

IBM z/OS Connect EE V3.0

Customization - Security when accessing an IMS Database



Lab Version Date: February 4, 2021

Table of Contents

| | |
|--|-----------|
| Overview | 4 |
| Enabling RACF Pass Tickets..... | 5 |
| <i>Test with RACF Pass Tickets not enabled</i> | <i>5</i> |
| <i>Test with identity propagation enabled using RACF Pass Tickets.....</i> | <i>7</i> |
| <i>Summary</i> | <i>9</i> |
| Configuring TLS security to an IMS Subsystem | 10 |
| <i>Creating IMS SAF resources</i> | <i>10</i> |
| <i>Configure the AT-TLS policies</i> | <i>16</i> |
| Activating the AT-TLS configuration | 48 |
| <i>Test the TLS connection from the zCEE Server to IMS</i> | <i>51</i> |
| <i>Optional</i> | <i>53</i> |
| Summary | 54 |
| Appendix – AT-TLS Policy Agent Configuration File | 54 |

Important: On the desktop there is a file named *Security CopyPaste.txt*. This file contains commands and other text used in this workshop. Locate that file and open it. Use the copy-and-paste function (**Ctrl-C** and **Ctrl-V**) to enter commands or text. It will save time and help avoid typo errors. As a reminder text that appears in this file will be highlighted in yellow.

General Exercise Information and Guidelines

- ✓ This exercise requires the completion of the *zCEE Basic Configuration* and *zCEE Basic Security Configurations* exercises before it can be performed.
- ✓ This exercise requires using z/OS user identities *FRED* and *USER1*. The password for these users will be provided by the lab instructions.
- ✓ There are examples of *server.xml* scattered through this exercise. Your *server.xml* may differ depending on which exercises have been previously performed. Be sure the **red lines** in these examples are either added or already present.
- ✓ The acronyms RACF (resource access control facility) and SAF (system authorization facility) are used in this exercise. RACF is the IBM security manager product whereas SAF is a generic term for any security manager product, e.g. ACF2 or Top Secret or RACF. An attempt has been to use SAF when referring to information appropriate for any SAF product and to use RACF when referring to specific RACF commands or examples.
- ✓ Any time you have any questions about the use of IBM z/OS Explorer, 3270 screens, features or tools, do not hesitate to ask the instructor for assistance.
- ✓ Text in **bold** and highlighted in **yellow** in this document should be available for copying and pasting in a file named *Security CopyPaste* file on the desktop.
- ✓ Please note that there may be minor differences between the screen shots in this exercise versus what you see when performing this exercise. These differences should not impact the completion of this exercise.
- ✓ For information regarding the use of the Personal Communication 3270 emulator, see the *Personal Communications Tips* PDF in the exercise folder.

Overview

This exercise demonstrates the steps required to enable security between a z/OS Connect EE (zCEE) server and IMS.

In part one of the exercise the use of RACF pass tickets will be configured. RACF pass tickets can be used to pass the z/OS Connect authenticated RACF identity to IMS Connect and this identity will subsequently be used for IMS authorization checks.

In part two of the exercise, TLS support will be added by configuring AT-TLS policies. The presence of these policies will act as a surrogate for handing the server role on behalf of IMS Connect and a surrogate for the z/OS Connect server as client.

Enabling RACF Pass Tickets

When sending request from an z/OS Connect server to IMS the identity used for IMS authorization checks will be by default the identity configured in the basic authentication element of the IMS connection factory. This identity is associated with the server and not the z/OS Connect authenticated identity under which the requests is running.

To provide identity assertion of the authenticated identity the use of RACF Pass Tickets is required. When RACF Pass Tickets are enabled, the zCEE server will obtain a pass ticket from RACF and send this ticket (token) along with the request to IMS Connect. When the request arrives at the IMS Connect the pass ticket will be validated with RACF and the z/OS Connect authenticated identity will be extracted and use for subsequent IMS authorization checks.

Test with RACF Pass Tickets not enabled

But first let's explore invoking an IMS API and observing the security behavior when identity propagation is not enabled.

1. Edit the *server.xml* configuration file for the *myServer* server, e.g. */var/zosconnect/servers/myServer/server.xml* and add includes for *shared.xml* and *imsDatabase.xml* (if they are not already present) see below:

```
<include location="${server.config.dir}/includes/imsDatabase.xml"/>
```

```
<include location="${server.config.dir}/includes/shared.xml"/>
```

```
<include location="${server.config.dir}/includes/safSecurity.xml"/>
<include location="${server.config.dir}/includes/ipic.xml"/>
<include location="${server.config.dir}/includes/keyringMutual.xml"/>
<include location="${server.config.dir}/includes/groupAccess.xml"/>
<include location="${server.config.dir}/includes/imsDatabase.xml"/>
<include location="${server.config.dir}/includes/shared.xml"/>
```

This will install some predefined services and APIs in the server.

2. Stop and restart the server with MVS commands **P BAQSTRT** and **S BAQSTRT**.

Tech-Tip: MVS and JES2 commands can be entered from SDSF by enter a / (slash) on the command line followed by the command itself (e.g. /D T). The command results can be found in the system log. If a command is especially long, then simply entering a / (slash) to display a *SDSF – System Command Extension* panel where a command can span multiple lines. When an MVS command must be entered, the instructions in these exercises will indicate that the command is a MVS command and you may enter the command at the prompt by using the / (slash) prefix or using the *SDSF – System Command Extension* panel.

___3. Open a DOS command prompt and go to directory *c:/z/admin*.

___4. Enter the cURL command below:

```
curl -X get --cacert certauth.pem --cert fred.p12:secret --cert-type P12  
https://wg31.washington.ibm.com:9443/imdb/contact/LAST3
```

```
c:\z\admin>curl -X get --cacert certauth.pem --cert fred.p12:secret --cert-type P12  
https://wg31.washington.ibm.com:9443/imdb/contact/LAST3  
{ "response": { "result": [ { "firstName": "FIRST3", "zipCode": "D03\ /R03", "lastName": "LAST3", "  
phoneNumber": "8-111-3333" } ] } }
```

___5. Enter the cURL command below:

```
curl -X GET --cacert certauth.pem --cert user1.p12:secret --cert-type P12  
https://wg31.washington.ibm.com:9443/imdb/contact/LAST3
```

You should see the same results because the requests to IMS Connect are using the basic authentication as configured in the connection factory in *imsDatabase.xml* (see below).

```
<connectionFactory id="DFSIVPAConn">  
<properties.imsudbJLocal  
  databaseName="DFSIVPA"  
  dataStoreName="IVP1"  
  dataStoreServer="wg31.washington.ibm.com"  
  driverType="4"  
  portNumber="5555"  
  user="USER1"  
  password="USER1"  
  flattenTables="True"/>  
</connectionFactory>
```

___6. To confirm that USER1 is being used, locate the outstanding reply for IMS Connect in the SDSF log and respond with **VIEWHWS**, as in ##VIEWHWS (where ## is the reply number). You should see two requests for port 5555 both with the same *CLIENTID* of *USER1*.

```
HWSC0001I      PORT=5555D      STATUS=ACTIVE      KEEPAPV=0  NUMSOC=3  
EDIT=          TIMEOUT=6000  
HWSC0001I      CLIENTID USERID      TRANCODE  DATASTORE  STATUS      SECOND  
CLNTPORT IP-ADDRESS      APSB-TOKEN  
HWSC0001I      ODB970D4  USER1      IVP15OOD  RECV        44  
1423  192.168.017.220  
HWSC0001I      ODB36ED4  USER1      IVP15OOD  RECV        153  
1349  192.168.017.220  
HWSC0001I      TOTAL CLIENTS=2  RECV=2  READ=0  CONN=0  XMIT=0  OTHER=0
```

Test with identity propagation enabled using RACF Pass Tickets

Next enable the use of RACF pass tickets in the server.xml file and retest and the observe the results.

___1. Begin by submit the job in member *IMSPTKT* in data set *USER1.ZCEE30.CNTL*.

```
ADDGROUP ZCEEIMS

CONNECT (FRED,USER1,LIBSERV GROUP(ZCEEIMS)

SETROPTS CLASSACT(PTKTDATA) RACLIST(PTKTDATA)
SETROPTS GENERIC(PTKTDATA)

RDEFINE PTKTDATA IMSAPPL SSIGNON(KEYMASK(123456789ABCDEF0)) +
APPLDATA('NO REPLAY PROTECTION')

RDEFINE PTKTDATA IRRPTAUTH.IMSAPPL.* UACC(NONE)
PERMIT IRRPTAUTH.IMSAPPL.* ID(ZCEEIMS) CLASS(PTKTDATA) ACC(UPDATE)

SETROPTS RACLIST(PTKTDATA) REFRESH
```

These commands define the required *PTKTDATA* resource *IMSAPPL*.

Tech-Tip: The value *IMSAPPL* was derived from the IMS Connect *APPL* attribute for the ODACCESS configuration entry, see sample below:

```
HWS=(ID=IMS15HWS,XIBAREA=100,RACF=Y,RRS=Y)
TCPIP=(HOSTNAME=TCPIP,PORTID=(4000,LOCAL),RACFID=JOHNSON,TIMEOUT=5000)
DATASTORE=(GROUP=OTMAGRP,ID=IVP1,MEMBER=HWSMEM,DRU=HWSYDRU0,
TMEMBER=OTMAMEM,APPL=IMSAPPL)
ODACCESS=(ODBMAUTOCONN=Y,IMSPLEX=(MEMBER=IMS15HWS,TMEMBER=PLEX1),
DRDAPORT=(ID=5555,PORTTMOT=6000),ODBMTMOT=6000,APPL=IMSAPPL)
```

The value for the key mask was an arbitrary 16 hexadecimal string. If multiple RACF databases are involved this value must be the same for all.

- ___2. Edit the server's server.xml file and change the include for *imsdatabase.xml* to an include for *imsDatabasePassTicket.xml*.

```
<include location="${server.config.dir}/includes/imsDatabasePassTicket.xml"/>
```

```
<include location="${server.config.dir}/includes/safSecurity.xml"/>
<include location="${server.config.dir}/includes/ipic.xml"/>
<include location="${server.config.dir}/includes/keyringMutual.xml"/>
<include location="${server.config.dir}/includes/groupAccess.xml"/>
<include location="${server.config.dir}/includes/imsDatabasePassTicket.xml"/>
<include location="${server.config.dir}/includes/shared.xml"/>
```

The contents of *imsDatabasePassTicket.xml* are shown below

```
<connectionFactory id="DFSIVPAConn">
<properties.imsudbJLocal
  databaseName="DFSIVPA"
  dataStoreName="IVP1"
  dataStoreServer="wg31.washington.ibm.com"
  driverType="4"
  portNumber="5555"
  applicationName="IMSAPPL"
  flattenTables="True"/>
</connectionFactory>
```

- ___3. Refresh the server's configuration using the MVS command **F BAQSTRT,REFRESH,CONFIG**

Tech-Tip: A refresh should be sufficient, but a complete restart of the server might be better. The TCPIP connects linger for a while and restart of the server will break these connections and provide distinct results between tests.

- ___4. Enter the cURL command below:

```
curl -X get --cacert certauth.pem --cert fred.p12:secret --cert-type P12
https://wg31.washington.ibm.com:9443/imdb/contact/LAST3
```

```
c:\z\admin>curl -X get --cacert certauth.pem --cert fred.p12:secret --cert-type P12
https://wg31.washington.ibm.com:9443/imdb/contact/LAST3
{"response":{"result":[{"firstName":"FIRST3","zipCode":"D03\R03","lastName":"LAST3","
phoneNumber":"8-111-3333"}]}}
```

:

You should see the same results.

5. To confirm the FRED identity (fred.p12) is being used, locate the outstanding reply for IMS Connect in the SDSF log again and respond with IMS Connect command *VIEWHWS*, as in *##VIEWHWS* (where ## is the outstanding reply number for IMS Connect). You should see two requests for port 5555, with one *CLIENTID* for FRED and another *CLIENTID* for USER1.

| | | | | | | |
|-----------|-----------------|---------------|----------|-----------|--------|--------|
| HWSC0001I | PORT=5555D | STATUS=ACTIVE | KEEPAV=0 | NUMSOC=3 | | |
| EDIT= | TIMEOUT=6000 | | | | | |
| HWSC0001I | CLIENTID | USERID | TRANCODE | DATASTORE | STATUS | SECOND |
| CLNTPORT | IP-ADDRESS | APSB-TOKEN | | | | |
| HWSC0001I | ODBC70D1 | FRED | IVP15OOD | RECV | | 23 |
| 1547 | 192.168.017.220 | | | | | |
| HWSC0001I | ODBA4CD5 | USER1 | IVP15OOD | RECV | | 251 |
| 1523 | 192.168.017.220 | | | | | |
| HWSC0001I | TOTAL | CLIENTS=2 | RECV=2 | READ=0 | CONN=0 | XMIT=0 |
| | | | | OTHER=0 | | |

Summary

In this section a simple REST client (cURL) has been used to invoke an API which accesses IMS. The API was initially tested without using RACF Pass Tickets using basic authentication from the server. Required RACF resources were then defined and changes were made to the server.xml so RACF Pass Tickets would be used between the server and IMS Connect. Finally, the REST client was used to demonstrate that the identity associated with the client certificates (fred.p12 and user1.p12) were propagated to IMS Connect for authorization checks.

Configuring TLS security to an IMS Subsystem

Adding TLS support to the connection between the z/OS Connect server and IMS requires the creation of a key ring belonging to the identity under which the IMS Connect task is executing (look for message IEF695I in the IMS15HWS task's JES messages). This key ring contains the personal and the certificate authority certificates that will be used during TLS handshakes. The creation of the key ring and the connection of certificates to the key ring are done using the RACDCERT RACF commands.

Creating IMS SAF resources

First, we may have to do some housekeeping depending on which exercises have been previously performed.

- ___1. Browse data set *USER1.ZCEE30.CNTL*. You should see the members in that data set.
- ___2. Browse member **ZCEETLSC** (TLS client role). You should see the RACF commands below. Submit the job for execution if this job has not been previously submitted in another exercise.

```
/* Create personal certificate for zCEE outbound client request */
racdcert id(libserv) gencert subjectsdn(cn('zCEE Client Cert') +
ou('ATS') o('IBM')) withlabel('zCEE Client Cert') signwith(certauth +
label('zCEE CA')) notafter(date(2022/12/31))

/* Create zCEE outbound key ring and connect certificates */
racdcert id(libserv) addring(zCEE.KeyRing)

racdcert id(libserv) connect(ring(zCEE.KeyRing) +
label('zCEE CA') certauth usage(certauth))

racdcert id(libserv) connect(ring(zCEE.KeyRing) +
label('Liberty CA') certauth usage(certauth))

/* Connect CA certificate to Liberty inbound key ring */
racdcert id(libserv) connect(ring(Liberty.KeyRing) +
label('zCEE CA') certauth usage(certauth))

/* Connect default personal certificate */
racdcert id(libserv) connect(ring(zCEE.KeyRing) +
label('zCEE Client Cert') default)

racdcert id(libserv) listring(zCEE.KeyRing)
racdcert id(libserv) list

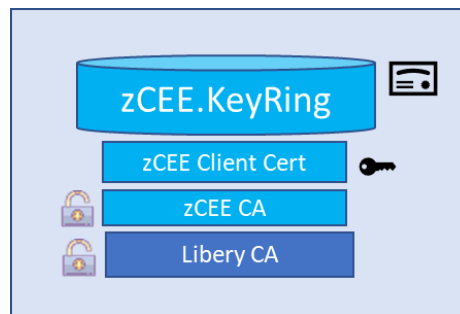
setr raclist(digtcert digtring) refresh

connect    libserv  group(zceeusrs)
connect    libserv  group(gminvoke)
```

These commands

- Define a personal certificate for the zCEE server for use during outbound handshakes.
- Define a key ring to be used for outbound handshakes.
- Connect the zCEE server personal certificate to this key ring.
- Connect the certificate authority (CA) public certificate used to sign the zCEE server's outbound personal certificate to this key ring.
- Connect the certificate authority (CA) public certificate used to sign the API provider server's certificate to this key ring.
- Connects the certificate authority (CA) public certificate used to sign the zCEE server's outbound personal certificate to the API provider's key ring.
- User LIBSERV is given the required authority to access their key ring and certificate.
- The in-storage profile for digital certificates resources are refreshed.
- User LIBSERV is connected to the groups that provide access to this zCEE instance.

Below is visual representation of the key ring just created



3. Edit the *server.xml* configuration file for the *myServer* server, located in directory */var/zosconnect/servers/myServer* and change the include for file *keyringMutual.xml* to an include of file *keyringOutboundMutua.xml*, see below:

```
<include location="/${server.config.dir}/includes/keyringOutboundMutual.xml"/>
```

___4. Next, browse member **IMSTLS**, you should see the RACF commands below. Submit the job for execution.

```
/* Create a CA certificate for IMS */
racdcert certauth gencert subjectsdn(cn('IMS CA') ou('ATS') +
ou('ATS') o('IBM')) withlabel('IMS CA') keyusage(certsign) +
notafter(date(2022/12/31))

/* Create a server certificate for IMS client request */
racdcert id(IMSSTC) gencert subjectsdn(cn('wg31.washington.ibm.com') +
ou('ATS') o('IBM')) withlabel('IMSSTC') signwith(certauth +
label('IMS CA')) notafter(date(2021/12/31))

setr raclist(digtcert,digtnmap) refresh

/* Create IMS key ring and connect CA and personal certificates */
racdcert id(IMSSTC) addring(IMS.KeyRing)

racdcert id(IMSSTC) connect(ring(IMS.KeyRing) +
label('IMS CA') certauth usage(certauth))

racdcert id(IMSSTC) connect(ring(IMS.KeyRing) +
label('zCEE CA') certauth usage(certauth))

racdcert id(libserv) connect(ring(zCEE.KeyRing) +
label('IMS CA') certauth usage(certauth))

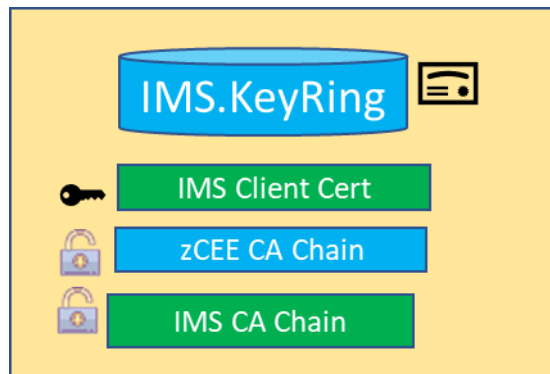
/* Connect default personal certificate */
racdcert id(IMSSTC) connect(ring(IMS.KeyRing) +
label('IMSSTC') default

setropts raclist(digtring,digtnmap) refresh
```

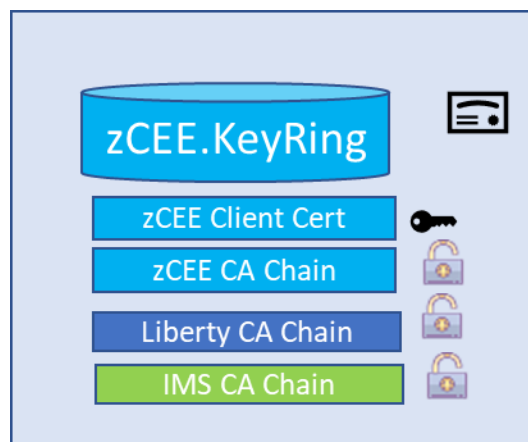
These commands

- Define a certificate authority certificate used to sign IMS certificates used during TLS handshakes.
- Define a personal certificate for the IMS server for use during TLS handshakes.
- Define a key ring to be used for TLS handshakes.
- Connect the IMS server personal certificate to this key ring.
- Connect the certificate authority (CA) public certificate used to sign the IMS server's certificate to this key ring.
- Connect the certificate authority (CA) public certificate used to sign the zCEE server's outbound personal certificate to this key ring.
- The in-storage profile for digital certificates resources are refreshed.

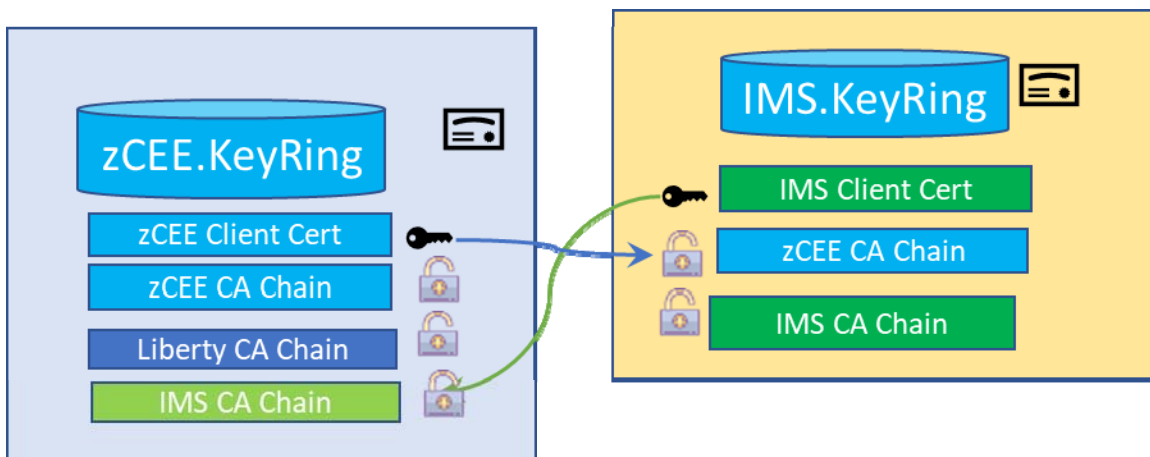
Below is visual representation of the key ring just created



The update made to the zCEE server's outbound keyring



And the handshakes will flow as shown below



5. Edit the *server.xml* configuration file for the *myServer* server, found in directory */var/zosconnect/servers/myServer* and change the include for file *keyringMutual.xml* to an include of file *keyringOutBoundMutual.xml*, see below:

```
<include location="{server.config.dir}/includes/keyringOutboundMutual.xml"/>
```

```
<include location="{server.config.dir}/includes/safSecurity.xml"/>
<include location="{server.config.dir}/includes/ipicIDProp.xml"/>
<include location="{server.config.dir}/includes/keyringOutboundMutual.xml"/>
<include location="{server.config.dir}/includes/groupAccess.xml"/>
<include location="{server.config.dir}/includes/apiRequesterHTTPS.xml"/>
<include location="{server.config.dir}/includes/imsDatabasePassTicket.xml"/>
<include location="{server.config.dir}/includes/db2.xml"/>
<include location="{server.config.dir}/includes/shared.xml"/>
```

The contents of *keyringOutboundMutual.xml* are shown below:

```
<!-- Enable features -->
<featureManager>
  <feature>transportSecurity-1.0</feature>
</featureManager>

<sslDefault sslRef="DefaultSSLSettings"
  outboundSSLRef="OutboundSSLSettings" />

<ssl id="DefaultSSLSettings"
  keyStoreRef="CellDefaultKeyStore"
  trustStoreRef="CellDefaultKeyStore"
  clientAuthenticationSupported="true"
  clientAuthentication="true"/>

<keyStore id="CellDefaultKeyStore"
  location="safkeyring:///Keyring.LIBERTY"
  password="password" type="JCERACFKS"
  fileBased="false" readOnly="true" />

<ssl id="OutboundSSLSettings"
  keyStoreRef="OutboundKeyStore"
  trustStoreRef="OutboundKeyStore"/>

<keyStore id="OutboundKeyStore"
  location="safkeyring:///zCEE.KeyRing"
  password="password" type="JCERACFKS"
  fileBased="false" readOnly="true" />
```

- ___6. Enter MVS commands *P BAQSRT and S BASSTR* to refresh the zCEE server's runtime configuration.

Tech-Tip: Updates to keyrings could have been refreshed in the server by using this command :

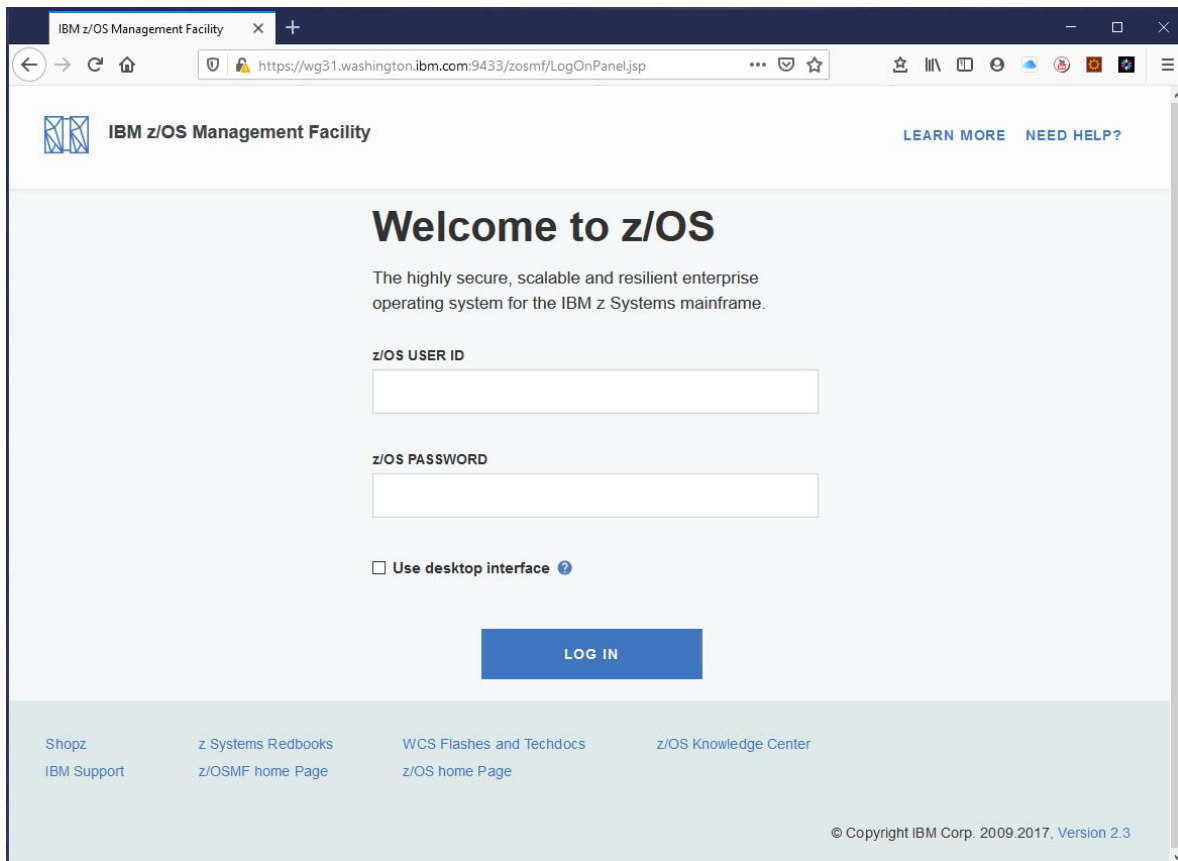
F BAQSTR,REFRESH,KEYSTORE

This would have dynamically made the information about IMS CA certificate available in the zCEE runtime

Configure the AT-TLS policies

z/OSMF will be used in this section to configure the AT-TLS configuration for the desired inbound and outbound policies.

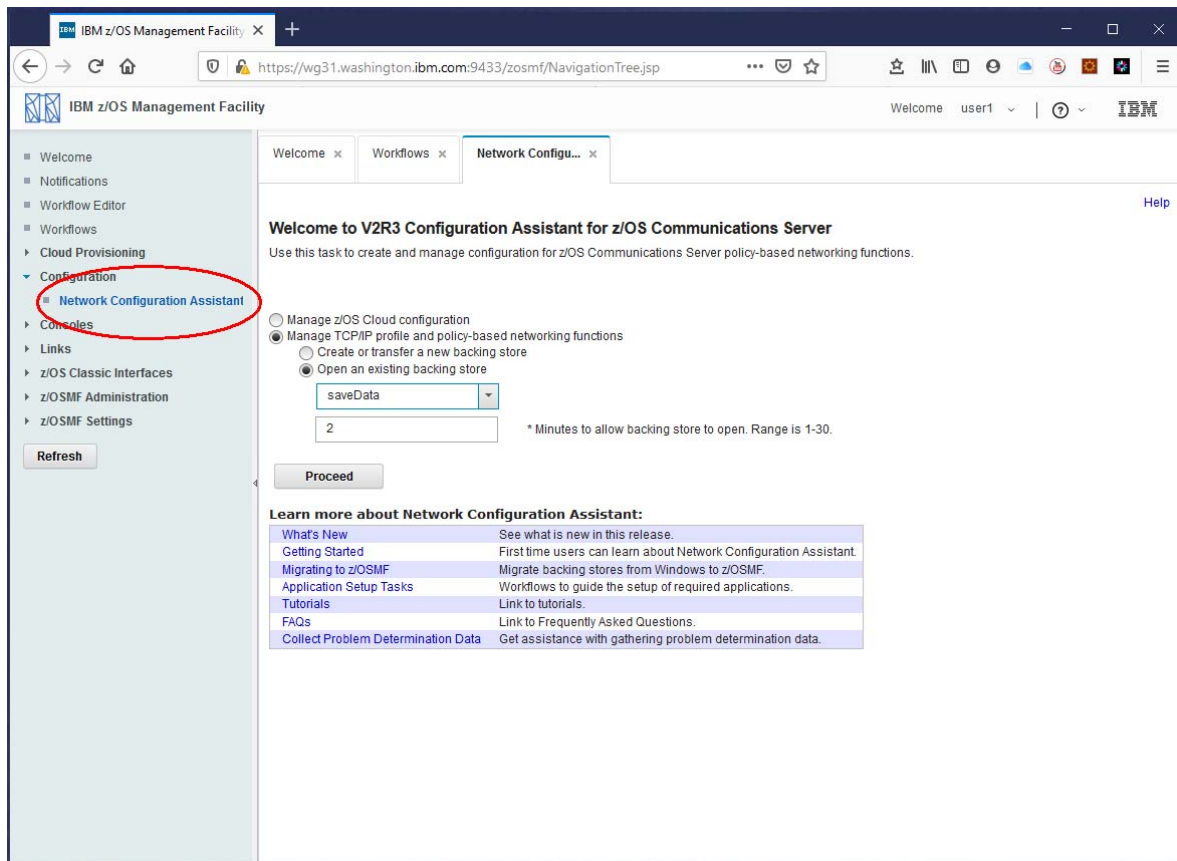
1. In a Firefox browser enter URL <https://wg31.washington.ibm.com:9433/zosmf> and you should see the *IBM z/OS Management Facility* window.



Note that some of the AT-TLS configuration steps described here may have been performed in another exercise.

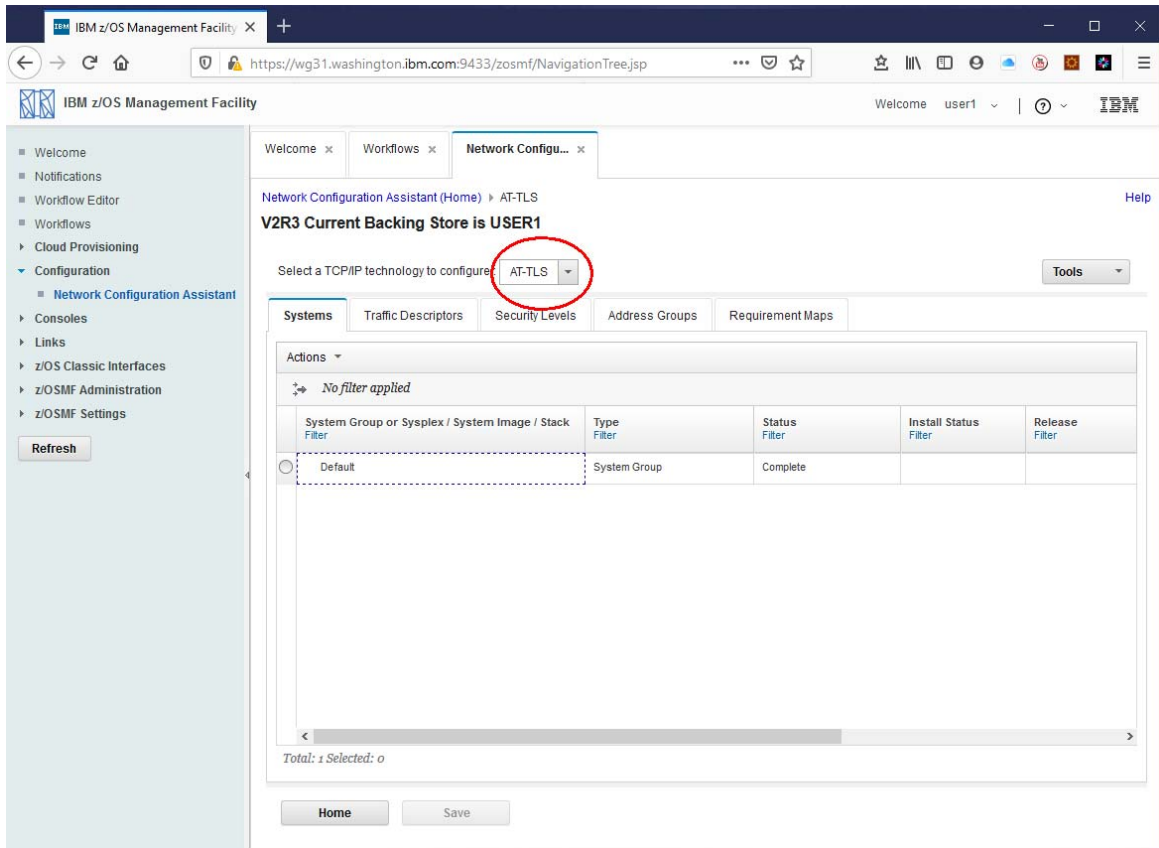
2. Enter *USER1* as the *z/OS USER ID* and *USER1*'s password and click the **LOG IN** button.

- ___3. The *Welcome* screen should be displayed. On the left-hand side expand the *Configuration* tab to expose the *Network Configuration Assistance* option. Select this option to expose the *Network Configuration* tab.

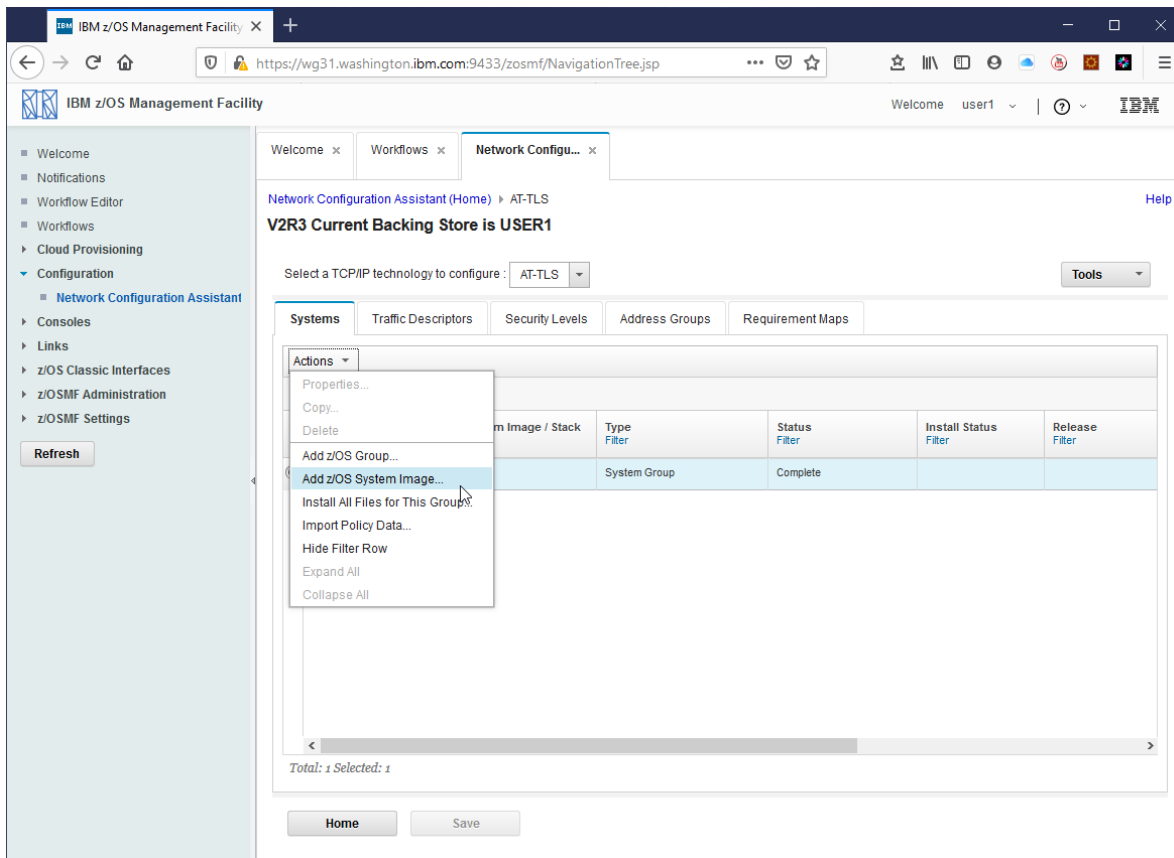


- ___4. Select the radio button beside *Create or transfer a new backing store* option and click the **Proceed** button.
- ___5. On the next screen select the radio button beside *Create a New Backing Store File* and enter **USER1** in the area beside *File Name*. Press the **OK** button and press the **OK** button on the Information pop-up.

___6. On the *Network Configuration* tab use the pull-down arrow to select *AT-TLS* as the *TCP/IP technology* to configure.



- ___7. Select the radio button beside the *Default - System Group* and use the *Action* pull-down button to select *Add z/OS System Image* option.



- ___8. On the *Add z/OS System Image* window enter **WG31** for the image *Name* and check the radio button beside *Simple name (as in an SAF product...)* and enter **Liberty.KeyRing** as the default AT-TLS key ring name. Click **OK** to continue.

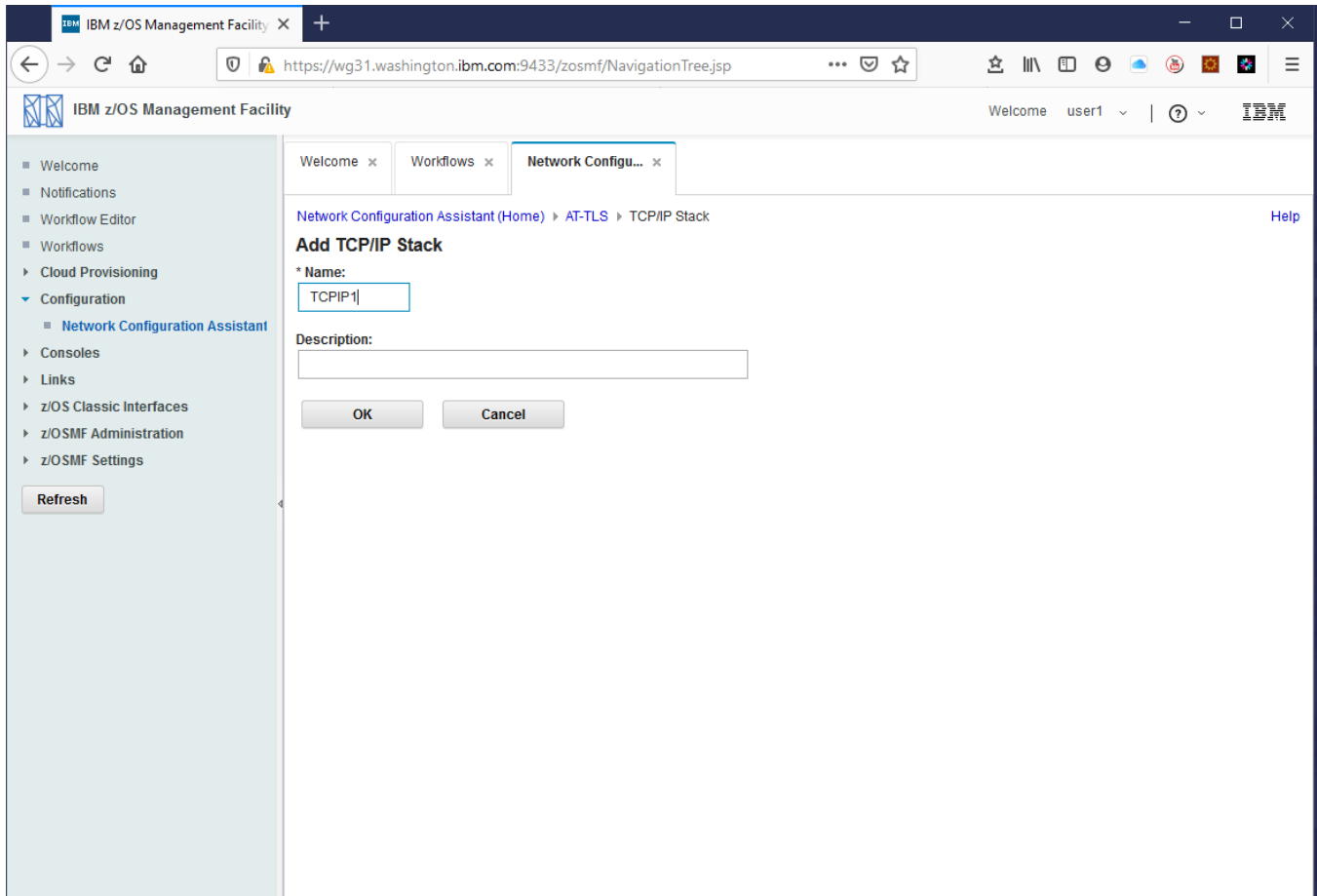
The screenshot shows the 'Add z/OS System Image' dialog in the IBM z/OS Management Facility. The 'Name' field is set to 'WG31'. The 'z/OS Release' is set to 'V2R3'. Under the 'Default AT-TLS key ring database' section, the 'Simple name (as in an SAF product or in PKCS #11 token format)' radio button is selected, and the 'Key ring' field is set to 'Liberty.KeyRing'. The 'OK' button is highlighted.

Tech Tip: The value for the key ring will be used if an explicit key ring is not provided for a policy in a *Traffic Descriptor*.

We recommend establishing a naming convention for key rings with each SAF identity using the same key ring name in the same context. Using this name as an example you could create a unique key ring named *Liberty.KeyRing* for SAF identities USER1, USER2, FRED, etc. Each user's key ring would have the same name but a different set of connected certificates. One default key ring specified at the image level covers all users.

- ___9. On the *Proceed to the Next Step?* pop-up click the **Proceed** button.

10. The *Add TCP/IP Stack* screen should be displayed. Select this option to expose the *Network Configuration* tab. Enter **TCPIP1** as the name of the stack. Click **OK** to continue.



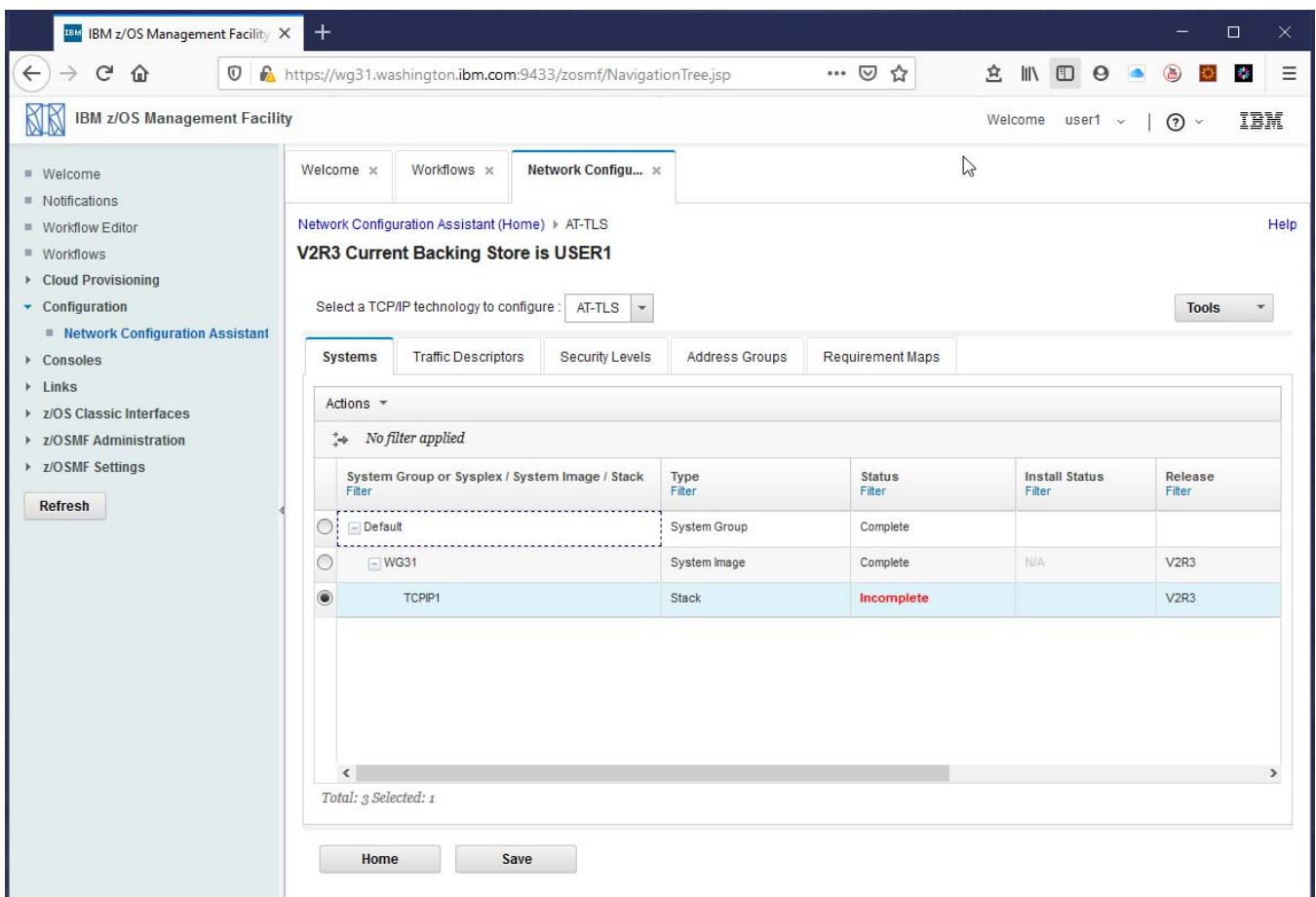
Tech-Tip: The value for the stack name was determined by the TCPIP Name display by entering the MVS command D TCPIP.

```
EZAOP50I TCPIP STATUS REPORT 007
COUNT   TCPIP NAME   VERSION   STATUS
-----
      1   TCPIP1      CS V2R3   ACTIVE
*** END TCPIP STATUS REPORT ***
EZAOP41I 'DISPLAY TCPIP' COMMAND COMPLETED SUCCESSFULLY
```

- ___11. Before any TCP/IP stack rules can be added, *Traffic Descriptors*, *Address Groups* and *Requirement Maps* need to be defined. Click **Cancel** on the *Proceed to the Next Step?* displayed at this time.

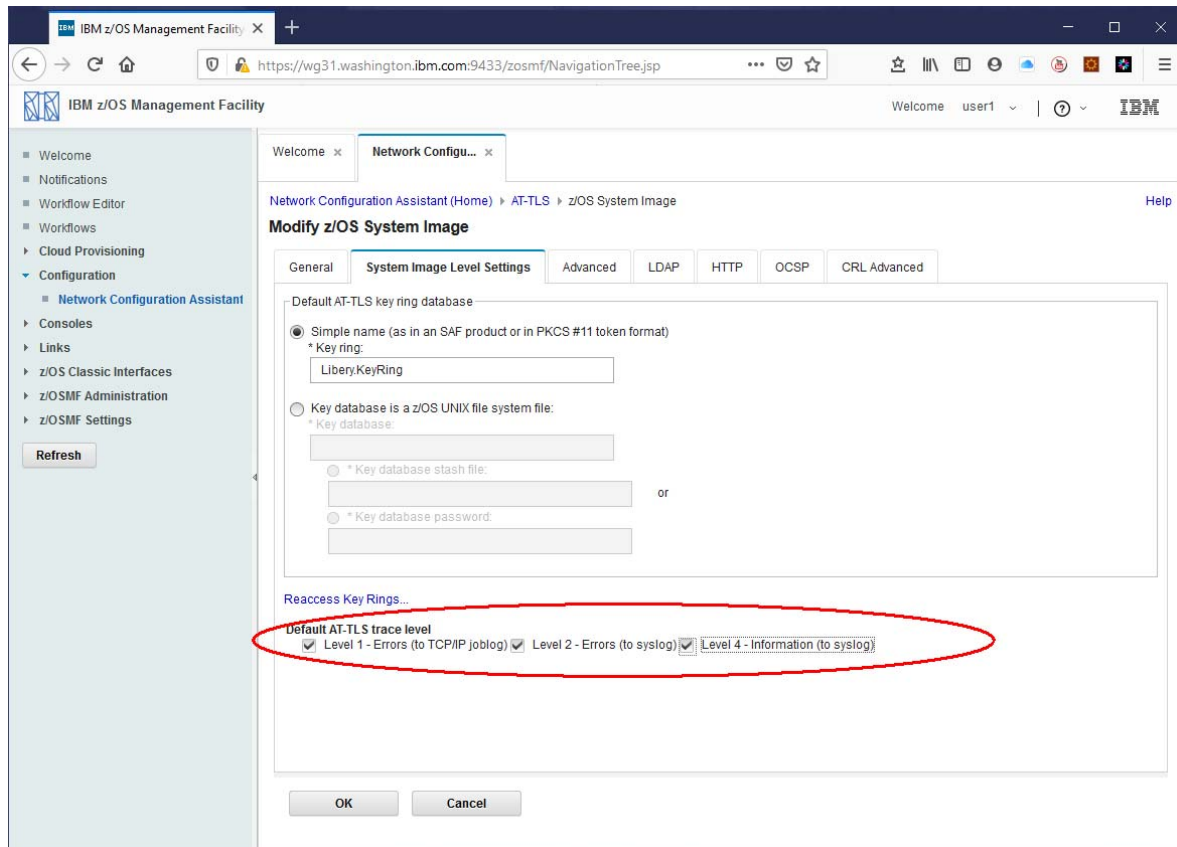


- ___12. This will display the window below:

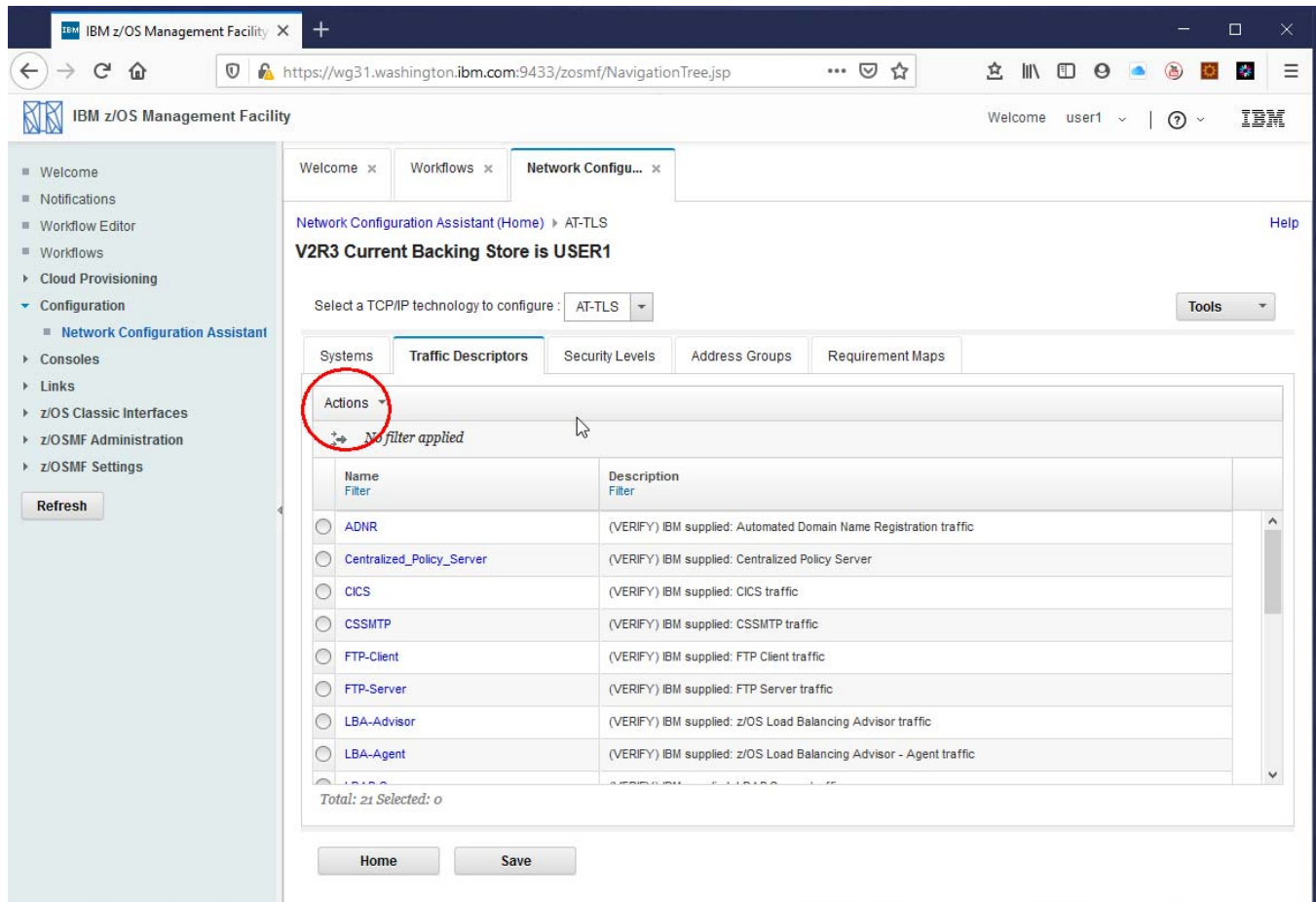


Tech Tip: The **Incomplete** warning will be addressed shortly.

13. Select the radio button beside *WG31* and use the *Actions* pull-down to select *Properties*. On the *Modify z/OS System Image* window select the *System Image Level Settings* tab and check all the trace level boxes as shown below. This is being done so we can confirm AT-TLS is being invoked and identify issues. Press **OK** to continue.



___14. Select the *Traffic Descriptors* tab and use the *Actions* pull-down to select *New*.



The screenshot shows the IBM z/OS Management Facility Network Configuration Assistant (Home) page. The 'Traffic Descriptors' tab is selected, and the 'Actions' pull-down menu is open, showing a list of traffic descriptors. The 'New' action is highlighted.

Network Configuration Assistant (Home) > AT-TLS

V2R3 Current Backing Store is USER1

Select a TCP/IP technology to configure: AT-TLS

Tools

Systems Traffic Descriptors Security Levels Address Groups Requirement Maps

Actions

No filter applied

| Name Filter | Description Filter |
|---|--|
| <input type="radio"/> ADNR | (VERIFY) IBM supplied: Automated Domain Name Registration traffic |
| <input type="radio"/> Centralized_Policy_Server | (VERIFY) IBM supplied: Centralized Policy Server |
| <input type="radio"/> CICS | (VERIFY) IBM supplied: CICS traffic |
| <input type="radio"/> CSSMTP | (VERIFY) IBM supplied: CSSMTP traffic |
| <input type="radio"/> FTP-Client | (VERIFY) IBM supplied: FTP Client traffic |
| <input type="radio"/> FTP-Server | (VERIFY) IBM supplied: FTP Server traffic |
| <input type="radio"/> LBA-Advisor | (VERIFY) IBM supplied: z/OS Load Balancing Advisor traffic |
| <input type="radio"/> LBA-Agent | (VERIFY) IBM supplied: z/OS Load Balancing Advisor - Agent traffic |

Total: 21 Selected: 0

Home Save

15. On the *New Traffic Descriptor* window enter **IMSConnectDB** as the name and use the *Actions* pull-down and select *New* to start the definition of a new traffic descriptor type.

IBM z/OS Management Facility on WG31.DMZ — Mozilla Firefox

IBM z/OS Management Facility

Welcome user1

Network Configuration Assistant (Home) > AT-TLS > Traffic Descriptor

New Traffic Descriptor

Traffic descriptors contain details of traffic types which are mapped to security levels within requirement maps. A traffic descriptor can contain a single type of traffic or multiple types of traffic.

* Name:

Description:

List of traffic types in this traffic descriptor

| Protocol | Local Port | Remote Port | Connect Direction | Job Name | User ID |
|------------------------------|------------|-------------|-------------------|----------|---------|
| There is no data to display. | | | | | |

Total: 0 Selected: 0

OK Cancel

16. On the *New Traffic Type – TCP* window select the radio button beside *Single ports* under *Local port* and enter **5555** as the port number. Select the radio button *All ports* under *Remote port*. Select the radio button beside *Inbound only* under *Indicate the TCP connection direction*. Enter **IMS15HWS** in the area under *Jobname* and finally select the radio button beside *Server* under *AT-TLS Handshake Role*. Next click on the *KeyRing* tab to continue.

The screenshot shows the IBM z/OS Management Facility Network Configuration Assistant (Home) - AT-TLS - Traffic Descriptor - Traffic Type - TCP. The 'New Traffic Type - TCP' window is open, showing configuration options for Local port, Remote port, TCP connection direction, Jobname, User ID, and AT-TLS Handshake Role.

Local port:

- ☐ All ports
- ☒ Single port (5,555)
- ☐ Port range (Lower port: 100, Upper port: 101)
- ☐ Ephemeral ports

Remote port:

- ☒ All ports
- ☐ Single port (100)
- ☐ Port range (Lower port: 100, Upper port: 101)
- ☐ Ephemeral ports

Indicate the TCP connect direction:

- ☐ Either
- ☒ Inbound only
- ☐ Outbound only

Jobname: IMS15HWS

User ID:

AT-TLS Handshake Role:

- ☒ Server
- ☐ Client

Client authentication role is set in the security level.

Buttons: OK, Cancel

Tech-Tip: This traffic definition is triggered when a client attempts to connect to port 5555. Port 5555 was identified in the IMS Connect configuration.

```
HWS=(ID=IMS15HWS,XIBAREA=100,RACF=Y,RRS=Y)
TCPIP=(HOSTNAME=TCPIP,PORTID=(4000,LOCAL),RACFID=JOHNSON,TIMEOUT=5000)
DATASTORE=(GROUP=OTMAGRP,ID=IVP1,MEMBER=HWSMEM,DRU=HWSYDRU0,
TMEMBER=OTMAMEM,APPL=IMSAPPL)
ODACCESS=(ODBMAUTOCONN=Y,IMSPLEX=(MEMBER=IMS15HWS,TMEMBER=PLEX1),
DRDAPORT=(ID=5555,PORTTMOT=6000),ODBMTMOT=6000,APPL=IMSAPPL)
```

If all the defined conditions are met, AT-TLS will act as a surrogate for the server during a TLS handshake. Note the *KeyRing* tab can be used to specify the name of the key ring to be used for this handshake, e.g. IMS.KeyRing. Otherwise the default is to use the same key ring name defined for the z/OS System image, e.g. Liberty.KeyRing.

- ___17. On the *KeyRing* tab select the radio button beside *Use a Simple name* and enter **IMS.KeyRing** as the key ring name. Click **OK** twice to continue.

IBM z/OS Management Facility on WG31.DMZ - Mozilla Firefox

File Edit View History Bookmarks Tools Help

IBM z/OS Management Facility x +

https://wg31.washington.ibm.com:9433/zosmf/NavigationTree.jsp

IBM z/OS Management Facility Welcome user1 | ? IBM

Network Configuration Assistant (Home) > AT-TLS > Traffic Descriptor > Traffic Type - TCP Help

New Traffic Type - TCP

Details KeyRing Advanced

Specify the key ring database to use for the traffic type specified on the Details tab.

☐ Use the key ring database defined for the z/OS system image.

☒ Use a Simple name (as in a SAF product or in PKCS #11 Token format):

* Key ring:

IMS.KeyRing

☐ Use this z/OS UNIX file system key database:

* Key database:

* Key database stash file:

* Key database password:

Certificate Label:

☐ Specified server certificate labels to be used by server to accommodate clients with different types of public keys. The certificates are in V2R3.

Actions

| Certificate Label | Name | Cert Owner | USAGE | DEFAULT |
|-------------------|------|---------------|----------|---------|
| IMS CA | | CERTAUTH | CERTAUTH | NO |
| zCEE CA | | CERTAUTH | CERTAUTH | NO |
| IMSSTC | | ID (IMSSTC) | PERSONAL | YES |

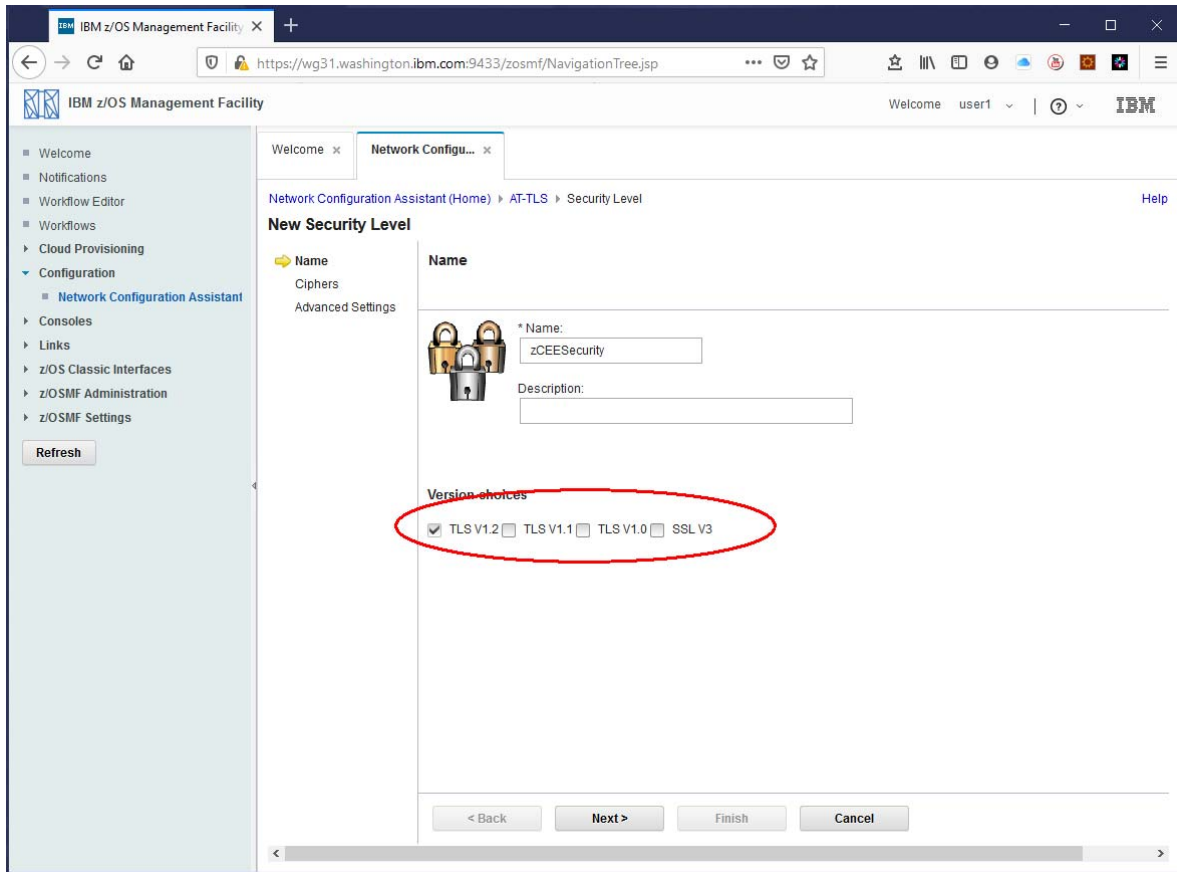
Tech Tip: The key ring specified here belongs to identity IMSSTC. This is the identity under which the IMS Connect task is running. This ring has these certificates connected.

Ring:

```
>IMS.KeyRing<
```

| Certificate Label | Name | Cert Owner | USAGE | DEFAULT |
|-------------------|------|---------------|----------|---------|
| IMS CA | | CERTAUTH | CERTAUTH | NO |
| zCEE CA | | CERTAUTH | CERTAUTH | NO |
| IMSSTC | | ID (IMSSTC) | PERSONAL | YES |

18. Next, click the *Security Levels* tab and use the *Actions* pull-down button and to select the *New* option. On the *New Security Level* windows, enter **zCEESecurity** for the *Name* and check the box beside *TLS V1.2* and uncheck the other boxes. Click **Next** to display the *Cipher selection* options. Click **Next** to display the *Advanced Settings* options exploring as you like but there is no need to make any changes. Click **Finish** to continue.



___19. Next, click the *Requirement Maps* tab. Use the *Actions* pull-down button and to select the *New* option.

IBM z/OS Management Facility

Welcome user1

Network Configuration Assistant (Home) > AT-TLS

V2R3 Current Backing Store is USER1

Select a TCP/IP technology to configure: AT-TLS

Tools

Systems Traffic Descriptors Security Levels Address Groups **Requirement Maps**

Actions

No filter applied

| Name Filter | Description Filter |
|----------------|--|
| AT-TLS_Sample | IBM supplied: AT-TLS sample: CICS and TN3270 |

Total: 1 Selected: 1

Home Save

20. On the *New Requirement Map* window enter **IMSDBRequirementMap** as the *Name* and use the pull-down arrows to select **IMSConnectDB** as the *Traffic Descriptor* and **zCEESecurity** as the *Security Level* for this map. Click **OK** to continue.

IBM z/OS Management Facility on WG31.DMZ — Mozilla Firefox

IBM z/OS Management Facility x +

https://wg31.washington.ibm.com:9433/zosmf/NavigationTree.jsp

Welcome user1 | ? v IBM

■ Welcome
■ Notifications
■ Workflow Editor
■ Workflows
▶ Cloud Provisioning
▼ Configuration
 ■ Network Configuration Assistant
▶ Consoles
▶ Links
▶ z/OS Classic Interfaces
▶ z/OSMF Administration
▶ z/OSMF Settings

Refresh

Welcome x Network Configu... x

Network Configuration Assistant (Home) ▶ AT-TLS ▶ Requirement Map Help

Modify Requirement Map

A requirement map is an object that maps each IP traffic type (traffic descriptor) to a specific level of security (security level).

To add a new mapping to the requirement map:

1. Click the "Add Row" action or use an existing row
2. Click a table cell to select a traffic descriptor from the list
3. Click a table cell to select a security level from the list

* Name:
IMSDBRequirementMap

Description:

Mappings table

| Actions | | Move Up | Move Down |
|-----------------------|--------------------|----------------|-----------|
| | Traffic Descriptor | Security Level | |
| <input type="radio"/> | IMSConnectDB | zCEESecurity | |

Total: 1 Selected: 0

OK Cancel

- ___21. Select the radio button beside *IMSDBRequirementMap*. Use the *Actions* pull-down to select the *View Details* options to display the window below. Review the details and click the **Close** button to continue.

IBM z/OS Management Facility on WG31.DMZ — Mozilla Firefox

IBM z/OS Management Facility x +

https://wg31.washington.ibm.com:9433/zosmf/NavigationTree.jsp

IBM z/OS Management Facility Welcome user1 | ? IBM

Network Configuration Assistant (Home) > AT-TLS > View Details Help

View Details

Close Printable page

Application / Requirement Map: IMSDBRequirementMap

Requirement map summary

| | |
|--------------------|-----------------------|
| Traffic Descriptor | AT-TLS Security Level |
| IMSConnectDB | zCEESESecurity |

Requirement Map traffic - Shown in Configured Order

| Traffic Descriptor | | | | | AT-TLS Security Level | |
|--------------------|----------|------------|-------------|-------------------|-----------------------|--|
| Name | Protocol | Local Port | Remote Port | Connect Direction | Name | Ciphers |
| IMSConnectDB | TCP | 5555 | All Ports | Inbound | zCEESESecurity | TLS Version 1: System SSL V3 Defaults |

=====

Security Level Details

=====

Security Level: zCEESESecurity

Type:
AT-TLS

Encryption:
System SSL V3 Defaults

Use TLS Version 1.0:
No

Use TLS Version 1.1:
Yes

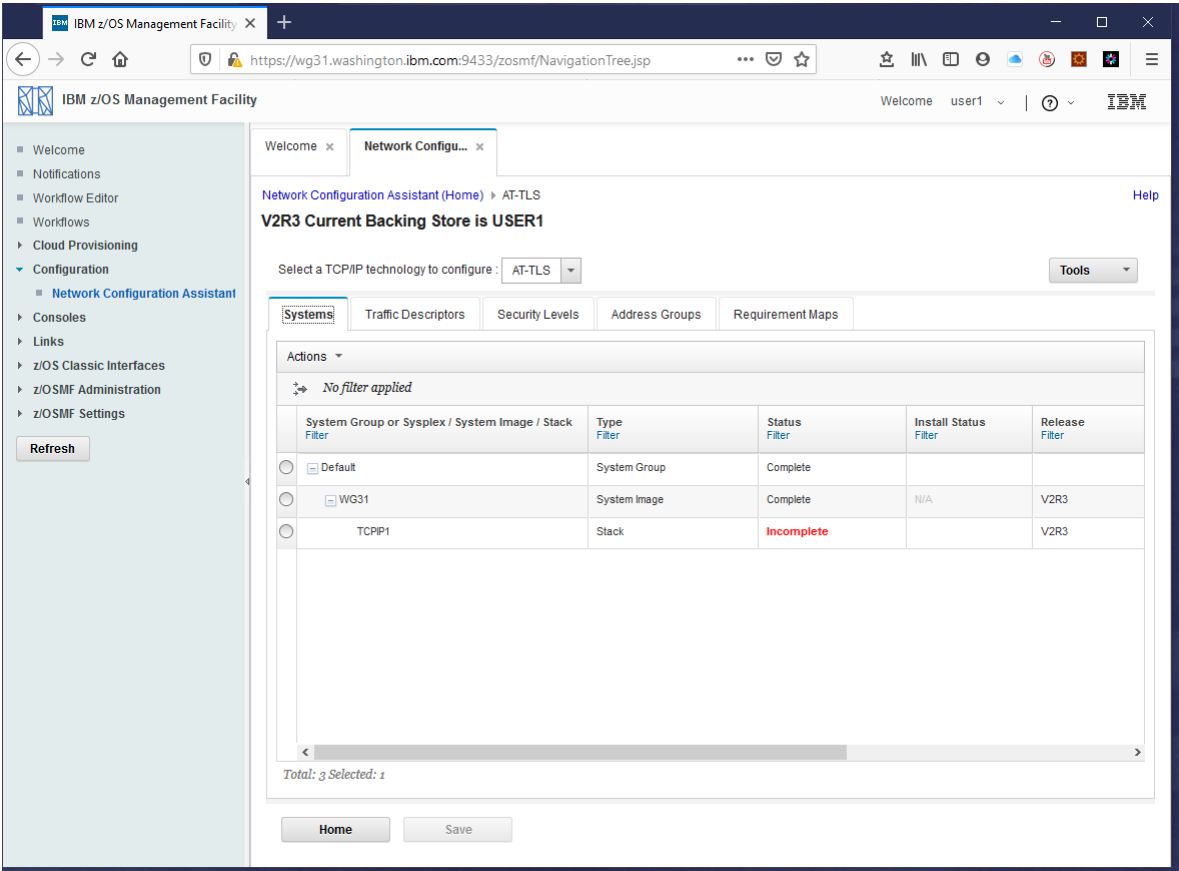
Use TLS Version 1.2:
Yes

Use SSL Version 3:
No

Close Back to Top

- ___22. Click the **Save** button to save the configuration.

23. When the save has complete click on the *Systems* tab to return to this window.



24. Select the radio button beside *TCPIPI1*. Use the *Actions* pull-down to select *Rules*. This is where these definitions will be tied together. Use the *Actions* pull-down again and select *New* to create a new connectivity rule. Enter ***IMSDBCConnectRule*** for the *Connectivity rule name* and press **Next** to continue.

IBM z/OS Management Facility on WG31.DMZ — Mozilla Firefox

IBM z/OS Management Facility x +

https://wg31.washington.ibm.com:9433/zosmf/NavigationTree.jsp

Welcome user1 | ? IBM

Network Configuration Assistant (Home) > AT-TLS > TCP/IP Stack > Connectivity Rule Help

New Connectivity Rule

Data Endpoints

Requirement Map
Advanced Settings

* Connectivity rule name:
IMSDBCConnectRule

Select the address groups of the host endpoints of the traffic you want to protect.

Local data endpoint

☒ Address group:
All_IPv4_Addresses

☐ * IPv4 or IPv6 address, subnet, or range:
Examples: xxx.xxxx, xxx.x/yy, xxx.x-yy.zy
xx, x.x/yyy, x.x-y.zy

Remote data endpoint

☒ Address group:
All_IPv4_Addresses

☐ * IPv4 or IPv6 address, subnet, or range:
Examples: xxx.xxxx, xxx.x/yy, xxx.x-yy.zy
xx, x.x/yyy, x.x-y.zy

< >

< Back Next > Finish Cancel

25. On the *New Connectivity Rule – Requirement Map* window select the radio button beside *Select an existing requirement map* and use the pull-down to select *IMSDBRequirementMap*. This should automatically populate the mapping table with *IMSDBConnect* as the traffic descriptor and *zCEESecurity* as the security level. Press **Next** and then **Finish** to continue.

IBM z/OS Management Facility on WG31.DMZ — Mozilla Firefox

IBM z/OS Management Facility x +

https://wg31.washington.ibm.com:9433/zosmf/NavigationTree.jsp

Welcome user1 | ? IBM

Network Configuration Assistant (Home) > AT-TLS > TCP/IP Stack > Connectivity Rule

New Connectivity Rule

☒ Data Endpoints
☒ Requirement Map
 Advanced Settings

Requirement Map

Requirement maps are reusable objects that combine your traffic definitions (traffic descriptors) with your security definitions (security levels).

☐ Create a new requirement map
☒ Select an existing requirement map

IMSDBRequirementMap

IMSDBRequirementMap properties

* Name: IMSDBRequirementMap

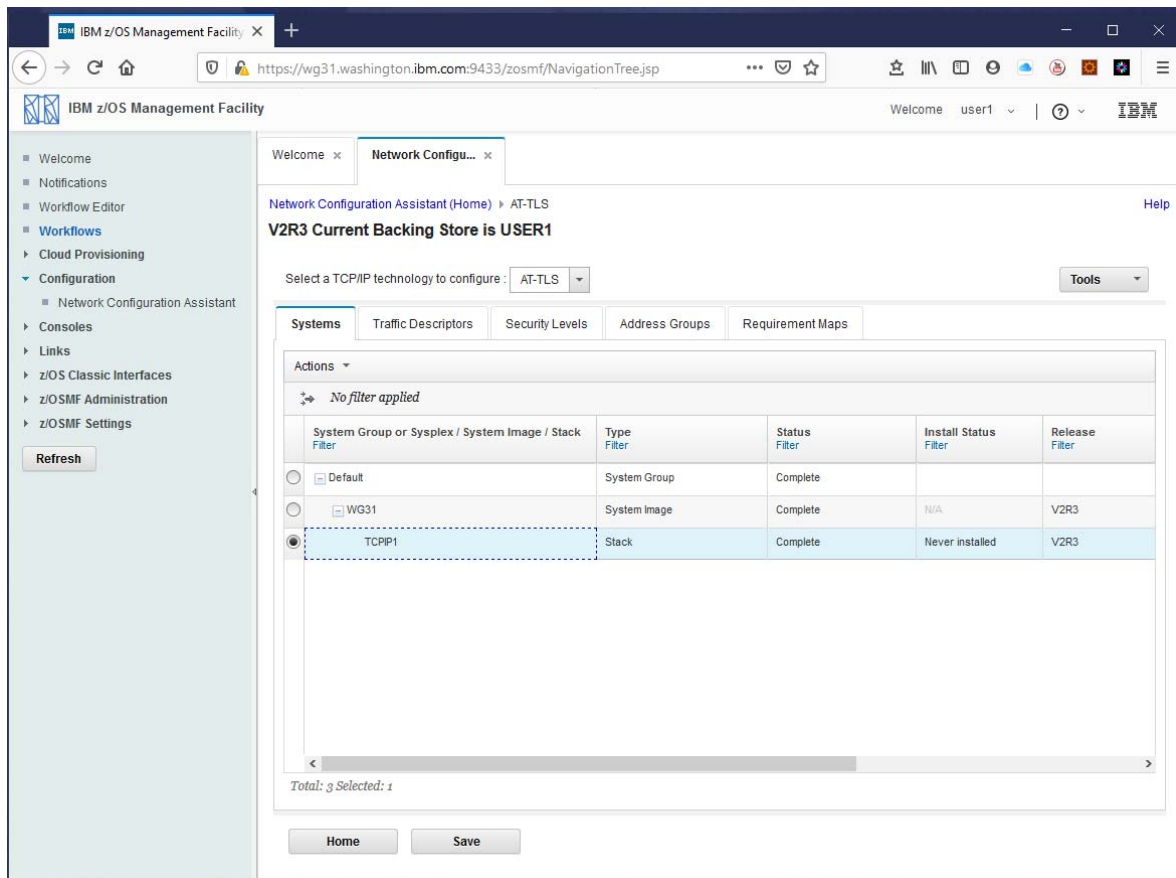
Description:

Mappings table

| Traffic Descriptor | Security Level |
|--------------------|----------------|
| IMSConnectDB | zCEESecurity |

< Back Next > Finish Cancel

26. Press **Close** to return to this window. Note that the status of the configuration is now complete.



This completes the configuration of the inbound policy for the server side of the handshake. Now an outbound policy for the client side of the handshake needs to be configured

27. Select the *Traffic Descriptors* tab. Use the *Actions* pull-down to select *New*.

IBM z/OS Management Facility on WG31.DMZ - Mozilla Firefox

File Edit View History Bookmarks Tools Help

IBM z/OS Management Facility x +

https://wg31.washington.ibm.com:9433/zosmf/NavigationTree.jsp

Welcome user1 | IBM

IBM z/OS Management Facility

Welcome x Network Configu... x

Network Configuration Assistant (Home) > AT-TLS Help

V2R3 Current Backing Store is USER1

Select a TCP/IP technology to configure: AT-TLS Tools

Systems Traffic Descriptors Security Levels Address Groups Requirement Maps

Actions

No filter applied

| Name Filter | Description Filter |
|---|--|
| <input checked="" type="radio"/> IMSConnect | |
| <input type="radio"/> ADNR | (VERIFY) IBM supplied: Automated Domain Name Registration traffic |
| <input type="radio"/> Centralized_Policy_Server | (VERIFY) IBM supplied: Centralized Policy Server |
| <input type="radio"/> CICS | (VERIFY) IBM supplied: CICS traffic |
| <input type="radio"/> CSSMTP | (VERIFY) IBM supplied: CSSMTP traffic |
| <input type="radio"/> FTP-Client | (VERIFY) IBM supplied: FTP Client traffic |
| <input type="radio"/> FTP-Server | (VERIFY) IBM supplied: FTP Server traffic |
| <input type="radio"/> LBA-Advisor | (VERIFY) IBM supplied: z/OS Load Balancing Advisor traffic |
| <input type="radio"/> LBA-Agent | (VERIFY) IBM supplied: z/OS Load Balancing Advisor - Agent traffic |
| <input type="radio"/> LBA-Server | (VERIFY) IBM supplied: LBA-Server traffic |

Total: 22 Selected: 1

Home Save

28. On the *New Traffic Descriptor* window enter **IMSDBClient** as the name. Use the *Actions* pull-down and select *New* to start the definition of a new traffic descriptor type.

IBM z/OS Management Facility on WG31.DMZ — Mozilla Firefox

IBM z/OS Management Facility x +

https://wg31.washington.ibm.com:9433/zosmf/NavigationTree.jsp

Welcome user1 | ? IBM

Welcome x Network Configu... x

Network Configuration Assistant (Home) > AT-TLS > Traffic Descriptor Help

New Traffic Descriptor

Traffic descriptors contain details of traffic types which are mapped to security levels within requirement maps. A traffic descriptor can contain a single type of traffic or multiple types of traffic.

* Name:

Description:

List of traffic types in this traffic descriptor

| Protocol | Local Port | Remote Port | Connect Direction | Job Name | User ID |
|------------------------------|------------|-------------|-------------------|----------|---------|
| There is no data to display. | | | | | |

Total: 0 Selected: 0

OK Cancel

29. On the *New Traffic Type – TCP* window, select the radio button beside *Ephemeral ports* under *Local port*/. Select the radio button *Single ports* under *Remote port* and enter **5555**. Select the radio button beside *Outbound only* under *Indicate the TCP connection direction*. Finally select the radio button beside *Client* under *AT-TLS Handshake Role*. Next click on the *KeyRing* tab to continue.

IBM z/OS Management Facility on WG31.DMZ - Mozilla Firefox

File Edit View History Bookmarks Tools Help

IBM z/OS Management Facility x +

https://wg31.washington.ibm.com:9433/zosmf/NavigationTree.jsp

IBM z/OS Management Facility Welcome user1 ? IBM

Network Configuration Assistant (Home) > AT-TLS > Traffic Descriptor > Traffic Type - TCP Help

New Traffic Type - TCP

Details KeyRing Advanced

Local port

☐ All ports

☐ Single port

5,555

☐ Port range

* Lower port: 100 * Upper port: 101

☒ Ephemeral ports

Remote port

☐ All ports

☒ Single port

5,555

☐ Port range

* Lower port: 100 * Upper port: 101

☐ Ephemeral ports

Indicate the TCP connect direction

☐ Either ☐ Inbound only ☒ Outbound only

Jobname:

User ID:

AT-TLS Handshake Role

☐ Server ☒ Client

Client authentication role is set in the security level.

OK Cancel

30. On the *KeyRing* tab select the radio button beside *Use a Simple name* and enter *zCEE.KeyRing* as the key ring name. Click **OK** twice to continue.

IBM z/OS Management Facility on WG31.DMZ - Mozilla Firefox

File Edit View History Bookmarks Tools Help

IBM z/OS Management Facility x +

https://wg31.washington.ibm.com:9433/zosmf/NavigationTree.jsp

Welcome user1 | ? IBM

Welcome x Network Configu... x

Network Configuration Assistant (Home) > AT-TLS > Traffic Descriptor > Traffic Type - TCP Help

New Traffic Type - TCP

Details KeyRing Advanced

Specify the key ring database to use for the traffic type specified on the Details tab.

☐ Use the key ring database defined for the z/OS system image.

☒ Use a Simple name (as in a SAF product or in PKCS #11 Token format):

* Key ring:

zCEE.KeyRing

☐ Use this z/OS UNIX file system key database:

* Key database:

* Key database stash file:

* Key database password:

Certificate Label:

☐ Specified server certificate labels to be used by server to accommodate clients with different types of public keys. The certificates are available beginning with V2R3.

Actions

| Certificate Label | Cert Owner | USAGE | DEFAULT |
|-------------------|-------------|----------|---------|
| zCEE CA | CERTAUTH | CERTAUTH | NO |
| Liberty CA | CERTAUTH | CERTAUTH | NO |
| zCEE Client Cert | ID(LIBSERV) | PERSONAL | YES |
| zCEE-CertAuth | CERTAUTH | CERTAUTH | NO |
| IMS CA | CERTAUTH | CERTAUTH | NO |

Tech Tip: The key ring specified here belongs to identity LIBSERV This is the identity under which the z/OS Connect server is running. This ring has these certificates connected.

Ring:

```
>zCEE.KeyRing<
```

| Certificate Label Name | Cert Owner | USAGE | DEFAULT |
|------------------------|-------------|----------|---------|
| zCEE CA | CERTAUTH | CERTAUTH | NO |
| Liberty CA | CERTAUTH | CERTAUTH | NO |
| zCEE Client Cert | ID(LIBSERV) | PERSONAL | YES |
| zCEE-CertAuth | CERTAUTH | CERTAUTH | NO |
| IMS CA | CERTAUTH | CERTAUTH | NO |

___31. Next, click the *Requirement Maps* tab. Use the *Actions* pull-down button and to select the *New* option.

The screenshot shows the IBM z/OS Management Facility web interface in a Mozilla Firefox browser. The address bar shows the URL: `https://wg31.washington.ibm.com:9433/zosmf/NavigationTree.jsp`. The page title is "IBM z/OS Management Facility". The left sidebar contains a navigation menu with items: Welcome, Notifications, Workflow Editor, Workflows, Cloud Provisioning, Configuration (selected), Consoles, Links, z/OS Classic Interfaces, z/OSMF Administration, and z/OSMF Settings. Under "Configuration", "Network Configuration Assistant" is selected. The main content area shows the "Network Configuration Assistant (Home)" page for "AT-TLS". A message states "V2R3 Current Backing Store is USER1". Below this, there is a dropdown menu for "Select a TCP/IP technology to configure:" set to "AT-TLS". The "Requirement Maps" tab is active, showing a table with two rows: "IMSRequirementMap" and "AT-TLS_Sample". The "AT-TLS_Sample" row has a description: "IBM supplied: AT-TLS sample: CICS and TN3270". At the bottom, there are "Home" and "Save" buttons.

IBM z/OS Management Facility on WG31.DMZ - Mozilla Firefox

File Edit View History Bookmarks Tools Help

IBM z/OS Management Facility x

https://wg31.washington.ibm.com:9433/zosmf/NavigationTree.jsp

Welcome user1 | ? IBM

Welcome x Network Configur... x

Network Configuration Assistant (Home) > AT-TLS Help

V2R3 Current Backing Store is USER1

Select a TCP/IP technology to configure: AT-TLS Tools

Systems Traffic Descriptors Security Levels Address Groups **Requirement Maps**

Actions

No filter applied

| Name Filter | Description Filter |
|---|--|
| <input type="radio"/> IMSRequirementMap | |
| <input type="radio"/> AT-TLS_Sample | IBM supplied: AT-TLS sample: CICS and TN3270 |

Total: 2 Selected: 0

Home Save

32. On the *New Requirement Map* window enter **IMSDBClientRequirementMap** as the *Name*. Use the pull-down arrows to select **IMSDBClient** as the *Traffic Descriptor* and **zCEESecurity** as the *Security Level* for this map. Click **OK** to continue.

IBM z/OS Management Facility on WG31.DMZ — Mozilla Firefox

IBM z/OS Management Facility x +

https://wg31.washington.ibm.com:9433/zosmf/NavigationTree.jsp

Welcome user1 | ? IBM

■ Welcome
■ Notifications
■ Workflow Editor
■ Workflows
▶ Cloud Provisioning
▼ Configuration
 ■ Network Configuration Assistant
▶ Consoles
▶ Links
▶ z/OS Classic Interfaces
▶ z/OSMF Administration
▶ z/OSMF Settings

Refresh

Welcome x Network Configu... x

Network Configuration Assistant (Home) ▶ AT-TLS ▶ Requirement Map Help

New Requirement Map

A requirement map is an object that maps each IP traffic type (traffic descriptor) to a specific level of security (security level).

To add a new mapping to the requirement map:

1. Click the "Add Row" action or use an existing row
2. Click a table cell to select a traffic descriptor from the list
3. Click a table cell to select a security level from the list

* Name:
IMSDBClientRequirementMap

Description:

Mappings table

| Actions ▼ Move Up Move Down | |
|---|---|
| Traffic Descriptor | Security Level |
| <input type="radio"/> IMSDBClient | <input type="radio"/> zCEESecurity |
| <input type="radio"/> Select a traffic descriptor | <input type="radio"/> Select a security level |
| <input type="radio"/> Select a traffic descriptor | <input type="radio"/> Select a security level |

Total: 3 Selected: 0

OK Cancel

- ___33. Select the radio button beside *IMSClientRequirementMap*, Use the *Actions* pull-down to select the *View Details* options to display the window below. Review the details and click the **Close** button to continue.

The screenshot shows the IBM z/OS Management Facility Network Configuration Assistant (NCA) interface. The left sidebar contains a navigation menu with options like Welcome, Notifications, Workflow Editor, Workflows, Cloud Provisioning, Configuration (selected), Consoles, Links, z/OS Classic Interfaces, z/OSMF Administration, and z/OSMF Settings. The main content area is titled 'Network Configuration Assistant (Home) > AT-TLS > View Details'. It displays the 'View Details' page for the 'Application / Requirement Map: IMSDBClientRequirementMap'. The page includes a 'Requirement map summary' table, a 'Requirement Map traffic - Shown in Configured Order' table, and 'Security Level Details' for the 'zCEESESecurity' level. The 'Security Level Details' section shows the type as 'AT-TLS', encryption as 'System SSL V3 Defaults', and various TLS/SSL version settings.

Requirement map summary

| Traffic Descriptor | AT-TLS Security Level |
|--------------------|-----------------------|
| IMSDBClient | zCEESESecurity |

Requirement Map traffic - Shown in Configured Order

| Traffic Descriptor | | | | | AT-TLS Security Level | |
|--------------------|----------|------------|-------------|-------------------|-----------------------|--|
| Name | Protocol | Local Port | Remote Port | Connect Direction | Name | Ciphers |
| IMSDBClient | TCP | 1024-65535 | 5555 | Outbound | zCEESESecurity | TLS Version 1: System SSL V3 Defaults |

Security Level Details

Security Level: zCEESESecurity

Type:
AT-TLS

Encryption:
System SSL V3 Defaults

Use TLS Version 1.0:
No

Use TLS Version 1.1:
Yes

Use TLS Version 1.2:
Yes

Use SSL Version 3:
No

- ___34. Click the **Save** button to save the configuration.

___35. When the save has complete click on the *Systems* tab to return to this window.

A connectivity rule for the IMS DB Client now needs to be added.

___36. Select the radio button beside *TCPIPI1*. Use the *Actions* pull-down to select *Rules*. This is where these client definitions will be tied together. Use the *Actions* pull-down again and select *New* to create a new connectivity rule. Enter ***IMSDBClientRule*** for the *Connectivity rule name* and press **Next** to continue.

IBM z/OS Management Facility on WG31.DMZ — Mozilla Firefox

IBM z/OS Management Facility x +

https://wg31.washington.ibm.com:9433/zosmf/NavigationTree.jsp

Welcome user1 | ? IBM

IBM z/OS Management Facility

Network Configuration Assistant (Home) > AT-TLS > TCP/IP Stack > Connectivity Rule Help

New Connectivity Rule

Data Endpoints

Requirement Map

Advanced Settings

* Connectivity rule name:

IMSDBClientRule

Select the address groups of the host endpoints of the traffic you want to protect.

Local data endpoint

☒ Address group:

All_IPv4_Addresses

☐ * IPv4 or IPv6 address, subnet, or range:

Examples: xxx.xxxx.yy, xxx-yy.yy
xx, xxxxyy, xx-yy

Remote data endpoint

☒ Address group:

All_IPv4_Addresses

☐ * IPv4 or IPv6 address, subnet, or range:

Examples: xxx.xxxx.yy, xxx-yy.yy
xx, xxxxyy, xx-yy

< >

< Back Next > Finish Cancel

37. On the *New Connectivity Rule – Requirement Map* window select the radio button beside *Select an existing requirement map*. Use the pull-down to select *IMSDbClientRequirementMap*. This should automatically populate the mapping table with *IMSDbClient* as the traffic descriptor and *zCEESecurity* as the security level. Press **Next** and then **Finish** to continue.

IBM z/OS Management Facility on WG31.DMZ — Mozilla Firefox

IBM z/OS Management Facility x +

https://wg31.washington.ibm.com:9433/zosmf/NavigationTree.jsp

IBM z/OS Management Facility Welcome user1 | ? IBM

■ Welcome
■ Notifications
■ Workflow Editor
■ Workflows
▶ Cloud Provisioning
▼ Configuration
 ■ Network Configuration Assistant
▶ Consoles
▶ Links
▶ z/OS Classic Interfaces
▶ z/OSMF Administration
▶ z/OSMF Settings

Refresh

Welcome x Network Configu... x

Network Configuration Assistant (Home) ▶ AT-TLS ▶ TCP/IP Stack ▶ Connectivity Rule Help

New Connectivity Rule

✓ Data Endpoints
🔧 Requirement Map
Advanced Settings

Requirement Map

Requirement maps are reusable objects that combine your traffic definitions (traffic descriptors) with your security definitions (security levels).

☐ Create a new requirement map
☒ Select an existing requirement map

IMSDbClientRequirementMap

IMSDbClientRequirementMap properties

* Name:
IMSDbClientRequirementMap

Description:

Mappings table

| Traffic Descriptor | Security Level |
|--------------------|----------------|
| IMSDbClient | zCEESecurity |

< Back Next > Finish Cancel

- ___38. Click **Close** to return the main screen. Select the radio button beside *TCPIP1* and use the *Actions* pull-down to select *Install All Files for This Group*.

IBM z/OS Management Facility on WG31.DMZ - Mozilla Firefox

File Edit View History Bookmarks Tools Help

IBM z/OS Management Facility

https://wg31.washington.ibm.com:9433/zosmf/NavigationTree.jsp

Welcome user1

IBM

Network Configuration Assistant (Home) AT-TLS Help

V2R3 Current Backing Store is USER1

Select a TCP/IP technology to configure : AT-TLS Tools

Systems Traffic Descriptors Security Levels Address Groups Requirement Maps

Actions

No filter applied

| System Group or Sysplex / System Image / Stack | Type | Status | Install Status | Release |
|--|--------------|----------|----------------|---------|
| Default | System Group | Complete | | |
| WG31 | System Image | Complete | N/A | V2R3 |
| TCPIP1 | Stack | Complete | Needs install | V2R3 |

Total: 3 Selected: 1

Home Save

- ___39. On the *List of Configuration Files for All Systems Images in Group Default* window, select *WG31* and use the *Actions* pull-down to select *Install*.

IBM z/OS Management Facility

Welcome user1

Network Configuration Assistant (Home) > AT-TLS > Configuration Files

List of Configuration Files for All System Images In Group Default

List of Configuration Files for All System Images In Group Default

| System Image | Configuration Type | Status | Last Install | Configured File Name | Configured Host Name | Configured Installation Method |
|--------------|------------------------|-----------------|--------------|---|----------------------|--------------------------------|
| WG31 | TCP/IP - AT-TLS Policy | Never installed | Never | /etc/cfgasst/v2r3/WG31 /TCP/IP1/tlsPol | | Save to disk |

Total: 1 Selected: 1

Close

___40. On the *Install File for Default.WG31.TCPIP1* window click the **GO** button to continue.

___41. Click **OK** twice to continue.

___42. Next click on *AT-TLS* as shown below to return to the primary window.

___43. The AT-TLS configuration has been completed and is installed. But it is not active yet.

Activating the AT-TLS configuration

The AT-TLS configuration has been saved in an OMVS file but has not been installed in an active policy agent task (e.g. PAGENT).

- ___1. This instance of the policy agent has been configured to use the *SYSLOGD* daemon task to log messages

```
//PAGENT EXEC PGM=PAGENT,REGION=0K,TIME=NOLIMIT,
//  PARM='ENVAR("_CEE_ENVFILE_S=DD:STDENV")/-I SYSLOGD'
```

- ___2. The *SYSLOGD* daemon has been configured to write all log messages to file */var/syslogd/syslogall.log* (see the *syslog.conf* file in the */etc* subdirectory).

```
#####
#
# Write all messages with priority err and higher to log file errors.
#
#*.err                /var/log/%Y/%m/%d/errors
*.*                  /var/syslogd/syslogall.log
#
```

- ___3. Use ISPF option 3.4 to access directory */var/syslogd* and the *v* line command to view *syslogall.log*. Go the bottom of the file and you will see something like what is shown below:

```
VIEW /SYSTEM/var/syslogd/syslogall.log Columns 00063 00134
Command ==> Scroll ==> 4
003388 YFT18I Using catalog '/usr/lib/nls/msg/C/ftpdmsg.cat' for FTP messages.
003389 Y2697I IBM FTP CS V2R3 19:44:07 on 03/23/20
003390 Y2640I Using dd:SYSFTPD=SYS1.TCPPARMS(FTPDATA) for local site configurat
003391 YFT147I dd:SYSFTPD=SYS1.TCPPARMS(FTPDATA) file, line 10: Ignoring keyword
003392 YFT147I dd:SYSFTPD=SYS1.TCPPARMS(FTPDATA) file, line 11: Ignoring keyword
003393 YFT147I dd:SYSFTPD=SYS1.TCPPARMS(FTPDATA) file, line 13: Ignoring keyword
003394 YFT147I dd:SYSFTPD=SYS1.TCPPARMS(FTPDATA) file, line 49: Ignoring keyword
003395 YFT147I dd:SYSFTPD=SYS1.TCPPARMS(FTPDATA) file, line 54: Ignoring keyword
003396 YFT21I Using catalog '/usr/lib/nls/msg/C/ftpdprly.cat' for FTP replies.
003397 YFT26I Using 7-bit conversion derived from 'ISO8859-1' and 'IBM-1047' fo
003398 YFT32I Using the same translate tables for the control and data connecti
003399 YFT09I system information for WG31: z/OS version 2 release 3 (3906)
003400 pFixLevel: Fix level: NONEFND Data: EZB0ECPR
003401 pFixLevel: Fix level: HIP6230 Data: EZAFTPD1 EZAFTPD4 EZAFTPGA
003402 pFixLevel: Fix level: " Data: EZAFTPG1 EZAFTPXC EZAFTPB1 EZAFTPDF
003403 pFixLevel: Fix level: " Data: EZAFTPDH EZAFTPDM EZAFTPEA EZAFTPED
003404 pFixLevel: Fix level: " Data: EZAFTPEJ EZAFTPER EZAFTPET EZAFTPGU
003405 pFixLevel: Fix level: " Data: EZAFTPGV EZAFTPNX EZAFTPSD EZAITUTI
003406 pFixLevel: Fix level: UI53145 Data: EZAFTPNY
003407 pFixLevel: Fix level: UI56159 Data: EZAFTPEP
003408 pFixLevel: Fix level: UI57631 Data: EZAFTPF5
003409 pFixLevel: Fix level: 24/ 24 Data: OBJECTS PROCESSED. AV-BUFR: 0005087
003410 Y2700I Using port FTP control (21)
003411 Y2701I Inactivity time is 12000
003412 Y2702I Server-FTP: Initialization completed at 19:44:07 on 03/23/20.
003413 YFT141I Server-FTP: process id 83886182, server job name FTPSERVE
003414 ning on 0.0.0.0 port 22.
***** Bottom of Data *****
MA C 04/015
Connected to remote server/host wg31 using lu/pool TCP00109 and port 23
```


- ___4. Start the policy agent task using MVS command *S PAGENT*
- ___5. Exit the syslogall.log view session and reopen the file do a find for a subset of string *EZZ8431I PAGENT STARTING* and you should see these messages.

```

003414 0.0.0 port 22.
003415 main: EZZ8431I PAGENT STARTING
003416 main: Compiled on Sep 26 2016 at 18:37:59
003417 main: Use environment PAGENT_CONFIG_FILE = '/etc/pagent.conf'
003418 main: List all environment variables:
003419 main:   EXPORT '_CEE_ENVFILE_S=DD:STDENV'
003420 main:   EXPORT 'LIBPATH=/usr/lib:.'
003421 main:   EXPORT 'PAGENT_CONFIG_FILE=/etc/pagent.conf'
003422 main:   EXPORT 'PAGENT_LOG_FILE=SYSLOGD'
003423 main:   EXPORT 'TZ=EST5EDT'
003424 main:   EXPORT 'GSK_TRACE=0xFFFF'
003425 main: using code page 'IBM-1047'
003426 main: Using log level 511

```

- ___6. Do a find for the character string *TTLSSRule*, e.g. *f TTLSSRule* and you see multiple occurrences where the AT-TLS configuration elements added earlier are being processed.

```

profile: Processing Image TLS config file: '/etc/cfgasst/v2r3/WG31/TCPI
Processing: 'TTLSSRule                               IMSDBConnectRule~1'
Processing: 'TTLSSRule                               IMSDBClientRule~2'
Processing: 'TTLSSGroupAction                         gAct1'
Processing: 'TTLSEnvironmentAction                   eAct1~IMSDBConnect'
Processing: 'TTLSEnvironmentAction                   eAct2~IMSDBClient'
Processing: 'TTLSSConnectionAction                   cAct1~IMSDBConnect'
Processing: 'TTLSSConnectionAction                   cAct2~IMSDBClient'
Processing: 'TTLSSConnectionAdvancedParms           cAdv1~IMSDBConnect'
Processing: 'TTLSSConnectionAdvancedParms           cAdv2~IMSDBClient'
Processing: 'TTLSSKeyringParms                       keyR1'
Processing: 'TTLSSKeyringParms                       keyR2'
Processing: 'IpAddrSet                               addr1'
Processing: 'PortRange                               portR1'
Processing: 'PortRange                               portR2'
profile: Finished processing Image TLS config file
rocessing TLS Group action 'gAct1'
rocessing TLS Connection action 'cAct1~IMSDBConnect'
rocessing TLS Connection action 'cAct2~IMSDBClient'
rocessing TLS Environment action 'eAct1~IMSDBConnect'
rocessing TLS Environment action 'eAct2~IMSDBClient'
rocessing TLS rule 'IMSDBClientRule~2'
rocessing TLS rule 'IMSDBConnectRule~1'

```

___7. Go the bottom of this file and you see these messages

```
EZD1579I PAGENT POLICIES ARE NOT ENABLED FOR TCPIP1 : TTLS
EZZ8771I PAGENT CONFIG POLICY PROCESSING COMPLETE FOR TCPIP1 : QOS
EZZ8771I PAGENT CONFIG POLICY PROCESSING COMPLETE FOR TCPIP1 : TTLS
EZD1586I PAGENT HAS INSTALLED ALL LOCAL POLICIES FOR TCPIP1
Finished main config file update
```

Tech-Tip: If a policy or otherwise changed the new or updated policy can be installed with an MVS modify command, ***F PAGENT,REFRESH.***

___8. The policy agent is active. The policies have been loaded but there is one remaining step. The TCPIP stack has not been modified to enable TTLS. On this image this has been configure this way so the AT-TLS is disabled by default and must be explicitly enabled. This is done by an MVS VARY command,

V TCPIP,,OBEY,SYS1.TCPPARMS(TTLS)

Where the contents of SYS1.TCPPARMS(TTLS) is simply *TCPCONFIG TTLS*.

Issue this command and you should see these messages in the console.

```
V TCPIP,,OBEY,SYS1.TCPPARMS(TTLS)
EZZ0060I PROCESSING COMMAND: VARY TCPIP,,OBEY,SYS1.TCPPARMS(TTLS)
EZZ0300I OPENED OBEYFILE FILE 'SYS1.TCPPARMS(TTLS)'
EZZ0309I PROFILE PROCESSING BEGINNING FOR 'SYS1.TCPPARMS(TTLS)'
EZZ0316I PROFILE PROCESSING COMPLETE FOR FILE 'SYS1.TCPPARMS(TTLS)'
EZZ0053I COMMAND VARY OBEY COMPLETED SUCCESSFULLY
```

Tech-Tip: AT-TLS can be also be disabled with a VARY command, ***V TCPIP,,OBEY,SYS1.TCPPARMS(NOTTLS)*** where the contents of SYS1.TCPPARMS(NOTTLS) are *TCPCONFIG NOTTLS*

___9. Stop and restart the server with MVS commands ***P BAQSTRT*** and ***S BAQSTRT***.

Tech-Tip: The server must be stopped and restart because there is an active session between the zCEE server and IMS Connect. The policies are not trigger until the socket session is restarted.

Test the TLS connection from the zCEE Server to IMS

Now use the REST client to test the API with AT-TLS enabled.

- ___1. Open a DOS command prompt and change to directory *c:/z/admin*.
- ___2. Enter the cURL commands below:

```
c:\z\admin>curl -X get --cacert certauth.pem --cert user1.p12:secret --cert-type P12  
https://wg31.washington.ibm.com:9443/imdb/contact/LAST3
```

You should see the same results as before.

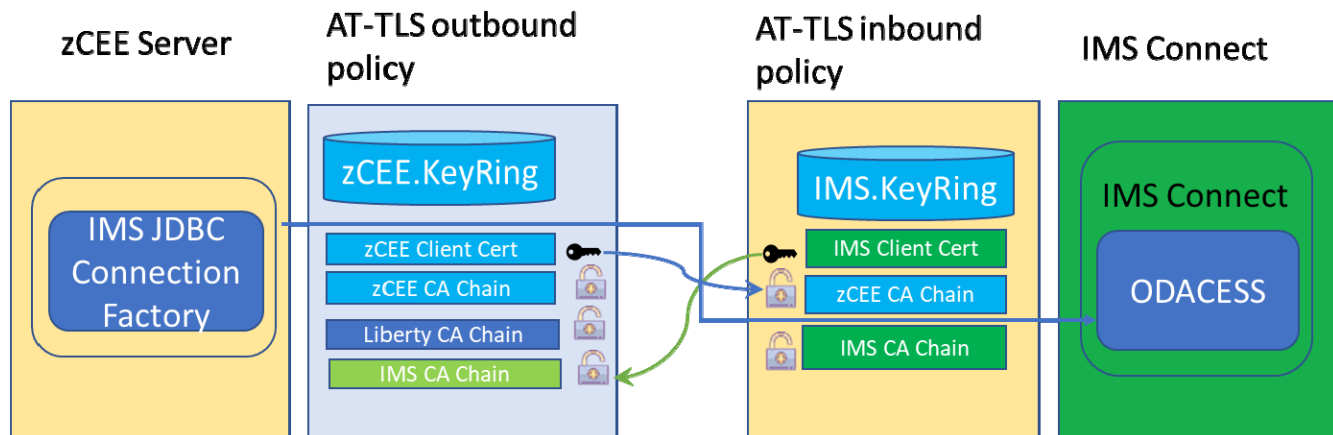
- ___3. View the *syslogd.log* file again and you should find the messages like the ones below. These messages are tracing the handshake between the outbound policy acting a client and the inbound policy acting as the server.

```
EZD1281I TTLS Map CONNID: 00000A35 LOCAL: 192.168.17.220..2693 REMOTE :  
192.168.17.220..5555 JOBNAME: BAQSTRT USERID: LIBSERV TYPE: OutBound STATUS:  
Enabled RULE: IMSClientRule~2 ACTIONS: gAct1 eAct2~IMSClient cAc2~IMSClient  
  
EZD1281I TTLS Map CONNID: 00000A36 LOCAL: 192.168.17.220..5555 REMOTE :  
192.168.17.220..2693 JOBNAME: IMS15HWS USERID: IMSSTC TYPE: InBound STATUS:  
Enabled RULE: IMSConnectRule~1 ACTIONS: gAct1 eAct1~IMSConnect cAct1~IMSConnect  
  
EZD1283I TTLS Event GRPID: 00000009 ENVID: 00000009 CONNID: 00000A36 R C: 0  
Initial Handshake 000000501142EE90 0000005011429850 TLSV1.2 F0F0F3F5  
  
EZD1283I TTLS Event GRPID: 00000009 ENVID: 00000008 CONNID: 00000A35 R C: 0  
Initial Handshake 0000005011427EB0 0000005011422750 TLSV1.2 F0F 0F3F5
```

- ___4. Entering IMS Connect *VIEWHWS* command should show FRED and/or USER1 as the CLIENTIDs.

```
HWSC0001I PORT=5555D STATUS=ACTIVE KEEPAV=0 NUMSOC=3  
EDIT= TIMEOUT=6000  
HWSC0001I CLIENTID USERID TRANCODE DATASTORE STATUS SECOND  
CLNTPORT IP-ADDRESS APSB-TOKEN  
HWSC0001I ODBB90D3 FRED IVP15OOD RECV 9  
2735 192.168.017.220  
HWSC0001I ODBD40D8 USER1 IVP15OOD RECV 424  
2693 192.168.017.220  
HWSC0001I TOTAL CLIENTS=2 RECV=2 READ=0 CONN=0 XMIT=0 OTHER=0
```

The diagram below shows the flow of the request from the z/OS Connect server to IMS Connect. The server and IMS Connect are unaware of the involvement of the AT-TLS the TLS handshake and the fact that the message is encrypted between the two endpoints.



- ___5. There is information in the AT-TLS Knowledge Center for describing AT-TLS return codes (see URL https://www.ibm.com/support/knowledgecenter/SSLTBW_2.4.0/com.ibm.zos.v2r4.hald001/comtls.htm) For example, if the return code had been 202 it would be caused by the explanation below.

The key ring cannot be opened because the user does not have permission. Check the following items:

- Look at message EZD1281 to verify the user ID being used for this connection and the TTLSEnvironmentAction statement that is mapped to this connection. If you are configuring by using the IBM Configuration Assistant for z/OS® Communications Server, you can specify the key ring on either the AT-TLS: Image Level Settings panel or on each Traffic Descriptor.
- Ensure that the correct key ring is specified

This simply means the user does not have the required access to either of the RACF FACILITY resources IRR.DIGTCERT.LIST and IRR.DIGTCERT.LISTING

If the return code had been 414 and explanation can be found in the z/OS Cryptographic Services System SSL Programming (SC14-7495-40) manual or at URL https://www.ibm.com/support/knowledgecenter/SSLTBW_2.4.0/com.ibm.zos.v2r4.gska100/ssl2msg1000885.htm

414 Certificate is not valid.

Explanation: Either the local certificate or the peer certificate is not valid.

User response: Ensure that a valid certificate is being sent by the communication partner. Collect a System SSL trace containing a dump of the incorrect certificate and then contact your service representative if the error persists.

This is probably caused because the certificate authority certificate used to sign a server or personal certificate is not connect to the key ring. Or not properly connected to the key ring.

- ___6. The JCL in member *PASEARCH* in data set *USER1.ZCEE30.CNTL* can be used to display AT-TLS policies. Submit this job and see a display of the contents of the policy agent's configuration file. Without the Configuration Assistant provided by z/OSMF this file would need to be maintained manually.

```
//BPXBATCH EXEC PGM=BPXBATCH,REGION=8M
//STDOUT DD PATH='/tmp/paStd.out',
//          PATHOPTS=(OWRONLY,OCREAT),PATHMODE=SIRWXU
//STDERR DD PATH='/tmp/paStd.err',
//          PATHOPTS=(OWRONLY,OCREAT),PATHMODE=SIRWXU
//STDPARM DD *
SH echo pasearch -t | su
//COPY EXEC PGM=IKJEFT01,DYNAMNBR=300
//SYSTSPRT DD SYSOUT=*
//PASTDOUT DD PATH='/tmp/paStd.out',PATHDISP=(DELETE,DELETE)
//PASTDERR DD PATH='/tmp/paStd.err',PATHDISP=(DELETE,DELETE)
//STDOUT DD SYSOUT=*,DCB=(LRECL=1000,RECFM=V)
//STDERR DD SYSOUT=*,DCB=(LRECL=1000,RECFM=V)
//SYSPRINT DD SYSOUT=*
//SYSTSIN DD *
OCOPY INDD(PASTDERR) OUTDD(STDERR)
OCOPY INDD(PASTDOUT) OUTDD(STDOUT)
```

Optional

Disable the use of RACF Passtickets and retest using only TLS and see what difference this makes.

Summary

In this step you have created AT-TLS inbound and outbound policies which protect the IMS Connect ODBA port of 5555. These policies respectively act as client and server surrogates for the z/OS Connect server and IMS Connect.

Appendix – AT-TLS Policy Agent Configuration File

```
##
## AT-TLS Policy Agent Configuration file for:
##   Image: WG31
##   Stack: TCPIP1
##
## Created by the IBM Configuration Assistant for z/OS Communications Server
## Version 2 Release 3
## Backing Store = USER1
## Install History:
## 2020-06-12 13:29:32 : Save To Disk
## 2020-06-12 13:15:40 : Save To Disk
##
## End of Network Configuration Assistant information
TTLSRule                                IMSDBConnectRule~1
{
  LocalAddrSetRef                        addr1
  RemoteAddrSetRef                       addr1
  LocalPortRangeRef                     portR1
  Jobname                                IMS15HWS
  Direction                              Inbound
  Priority                                255
  TTLSGroupActionRef                     gAct1
  TTLSEnvironmentActionRef               eAct1~IMSDBConnect
  TTLSConnectionActionRef                cAct1
}
TTLSRule                                IMSDBClientRule~2
{
  LocalAddrSetRef                        addr1
  RemoteAddrSetRef                       addr1
  LocalPortRangeRef                     portR2
  RemotePortRangeRef                    portR1
  Direction                              Outbound
  Priority                                254
  TTLSGroupActionRef                     gAct1
  TTLSEnvironmentActionRef               eAct2~IMSDBClient
  TTLSConnectionActionRef                cAct1
}
TTLSGroupAction                          gAct1
{
  TTLSEnabled                            On
  Trace                                  7
}
TTLSEnvironmentAction                    eAct1~IMSDBConnect
{
  HandshakeRole                          Server
  EnvironmentUserInstance                 0
  TTLSKeyringParmsRef                    keyR1
}
```

```

TTLSEnvironmentAction          eAct2~IMSDBClient
{
  HandshakeRole                Server
  EnvironmentUserInstance      0
  TLSKeyringParmsRef          keyR2
}
TLSConnectionAction           cAct1
{
  HandshakeRole                Server
  TLSConnectionAdvancedParmsRef cAdv1
  CtraceClearText              Off
  Trace                        7
}
TLSConnectionAdvancedParms    cAdv1
{
  SSLv3                        Off
  TLSv1                        Off
  TLSv1.1                      Off
  SecondaryMap                  Off
  TLSv1.2                      On
}
TLSKeyringParms               keyR1
{
  Keyring                      IMS.KeyRing
}
TLSKeyringParms               keyR2
{
  Keyring                      zCEE.KeyRing
}
IpAddrSet                     addr1
{
  Prefix                       0.0.0.0/0
}
PortRange                      portR1
{
  Port                          5555
}
PortRange                      portR2
{
  Port                          1024-65535
}

```