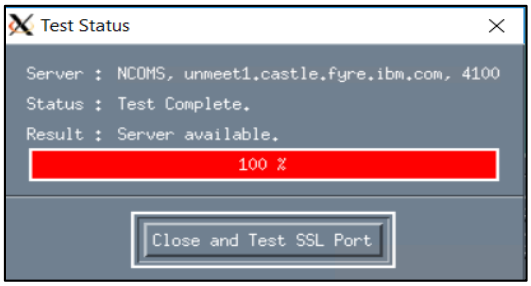
```
[root@unmeet1 bin]# ./nc_gskcmd -cert -sign -db "/Miha/opt/IBM/tivoli/netcool/et
c/security/keys/omni.kdb" -pw netcool -label "CA" -target "/Miha/opt/IBM/tivoli/
netcool/etc/security/keys/NCOMS_req.arm" -expire 3660 -file  "/Miha/opt/IBM/tivo
li/netcool/etc/security/keys/NCOMS_req.arm"
```

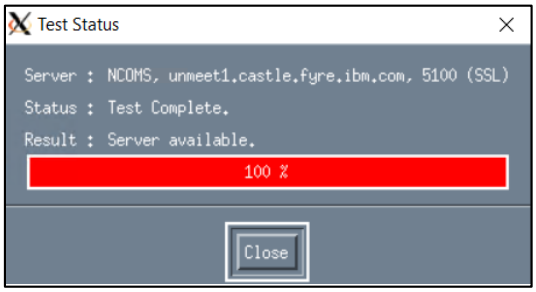
3.6. Receive the signed certificate in omni.kdb file:

./nc_gskcmd -cert -receive -db "/Miha/opt/IBM/tivoli/netcool/etc/security/keys/omni.kdb" -pw netcool -file "/Miha/opt/IBM/tivoli/netcool/etc/security/keys/NCOMS_req.arm"

```
[root@unmeet1 bin]# ./nc_gskcmd -cert -receive -db "/Miha/opt/IBM/tivoli/netcool
/etc/security/keys/omni.kdb" -pw netcool -file "/Miha/opt/IBM/tivoli/netcool/etc
/security/keys/NCOMS_req.arm"
```

3.7. Restart Object server and test SSL for OMNI





Configure Netcool/Impact for SSL (ImpactUI and Impact Server installed on same server)

Complete documentation steps:
https://www.ibm.com/support/knowledgecenter/en/SSSHYH_7.1.0.15/com.ibm.netcoolimpact.doc/admin/ssl_for_objectserver_user_authentication.html

For ImpactUI and Server on separate servers the certificates will also need to be exchanged.
Within this example both components are installed on the same server. Impact server name in this example is TBSM.

1. To enable SSL, run the following command:

./configImpactSSL.sh enable <keystore password>

Where <keystore password> is the keystore password that is set during the Netcool/Impact installation.

```
[root@unmeet1 eclipse]# cd /Miha/opt/IBM/tivoli/impact/install/security/
[root@unmeet1 security]#
[root@unmeet1 security]# ./configImpactSSL.sh enable netcool
```

```
BUILD SUCCESSFUL
Total time: 43 seconds
Done. Please exchange the SSL certificates between all of the Netcool/Impact and
 GUI servers, and then start the primary server first, followed by the secondary
 servers.
```

2. Restart Impact:

```
[root@unmeet1 security]# /Miha/opt/IBM/tivoli/impact/bin/stopImpactServer.sh
Stopping server TBSM.
Server TBSM is not running.
[root@unmeet1 security]# /Miha/opt/IBM/tivoli/impact/bin/stopGUIServer.sh
Stopping server ImpactUI.
Server ImpactUI is not running.
```

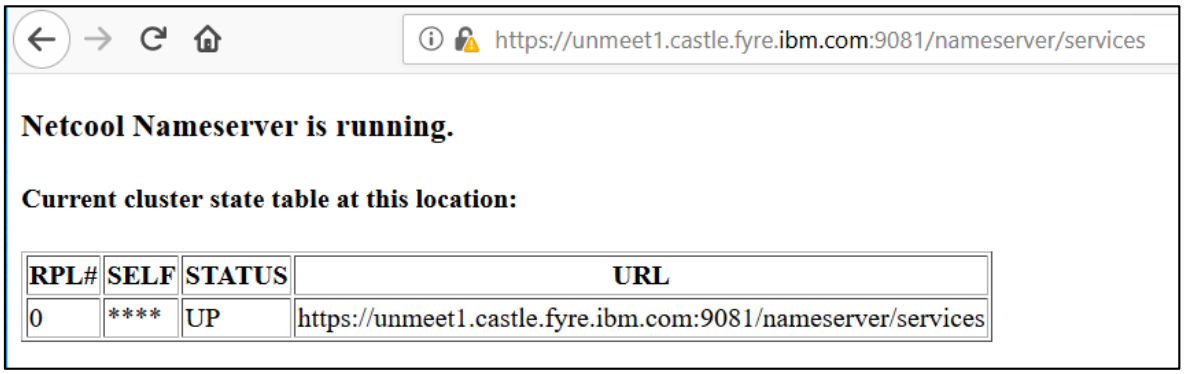
```
[root@unmeet1 security]# /Miha/opt/IBM/tivoli/impact/bin/startImpactServer.sh
Starting server TBSM.
Server TBSM started with process ID 2577.
[root@unmeet1 security]#  /Miha/opt/IBM/tivoli/impact/bin/startGUIServer.sh
Starting server ImpactUI.
Server ImpactUI started with process ID 3829.
```

3. Checking SSL:

/Miha/opt/IBM/tivoli/impact/wlp/usr/servers/TBSM/apps/nameserver.war/WEB-INF/web.xml

```
<!-- SSL ENABLE -->
<context-param>
    <param-name>SSL_ENABLED</param-name>
    <param-value>true</param-value>
</context-param>
```

https://unmeet1.castle.fyre.ibm.com:9081/nameserver/services



4. Configure SSL between Netcool/Impact and OMNIbus

4.1. Obtained object server certificate:

/Miha/opt/IBM/tivoli/netcool/etc/security/keys/cacert.arm

4.2. Import the certificate into the Impact Server and GUI Server trust-store.

- on the Impact Server

```
[root@unmeet1 bin]# ./keytool -importcert -alias ncomscert -file /Miha/opt/IBM/t
ivoli/netcool/etc/security/keys/cacert.arm -keystore /Miha/opt/IBM/tivoli/impact
/wlp/usr/servers/TBSM/resources/security/trust.jks -storepass netcool
```

```
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

- on the ImpactUI server

```
[root@unmeet1 bin]# ./keytool -importcert -alias ncomscert -file /Miha/opt/IBM/t
ivoli/netcool/etc/security/keys/cacert.arm -keystore /Miha/opt/IBM/tivoli/impact
/wlp/usr/servers/ImpactUI/resources/security/trust.jks -storepass netcool
```

```
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

4.3. Restart Impact:

```
[root@unmeet1 bin]# /Miha/opt/IBM/tivoli/impact/bin/stopImpactServer.sh
Stopping server TBSM.
Server TBSM stopped.
[root@unmeet1 bin]#  /Miha/opt/IBM/tivoli/impact/bin/stopGUIServer.sh
Stopping server ImpactUI.
Server ImpactUI stopped.
```

```
[root@unmeet1 bin]#  /Miha/opt/IBM/tivoli/impact/bin/startImpactServer.sh
Starting server TBSM.
Server TBSM started with process ID 12134.
[root@unmeet1 bin]# /Miha/opt/IBM/tivoli/impact/bin/startGUIServer.sh
Starting server ImpactUI.
Server ImpactUI started with process ID 12369.
```

4.4. Update the $IMPACT_HOME/install/security/impactncos.properties file

- Enter the ObjectServer information.
- Ensure that the correct port for SSL is used.
- Set the NCOSSSLEnabled property to true.

```
[root@unmeet1 bin]# vi /Miha/opt/IBM/tivoli/impact/install/security/impactncos.p
roperties
```

```
# Netcool/OMNIbus ObjectServer Primary Hostname or IP address
NCOSPrimaryHost="unmeet1.castle.fyre.ibm.com"

# Netcool/OMNIbus ObjectServer Primary Port Number
NCOSPrimaryPort="5100"

# Netcool/OMNIbus ObjectServer Administrator User
# Note: user must be enabled and have access to users.security table
NCOSUsername="root"

# Enable SSL Communication to the ObjectServer
# Note: must exchange certificates between Impact and the ObjectServer before en
abling
NCOSSSLEnabled="true"
```

4.5. In $IMPACT_HOME/install/security, run the confAuth4OMNIbus script, then enter the enable command

```
[root@unmeet1 security]# ./confAuth4OMNIbus.sh enable impactadmin netcool
Buildfile: /Miha/opt/IBM/tivoli/impact/install/security/cfg_scripts/confAuth4OMN
```

```
BUILD SUCCESSFUL
Total time: 2 minutes 31 seconds
[root@unmeet1 security]#
```

4.6. Restart the Impact Server

4.7. Connect to Impact console and in the ObjectServer data source, select the SSL Mode check box and check that you are using the appropriate SSL port. Afterwards click Test Connection to ensure that you can communicate on the SSL port.