" z/OSMF Configuration Assistant for z/OS Communications Server" Hands-on Lab - Part 2 of 2

Part 1: IPsec Rule
Part 2: AT-TLS Rule

SHARE 16946

Hands-on Lab Guide

Revision date - Friday, 27 February 2015

This edition applies to IBM z/OS Configuration Assistant V2R1 running in zOSMF on a z/OS V2.1 platform.

Attention:

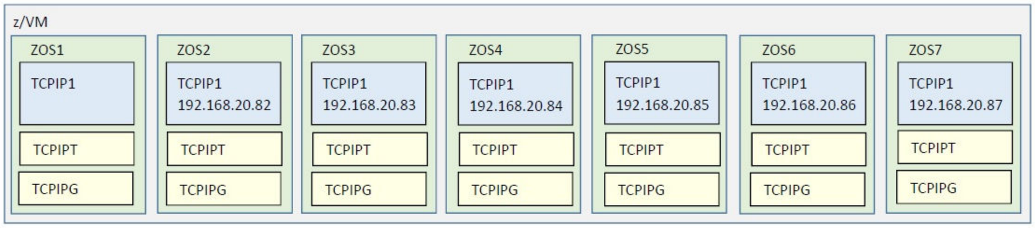
Information in this document was developed in conjunction with use of the equipment specified, and is limited in application to those specific hardware and software products and levels.

Table of Contents

Introduction: Lab Description

z/OS Systems

There are 8 z/OS systems running as guests under a single z/VM system.



Each student ZOS (MVS) system has three TCP/IP stacks running in it: TCPIP***1***, TCPIP***T***, and TCPIP***G***.

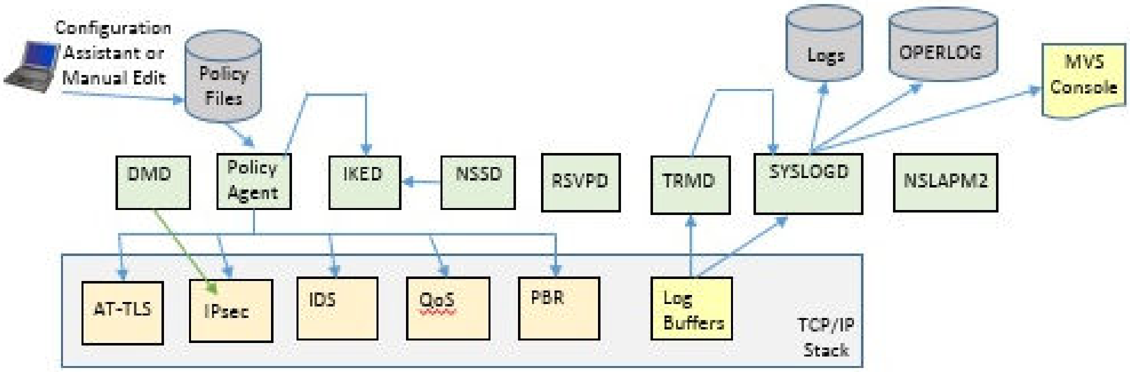
The basic TCPIP stack is used for access only and not testing and is named TCPIP***1***. The TN3270 procedure that has affinity to the access TCPIP***1*** is named TN3270. The FTP procedure that has affinity to TCPIP***1*** is named FTPCCL(1).

In our labs you use TCPIP***1*** for basic maintenance on your MVS***n*** until you have finished building your own student TCP/IP stacks and procedures. You telnet into TCPIP1 to reach ISPF and UNIX for building the procedures that should run together with the student TCP/IP test stack.

There are six **"Student z/OS (MVS) systems"** that you will be working on: MVS***2***-MVS*7*. The student TCP/IP stacks on these systems are named TCPIP***T*** and TCPIP***G***. The students customize a test stack and ***not*** the instructor "maintenance" stack. The students also customize any other procedures that are part of the security labs and that are to have affinity with TCPIP***T*** and TCPIP***G***.

Policy Agent Environment

There are lots of different elements in the Policy Agent (PAGENT) environment. The Configuration Assistant for z/OS can simplify the creation of this environment.

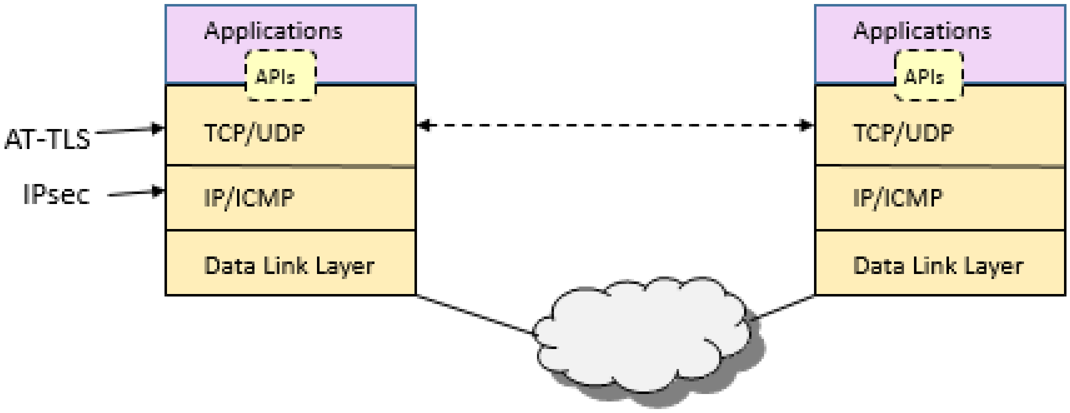


This lab does not have time to go into all the different parts of the z/OS Communications Server Policy Agent environment listed above. For more information please refer to the standard manuals and Redbooks.

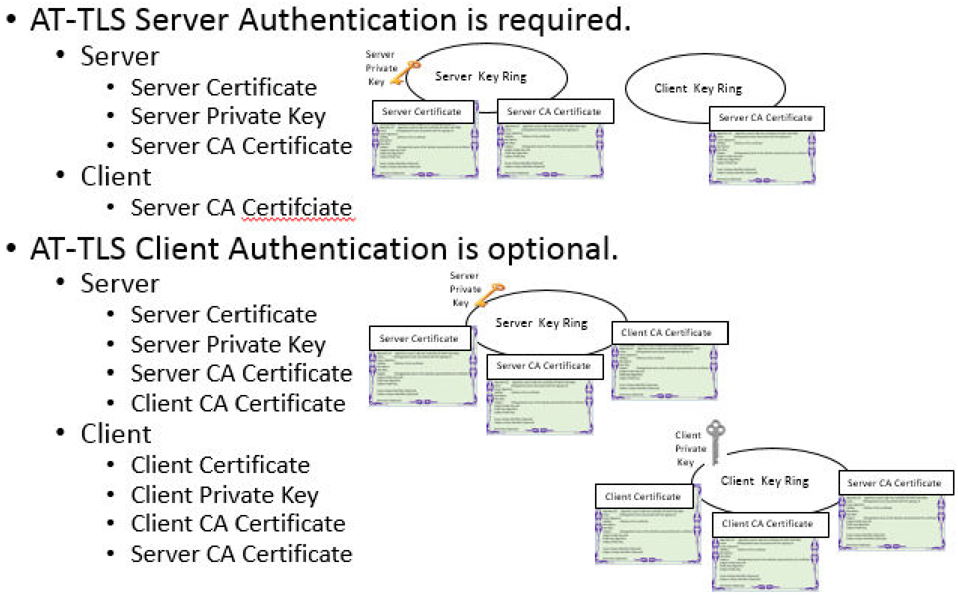
- IP Configuration Guide, SC27-3650
- IP Configuration Reference, SC27-3651
- Redbook IBM z/OS V2R1 CS TCP/IP Implementation Vol 4: Security and Policy-Based Networking, SG24-8099

AT-TLS Lab

Application Transparent – Transport Layer Security (AT-TLS) is the name of the TLS support provided by Policy Agent. TLS may be used to encrypt traffic between two hosts.

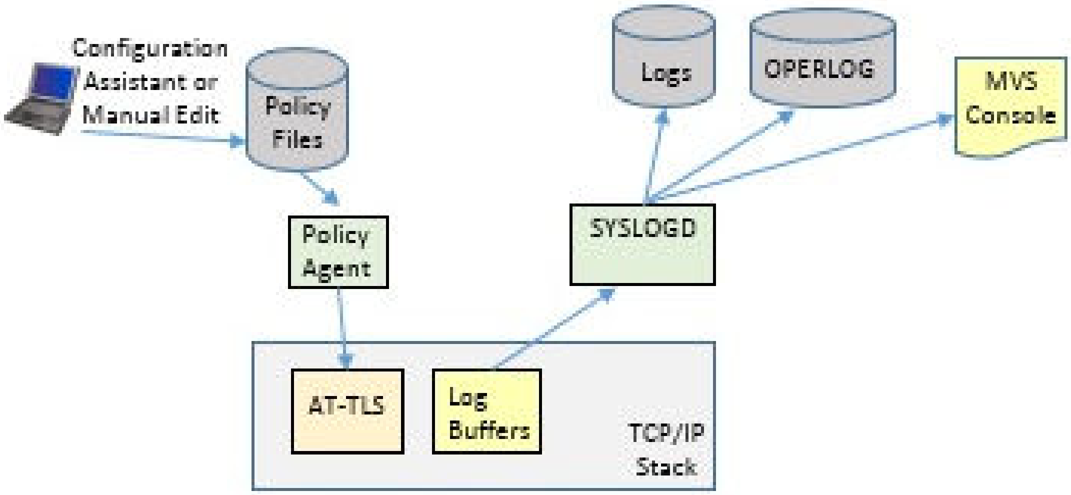


AT-TLS requires X.509 Certificates and Key Rings.

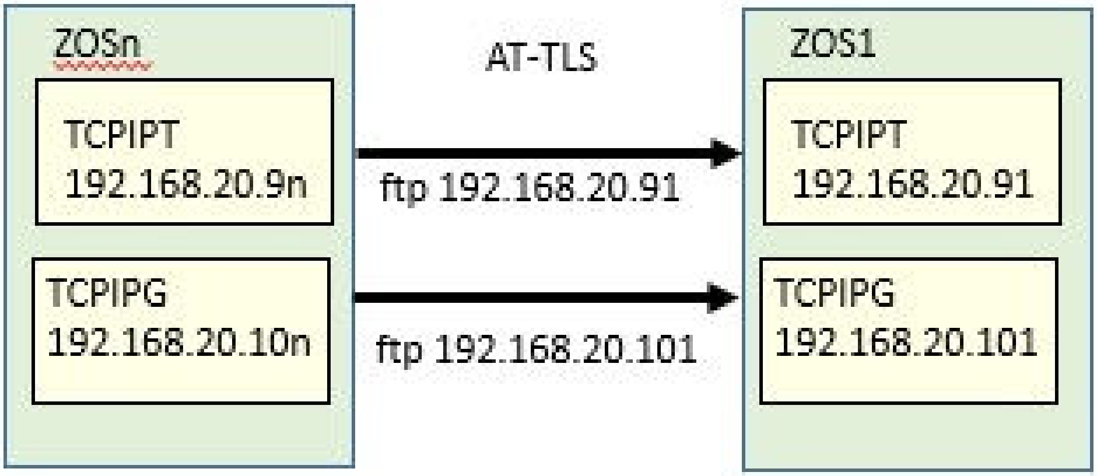


- AT-TLS Server Authentication is required.
  - Server
    - Server Certificate
    - Server Private Key
    - Server CA Certificate
  - Client
    - Server CA Certifciate
- AT-TLS Client Authentication is optional.
  - Server
    - Server Certificate
    - Server Private Key
    - Server CA Certificate
    - Client CA Certificate
  - Client
    - Client Certificate
    - Client Private Key
    - Client CA Certificate
    - Server CA Certificate

Policy Agent reads in the policy files and installs them into the TCP/IP stack. It is the TCP/IP stack that enforces the policies.



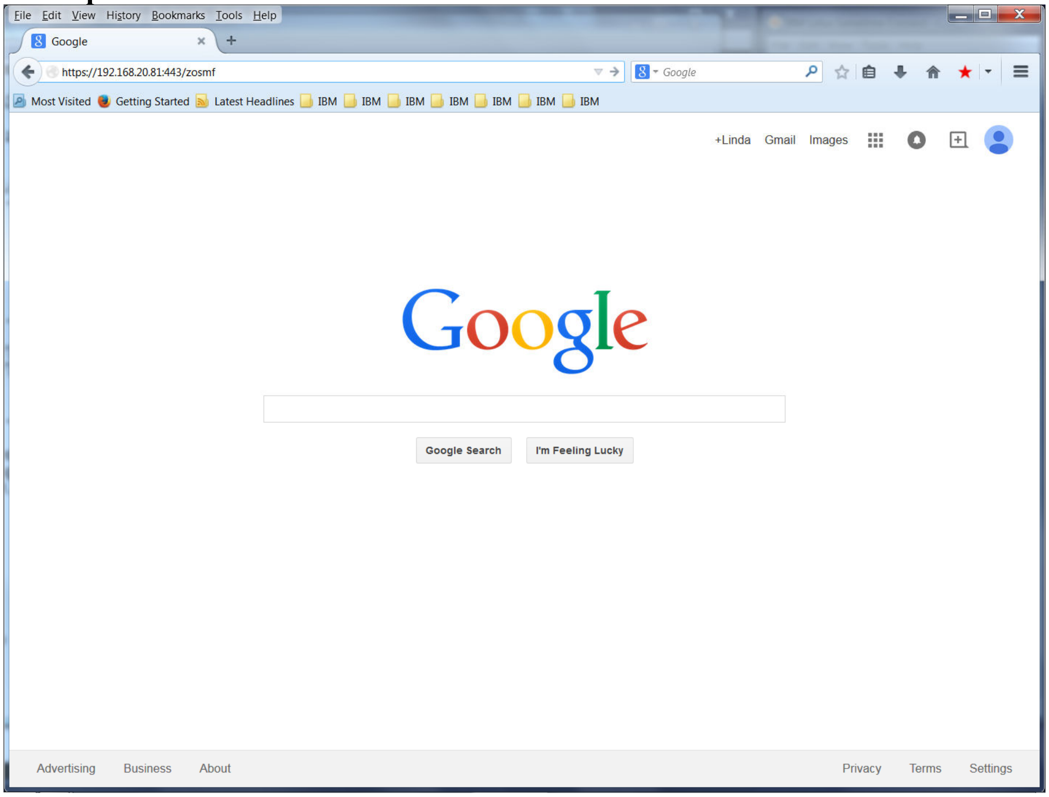
In this lab you will test AT-TLS using FTP.



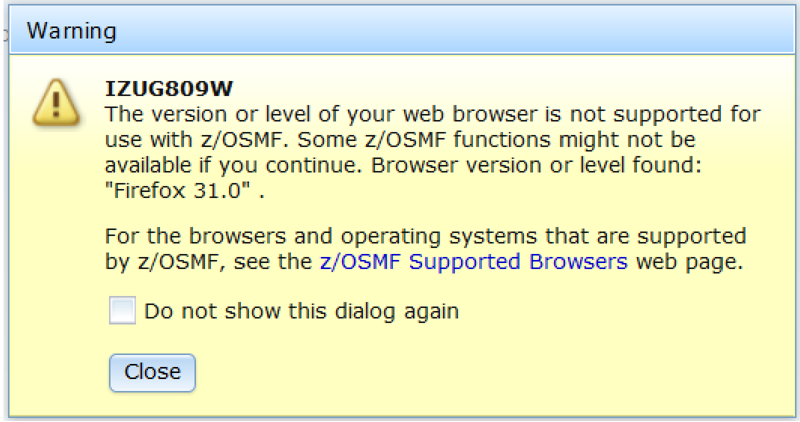
Scenario 1: Use zOSMF on ZOS1 for the First Time

If you already connected to zOSMF for a previous lab, then skip this Scenario and proceed to Scenario 2, otherwise proceed through this section.

1. Open a Web Browser window and go to URL: **https://192.168.20.81:443/zosmf**



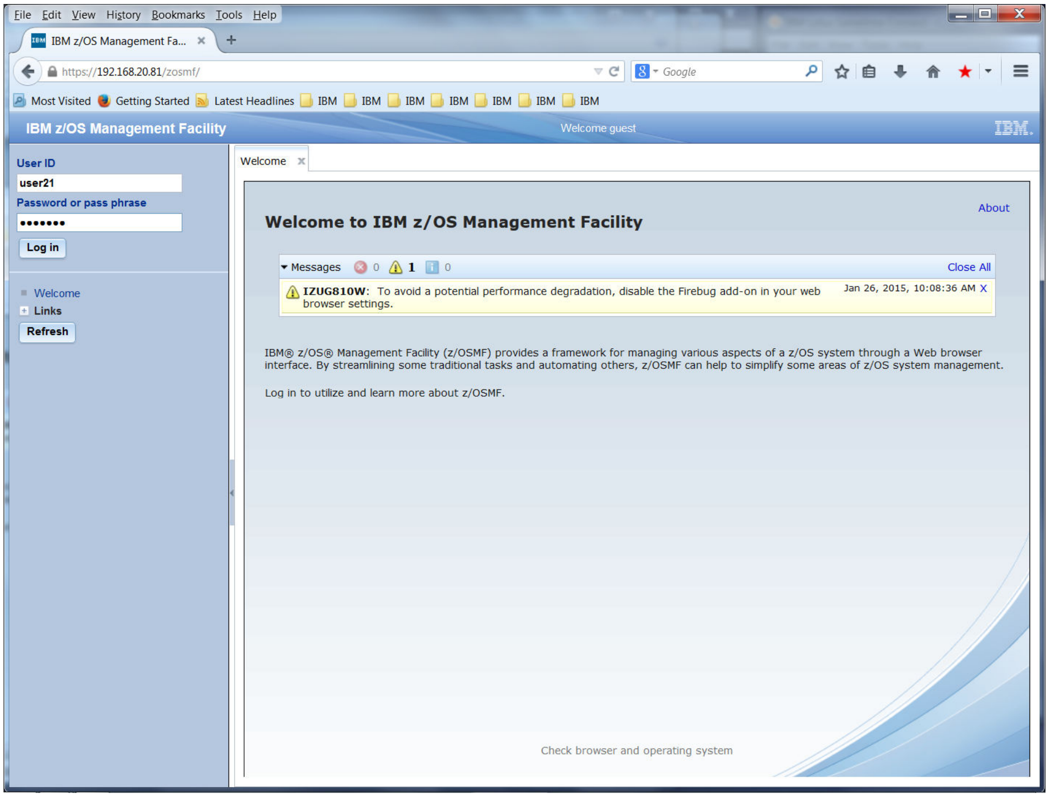
2. If a pop-up appears with warning IZUG809W warning "The version or level of your web browser is not supported for use with z/OSMF." Just ignore it and click on **Close** button.



IZUG809W
The version or level of your web browser is not supported for use with z/OSMF. Some z/OSMF functions might not be available if you continue. Browser version or level found: "Firefox 31.0" .

For the browsers and operating systems that are supported by z/OSMF, see the z/OSMF Supported Browsers web page.

3. Logon using your Team Information Sheet to determine your z/OS User ID and password.


File Edit View History Bookmarks Tools Help
IBM z/OS Management Fa...
https://192.168.20.81/zosmf/
Google
Most Visited
Getting Started
Latest Headlines
IBM
IBM z/OS Management Facility
Welcome guest
IBM.
Log in
Welcome
Links
Refresh
Messages
Close All

User ID
user21
Password or pass phrase
•••••••

Welcome to IBM z/OS Management Facility

About

Messages 0 1 0

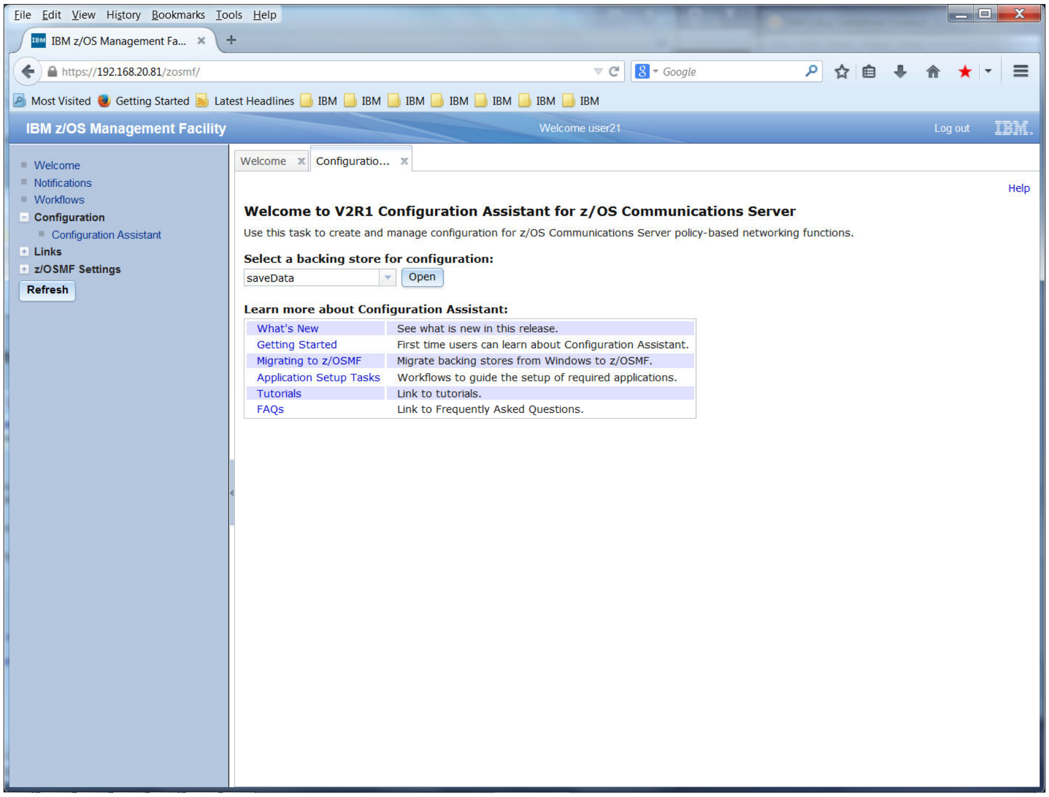
IZUG810W: To avoid a potential performance degradation, disable the Firebug add-on in your web browser settings. Jan 26, 2015, 10:08:36 AM X

IBM® z/OS® Management Facility (z/OSMF) provides a framework for managing various aspects of a z/OS system through a Web browser interface. By streamlining some traditional tasks and automating others, z/OSMF can help to simplify some areas of z/OS system management.

Log in to utilize and learn more about z/OSMF.

Check browser and operating system

4. You should be presented with the "Welcome to IBM z/OS Management Facility" panel.
5. Feel free to click on the numerous links to learn more about zOSMF. There three links under the heading "Learn More:" at the bottom of the page, and there are several links in the left area of the page including the link to the current "Welcome" page. Since all these links, except "Configuration", pertain to zOSMF rather than the “z/OS Configuration Assistant for Communications Server” the lab instructor is not able to answer any question about them.
6. When you are finished exploring the page, expand the “**Configuration**” section in the list on the left side of the page if it is not already expanded (“+” means it is not expanded and “–” means that it is already expanded), and click on “**Configuration Assistant**” which is the only option in the expanded section.



Welcome to V2R1 Configuration Assistant for z/OS Communications Server

Use this task to create and manage configuration for z/OS Communications Server policy-based networking functions.

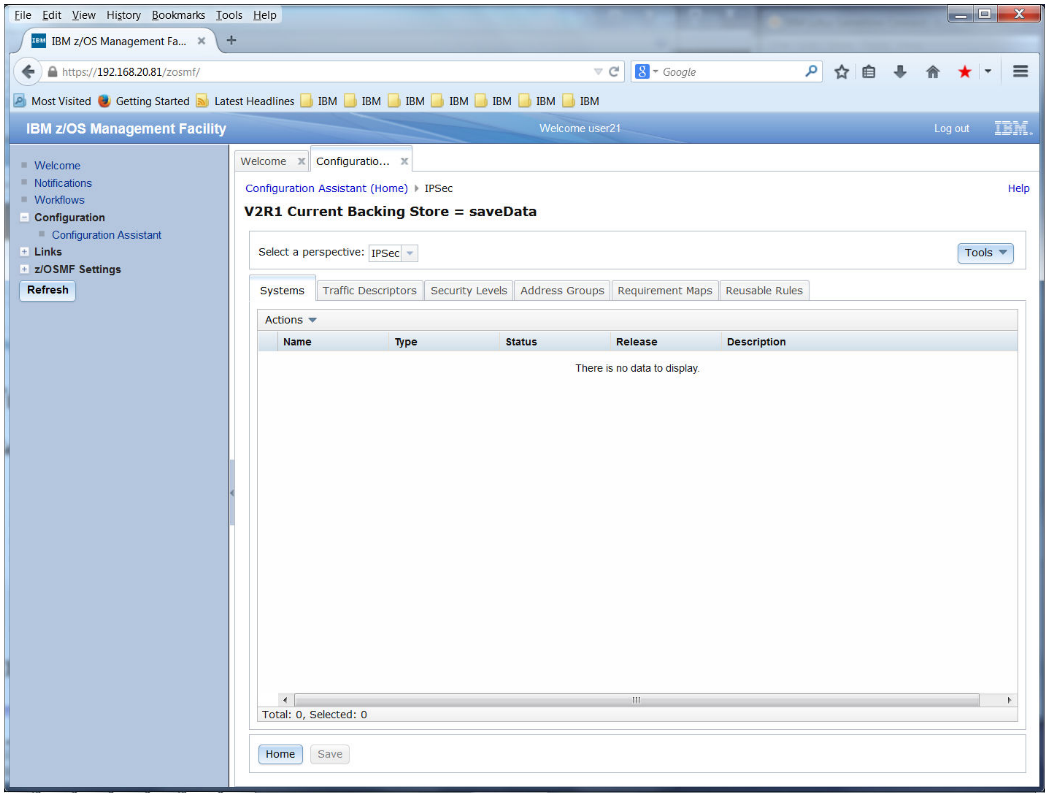
Select a backing store for configuration:

saveData Open

Learn more about Configuration Assistant:

What's New	See what is new in this release.
Getting Started	First time users can learn about Configuration Assistant.
Migrating to z/OSMF	Migrate backing stores from Windows to z/OSMF.
Application Setup Tasks	Workflows to guide the setup of required applications.
Tutorials	Link to tutorials.
FAQs	Link to Frequently Asked Questions.

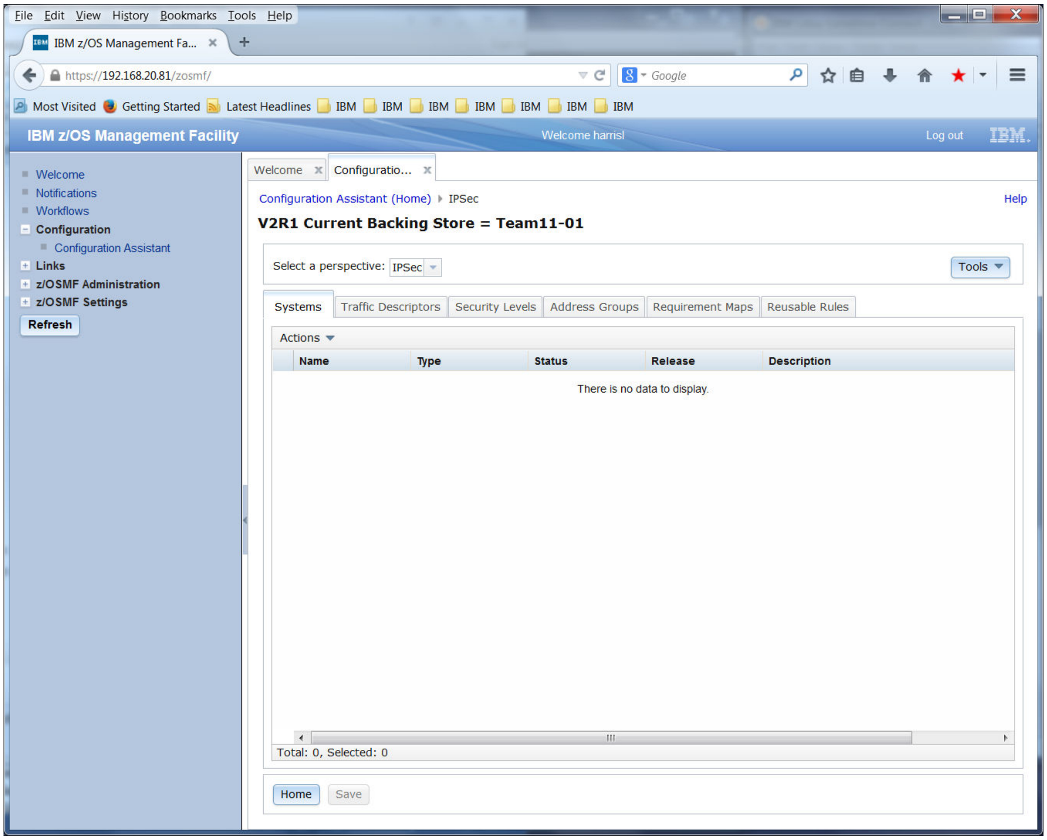
7. Feel free to click on the “Help” link in the top right corner of the page. This type of help is available as you navigate through the Configuration Assistant panels. When you are finished exploring the Help section you may close this page using the “X” in the top right corner to return to the “Welcome” page.
8. Feel free to click on each of the links under “Learn more about Configuration Assistant:” to view other Help sections. When you are finished exploring each one you may close the page using the X in the top right corner.
   a) What’s New
   b) Getting Started
   c) Migrating to z/OSMF
   d) Application Setup Tasks
   e) Tutorials
   f) FAQs
9. Configurations created by the Configuration Assistant tool are saved as Backing Store files. These files are binary files that are only usable by a Configuration Assistant tool.
   a) If necessary use the drop-down beside the “Select a backing store for configuration” field to select Backing Store file “saveData”.
   b) Click on the **Open** button.



V2R1 Current Backing Store = saveData

There is no data to display.

10. Click on the “**Tools**” drop down button on the right side of the page.
11. Feel free to check out the “History”, “Preferences”, and “Log level” sections, using the “Close” and “Cancel” to return to the above page. Then Click on the “**Manage Backing Stores**” link from the drop down.
    a) Manage Backing Stores
    b) History – shows the history of save actions for the current Backing Store file
    c) Preferences – allows customization of save options
    d) Log level – allows customization of log level options (see Help for more details)
12. Click on the “**Actions**” drop down button and then select “**Save As…**”
13. Fill in “File name” of your team name:
    a) Team21
    b) Team22
    c) Team31
    d) Team32
    e) Team41
    f) Team42
    g) Team51
    h) Team52
    i) Team61
    j) Team62
    k) Team71
    l) Team72
    m) Team201
    n) Team201
    o) Team301
    p) Team302
    q) Team401
    r) Team402
    s) Team501
    t) Team502
    u) Team601
    v) Team602
    w) Team701
    x) Team702
14. Optionally fill in a comment and click on the **OK** button.
15. If you are presented with a pop-up window “You are now working on backing store file: Team21”, then click on the **OK** button.
16. Click on the **Close** button to return to the configuration panel.



V2R1 Current Backing Store = Team11-01

Select a perspective: IPSec

Name	Type	Status	Release	Description

There is no data to display.

Total: 0, Selected: 0

17. You have already seen the options available with the “Tools” drop-down on the right side of the screen.
18. There are multiple tabs available for configuration:
    a) Systems – Configure z/OS images, TCP/IP stack, and start wizard for Connectivity rules.
    b) Traffic Descriptors – Define types of traffic (i.e. FTP Server traffic).
    c) Security Levels – Define security to be applied to traffic.
    d) Address Groups – IP addresses may be defined as a single IP Address, an IP subnet, a range of IP addresses, or an IP Address Group.
    e) Requirement Maps – Associate Security Levels to Traffic Descriptors.
    f) Reusable Rules – Define reusable Connectivity Rules.
19. Notice that the “Perspective” displayed is the “IPSec” perspective. Use the pull-down beside IPSec to see the different perspectives available for configuration:
    a) AT-TLS – Application Transparent – Transport Layer Security is the z/OS TLS standard protocol support available in the TCP/IP stack that can provide encryption to remote hosts with TLS support.
    b) DMD – Defence Manager Daemon provides the capability to dynamically (via the ipsec command) add IP Filter rules for a specified time frame.
    c) IDS – Intrusion Detection Services provides TCP/IP stack protection against Scans, Attacks, and also allows connection limits to be defined.
    d) IPSec – is the standard protocol support in the TCP/IP stack that can provide encryption to remote hosts with IPSec support.
    e) NSS – Network Security Server provides support to remote IKED (Internet Key Exchange Daemon) for central certificate storage, support to remote DataPower devices for certificate retrieval, and IKEv2 support.
    f) PBR – Policy Based Routing provides the capability for choosing network routes depending upon traffic types.

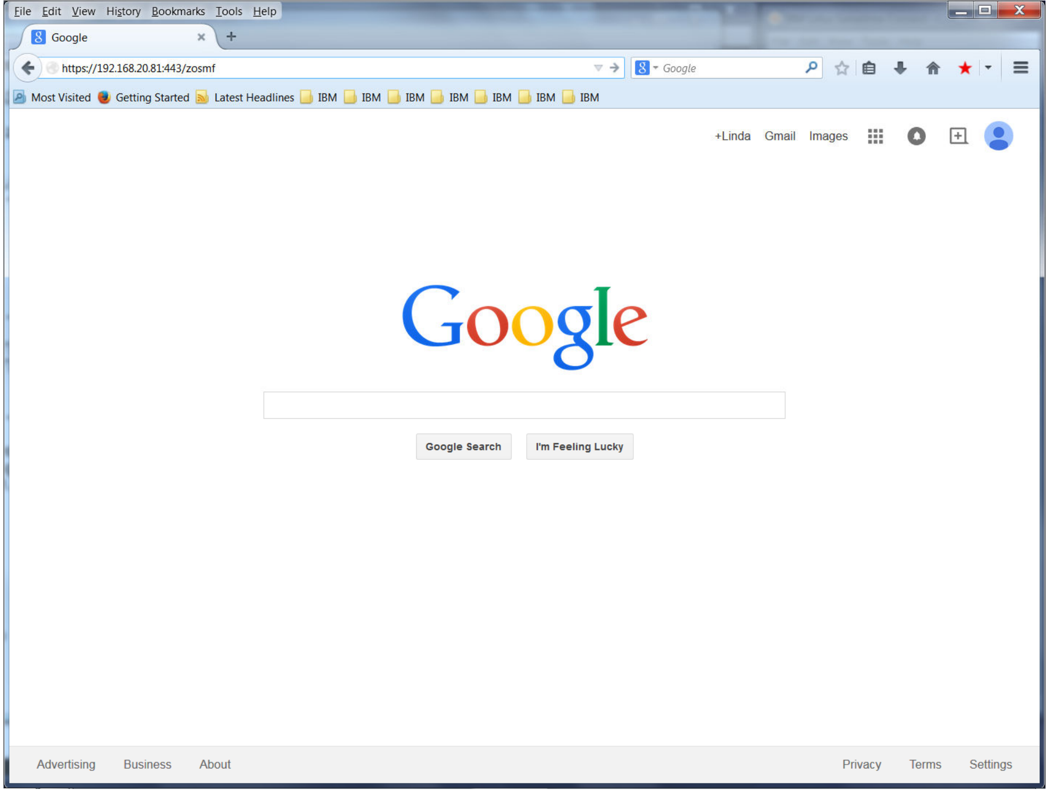
   g) QoS – Quality of Service provides different priority through the network depending upon the traffic types, and may be used to block traffic.

20. Use the "Perspective" pull-down to select "**AT-TLS**".
21. Click on the "**Actions**" pull-down.
22. Select "**Add z/OS Image…**"
23. Enter a z/OS Image Name of your z/OS name:
    a) ZOS2
    b) ZOS3
    c) ZOS4
    d) ZOS5
    e) ZOS6
    f) ZOS7
24. Optionally add a description (i.e. z/OS image 2).
25. Our systems are running z/OS V2.1 so leave the default setting for z/OS Release, V2R1.
26. Click on the **OK** button.
27. You should be presented with a pop-up window "Proceed to the Next Step?" asking about creating a TCP/IP stack for the z/OS image.
    1) Click on the **Proceed** button.
28. Enter the TCP/IP Stack Name of **TCPIPT** or **TCPIPG**.
29. Optionally add a description (i.e. TCP/IP stack T).
30. You should be presented with a pop-up window "Proceed to the Next Step?" asking if you want to be directed to the TCP/IP stack rules panel.
    1) Click on the **Proceed** button.
31. You should be presented with a pop-up window "Proceed to the Next Step?" asking if you want to start a wizard to create a connectivity rule.
    1) Click on the **Cancel** button.
32. Skip Scenario 2 and continue with Scenario 3.

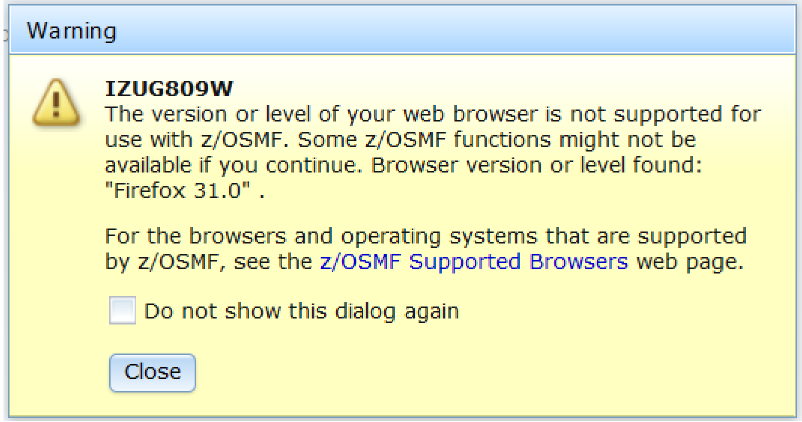
Scenario 2: Use zOSMF on ZOS1 Again

Complete this Scenario if you already connected to zOSMF for a previous lab.

1. Open a Web Browser window and go to URL:
   https://192.168.20.81:443/zosmf


File Edit View History Bookmarks Tools Help
Google
https://192.168.20.81:443/zosmf
Google
Most Visited Getting Started Latest Headlines IBM IBM IBM IBM IBM IBM IBM
+Linda Gmail Images
Google
Google Search I'm Feeling Lucky
Advertising Business About Privacy Terms Settings

2. If a pop-up appears with warning IZUG809W warning "The version or level of your web browser is not supported for use with z/OSMF." Just ignore it and click on **Close** button.

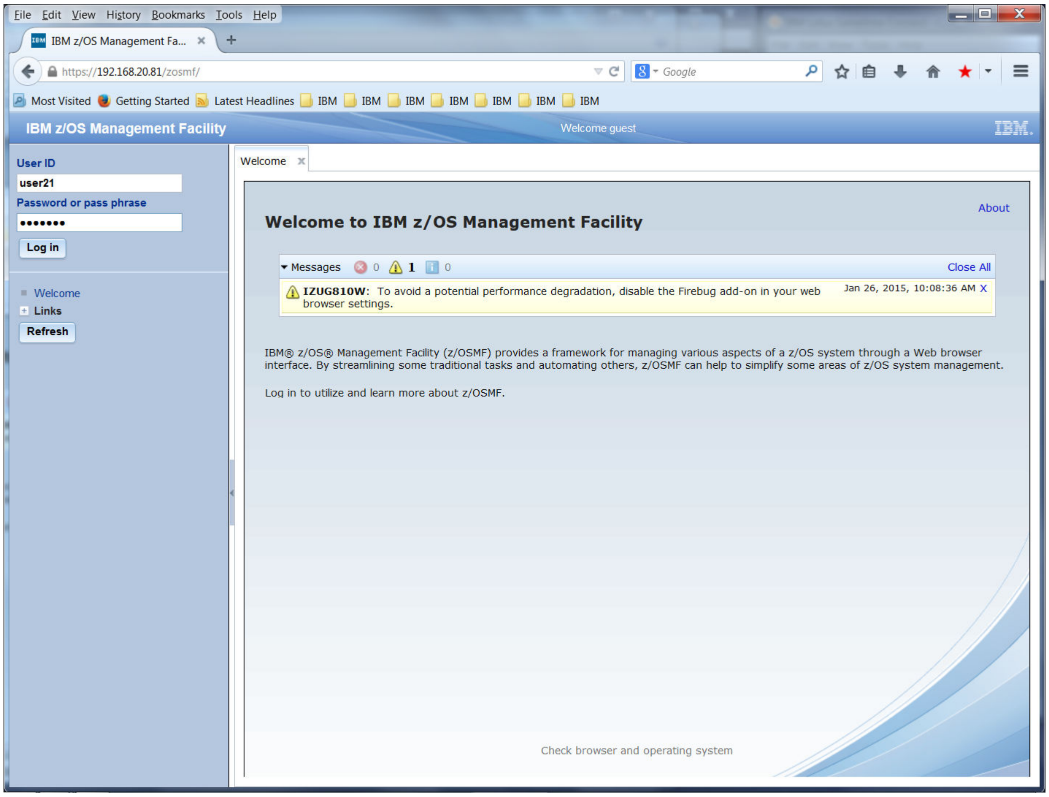


IZUG809W
The version or level of your web browser is not supported for use with z/OSMF. Some z/OSMF functions might not be available if you continue. Browser version or level found: "Firefox 31.0" .

For the browsers and operating systems that are supported by z/OSMF, see the z/OSMF Supported Browsers web page.

□ Do not show this dialog again

3. Logon using your Team Information Sheet to determine your z/OS User ID and password.


File Edit View History Bookmarks Tools Help
IBM z/OS Management Fa...
https://192.168.20.81/zosmf/
Google
Most Visited Getting Started Latest Headlines IBM IBM IBM IBM IBM IBM IBM
IBM z/OS Management Facility
Welcome guest
IBM.
Log in
Welcome
Links
Refresh
Welcome
About
Messages 0 1 0
Close All
Check browser and operating system

User ID: user21

Password or pass phrase: •••••••

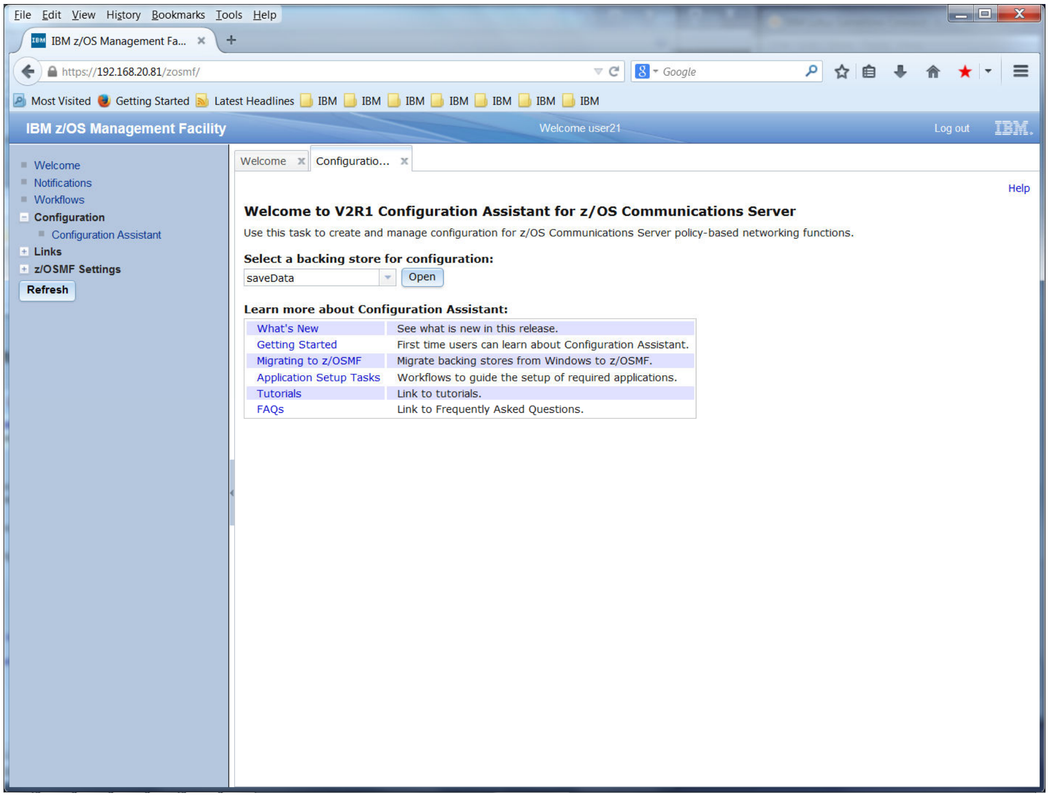
Welcome to IBM z/OS Management Facility

IZUG810W: To avoid a potential performance degradation, disable the Firebug add-on in your web browser settings. Jan 26, 2015, 10:08:36 AM

IBM® z/OS® Management Facility (z/OSMF) provides a framework for managing various aspects of a z/OS system through a Web browser interface. By streamlining some traditional tasks and automating others, z/OSMF can help to simplify some areas of z/OS system management.

Log in to utilize and learn more about z/OSMF.

4. You should be presented with the "Welcome to IBM z/OS Management Facility" panel.
5. Expand the "**Configuration**" section in the list on the left side of the page if it is not already expanded ("+" means it is not expanded and "–" means that it is already expanded), and click on "**Configuration Assistant**" which is the only option in the expanded section.



Welcome to V2R1 Configuration Assistant for z/OS Communications Server

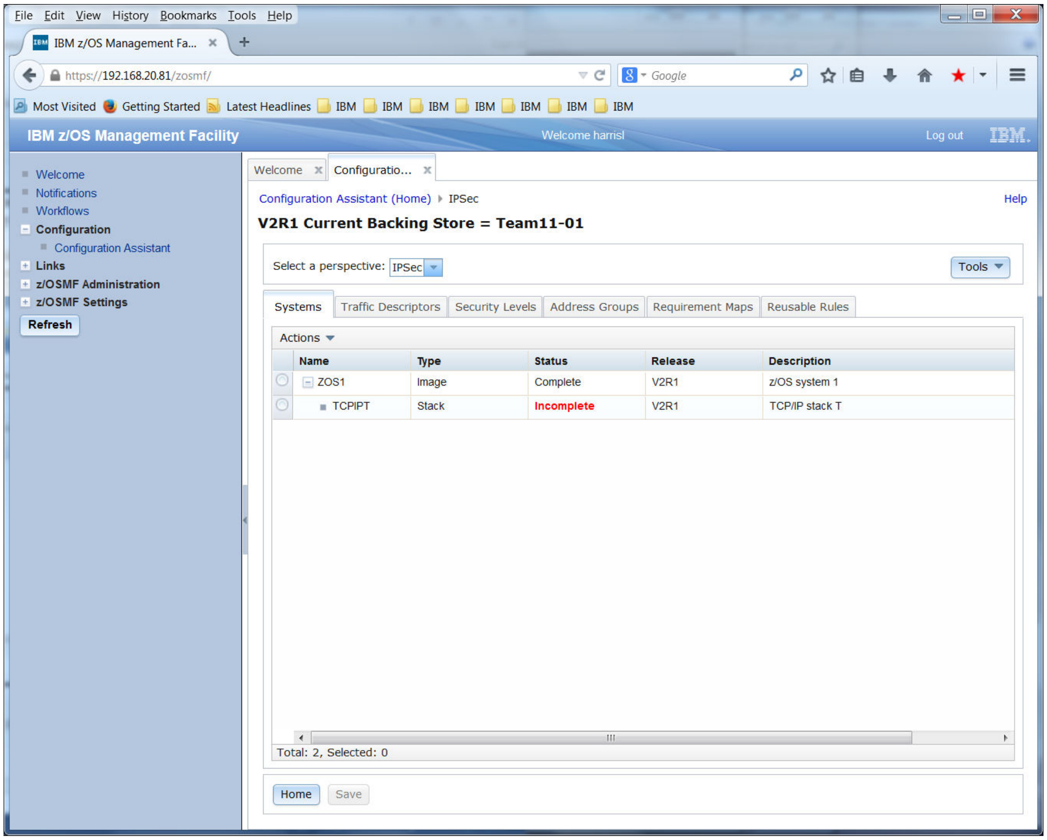
Use this task to create and manage configuration for z/OS Communications Server policy-based networking functions.

Select a backing store for configuration: saveData

Learn more about Configuration Assistant:

What's New	See what is new in this release.
Getting Started	First time users can learn about Configuration Assistant.
Migrating to z/OSMF	Migrate backing stores from Windows to z/OSMF.
Application Setup Tasks	Workflows to guide the setup of required applications.
Tutorials	Link to tutorials.
FAQs	Link to Frequently Asked Questions.

6. Configurations created by the Configuration Assistant tool are saved as Backing Store files. These files are binary files that are only usable by a Configuration Assistant tool.
   a) Select your last Backing Store file.
   b) Click on the **Open** button.



Configuration Assistant (Home) ▸ IPSec

V2R1 Current Backing Store = Team11-01

Select a perspective: IPSec

	Name	Type	Status	Release	Description
○	ZOS1	Image	Complete	V2R1	z/OS system 1
○	TCPIPT	Stack	Incomplete	V2R1	TCP/IP stack T

Total: 2, Selected: 0

7. If necessary use the drop-down to select the **AT-TLS** perspective.
8. Click on the radio button beside your test TCP/IP stack TCPIPT or TCPIPG.
9. Click on the "**Actions**" pull-down.
10. Select "**Rules…**"
11. If a pop-up appears asking if you would like a wizard to start for AT_TLS configuration click on the **Cancel** button.

Scenario 3: Configure AT-TLS Rules

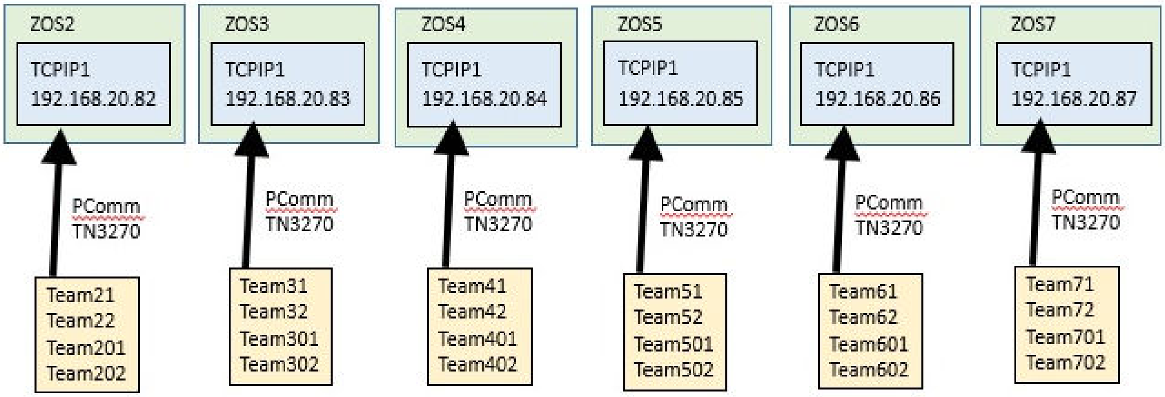
1. Use the “**Actions**” pull-down to select “**New…**”
2. Enter a Connectivity rule name (ie. **FTP-Client**).
3. Select the radio buttons beside the IPv4 address range for **Local data endpoint** and **Remote data endpoint**.
4. Enter Local and Remote data endpoint IP address range **192.168.20.91-192.168.20.107**.
5. Click on the **Next** button.
6. Enter a New Requirement Map Name (ie. **FTPClforATTLS**).
7. Optionally add a description.
8. Select the radio button beside the first row under the “Traffic Descriptor” heading.
9. Double click the “Select a traffic descriptor” field in the first row until the pull-down arrow appears on the right.
10. Use the pull-down to select the **FTP-Client**.
11. Double click the “Select a security level” field in the first row until the pull-down arrow appears on the right.
12. Use the pull-down to select the **AT-TLS_Gold**.
13. Click the radio button beside each of the following rows in turn and use the Action pull-down to select **Remove Row**.
14. Click on the **Next** button.
15. Click the **Finish** button.
16. Click the **Close** button.
17. Click on the **Traffic Descriptors** tab.
18. Use the radio button to select the **FTP-Client**.
19. Use the **Actions** pull-down to select “**Modify…**”
20. Use the radio button to select the only traffic type (Protocol = TCP, Local Port = All Ephemeral, Remote Port = 21, Connection Direction = Outbound)
21. Use the **Actions** pull-down to select “**Modify…**”
22. Click on the **KeyRing** tab.
23. In the Default AT-TLS key ring database section click the radio button for **Simple name**.
24. Enter Key ring name:
    a) USER21/LabClientRing
    b) USER22/LabClientRing
    c) USER31/LabClientRing
    d) USER32/LabClientRing
    e) USER41/LabClientRing
    f) USER42/LabClientRing
    g) USER51/LabClientRing
    h) USER52/LabClientRing
    i) USER61/LabClientRing
    j) USER62/LabClientRing
    k) USER71/LabClientRing
    l) USER72/LabClientRing
    m) USER201/LabClientRing
    n) USER202/LabClientRing
    o) USER301/LabClientRing
    p) USER302/LabClientRing
    q) USER401/LabClientRing
    r) USER402/LabClientRing
    s) USER501/LabClientRing
    t) USER502/LabClientRing
    u) USER601/LabClientRing
    v) USER602/LabClientRing
    w) USER701/LabClientRing
    x) USER702/LabClientRing
25. Click on the **OK** button twice.
26. You should get a warning pop-up message that the Traffic Descriptor that you are changing may be used by Connectivity Rules.
27. Click on **Proceed**.

28. You should get a warning pop-up message that your TCP/IP was modified as a result of the Traffic Descriptor change.
29. Click on the **OK** button.
30. Click on the **Save** button.
31. Optionally enter comments and click on **OK** button.
32. Click on the **Systems** tab.

Scenario 4: Install AT-TLS Rules

1. Click on the "**Actions**" drop down button and then select "**Install Configuration Files…**"
2. Select the "TCPIPT – AT-TLS Policy".
3. Click on the "**Actions**" drop down button and then select "**Install**".
4. Fill in your userid's unix home directory and file name with your TCP/IP stack name:
   a) /u/user21/ZOS2_TCPIP**T**_TTLS.policy
   b) /u/user22/ZOS2_TCPIP**T**_TTLS.policy
   c) /u/user31/ZOS3_TCPIP**T**_TTLS.policy
   d) /u/user32/ZOS3_TCPIP**T**_TTLS.policy
   e) /u/user41/ZOS4_TCPIP**T**_TTLS.policy
   f) /u/user42/ZOS4_TCPIP**T**_TTLS.policy
   g) /u/user51/ZOS5_TCPIP**T**_TTLS.policy
   h) /u/user52/ZOS5_TCPIP**T**_TTLS.policy
   i) /u/user61/ZOS6_TCPIP**T**_TTLS.policy
   j) /u/user62/ZOS6_TCPIP**T**_TTLS.policy
   k) /u/user71/ZOS7_TCPIP**T**_TTLS.policy
   l) /u/user72/ZOS7_TCPIP**T**_TTLS.policy
   m) /u/user201/ZOS2_TCPIP**G**_TTLS.policy
   n) /u/user202/ZOS2_TCPIP**G**_TTLS.policy
   o) /u/user301/ZOS3_TCPIP**G**_TTLS.policy
   p) /u/user302/ZOS3_TCPIP**G**_TTLS.policy
   q) /u/user401/ZOS4_TCPIP**G**_TTLS.policy
   r) /u/user402/ZOS4_TCPIP**G**_TTLS.policy
   s) /u/user501/ZOS5_TCPIP**G**_TTLS.policy
   t) /u/user502/ZOS5_TCPIP**G**_TTLS.policy
   u) /u/user601/ZOS6_TCPIP**G**_TTLS.policy
   v) /u/user602/ZOS6_TCPIP**G**_TTLS.policy
   w) /u/user701/ZOS7_TCPIP**G**_TTLS.policy
   x) /u/user702/ZOS7_TCPIP**G**_TTLS.policy
5. Click the radio button beside **FTP** to select the installation method.
6. Enter your TCPIP1 IP address for the system Host name:
   a) 192.168.20.82 for ZOS2
   b) 192.168.20.83 for ZOS3
   c) 192.168.20.84 for ZOS4
   d) 192.168.20.85 for ZOS5
   e) 192.168.20.86 for ZOS6
   f) 192.168.20.87 for ZOS7
7. Fill in your userid and password.
8. Click on the **Go** button.
9. When the pop-up "The FTP file transfer was successful.", click on the **OK** button.
10. Click on the **Close** button.
11. Optionally enter a comment and click on the **OK** button.
12. Click on the **Close** button.

Scenario 5: Test AT-TLS Policy on z/OS



1. On your Lab PC use PComm to logon to your z/OS system:
   a) 192.168.20.82 for ZOS2
   b) 192.168.20.83 for ZOS3
   c) 192.168.20.84 for ZOS4
   d) 192.168.20.85 for ZOS5
   e) 192.168.20.86 for ZOS6
   f) 192.168.20.87 for ZOS7
2. When you see the Message 10 screen from the TN3270 server, provide your userid with the logon command that has been built for this system. (The logon command is named "TSO", but it is a VTAM LOGON nevertheless.)
   a) **TSO <userid>**
3. On the ISPF signon screen, provide the password you were given in class.
   a) **<password>**
   b) Press **ENTER** (the PComm **ENTER key** is the **Right Ctrl** key)
4. Move to the SDSF panel when you see the **READY** prompt:
   a) **ispf**
5. Move to the TSO command interface:
   a) **6**
6. View the FTP Server Key Ring:
   a) **RACDCERT ID(FTPD) LISTRING(ServerRing1)**
7. View the FTP Server Certificate:
   a) **RACDCERT ID(TCPIP) LIST(LABEL('FTP on ANY ZOS')**
8. View your Key Ring:
   a) RACDCERT ID(USER21) LISTRING(LabClientRing)
   b) RACDCERT ID(USER22) LISTRING(LabClientRing)
   c) RACDCERT ID(USER31) LISTRING(LabClientRing)
   d) RACDCERT ID(USER32) LISTRING(LabClientRing)
   e) RACDCERT ID(USER41) LISTRING(LabClientRing)
   f) RACDCERT ID(USER42) LISTRING(LabClientRing)
   g) RACDCERT ID(USER51) LISTRING(LabClientRing)
   h) RACDCERT ID(USER52) LISTRING(LabClientRing)
   i) RACDCERT ID(USER61) LISTRING(LabClientRing)
   j) RACDCERT ID(USER62) LISTRING(LabClientRing)
   k) RACDCERT ID(USER71) LISTRING(LabClientRing)

   l) RACDCERT ID(USER72) LISTRING(LabClientRing)
   m) RACDCERT ID(USER201) LISTRING(LabClientRing)
   n) RACDCERT ID(USER202) LISTRING(LabClientRing)
   o) RACDCERT ID(USER301) LISTRING(LabClientRing)
   p) RACDCERT ID(USER302) LISTRING(LabClientRing)
   q) RACDCERT ID(USER401) LISTRING(LabClientRing)
   r) RACDCERT ID(USER402) LISTRING(LabClientRing)
   s) RACDCERT ID(USER501) LISTRING(LabClientRing)
   t) RACDCERT ID(USER502) LISTRING(LabClientRing)
   u) RACDCERT ID(USER601) LISTRING(LabClientRing)
   v) RACDCERT ID(USER602) LISTRING(LabClientRing)
   w) RACDCERT ID(USER701) LISTRING(LabClientRing)
   x) RACDCERT ID(USER702) LISTRING(LabClientRing)

9. View your Certificate:
   a) RACDCERT ID(USER21) LIST(LABEL('USER21 on ANY ZOS')
   b) RACDCERT ID(USER22) LIST(LABEL('USER22 on ANY ZOS')
   c) RACDCERT ID(USER31) LIST(LABEL('USER31 on ANY ZOS')
   d) RACDCERT ID(USER32) LIST(LABEL('USER32 on ANY ZOS')
   e) RACDCERT ID(USER41) LIST(LABEL('USER41 on ANY ZOS')
   f) RACDCERT ID(USER42) LIST(LABEL('USER42 on ANY ZOS')
   g) RACDCERT ID(USER51) LIST(LABEL('USER51 on ANY ZOS')
   h) RACDCERT ID(USER52) LIST(LABEL('USER52 on ANY ZOS')
   i) RACDCERT ID(USER61) LIST(LABEL('USER61 on ANY ZOS')
   j) RACDCERT ID(USER62) LIST(LABEL('USER62 on ANY ZOS')
   k) RACDCERT ID(USER71) LIST(LABEL('USER71 on ANY ZOS')
   l) RACDCERT ID(USER72) LIST(LABEL('USER72 on ANY ZOS')
   m) RACDCERT ID(USER201) LIST(LABEL('USER201 on ANY ZOS')
   n) RACDCERT ID(USER202) LIST(LABEL('USER202 on ANY ZOS')
   o) RACDCERT ID(USER301) LIST(LABEL('USER301 on ANY ZOS')
   p) RACDCERT ID(USER302) LIST(LABEL('USER302 on ANY ZOS')
   q) RACDCERT ID(USER401) LIST(LABEL('USER401 on ANY ZOS')
   r) RACDCERT ID(USER402) LIST(LABEL('USER402 on ANY ZOS')
   s) RACDCERT ID(USER501) LIST(LABEL('USER501 on ANY ZOS')
   t) RACDCERT ID(USER502) LIST(LABEL('USER502 on ANY ZOS')
   u) RACDCERT ID(USER601) LIST(LABEL('USER601 on ANY ZOS')
   v) RACDCERT ID(USER602) LIST(LABEL('USER602 on ANY ZOS')
   w) RACDCERT ID(USER701) LIST(LABEL('USER701 on ANY ZOS')
   x) RACDCERT ID(USER702) LIST(LABEL('USER702 on ANY ZOS')

10. When you are finished reviewing the certificate information return to the main ISPF panel:
    a) **PF3**

11. Enter **O.4** (the letter "O") to go to the OMVS Unix environment. Remember the PComm ENTER key is the Right Ctrl key.

12. Enter **su** to change into Super User mode.

13. View the Main Pagent Configuration file:
    a) **obrowse /etc/PAGT1/pagentt.conf**

14. Notice that the Main Pagent Configuration file points to the two z/OS image files:
    a) /etc/PAGT1/pagent.tcpipt.conf for TCP/IP stack TCPIPT
    b) /etc/PAGT1/pagent.tcpipg.conf for TCP/IP stack TCPIPG

15. **PF3** to exit out of browse.

16. View an image file that has been provided for you in your home directory:

a) **obrowse /u/user21/pagent.tcpipt.conf** for Team21
b) **obrowse /u/user22/pagent.tcpipt.conf** for Team22
c) **obrowse /u/user31/pagent.tcpipt.conf** for Team31
d) **obrowse /u/user32/pagent.tcpipt.conf** for Team32
e) **obrowse /u/user41/pagent.tcpipt.conf** for Team41
f) **obrowse /u/user42/pagent.tcpipt.conf** for Team42
g) **obrowse /u/user51/pagent.tcpipt.conf** for Team51
h) **obrowse /u/user52/pagent.tcpipt.conf** for Team52
i) **obrowse /u/user61/pagent.tcpipt.conf** for Team61
j) **obrowse /u/user62/pagent.tcpipt.conf** for Team62
k) **obrowse /u/user71/pagent.tcpipt.conf** for Team71
l) **obrowse /u/user72/pagent.tcpipt.conf** for Team72
m) **obrowse /u/user201/pagent.tcpipg.conf** for Team201
n) **obrowse /u/user202/pagent.tcpipg.conf** for Team202
o) **obrowse /u/user301/pagent.tcpipg.conf** for Team301
p) **obrowse /u/user302/pagent.tcpipg.conf** for Team302
q) **obrowse /u/user401/pagent.tcpipg.conf** for Team401
r) **obrowse /u/user402/pagent.tcpipg.conf** for Team402
s) **obrowse /u/user501/pagent.tcpipg.conf** for Team501
t) **obrowse /u/user502/pagent.tcpipg.conf** for Team502
u) **obrowse /u/user601/pagent.tcpipg.conf** for Team601
v) **obrowse /u/user602/pagent.tcpipg.conf** for Team602
w) **obrowse /u/user701/pagent.tcpipg.conf** for Team701
x) **obrowse /u/user702/pagent.tcpipg.conf** for Team702

17. Notice the AT-TLS policy file that is defined:
    a) TTLSConfig /u/user21/ZOS2_TCPIPT_TTLS.policy FLUSH PURGE
    b) TTLSConfig /u/user22/ZOS2_TCPIPT_TTLS.policy FLUSH PURGE
    c) TTLSConfig /u/user31/ZOS3_TCPIPT_TTLS.policy FLUSH PURGE
    d) TTLSConfig /u/user32/ZOS3_TCPIPT_TTLS.policy FLUSH PURGE
    e) TTLSConfig /u/user41/ZOS4_TCPIPT_TTLS.policy FLUSH PURGE
    f) TTLSConfig /u/user42/ZOS4_TCPIPT_TTLS.policy FLUSH PURGE
    g) TTLSConfig /u/user51/ZOS5_TCPIPT_TTLS.policy FLUSH PURGE
    h) TTLSConfig /u/user52/ZOS5_TCPIPT_TTLS.policy FLUSH PURGE
    i) TTLSConfig /u/user61/ZOS6_TCPIPT_TTLS.policy FLUSH PURGE
    j) TTLSConfig /u/user62/ZOS6_TCPIPT_TTLS.policy FLUSH PURGE
    k) TTLSConfig /u/user71/ZOS7_TCPIPT_TTLS.policy FLUSH PURGE
    l) TTLSConfig /u/user72/ZOS7_TCPIPT_TTLS.policy FLUSH PURGE
    m) TTLSConfig /u/user201/ZOS2_TCPIPT_TTLS.policy FLUSH PURGE
    n) TTLSConfig /u/user202/ZOS2_TCPIPT_TTLS.policy FLUSH PURGE
    o) TTLSConfig /u/user301/ZOS3_TCPIPT_TTLS.policy FLUSH PURGE
    p) TTLSConfig /u/user302/ZOS3_TCPIPT_TTLS.policy FLUSH PURGE
    q) TTLSConfig /u/user401/ZOS4_TCPIPT_TTLS.policy FLUSH PURGE
    r) TTLSConfig /u/user402/ZOS4_TCPIPT_TTLS.policy FLUSH PURGE
    s) TTLSConfig /u/user501/ZOS5_TCPIPT_TTLS.policy FLUSH PURGE
    t) TTLSConfig /u/user502/ZOS5_TCPIPT_TTLS.policy FLUSH PURGE
    u) TTLSConfig /u/user601/ZOS6_TCPIPT_TTLS.policy FLUSH PURGE
    v) TTLSConfig /u/user602/ZOS6_TCPIPT_TTLS.policy FLUSH PURGE
    w) TTLSConfig /u/user701/ZOS7_TCPIPT_TTLS.policy FLUSH PURGE
    x) TTLSConfig /u/user702/ZOS7_TCPIPT_TTLS.policy FLUSH PURGE
18. **PF3** to exit out of browse.

19. If you did not previously complete the IPSec lab successfully you can use an IPSec policy file that has been provided to you.
    a) If you created an IPSec policy file that you would like to save rename it first:
        - cp /u/user21/IPSec.policy.test /u/user21/ZOS2_TCPIPT_IPSec.policy
        - cp /u/user22/IPSec.policy.test /u/user22/ZOS2_TCPIPT_IPSec.policy
        - cp /u/user31/IPSec.policy.test /u/user31/ZOS3_TCPIPT_IPSec.policy
        - cp /u/user32/IPSec.policy.test /u/user32/ZOS3_TCPIPT_IPSec.policy
        - cp /u/user41/IPSec.policy.test /u/user41/ZOS4_TCPIPT_IPSec.policy
        - cp /u/user42/IPSec.policy.test /u/user42/ZOS4_TCPIPT_IPSec.policy
        - cp /u/user51/IPSec.policy.test /u/user51/ZOS5_TCPIPT_IPSec.policy
        - cp /u/user52/IPSec.policy.test /u/user52/ZOS5_TCPIPT_IPSec.policy
        - cp /u/user61/IPSec.policy.test /u/user61/ZOS6_TCPIPT_IPSec.policy
        - cp /u/user62/IPSec.policy.test /u/user62/ZOS6_TCPIPT_IPSec.policy
        - cp /u/user71/IPSec.policy.test /u/user71/ZOS7_TCPIPT_IPSec.policy
        - cp /u/user72/IPSec.policy.test /u/user72/ZOS7_TCPIPT_IPSec.policy
        - cp /u/user201/IPSec.policy.test /u/user201/ZOS2_TCPIPG_IPSec.policy
        - cp /u/user202/IPSec.policy.test /u/user202/ZOS2_TCPIPG_IPSec.policy
        - cp /u/user301/IPSec.policy.test /u/user301/ZOS3_TCPIPG_IPSec.policy
        - cp /u/user302/IPSec.policy.test /u/user302/ZOS3_TCPIPG_IPSec.policy
        - cp /u/user401/IPSec.policy.test /u/user401/ZOS4_TCPIPG_IPSec.policy
        - cp /u/user402/IPSec.policy.test /u/user402/ZOS4_TCPIPG_IPSec.policy
        - cp /u/user501/IPSec.policy.test /u/user501/ZOS5_TCPIPG_IPSec.policy
        - cp /u/user502/IPSec.policy.test /u/user502/ZOS5_TCPIPG_IPSec.policy
        - cp /u/user601/IPSec.policy.test /u/user601/ZOS6_TCPIPG_IPSec.policy
        - cp /u/user602/IPSec.policy.test /u/user602/ZOS6_TCPIPG_IPSec.policy
        - cp /u/user701/IPSec.policy.test /u/user701/ZOS7_TCPIPG_IPSec.policy
        - cp /u/user702/IPSec.policy.test /u/user702/ZOS7_TCPIPG_IPSec.policy
20. **Warning!** In the next steps you must coordinate your testing with the other team that is using your TCP/IP stack, if there is another team.
21. These teams must coordinate testing:
    a) Team21 and Team22 both use TCPIPT on ZOS2
    b) Team31 and Team32 both use TCPIPT on ZOS3
    c) Team41 and Team42 both use TCPIPT on ZOS4
    d) Team51 and Team52 both use TCPIPT on ZOS5
    e) Team61 and Team62 both use TCPIPT on ZOS6
    f) Team71 and Team72 both use TCPIPT on ZOS7
    g) Team201 and Team202 both use TCPIPG on ZOS2
    h) Team301 and Team302 both use TCPIPG on ZOS3
    i) Team401 and Team402 both use TCPIPG on ZOS4
    j) Team501 and Team502 both use TCPIPG on ZOS5
    k) Team601 and Team602 both use TCPIPG on ZOS6
    l) Team701 and Team702 both use TCPIPG on ZOS7
22. Copy your image file to directory /etc/PAGT1:
    a) **cp /u/user21/pagent.tcpipt.conf /etc/PAGT1/.**
    b) **cp /u/user22/pagent.tcpipt.conf /etc/PAGT1.**
    c) **cp /u/user31/pagent.tcpipt.conf /etc/PAGT1.**
    d) **cp /u/user32/pagent.tcpipt.conf /etc/PAGT1.**
    e) **cp /u/user41/pagent.tcpipt.conf /etc/PAGT1.**
    f) **cp /u/user42/pagent.tcpipt.conf /etc/PAGT1.**

   g) **cp /u/user51/pagent.tcpipt.conf /etc/PAGT1.**
   h) **cp /u/user52/pagent.tcpipt.conf /etc/PAGT1.**
   i) **cp /u/user61/pagent.tcpipt.conf /etc/PAGT1.**
   j) **cp /u/user62/pagent.tcpipt.conf /etc/PAGT1.**
   k) **cp /u/user71/pagent.tcpipt.conf /etc/PAGT1.**
   l) **cp /u/user72/pagent.tcpipt.conf /etc/PAGT1.**
   m) **cp /u/user201/pagent.tcpipg.conf /etc/PAGT1.**
   n) **cp /u/user202/pagent.tcpipg.conf /etc/PAGT1.**
   o) **cp /u/user301/pagent.tcpipg.conf /etc/PAGT1.**
   p) **cp /u/user302/pagent.tcpipg.conf /etc/PAGT1.**
   q) **cp /u/user401/pagent.tcpipg.conf /etc/PAGT1.**
   r) **cp /u/user402/pagent.tcpipg.conf /etc/PAGT1.**
   s) **cp /u/user501/pagent.tcpipg.conf /etc/PAGT1.**
   t) **cp /u/user502/pagent.tcpipg.conf /etc/PAGT1.**
   u) **cp /u/user601/pagent.tcpipg.conf /etc/PAGT1.**
   v) **cp /u/user602/pagent.tcpipg.conf /etc/PAGT1.**
   w) **cp /u/user701/pagent.tcpipg.conf /etc/PAGT1.**
   x) **cp /u/user702/pagent.tcpipg.conf /etc/PAGT1.**

23. Return to the ISPF panel by entering **exit** command twice (once to get out of su mode and once to get out of OMVS).
24. Policy Agent is also referred to as PAGENT because that is the default procedure name. In our lab the procedure name is PAGENTT. Please don't be confused by this. The same Policy Agent provides support for all three TCP/IP stacks: TCPIP1 (even though there are no policies defined for this stack), TCPIPT, and TCPIPG.
25. When Policy Agent is started or when a Modify, "F", command is issued, the Policy Agent will read in the defined policies and load them into the appropriate TCP/IP stack. It is the TCP/IP stack that enforces those policies.
26. **3.4** and press Enter
27. Dsname Level **SYS1.CS.TCPPARMS** and press Enter
28. **B** to the left of SYS1.CS.TCPPARMS and press Enter
29. **B** to the left of your PROFILE.TCPIP file and press Enter:

a) TCPS25 for TCPIPT on ZOS2	m) TCPS26 for TCPIPG on ZOS2
b) TCPS35 for TCPIPT on ZOS3	m) TCPS36 for TCPIPG on ZOS3
c) TCPS45 for TCPIPT on ZOS4	m) TCPS46 for TCPIPG on ZOS4
d) TCPS55 for TCPIPT on ZOS5	m) TCPS56 for TCPIPG on ZOS5
e) TCPS65 for TCPIPT on ZOS6	m) TCPS66 for TCPIPG on ZOS6
f) TCPS75 for TCPIPT on ZOS7	m) TCPS76 for TCPIPG on ZOS7

30. You should be viewing the PROFILE.TCPIP file for your TCP/IP stack. Notice the following:
   a) IPCONFIG IPSECURITY – required for IP Filtering and IPSec
   b) TCPCONFIG TTLS – required for AT-TLS
   c) **PF3** to exit when you are done reviewing the file.
31. **B** to the left of your FTP Client FTP.DATA file FTPCLSEC and press Enter.
   a) Notice section "12. Security options"
   b) **PF3** to exit when you are done reviewing the file.
32. **B** to the left of the FTP Server FTP.DATA file FTPSHSVR and press Enter.
   a) Notice section "12. Security options"
   b) **PF3** to exit when you are done reviewing the file.
33. Go to the ISPD Log:
   a) **D.LOG**
34. Display your TCP/IP stack's configuration:

   a) **/D TCPIP,TCPIPT,NETSTAT,CONFIG**
   b) **/D TCPIP,TCPIPG,NETSTAT,CONIG**

35. Notice the following:
    a) **TTLS: YES** – a result of IPCONFIG IPSECURITY in the profile file
    b) **IPSECURITY: YES** – a result of TCPCONFIG TTLS in the profile file
36. **Warning!** In the next steps you must coordinate your testing with the other teams using the same Policy Agent as you are:
    a) Team21, Team22, Team201, and Team202 on ZOS2
    b) Team31, Team32, Team301, and Team302 on ZOS3
    c) Team41, Team42, Team401, and Team402 on ZOS4
    d) Team51, Team52, Team501, and Team502 on ZOS5
    e) Team61, Team62, Team601, and Team602 on ZOS6
    f) Team71, Team72, Team701, and Team702 on ZOS7
37. Cause the Policy Agent to reread its policy files:
    a) **/F PAGENTT,UPDATE**
38. Let the other Teams on the other TCP/IP stack know that you are done updating the Policy Agent. The Team on your same TCP/IP stack will still be impacted in the following steps.
    a) If you are using TCPIPT on system ZOSn then let the Teams using TCPIPG on system ZOSn know you are done updating the Policy Agent.
    b) If you are using TCPIPG on system ZOSn then let the Teams using TCPIPT on system ZOSn know you are done updating the Policy Agent.
39. Return to OMVS to test the AT-TLS policies:
    a) **=o.4**
40. Use your FTP Client to connect to FTP Server on ZOS1:
    a) ftp –r TLS –f "//'SYS1.CS.TCPPARMS(FTPCLSEC)'" –p TCPIP**T** 192.168.20.91
    b) ftp –r TLS –f "//'SYS1.CS.TCPPARMS(FTPCLSEC)'" –p TCPIP**G** 192.168.20.101
41. If you FTP connection was successful you can login and then use the **quit** command when you are done testing, or use the right mouse button, select **PA1**, use the **quit** command, and then **4** to return to OMVS.
42. If your FTP connection was successful you should look at the messages in SyslogD.
    a) While you are in OMVS:
       i. **su**
       ii. **obrowse /var/syslogall.log**
    b) You have finished the lab and do not need to proceed any further.
       i. Remember to let the other Team that shares your TCP/IP stack know that you are done testing.
43. If the FTP fails you should use the **quit** command if necessary and continue with the rest of the lab.
44. You should do web searches on the errors you are getting.
    a) Look for errors in the SyslogD error log while you are in OMVS:
       i. **su**
       ii. **obrowse /var/syslogall.log**
    b) Debug should be added to the client command by inserting "**–d**" between "ftp" and "-r".
    c) Look for errors in the console log (=D.LOG)
45. Back in OMVS, make sure you are in your own directory:
    a) **pwd**

b) If you are not in your home directory then change to your directory:

  i. cd /u/user21
  ii. cd /u/user22
  iii. cd /u/user31
  iv. cd /u/user32
  v. cd /u/user41
  vi. cd /u/user42
  vii. cd /u/user51
  viii. cd /u/user52
  ix. cd /u/user61
  x. cd /u/user62
  xi. cd /u/user71
  xii. cd /u/user72
  xiii. cd /u/user201
  xiv. cd /u/user202
  xv. cd /u/user301
  xvi. cd /u/user302
  xvii. cd /u/user401
  xviii. cd /u/user402
  xix. cd /u/user501
  xx. cd /u/user502
  xxi. cd /u/user601
  xxii. cd /u/user602
  xxiii. cd /u/user701
  xxiv. cd /u/user702

46. You can test the environment to make sure it is setup correctly by testing with a working policy file that has been created for you.

a) Rename your policy file to a different file name.

- mv ZOS2_TCPIPT_TTLS.policy ZOS2_TCPIPT_TTLS.policy.failed
- mv ZOS3_TCPIPT_TTLS.policy ZOS3_TCPIPT_TTLS.policy.failed
- mv ZOS4_TCPIPT_TTLS.policy ZOS4_TCPIPT_TTLS.policy.failed
- mv ZOS5_TCPIPT_TTLS.policy ZOS5_TCPIPT_TTLS.policy.failed
- mv ZOS6_TCPIPT_TTLS.policy ZOS6_TCPIPT_TTLS.policy.failed
- mv ZOS7_TCPIPT_TTLS.policy ZOS7_TCPIPT_TTLS.policy.failed

b) Copy the one provided for you:

- cp /u/user21/TTLS.policy.test /u/user21/ZOS2_TCPIPT_TTLS.policy
- cp /u/user22/TTLS.policy.test /u/user22/ZOS2_TCPIPT_TTLS.policy
- cp /u/user31/TTLS.policy.test /u/user31/ZOS3_TCPIPT_TTLS.policy
- cp /u/user32/TTLS.policy.test /u/user32/ZOS3_TCPIPT_TTLS.policy
- cp /u/user41/TTLS.policy.test /u/user41/ZOS4_TCPIPT_TTLS.policy
- cp /u/user42/TTLS.policy.test /u/user42/ZOS4_TCPIPT_TTLS.policy
- cp /u/user51/TTLS.policy.test /u/user51/ZOS5_TCPIPT_TTLS.policy
- cp /u/user52/TTLS.policy.test /u/user52/ZOS5_TCPIPT_TTLS.policy
- cp /u/user61/TTLS.policy.test /u/user61/ZOS6_TCPIPT_TTLS.policy
- cp /u/user62/TTLS.policy.test /u/user62/ZOS6_TCPIPT_TTLS.policy
- cp /u/user71/TTLS.policy.test /u/user71/ZOS7_TCPIPT_TTLS.policy
- cp /u/user72/TTLS.policy.test /u/user72/ZOS7_TCPIPT_TTLS.policy
- cp /u/user201/TTLS.policy.test /u/user201/ZOS2_TCPIPG_TTLS.policy
- cp /u/user202/TTLS.policy.test /u/user202/ZOS2_TCPIPG_TTLS.policy
- cp /u/user301/TTLS.policy.test /u/user301/ZOS3_TCPIPG_TTLS.policy
- cp /u/user302/TTLS.policy.test /u/user302/ZOS3_TCPIPG_TTLS.policy
- cp /u/user401/TTLS.policy.test /u/user401/ZOS4_TCPIPG_TTLS.policy
- cp /u/user402/TTLS.policy.test /u/user402/ZOS4_TCPIPG_TTLS.policy
- cp /u/user501/TTLS.policy.test /u/user501/ZOS5_TCPIPG_TTLS.policy
- cp /u/user502/TTLS.policy.test /u/user502/ZOS5_TCPIPG_TTLS.policy
- cp /u/user601/TTLS.policy.test /u/user601/ZOS6_TCPIPG_TTLS.policy
- cp /u/user602/TTLS.policy.test /u/user602/ZOS6_TCPIPG_TTLS.policy
- cp /u/user701/TTLS.policy.test /u/user701/ZOS7_TCPIPG_TTLS.policy
- cp /u/user702/TTLS.policy.test /u/user702/ZOS7_TCPIPG_TTLS.policy

47. Use what you learned previously to test again.

48. Let the other Team that shares your TCP/IP stack know that you are done testing.

End of the Lab

Appendix: System Files

TCPIPT Proc

```
//TCPIPT PROC
PARMS='CTRACE(CTIEZB00)',PROF=TCP&CL1.A,DATA=DAT&CL1.A,
//   CS=SYS1
//*   CS=USER
//TCPIP  EXEC PGM=EZBTCPIP,REGION=0M,TIME=1440,
//   PARM='&PARMS'
//*           PARM='&MODULE,ERRFILE(SYSERR),HEAP(512),&PARMS'
//*TEPLIB  DD DSN=SYS1.TCPIP.SEZATCP,DISP=SHR
//*        DD DSN=SYS1.TCPIP.SEZALINK,DISP=SHR
//SYSPRINT DD SYSOUT=*,DCB=(RECFM=FB,LRECL=137,BLKSIZE=137)
//ALGPRINT DD SYSOUT=*,DCB=(RECFM=FB,LRECL=137,BLKSIZE=137)
//SYSOUT   DD SYSOUT=*,DCB=(RECFM=FB,LRECL=137,BLKSIZE=137)
//CEEDUMP  DD SYSOUT=*,DCB=(RECFM=FB,LRECL=137,BLKSIZE=137)
//SYSERROR DD SYSOUT=*
//SYSMDUMP DD SYSOUT=*
//SYSERR   DD SYSOUT=*
//SYSDEBUG DD SYSOUT=*
//PROFILE  DD DSN=&CS..CS.TCPPARMS(&PROF),DISP=SHR
//SYSTCPD  DD DSN=&CS..CS.TCPPARMS(&DATA),DISP=SHR
```

TCPIPG Proc

```
//TCPIPG PROC
PARMS='CTRACE(CTIEZB00)',PROF=TCPS&CL1.3,DATA=DATAG,
//   CS=SYS1
//*   CS=USER
//TCPIP  EXEC PGM=EZBTCPIP,REGION=0M,TIME=1440,
//   PARM='&PARMS'
//*           PARM='&MODULE,ERRFILE(SYSERR),HEAP(512),&PARMS'
//*TEPLIB  DD DSN=SYS1.TCPIP.SEZATCP,DISP=SHR
//*        DD DSN=SYS1.TCPIP.SEZALINK,DISP=SHR
//SYSPRINT DD SYSOUT=*,DCB=(RECFM=FB,LRECL=137,BLKSIZE=137)
//ALGPRINT DD SYSOUT=*,DCB=(RECFM=FB,LRECL=137,BLKSIZE=137)
//SYSOUT   DD SYSOUT=*,DCB=(RECFM=FB,LRECL=137,BLKSIZE=137)
//CEEDUMP  DD SYSOUT=*,DCB=(RECFM=FB,LRECL=137,BLKSIZE=137)
//SYSERROR DD SYSOUT=*
//SYSMDUMP DD SYSOUT=*
//SYSERR   DD SYSOUT=*
//SYSDEBUG DD SYSOUT=*
//PROFILE  DD DSN=&CS..CS.TCPPARMS(&PROF),DISP=SHR
//SYSTCPD  DD DSN=&CS..CS.TCPPARMS(&DATA),DISP=SHR
```

Pagent Main Configuration File

```
# CHANGE RECORD
# =================================================================
# Change for Winter Share 2015                        LLH 02/22/15
# =================================================================
#
# LogLevel Statement
# LogLevel 31
# LogLevel 127
  LogLevel 511
#
# TcpImage and PEPInstance Statements (synonyms)
  TcpImage TCPIPT /etc/PAGT1/pagent.tcpipt.conf FLUSH PURGE 3600
  TcpImage TCPIPG /etc/PAGT1/pagent.tcpipg.conf FLUSH PURGE 3600
#
```

Pagent TCPIPT Image Configuration File

```
# CHANGE RECORD
# =================================================================
# Change for Winter Share 2015                        LLH 02/22/15
#
===================================================================
#
# IDSConfig Statements
  IDSConfig /u/user21/ZOS2_TCPIPT_IDS.policy FLUSH PURGE
#
# IPSecConfig Statements
  IPSecConfig /u/user11/ZOS2_TCPIPT_IPSec.policy
#
# RoutingConfig Statements
  RoutingConfig /u/user21/ZOS2_TCPIPT_Routing.policy
#
# TTLSConfig Statements
  TTLSConfig /u/user11/ZOS2_TCPIPT_TTLS.policy FLUSH PURGE
#
# QOSConfig Statement
  QOSConfig /u/user21/ZOS2_TCPIPT_QoS.policy
#
```

Pagent TCPIPG Image Configuration File

```
# CHANGE RECORD
# =================================================================
# Change for Winter Share 2015                        LLH 02/22/15
#
===================================================================
#
# IDSConfig Statements
  IDSConfig /u/user201/ZOS2_TCPIPG_IDS.policy FLUSH PURGE
```

```
#
# IPSecConfig Statements
 IPSecConfig /u/user201/ZOS2_TCPIPG_IPSec.policy
#
# RoutingConfig Statements
 RoutingConfig /u/user201/ZOS2_TCPIPG_Routing.policy
#
# TTLSConfig Statements
 TTLSConfig /u/user201/ZOS2_TCPIPG_TTLS.policy FLUSH PURGE
#
# QOSConfig Statement
 QOSConfig /u/user201/ZOS2_TCPIPG_QoS.policy
#
```

FTP Server Data File

```
;********************************************************
;                                                       *
;   Name of File: tcpip.SEZAINST(FTPSDATA)              *
;                                                       *
;   Descriptive Name: FTP.DATA  (for the FTP Server)    *
;                                                       *
…
; -------------------------------------------------------
;
; 12. Security options
;
; -------------------------------------------------------

EXTENSIONS        AUTH_TLS          ; Enable TLS
                                    ; authentication
                                   ; Default is disabled.

;SECURE_MECHANISM   TLS            ; Not used on Server
                                   ; Client only

TLSMECHANISM       ATTLS           ; FTP or ATTLS


SECURE_FTP        ALLOWED          ; Authentication
                                   ; indicator

SECURE_LOGIN      NO_CLIENT_AUTH   ; Authorization level
                                   ; indicator
                                   ; for TLS

SECURE_PASSWORD   REQUIRE          ; REQUIRED (D)
                                   ; User must enter
                                   ;     password

SECURE_CTRLCONN   PRIVATE         ; Minimum level of
```

```
                                   ; security for
                                   ; the control
                                   ; connection

SECURE_DATACONN   CLEAR            ; Minimum level of
                                   ; security for
                                   ; the data
                                   ; connection

TLSRFCLEVEL       RFC4217          ; Specify what level
                                   ; of RFC 4217
```

FTP Client

```
;********************************************************
;                                                       *
;   Name of File: tcpip.SEZAINST(FTCDATA)               *
;                                                       *
;   Descriptive Name: FTP.DATA  (for the FTP Client)    *
;                                                       *
…
; --------------------------------------------------------
;
; 12. Security options
;
; --------------------------------------------------------

SECURE_MECHANISM    TLS    ; Name of the security
                           ; mechanism
                           ; that the client uses when
                           ; it sends an AUTH command
                           ; to the server.

TLSMECHANISM       ATTLS           ; FTP or ATTLS


SECURE_FTP        ALLOWED          ; Authentication
                                   ; indicator

SECURE_CTRLCONN   PRIVATE         ; Minimum level of
                                   ; security for
                                   ; the control
                                   ; connection

SECURE_DATACONN   CLEAR            ; Minimum level of
                                   ; security for
                                   ; the data
                                   ; connection

TLSRFCLEVEL       RFC4217          ; Specify what level
                                   ; of RFC 4217
```

FTP Server Key Ring

```
Ring:
     >ServerRing1<
Certificate Label Name          Cert Owner   USAGE    DEFAULT
------------------------------ ----------   -------- -------
FTP on ANY ZOS                 ID(TCPIP)    PERSONAL YES
WSC LABS Certificate Authority CERTAUTH     CERTAUTH NO
```

FTP Server Certificate

```
Label: FTP on ANY ZOS
Certificate ID: 2QXjw9fJ18bj10CWlUDB1ehA6dbi
Status: TRUST
Start Date: 2009/02/09 00:00:00
End Date:   2020/02/09 23:59:59
Serial Number:
     >36<
Issuer's Name:
     >CN=WSCCA.LABS.IBM.COM.O=IBM.C=US<
Subject's Name:
     >CN=FTP.WSC.LABS.IBM.COM.O=IBM.C=US<
Subject's AltNames:
  EMail: FTP at WSC.LABS.IBM.COM
Signing Algorithm: sha1RSA
Key Type: RSA
Key Size: 1024
Private Key: YES
Ring Associations:
  Ring Owner: FTPD
  Ring:
     >ServerRing1<
```

User Key Ring

```
Ring:
     >LabClientRing<
Certificate Label Name          Cert Owner USAGE    DEFAULT
------------------------------ ---------- -------- -------
USER21 on ANY ZOS              ID(USER21) PERSONAL YES
WSC LABS Certificate Authority CERTAUTH   CERTAUTH NO
```

User Certificate

```
Label: USER21 on ANY ZOS
Certificate ID: 2Qbk4sXZ8vHk4sXZ8vFAlpVAwdXoQOnW4kBA
Status: TRUST
Start Date: 2009/02/09 00:00:00
End Date:   2020/02/09 23:59:59
Serial Number:
     >41<
Issuer's Name:
     >CN=WSCCA.LABS.IBM.COM.O=IBM.C=US<
Subject's Name:
     >CN=USER21.WSC.LABS.IBM.COM.O=IBM.C=US<
```

```
Subject's AltNames:
  EMail: USER21 at WSC.LABS.IBM.COM
Signing Algorithm: sha1RSA
Key Type: RSA
Key Size: 1024
Private Key: YES
Ring Associations:
  Ring Owner: FTPD
  Ring:
     >ClientRing1<
  Ring Owner: USER21
  Ring:
     >LabClientRing<
```