

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

"Familiarizing Yourself with the Lab Environment"

Hands-on Lab Guide (Workstation and z/OS Exercises)



The MVS assigned to me (MVS $\textcolor{blue}{n}$)

MVS _____

My userid (USER $\textcolor{blue}{nx}$)

USER _____

My password

HLQ of My MVS Datasets

USER.CS._____

My UNIX Subdirectory (/u/user $\textcolor{blue}{nx}$)

/u/user.....

The lab is divided into several sections:

- *Part 0: Familiarizing Yourself with the Lab Environment; Userids and Passwords*
- *Part 1: Customizing Your Workstation for the Labs*
- *Part 2: Reviewing the z/OS Environment at Your MVS Image*
- *Part 3: Reviewing the UNIX System Services (USS) or Open MVS (OMVS) Environment on the z/OS Lab Systems*

NOTE: This version of the lab utilizes the zOSMF (z/OS Management Facility) web application version of the Configuration Assistant.



- Please maintain the integrity of the lab systems!
- Do not customize the systems beyond what is asked of you in the labs!
- You may not use the provided Communications Server Configuration Assistant z/OSMF for any purposes outside of this Workshop.
- You are not authorized to copy or reproduce the materials for any purpose outside of this Workshop.

Revision date -

Friday, 13 June 2025

This edition applies to IBM z/OS Configuration Assistant running in zOSMF on z/OS V3.1.

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

Part 0: Lab Environment, Userids, Passwords for the Labs	4
Specific Lab Description: Familiarizing Yourself with the Lab Environment.....	5
IBM Box and Lecture Materials	5
Userids and Passwords.....	5
Workstation Configuration	6
Access to Files on z/OS	6
Userids and Assigned MVS Images	7
Part 1: Customizing Your Workstation for the Labs	9
Exploring the Workstation Directory for the Class	9
Accessing z/OSMF Configuration Assistant for z/OS Communications Server.....	10
Configuring PCOMM.....	28
Part 2: Reviewing the z/OS Environment at Your MVS Image	31
Part 3: Reviewing the UNIX Environment at Your MVS Image	35
End of Environment Lab.....	35

Part 0: Lab Environment, Userids, Passwords for the Labs

Each student ZOS (MVS) system has two TCP/IP stacks running in it. The basic TCPIP stack is named TCPIP1. The TN3270 procedure that has affinity to TCPIP1 is named TN3270. The FTP procedure that has affinity to TCPIP1 is named FTPCCL(1).

In our labs you use TCPIP1 for basic maintenance on ZOS until you begin working with 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 test TCP/IP stack named TCPIPT.

The students customize stack TCPIPT and not the “maintenance” stack, TCPIP1. The students also customize any other procedures that are part of the security labs and that are to have affinity with TCPIPT.

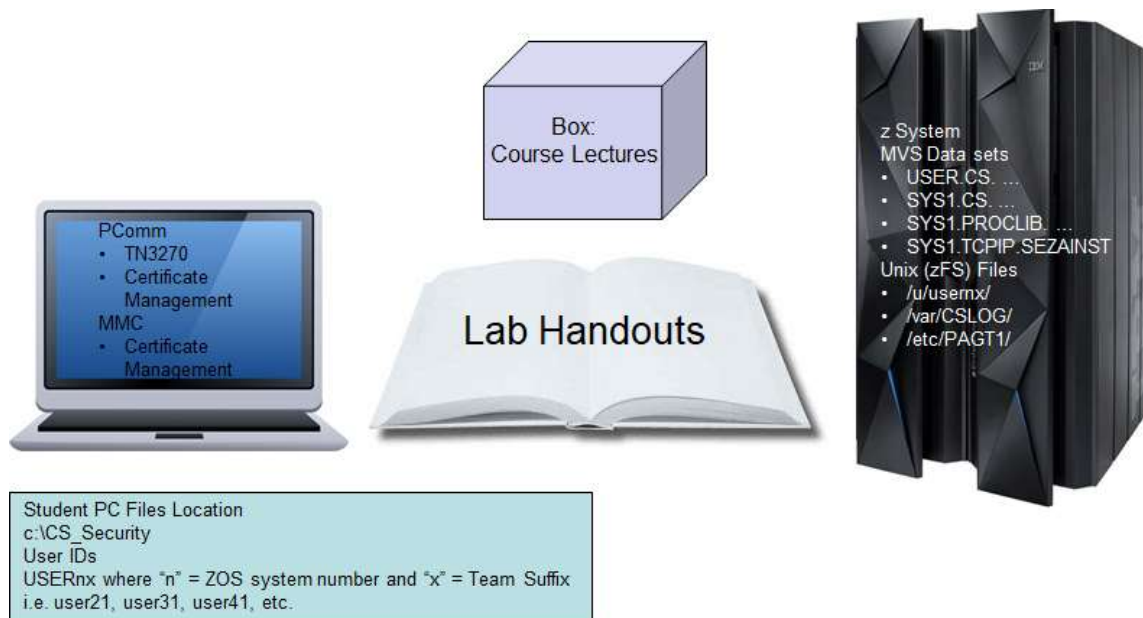
There are eight “Student ZOS (MVS) systems”.

Note that the labs are behind a firewall that performs Network Address Translation (NAT). On the lab systems themselves you will configure addresses in the 192.168.20.64/26 network.

Your workstations are also behind the firewall.

Please note that you have access to the INTERNET but NOT to the IBM INTRANET in these labs.

Specific Lab Description: Familiarizing Yourself with the Lab Environment



IBM Box and Lecture Materials

At the start of class you will be given access to IBM Box containing the Lecture Visuals and Notes in PDF format. You may follow the lectures from your workstation or from your own laptop if you have brought it with you.

Userids and Passwords

At the start of the class you will be assigned a Team USERID, in the form "USERIDnx," where "n" stands for the MVS number you are to work on and "x" represents your team suffix. (Up to three teams may be assigned to a single MVS system.) USERIDs are USER21, USER22, USER23 through USER93 on MVS systems ZOS2, ZOS3, ZOS4, ZOS5, ZOS6, ZOS7, ZOS8, and ZOS9. The password for the TSO Userids will be handed out before the first lab.

LEGEND for the TEAM Number:

TEAMnx, where "n" represents your ZOS suffix and "x" represents your userid suffix.

EXAMPLE: TEAM53 means ZOS5 and USERID of USER53.

Workstation Configuration

Your workstation contains most of the files you need in the C:\CS_Security directory under Windows.

In addition, you will be taking advantage of Personal Communications (PCOMM) for TN3270 connections to your MVS system. Also note that you may have a collection of technical manuals installed on your workstations. You may want to consult these manuals during the Labs.

Access to Files on z/OS

Your MVS (z/OS) system is set up to allow you full access to the MVS datasets that begin with the high-level qualifiers of USER.CS. You have READ access to the datasets that start with "SYS1." In UNIX you have permission to switch to SuperUser mode and will be told to do so during the labs.

You have UNIX identities on the MVS systems and you have a directory in /u/usernx (where "nx" is the number of your team). You are not a SuperUser, but you are permitted to BPX.SUPERUSER. (UNIXPRIV and RACF Access Control Lists – ACLs – are preferred over BPX.SUPERUSER in a highly secure UNIX environment, but these are lab systems that don't require that kind of control.)

Userids and Assigned MVS Images

1. LEGEND for the TEAM Number and USERID value:
 - a. USER_nx, where “n” represents your ZOS suffix number (e.g., 1 through 9) and “x” represents a suffix of 1 through 3).
 - b. EXAMPLE:
 - i. USER₅3 means Team53, ZOS5, and ZOS suffix number 3.
2. Examine the Full Network Logical Diagram above and note the TN3270 and FTP Addresses of the “maintenance” stack named TCPIP1.
 - a. **If you are assigned to MVS1, you connect to IP @ 192.168.20.81**
 - b. **If you are assigned to MVS2, you connect to IP @ 192.168.20.82**
 - c. **If you are assigned to MVS3, you connect to IP @ 192.168.20.83**
 - d. **If you are assigned to MVS4, you connect to IP @ 192.168.20.84**
 - e. **If you are assigned to MVS5, you connect to IP @ 192.168.20.85**
 - f. **If you are assigned to MVS6, you connect to IP @ 192.168.20.86**
 - g. **If you are assigned to MVS7, you connect to IP @ 192.168.20.87**
 - h. **If you are assigned to MVS8, you connect to IP @ 192.168.20.88**
 - i. **If you are assigned to MVS9, you connect to IP @ 192.168.20.89**
3. Here are the team assignments you will use in this workshop.
 - a. Team 21 codes for TCPIPT at **192.168.20.92 & 101 in MVS2**
 - i. Team 21 is User ID of “**USER21**”
 - b. Team 22 codes for TCPIPT at 192.168.20.92 & 101 in MVS2
 - i. Team 22 is User ID of “**USER22**”
 - c. Team 23 codes for TCPIPT at 192.168.20.92 & 101 in MVS2
 - i. Team 23 is User ID of “**USER23**”
 - d. Team 31 codes for TCPIPT at **192.168.20.93 & 102 in MVS3**
 - i. Team 31 is User ID of “**USER31**”
 - e. Team 32 codes for TCPIPT at 192.168.20.93 & 102 in MVS3
 - i. Team 32 is User ID of “**USER32**”
 - f. Team 33 codes for TCPIPT at 192.168.20.93 & 102 in MVS3
 - i. Team 33 is User ID of “**USER33**”
 - g. Team 41 codes for TCPIPT at **192.168.20.94 & 103 in MVS4**
 - i. Team 41 is User ID of “**USER41**”
 - h. Team 42 codes for TCPIPT at 192.168.20.94 & 103 in MVS4
 - i. Team 42 is User ID of “**USER42**”
 - i. Team 43 codes for TCPIPT at 192.168.20.94 & 103 in MVS4
 - i. Team 43 is User ID of “**USER43**”
 - j. Team 51 codes for TCPIPT at **192.168.20.95 & 104 in MVS5**
 - i. Team 51 is User ID of “**USER51**”
 - k. Team 52 codes for TCPIPT at 192.168.20.95 & 104 in MVS5
 - i. Team 52 is User ID of “**USER52**”
 - l. Team 53 codes for TCPIPT at 192.168.20.95 & 104 in MVS5
 - i. Team 53 is User ID of “**USER53**”

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

- m. Team 61 codes for TCPIPT at **192.168.20.96 & 105 in MVS6**
 - i. Team 61 is User ID of **“USER61”**
- n. Team 62 codes for TCPIPT at 192.168.20.96 & 105 in MVS6
 - i. Team 62 is User ID of **“USER62”**
- o. Team 63 codes for TCPIPT at 192.168.20.96 & 105 in MVS6
 - i. Team 63 is User ID of **“USER63”**
- p. Team 71 codes for TCPIPT at **192.168.20.97 & 106 in MVS7**
 - i. Team 71 is User ID of **“USER71”**
- q. Team 72 codes for TCPIPT at 192.168.20.97 & 106 in MVS7
 - i. Team 72 is User ID of **“USER72”**
- r. Team 73 codes for TCPIPT at 192.168.20.97 & 106 in MVS7
 - i. Team 73 is User ID of **“USER73”**
- s. Team 81 codes for TCPIPT at **192.168.20.98 & 107 in MVS8**
 - i. Team 81 is User ID of **“USER81”**
- t. Team 82 codes for TCPIPT at 192.168.20.98 & 106 in MVS8
 - i. Team 82 is User ID of **“USER82”**
- u. Team 83 codes for TCPIPT at 192.168.20.98 & 106 in MVS8
 - i. Team 83 is User ID of **“USER83”**
- v. Team 91 codes for TCPIPT at **192.168.20.99 & 108 in MVS9**
 - i. Team 91 is User ID of **“USER91”**
- w. Team 92 codes for TCPIPT at 192.168.20.99 & 106 in MVS9
 - i. Team 92 is User ID of **“USER92”**
- x. Team 93 codes for TCPIPT at 192.168.20.99 & 106 in MVS9
 - i. Team 93 is User ID of **“USER93”**

Part 1: Customizing Your Workstation for the Labs

You must accomplish three tasks:

- You are to explore the documentation available to you on the workstation.
- You are to connect to z/OSMF so that you can build your Security Policies with it.
- You are to create a Personal Communications (PCOMM) TN3270 client configuration to reach the “Maintenance” TCPIP1 stack at your MVS.

Exploring the Workstation Directory for the Class

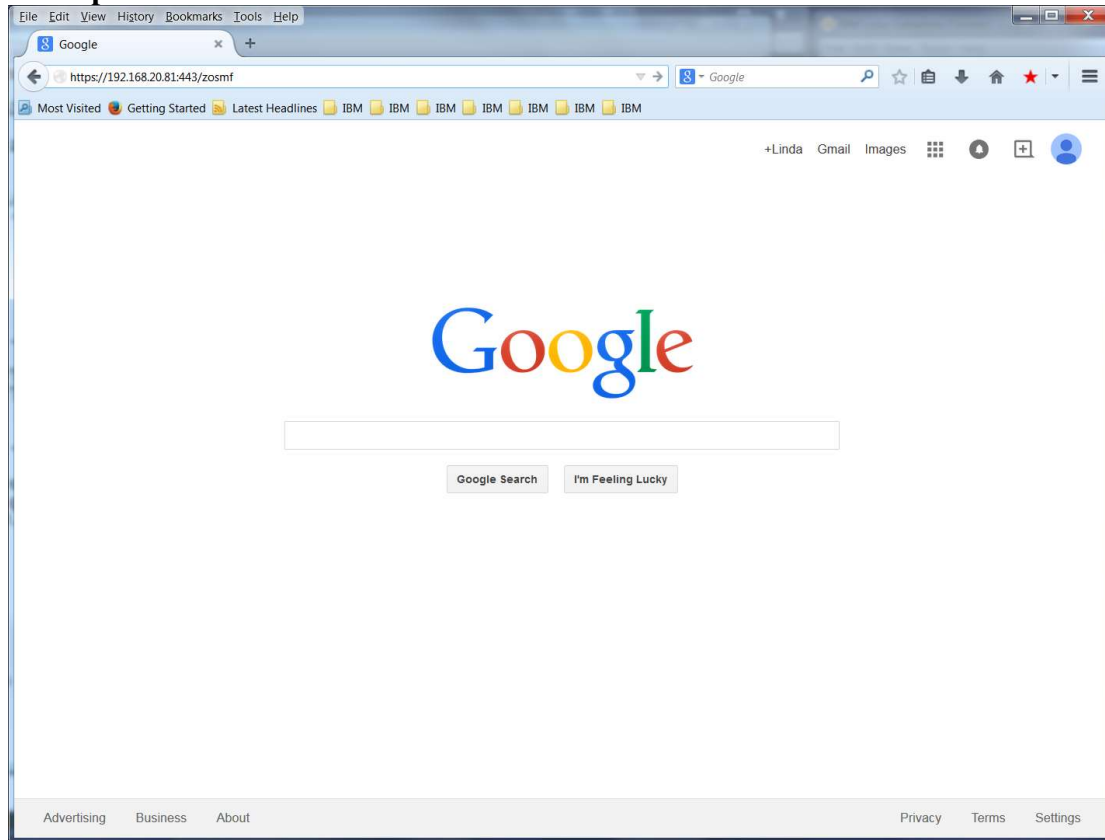
Workshop Policy Rule: *Maintain the integrity of the lab systems; please do not alter anything unless the labs indicate to do so.*

1. Examine the contents of the C:\CS_Security directory on your lab PC:
 - a. Click on the Windows **Start**
 - i. Select **Computer**
 - ii. Expand the **Computer** section
 - iii. Expand **Local Disk (C:)**
 - iv. Expand **CS_Security**
 - v. **If not on the C-drive, this folder may be stored elsewhere and you can perform a Windows search for it.**
 - b. Publications provided in the Pubs subdirectory. **Check to see that these publications are available to you during the workshop:**
 - i. **IP Configuration Guide**
 - ii. **IP Configuration Reference**
 - iii. **IP Diagnosis Guide**
 - iv. **IP System Administrator Guide (contains IP commands)**
 - v. **Redbook: Security Policy (IP Implementation Vol. 4)**
 - vi. **4 Volumes of IP Messages**
 - vii. **RACF Administrator Guide**
 - viii. **RACF Commands Reference**
 - ix. **System SSL Programming Guide**
 - x. **z/OS Migration Manual**
 - xi. **Additional miscellaneous manuals (ICSF, PKI Services, etc.)**

Accessing z/OSMF Configuration Assistant for z/OS Communications Server

1. Open a Web Browser window and go to URL:

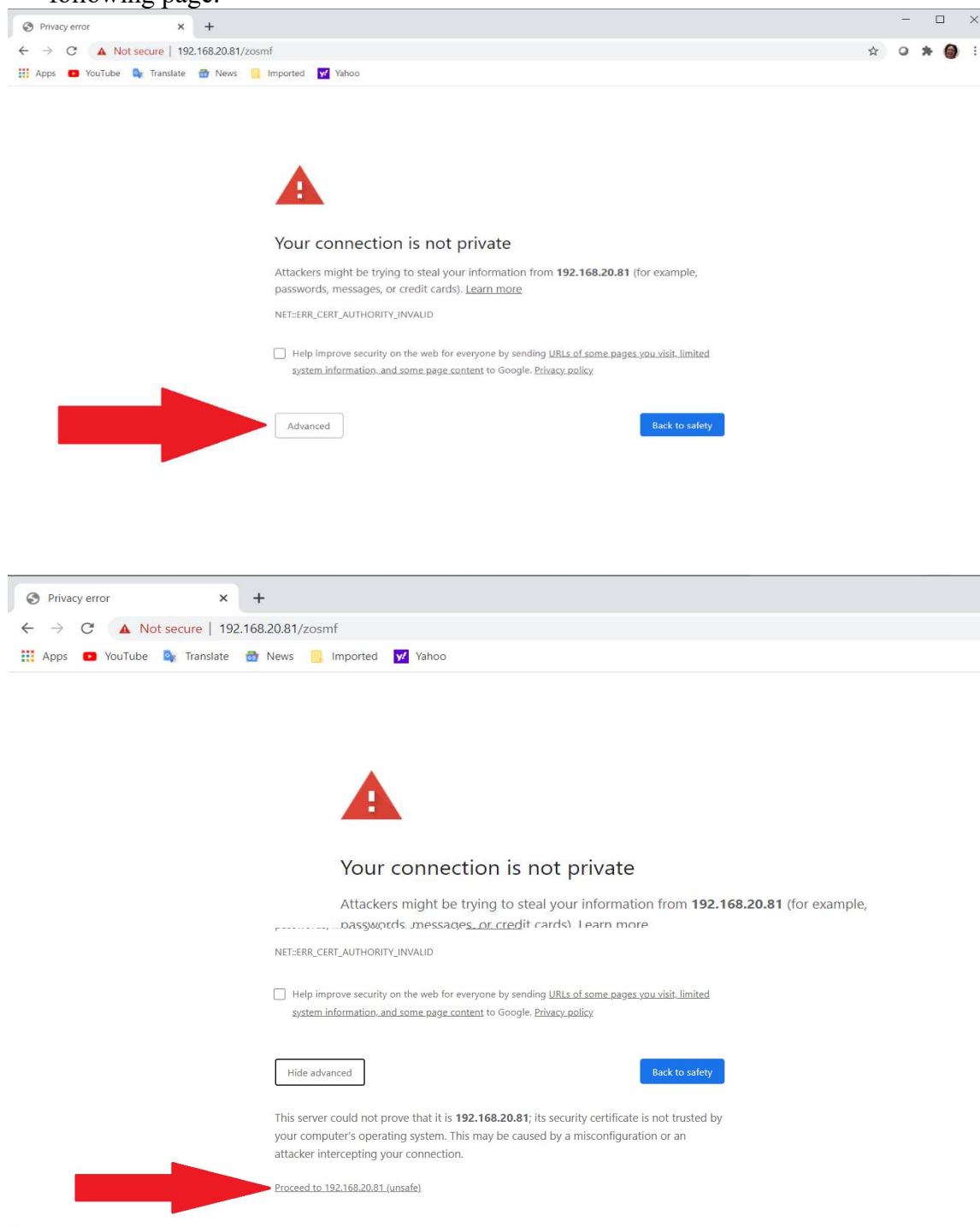
<https://192.168.20.81:443/zosmf>



Port 443 is the default HTTPS port so it actually may be omitted and **<https://192.168.20.81/zosmf>** will work just as well.

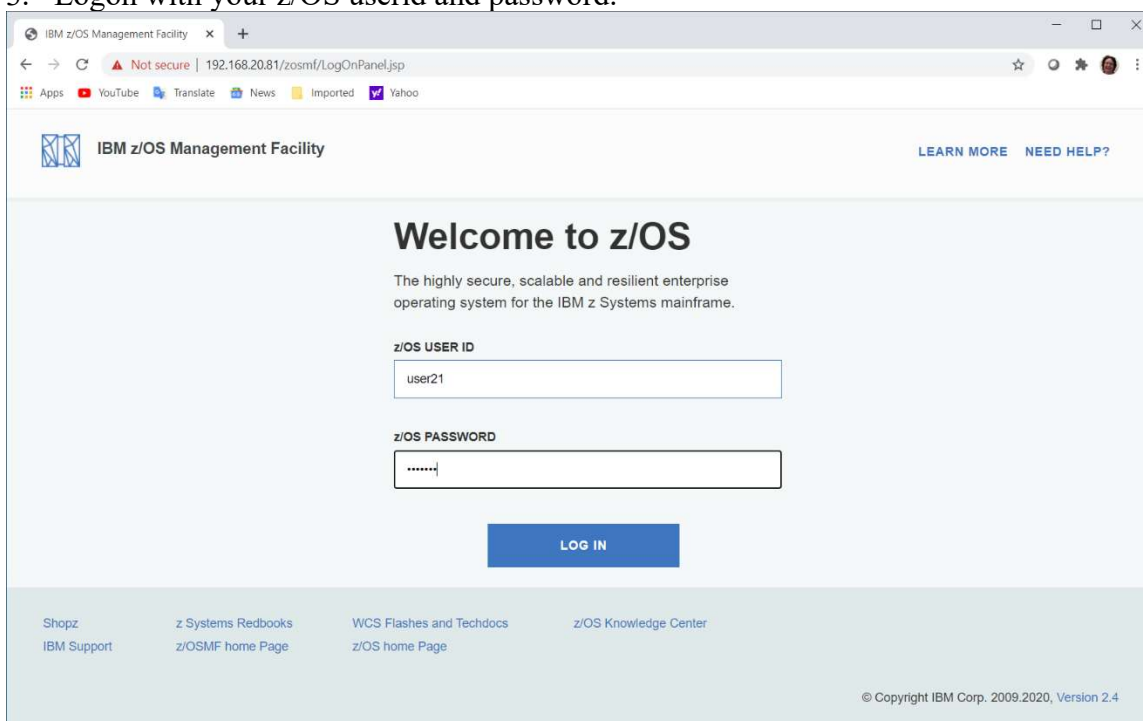
Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

2. If you receive a certificate error from your browser, click on “Advanced” and then “Proceed to 192.168.20.81”. Otherwise, skip down to the Login directions on the following page.

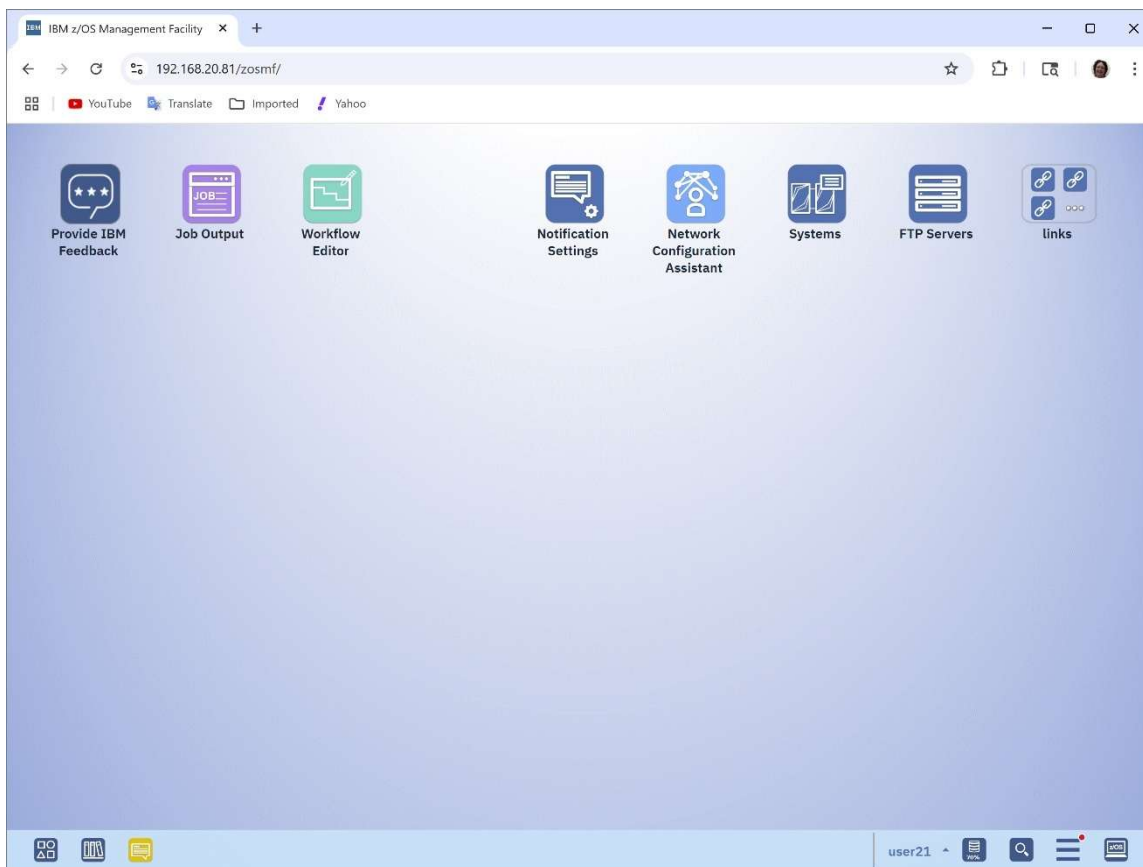


Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

3. Logon with your z/OS userid and password.



The screenshot shows a web browser window with the title "IBM z/OS Management Facility". The address bar shows the URL "192.168.20.81/zosmf/LogOnPanel.jsp". The page features the IBM logo and the text "IBM z/OS Management Facility" with links for "LEARN MORE" and "NEED HELP?". The main heading is "Welcome to z/OS", followed by the description: "The highly secure, scalable and resilient enterprise operating system for the IBM z Systems mainframe." Below this, there are two input fields: "z/OS USER ID" with the text "user21" and "z/OS PASSWORD" with masked characters. A blue "LOG IN" button is centered below the password field. At the bottom, there are links for "Shopz", "IBM Support", "z Systems Redbooks", "z/OSMF home Page", "WCS Flashes and Techdocs", "z/OS home Page", and "z/OS Knowledge Center". The footer text is "© Copyright IBM Corp. 2009.2020, Version 2.4".

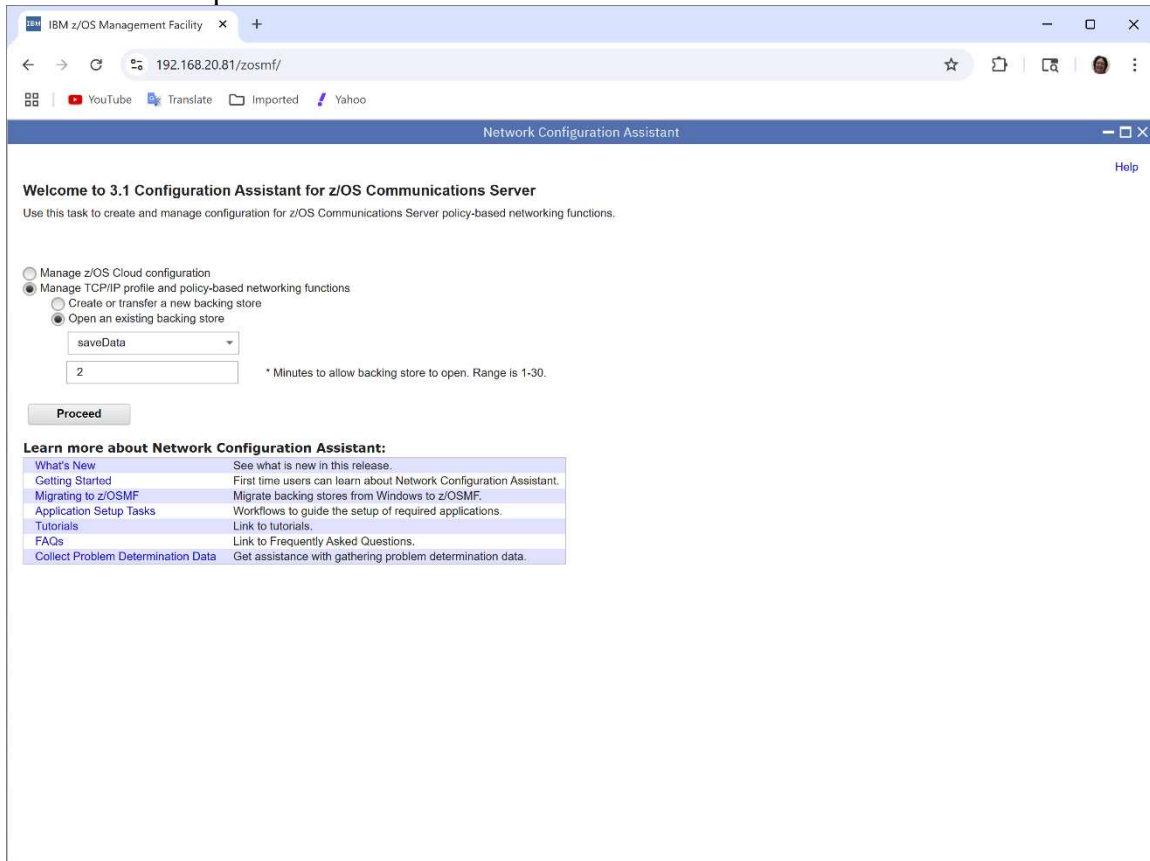


Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

4. Feel free to click on the numerous links to learn more about zOSMF. The lab instructor is not able to answer any question about them except the “Network Configuration Assistant”.
5. When you are finished exploring the page, double click on “**Network Configuration Assistant**”.

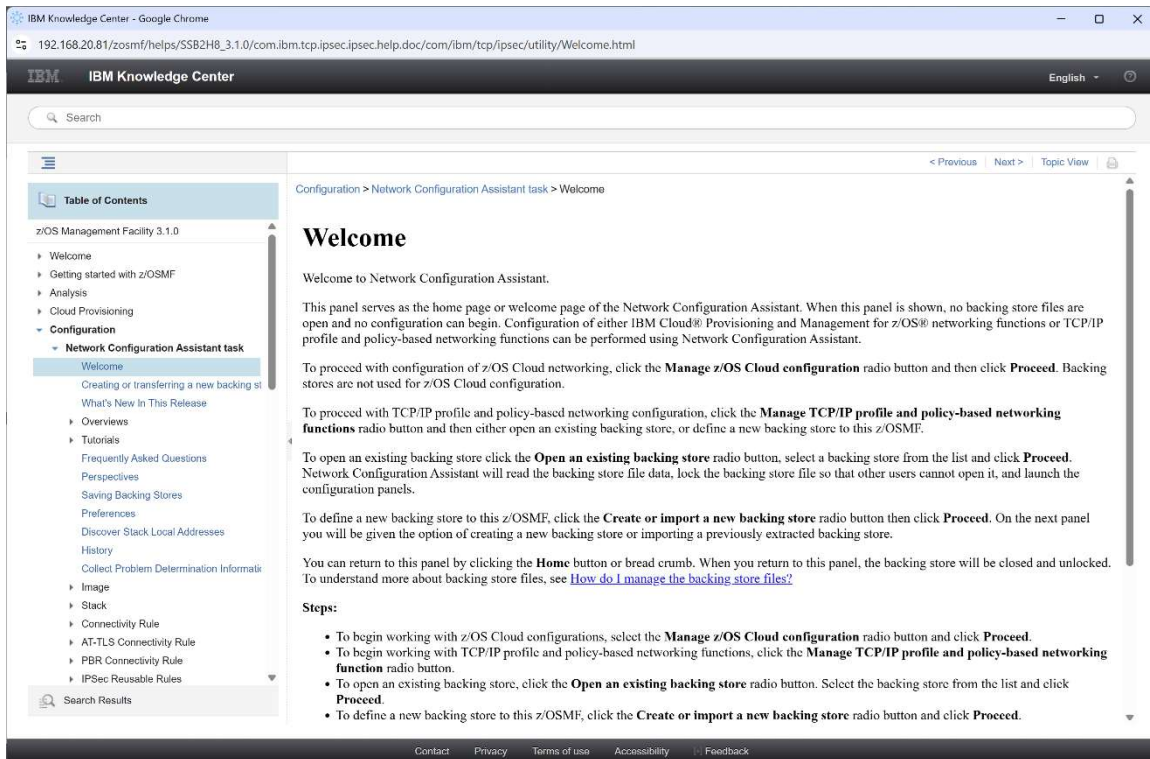
Note: All screen captures in this class are samples only. What is displayed on the panels as you go through the exercises might look a little differently. Always follow the written directions rather than rely solely on the sample screen captures.

6. You will be presented with a Welcome screen.



6. 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.

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent



7. 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.
9. 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.

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

a) What's New

IBM Knowledge Center - Google Chrome
192.168.20.81/zosmf/helps/5582H8_3.1.0/com.ibm.tcp.ipsec.ipsec.help.doc/com.ibm/tcp/ipsec/ipsec/Whats_New.html

IBM Knowledge Center

Search

Configuration > Network Configuration Assistant task > What's New In This Release

What's New in this Release

New in z/OS 3.1 APAR PH57412

- Support for new SSH Key Exchange algorithms in Z Encryption Readiness Technology (zERT) Policy Enforcement technology**
In an SSH Key Exchange protection characteristic object, there are four additional GSS algorithms available to select. For these new algorithms to be recognized by 3.1 z/OS Communications Server, APAR PH58110 must be applied.

New in z/OS 3.1

- Removal of support for configuring LAN Channel Station (LCS) interfaces in TCP/IP technology**
This function is no longer supported in z/OS 3.1. Configuration for this function remains in the Network Configuration Assistant, however, for stacks in 3.1 and later level images, configuration will not be generated for LCS interfaces.
- Configuration for persistent QUIESCE/RESUME support for Sysplex Distribution targets**
In the Additional Settings panel for a sysplex distribution, you can specify that the distribution will be installed in a paused state. To enable the distribution, the operator must specify a command to start distribution.

New in V2R5 APAR PH53064

- AT-TLS Configuration Support for specifying reference names for domain-based server certificate name validation**
In the advanced settings of the AT-TLS connectivity rule, you can now indicate list reference names for domain-based server certificate name validation.
- AT-TLS Configuration support for TLS 1.3 sysplex caching of session tickets**

Contact Privacy Terms of use Accessibility Feedback

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

b) Getting Started

The screenshot shows a web browser window displaying the IBM Knowledge Center. The page title is "Getting Started Tutorial" under the path "Configuration > Network Configuration Assistant task > Tutorials > Getting Started". The page is estimated to take 15 minutes to review and is page 1 of 7. It includes a "Welcome:" section with a "Next >" link. The main content explains that the welcome screen is shown when the Network Configuration Assistant is started and provides instructions on how to manage z/OS Cloud configuration or policy-based networking functions. It includes a list of tasks: "Manage z/OS Cloud configuration" (selected), "Manage TCP/IP profile and policy-based networking functions", "Create or transfer a new backing store", and "Open an existing backing store". The "Open an existing backing store" option is further detailed with a "saveData" dropdown menu and a numeric input field set to "2", with a note that minutes should be allowed for the backing store to open, with a range of 1-30. A "Proceed" button is at the bottom of the form.

IBM Knowledge Center - Google Chrome
192.168.20.81/zosmf/helps/5582H8_3.1.0/com.ibm.tcp.ipsec.ipsec.help.doc/com.ibm/tcp/ipsec/ipsec/Tutorial_Main0.html

IBM Knowledge Center

Search

Configuration > Network Configuration Assistant task > Tutorials > Getting Started

Getting Started Tutorial

estimated review time: 15 minutes

page 1 of 7

[Next >](#)

The welcome screen is seen when the Network Configuration Assistant is started. From this screen you can launch tutorials and review the new features for the release. Select whether to manage z/OS® Cloud configuration or policy-based networking functions.

- To manage z/OS Cloud configuration, see [Cloud: Getting Started](#).
- To manage policy-based networking functions, select whether to open an existing backing store or create or import a new backing store and click Proceed. Once the backing store is opened, use **Select a technology** to access the technology you want to configure.

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

☐ Manage z/OS Cloud configuration

☒ Manage TCP/IP profile and policy-based networking functions

☐ Create or transfer a new backing store

☒ Open an existing backing store

saveData

2

* Minutes to allow backing store to open. Range is 1-30.

[Proceed](#)

Contact Privacy Terms of use Accessibility Feedback

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

c) Migrating to z/OSMF

The screenshot shows a web browser window displaying the IBM Knowledge Center page for 'Migration of existing backing store files'. The page is titled 'Migration of existing backing store files' and is part of the 'Network Configuration Assistant task > Tutorials > Network Configuration Assistant - Additional Tutorials > Moving to z/OSMF' series. The left sidebar contains a 'Table of Contents' with a tree structure. The main content area includes an introduction paragraph, a list of five steps for migration, and a 'Parent topic' link.

Table of Contents

- Analysis
- Cloud Provisioning
- Configuration
 - Network Configuration Assistant task
 - Welcome
 - Creating or transferring a new backing store file
 - What's New In This Release
 - Overviews
 - Tutorials
 - Getting Started
 - AT/TLS: Getting Started
 - IPSec: Getting Started
 - IDS: Getting Started
 - QoS: Getting Started
 - PBR: Getting Started
 - NSS: Getting Started
 - TCP/IP: Getting Started
 - zERT: Getting Started
 - Cloud: Getting Started
 - Network Configuration Assistant -
 - Discovery of TCP/IP Stack Information
 - Application Setup Tasks
 - Installing Configuration Files
 - Backing Store Files
 - Moving to z/OSMF

Migration of existing backing store files

The Windows version of the Network Configuration Assistant allows you to store backing store files on your local drive, a LAN drive or on z/OS®. Using the Network Configuration Assistant in the z/OSMF environment requires that existing backing store files be migrated into the z/OSMF environment. If you migrate from a previous release of z/OSMF the Network Configuration Assistant automatically transfers the backing store files from the previous release. If you need to migrate files from a previous release of the Windows version of the Network Configuration Assistant then perform the following steps. Once the backing store files are transferred into z/OSMF, they will be known only by the file name. They will be placed in a directory managed by the Network Configuration Assistant and z/OSMF.

The following steps must be performed. Note that these steps will only be performed in the z/OSMF environment, as the Windows version of this configuration utility will allow you to open any backing store that is located on the workstation:

1. Ensure your backing store file is on z/OS DASD. If the backing store file is on your Windows local drive or LAN drive, FTP the file in binary to your z/OS system. If you do not know the location of your backing store file, use the **File > Properties** menu from the Windows Network Configuration Assistant to view its location.
2. Go to the backing store management technology perspective. Click **Actions > Transfer Backing Store file into z/OSMF** to perform the transfer.
3. Enter the name and path of your existing backing store file on z/OS. This required value may be an MVS™ data set or the directory and file on the z/OS system.
4. Enter the name for the backing store file to be used after the transfer into z/OSMF. This is the name by which the file will be known to the Network Configuration Assistant in the future.
5. Click the **Transfer** button to copy the backing store file into z/OSMF.

You have now transferred the file into the z/OSMF environment. The file can be used in all subsequent operations of Network Configuration Assistant.

Parent topic: [Network Configuration Assistant Tutorials](#)

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

d) Application Setup Tasks

The screenshot shows a web browser window displaying the IBM Knowledge Center. The page title is "Application Setup Tasks using the z/OSMF Workflow for IBM Cloud Provisioning and Management for z/OS". The breadcrumb trail indicates the path: Configuration > Network Configuration Assistant task > Tutorials > Network Configuration Assistant - Additional Tutorials > Application Setup Tasks. The page is labeled "page 1 of 3". A "Next >" link is visible. Below the title, there is a paragraph explaining that for each technology of Network Configuration Assistant including z/OS® Cloud, a number of setup tasks must be performed before the technology can be used. It mentions that setting up the Policy Agent is a basic requirement and that for IP Security, users can require the IKE, NSS, and DMD daemons. It also states that Syslogd and TRMD can be used for logging. The paragraph continues by saying that preparing this environment requires many steps that might include enabling RACF® permissions, defining start procedures, setting up support and configuration files for these service applications. After these setup tasks are complete, the administrator can then install policy configuration files for each of the technologies they have configured or work with IBM® Cloud Provisioning and Management for z/OS network configuration. Similarly, setting up the z/OS Cloud environment includes enabling multiple SAF permissions and allocating a data set with multiple data set members. Another paragraph states that prior to V2R1, setup tasks were provided as part of the Network Configuration Assistant using Application Setup Tasks. In V2R1, Application Setup Tasks have been replaced with the z/OSMF Workflow function. Workflows are provided which are a set of instructions that guide users through the setup of the environment required to run the policy-based networking technologies. A third paragraph mentions that many of these setup tasks can be performed once and will seldom need to be performed again. However, normal changes and updates to configuration such as adding a new z/OS image and TCP/IP stacks can require the need to re-run the workflow steps. Below this, it says "To use the workflows:" followed by a list item: "1 From z/OSMF navigation menu: select the Workflows link". The page footer includes links for Contact, Privacy, Terms of use, Accessibility, and Feedback.

IBM Knowledge Center - Google Chrome
Not secure | 192.168.20.81/zosmf/helps/SSB2H8_2.4.0/com.ibm.tcp.ipsec.ipsec.help.doc/com/ibm/tcp/ipsec/ipsec/SetupTasks_1.html

IBM Knowledge Center

Search

Configuration > Network Configuration Assistant task > Tutorials > Network Configuration Assistant - Additional Tutorials > Application Setup Tasks

Application Setup Tasks using the z/OSMF Workflow for IBM Cloud Provisioning and Management for z/OS

page 1 of 3

[Next >](#)

[Frequently Asked Questions](#)

For each technology of Network Configuration Assistant including z/OS® Cloud, a number of setup tasks must be performed before the technology can be used. Setting up the Policy Agent is a basic requirement. For IP Security, users can require the IKE, NSS, and DMD daemons. Syslogd and TRMD can be used for logging. Preparing this environment requires many steps that might include enabling RACF® permissions, defining start procedures, setting up support and configuration files for these service applications. After these setup tasks are complete, the administrator can then install policy configuration files for each of the technologies they have configured or work with IBM® Cloud Provisioning and Management for z/OS network configuration. Similarly, setting up the z/OS Cloud environment includes enabling multiple SAF permissions and allocating a data set with multiple data set members.

Prior to V2R1, setup tasks were provided as part of the Network Configuration Assistant using Application Setup Tasks. In V2R1, Application Setup Tasks have been replaced with the z/OSMF Workflow function. Workflows are provided which are a set of instructions that guide users through the setup of the environment required to run the policy-based networking technologies.

Many of these setup tasks can be performed once and will seldom need to be performed again. However, normal changes and updates to configuration such as adding a new z/OS image and TCP/IP stacks can require the need to re-run the workflow steps.

To use the workflows:

- 1 From z/OSMF navigation menu: select the **Workflows** link

Contact Privacy Terms of use Accessibility Feedback

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

e) Tutorials

The screenshot shows the IBM Knowledge Center interface in a Google Chrome browser. The address bar displays the URL: 192.168.20.81/zosmf/helps/5582H8_3.1.0/com.ibm.tcp.ipsec.ipsec.help.doc/com.ibm/tcp/ipsec/ipsec/TutorialsFolder.html. The page title is "IBM Knowledge Center".

The left sidebar contains a "Table of Contents" for "z/OS Management Facility 3.1.0". The "Configuration" section is expanded, showing "Network Configuration Assistant task" with sub-items: "Welcome", "Creating or transferring a new backing st...", "What's New In This Release", "Overviews", "Tutorials" (highlighted), "Frequently Asked Questions", "Perspectives", "Saving Backing Stores", "Preferences", "Discover Stack Local Addresses", "History", "Collect Problem Determination Informati...", "Image", "Stack", "Connectivity Rule", "AT-TLS Connectivity Rule", "PBR Connectivity Rule", and "IPSec Reusable Rules".

The main content area is titled "Tutorials Folder" and includes the text: "To view a tutorial, select one of the subtopics under this folder." Below this, a list of tutorial links is provided:

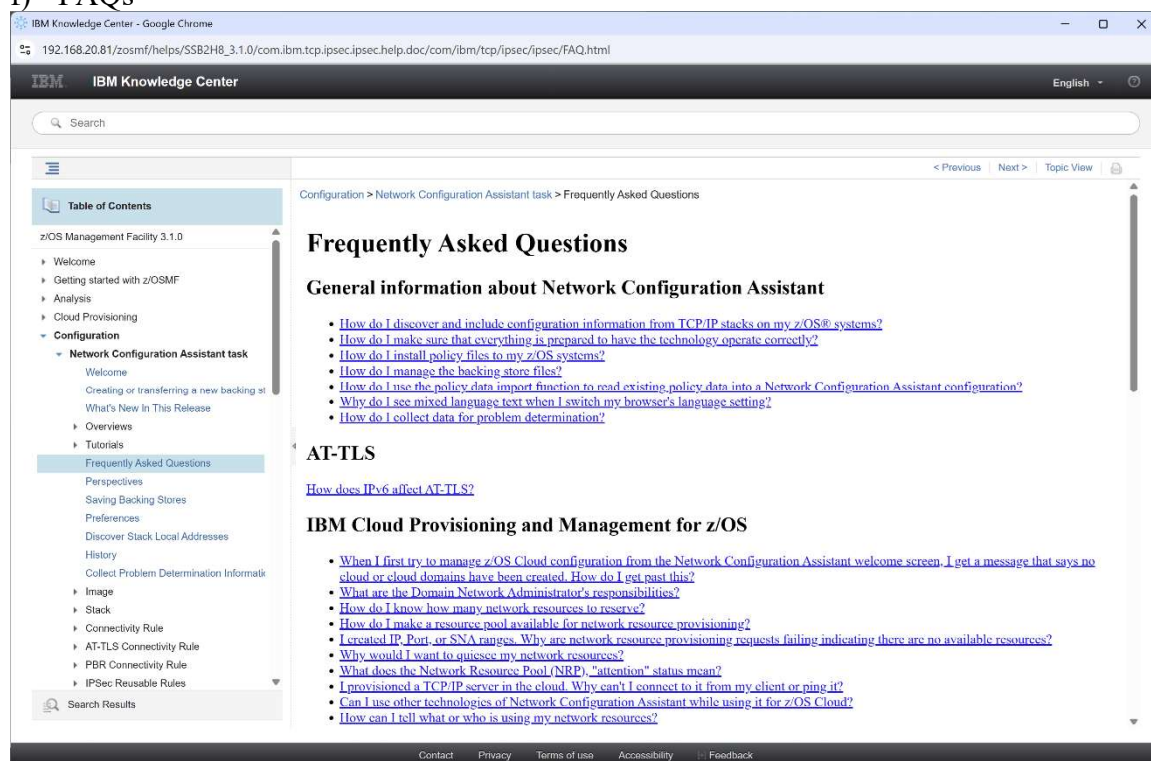
- [Getting Started Tutorial](#)
- [Getting Started Tutorial - AT-TLS](#)
- [Getting Started Tutorial - IPSec](#)
- [Getting Started Tutorial - IDS](#)
- [Getting Started Tutorial - QoS](#)
- [Getting Started Tutorial - PBR](#)
- [Getting Started Tutorial - NSS](#)
- [Getting Started Tutorial - TCP/IP](#)
- [Introduction to zERT Policy Enforcement](#)
- [Getting Started Tutorial - Cloud](#)
- [Network Configuration Assistant Tutorials](#)
- [AT-TLS Tutorials](#)
- [IDS Tutorials](#)
- [IPSec Tutorials](#)
- [QoS Tutorials](#)
- [Routine - Additional Tutorials](#)
- [TCP/IP Tutorials](#)
- [Cloud Tutorials](#)

Below the list, it says: "Parent topic: [Overviews Folder](#)".

The footer of the page contains links for "Contact", "Privacy", "Terms of use", "Accessibility", and "Feedback".

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

f) FAQs



The screenshot displays the IBM Knowledge Center interface in a Google Chrome browser. The address bar shows the URL: 192.168.20.81/zosmf/helps/5582H8_3.1.0/com.ibm.tcp.ipsec.ipsec.help.doc/com.ibm/tcp/ipsec/ipsec/FAQ.html. The page title is "IBM Knowledge Center". The left sidebar contains a "Table of Contents" with a tree structure. The "Configuration" section is expanded, and "Network Configuration Assistant task" is selected. The "Frequently Asked Questions" link is highlighted. The main content area shows the breadcrumb "Configuration > Network Configuration Assistant task > Frequently Asked Questions" and the heading "Frequently Asked Questions". Below this is the section "General information about Network Configuration Assistant" followed by a list of links. The "AT-TLS" section follows with a link. The "IBM Cloud Provisioning and Management for z/OS" section follows with a list of links. The footer contains links for "Contact", "Privacy", "Terms of use", "Accessibility", and "Feedback".

IBM Knowledge Center

Search

Configuration > Network Configuration Assistant task > Frequently Asked Questions

Frequently Asked Questions

General information about Network Configuration Assistant

- [How do I discover and include configuration information from TCP/IP stacks on my z/OS® systems?](#)
- [How do I make sure that everything is prepared to have the technology operate correctly?](#)
- [How do I install policy files to my z/OS systems?](#)
- [How do I manage the backing store files?](#)
- [How do I use the policy data import function to read existing policy data into a Network Configuration Assistant configuration?](#)
- [Why do I see mixed language text when I switch my browser's language setting?](#)
- [How do I collect data for problem determination?](#)

AT-TLS

[How does IPv6 affect AT-TLS?](#)

IBM Cloud Provisioning and Management for z/OS

- [When I first try to manage z/OS Cloud configuration from the Network Configuration Assistant welcome screen, I get a message that says no cloud or cloud domains have been created. How do I get past this?](#)
- [What are the Domain Network Administrator's responsibilities?](#)
- [How do I know how many network resources to reserve?](#)
- [How do I make a resource pool available for network resource provisioning?](#)
- [I created IP, Port, or SNA ranges. Why are network resource provisioning requests failing indicating there are no available resources?](#)
- [Why would I want to quiesce my network resources?](#)
- [What does the Network Resource Pool \(NRP\) "attention" status mean?](#)
- [I provisioned a TCP/IP server in the cloud. Why can't I connect to it from my client or ping it?](#)
- [Can I use other technologies of Network Configuration Assistant while using it for z/OS Cloud?](#)
- [How can I tell what or who is using my network resources?](#)

Contact Privacy Terms of use Accessibility Feedback

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

g) Collect Problem Determination Data

The screenshot shows the IBM Knowledge Center interface in a Google Chrome browser. The address bar displays the URL: 192.168.20.81/zosmf/helps/SSB2H8_3.1.0/com.ibm.tcp.ipsec.ipsec.help.doc/com.ibm/tcp/ipsec/utility/PDSave.html. The page title is "Collect Problem Determination Information". The left sidebar contains a "Table of Contents" for "z/OS Management Facility 3.1.0", with "Collect Problem Determination Information" highlighted. The main content area includes a breadcrumb trail: "Configuration > Network Configuration Assistant task > Collect Problem Determination Information". The title "Collect Problem Determination Information" is followed by a paragraph: "To collect and save problem determination information at the request of, and for the use of, IBM Service personnel for troubleshooting problems in the Configuration Assistant." Below this is a section titled "Steps for collecting problem determination information for all Configuration Assistant technologies except Cloud" with a numbered list of three steps. Step 1 involves restarting the z/OSMF server and clearing the browser cache. Step 2 involves transferring z/OSMF runtime log files. Step 3 involves using the "Tools" button to select "Manage Backing Stores" and clicking "Actions > Extract Transfer" to extract backing store files. A paragraph explains that z/OSMF creates log files in the product logs directory, with names like IZUGn.log, where n is a number in the range 0-9. It also mentions that the most current log file is always named IZUG0.log. A final paragraph states that the file can now be transferred out in binary. At the bottom of the page, there is a section titled "Extract Backing Store Files from z/OSMF".

IBM Knowledge Center - Google Chrome
192.168.20.81/zosmf/helps/SSB2H8_3.1.0/com.ibm.tcp.ipsec.ipsec.help.doc/com.ibm/tcp/ipsec/utility/PDSave.html
English

Search

Table of Contents
z/OS Management Facility 3.1.0
Welcome
Getting started with z/OSMF
Analysis
Cloud Provisioning
Configuration
Network Configuration Assistant task
Welcome
Creating or transferring a new backing store
What's New In This Release
Overviews
Tutorials
Frequently Asked Questions
Perspectives
Saving Backing Stores
Preferences
Discover Stack Local Addresses
History
Collect Problem Determination Information
Image
Stack
Connectivity Rule
AT-TLS Connectivity Rule
PBR Connectivity Rule
IPSec Reusable Rules
Search Results

Configuration > Network Configuration Assistant task > Collect Problem Determination Information

Collect Problem Determination Information

To collect and save problem determination information at the request of, and for the use of, IBM Service personnel for troubleshooting problems in the Configuration Assistant.

Steps for collecting problem determination information for all Configuration Assistant technologies except Cloud

1. You must take the following actions after the system release is updated or a new PTF was applied for z/OSMF or z/OSMF Configuration Assistant.
 - Restart the z/OSMF server to activate the updated Configuration Assistant code.
 - Clear your web browser cache before you access the updated Configuration Assistant code.
2. Transfer z/OSMF runtime log files, that contain Configuration Assistant logging, in binary.
3. Use the **Tools** button to select **Manage Backing Stores**, click **Actions > Extract Transfer** to extract your backing stores files from z/OSMF.

During normal operations, z/OSMF collects its runtime data including log messages and trace messages in log files. z/OSMF runtime data is created on the server or sent to the server by the client. Both types of messages are written to the z/OSMF runtime log files.

z/OSMF creates the log files in the product logs directory, which is, by default, /var/zosmf/data/logs. z/OSMF names the log files IZUGn.log, where n is a number in the range 0 - 9. z/OSMF creates log files in a "cascading" manner. The most current log file is always named IZUG0.log. When this log file reaches its predefined limit, z/OSMF saves it as IZUG1.log and begins writing to a new IZUG0.log file. When the IZUG0.log file is again full, z/OSMF saves it as IZUG1.log after renaming the existing IZUG1.log file to IZUG2.log. z/OSMF continues this process, saving each log file under the next available name, up to a maximum of ten log files. Thereafter, z/OSMF discards the oldest log file (IZUG9.log) whenever a new log file is to be created.

See the following example of extracting two backing stores to the system's /tmp directory. The file can now be transferred out in binary.

Extract Backing Store Files from z/OSMF

Contact Privacy Terms of use Accessibility Feedback

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

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.
11. Starting in z/OS V2.3 Communications Server cloud configuration has been added to the z/OS Communications Server Configuration Assistant. This is not covered in this class.
12. Create a new backing store file:
 - a) Leave the top selection of “Manage TCP/IP profile and policy-based networking function”.
 - b) Select “Create or transfer a new backing store”.
 - c) Click on the **Proceed** button.

The screenshot shows a web browser window titled "IBM z/OS Management Facility" with the address bar displaying "192.168.20.81/zosmf/". The page is titled "Network Configuration Assistant" and contains the following content:

Welcome to 3.1 Configuration Assistant for z/OS Communications Server
Use this task to create and manage configuration for z/OS Communications Server policy-based networking functions.

☐ Manage z/OS Cloud configuration
☒ Manage TCP/IP profile and policy-based networking functions

☒ Create or transfer a new backing store
☐ Open an existing backing store

saveData
2 * Minutes to allow backing store to open. Range is 1-30.

Proceed

Learn more about Network Configuration Assistant:

What's New	See what is new in this release.
Getting Started	First time users can learn about Network 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.
Collect Problem Determination Data	Get assistance with gathering problem determination data.

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

13. Fill in the “File name” with your team name, **Teamnx**, where Teamnx is your team name (where **n** = ZOSn and **x** is 1 or 2 or 3).

- a) Team21
- b) Team31
- c) Team41
- d) Team51
- e) Team61
- f) Team71
- g) Team81
- h) Team91

IBM z/OS Management Facility

192.168.20.81/zosmf/

Network Configuration Assistant

Network Configuration Assistant (Home) > Create or transfer a new backing store

Create or transfer a new backing store

☒ Create a New Backing Store File

* File name: Team21

☐ Transfer Backing Store File to z/OSMF

Use this panel to transfer your backing store files into z/OSMF.

Specify the full zFS path name of the backing store file to transfer and the name to be used within z/OSMF.

Once the files are transferred, z/OSMF will keep track of them.

* Backing store file name and location:

* z/OSMF backing store name:


Minutes to allow backing store to open. Range is 1-30.

2

OK Cancel

14. Click on the **OK** button.

Information

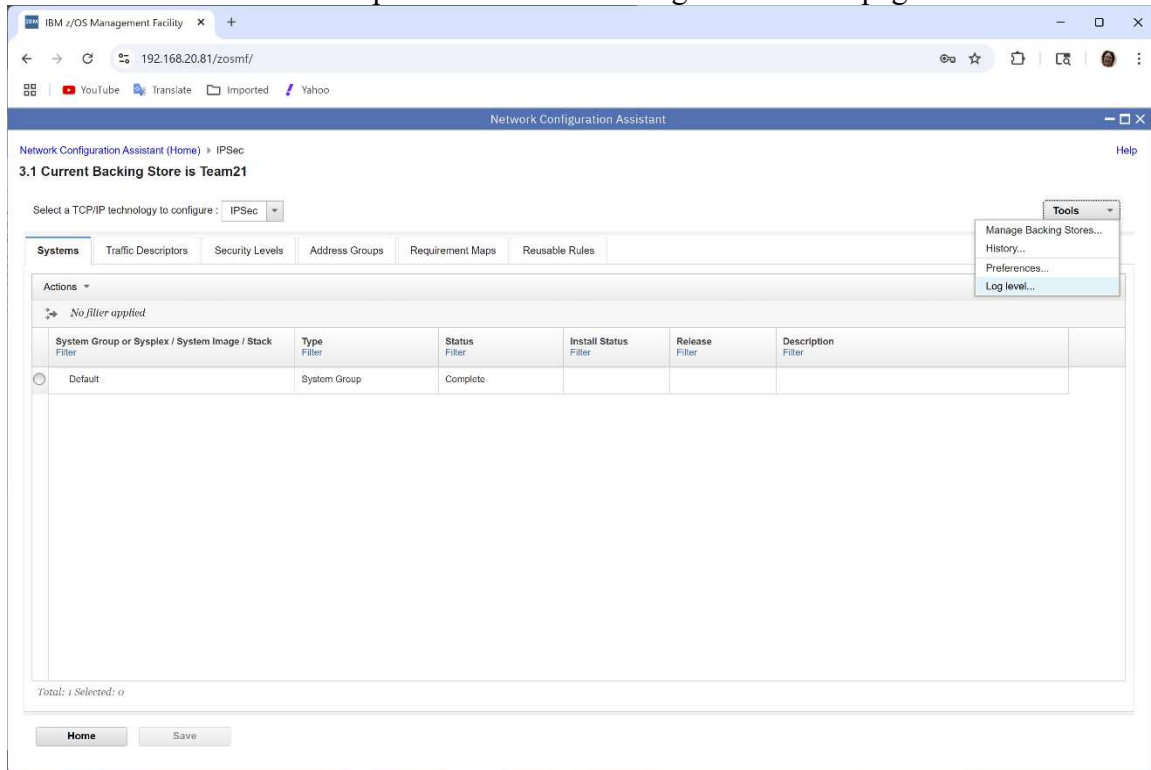
 You are now working on backing store file: **Team21**

OK

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

15. Click on the **OK** button again.

16. Click on the “**Tools**” drop down button on the right side of the page.



17. Feel free to check out the different options:

- 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)

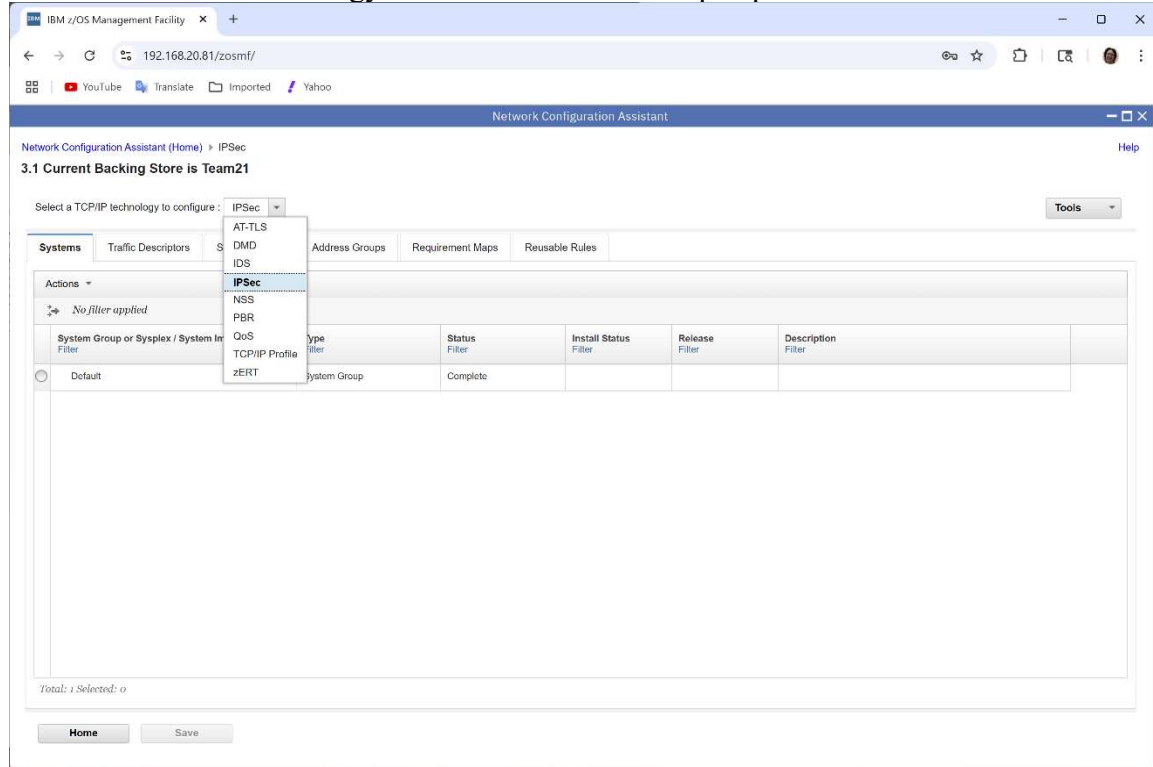
18. When finished return to the Main configuration panel. Click on the **Cancel** and **Close** button as necessary.

19. 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.

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

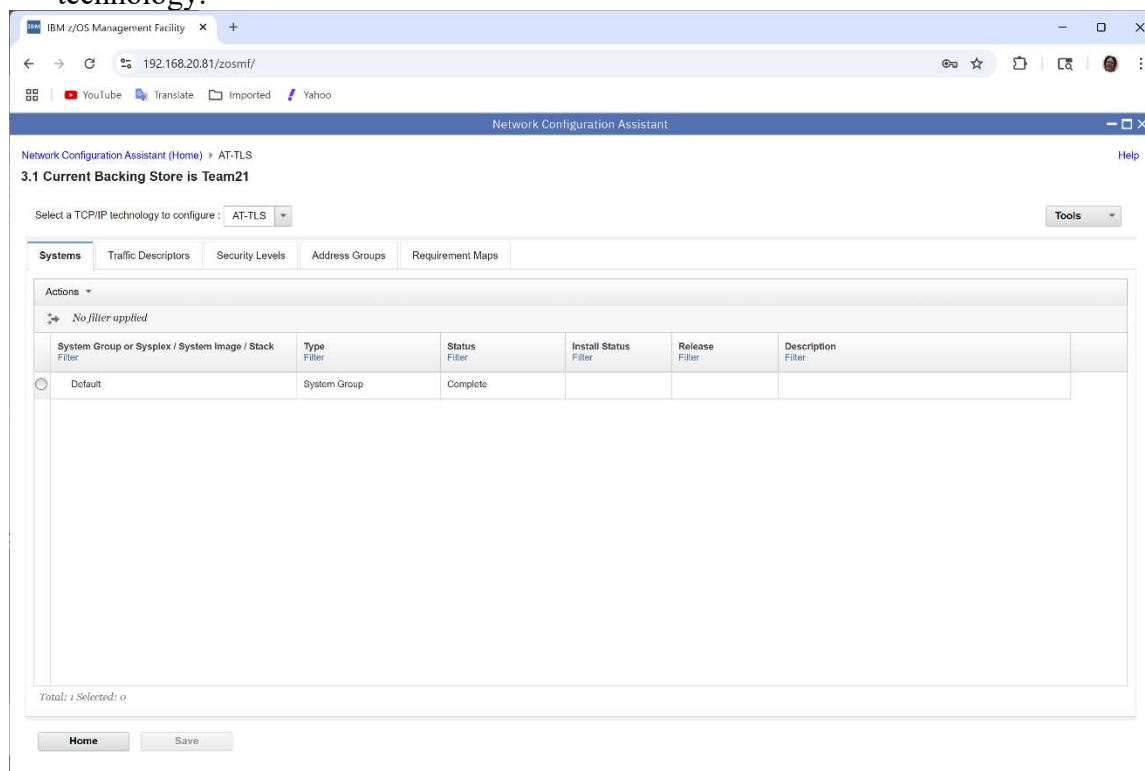
20. Use the pull-down to change the “TCP/IP technology to configure”. In previous releases the “technology” was referred to as the “perspective” in the tool.



21. Notice the different technologies available for configuration:
- 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.
 - DMD – Defence Manager Daemon provides the capability to dynamically (via the ipsec command) add IP Filter rules for a specified time frame.
 - IDS – Intrusion Detection Services provides TCP/IP stack protection against Scans, Attacks, and also allows connection limits to be defined.
 - IPSec – is the standard protocol support in the TCP/IP stack that can provide encryption to remote hosts with IPSec support.
 - 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.
 - PBR – Policy Based Routing provides the capability for choosing network routes depending upon traffic types.
 - QoS – Quality of Service provides different priority through the network depending upon the traffic types, and may be used to block traffic.
 - TCP/IP Profile – The PROFILE.TCPIP file may be customized. (New in z/OS V2.2)
 - zERT – z/OS Encryption Readiness Tool provides information about encrypted traffic.

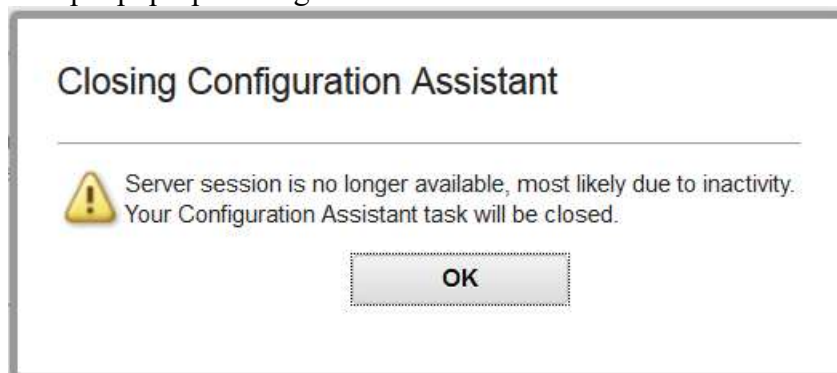
Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

22. When you are finished reviewing the different technologies, select the **AT-TLS** technology.



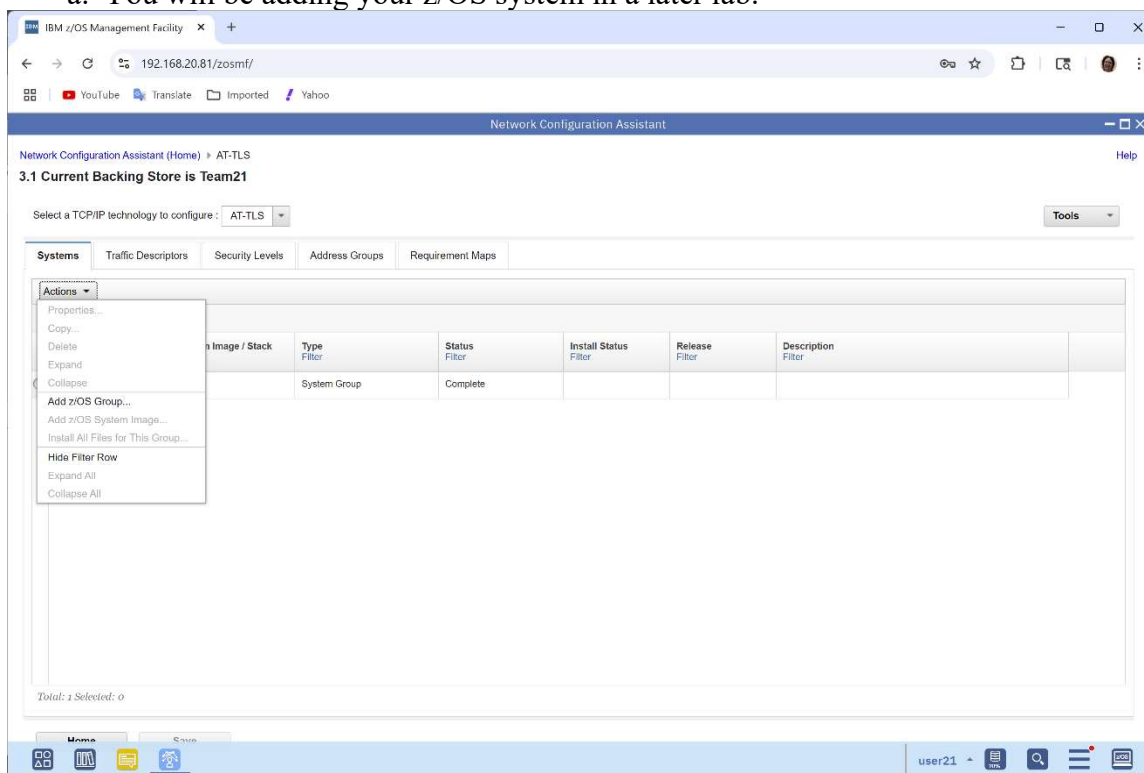
23. Note the Save button. It is “greyed out” because you have not made any changes that need to be saved yet. If you are working in the tool it is recommended that you always save your changes with the Save button before you take a break. If you take too long between configuration changes and saving those changes you may be presented with a message indicating that your session has dropped and all your changes have been lost since your last save. In this class please **Save** often, even if you are not specifically told to do so, especially if you want to take a break!

Example pop-up message:



Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

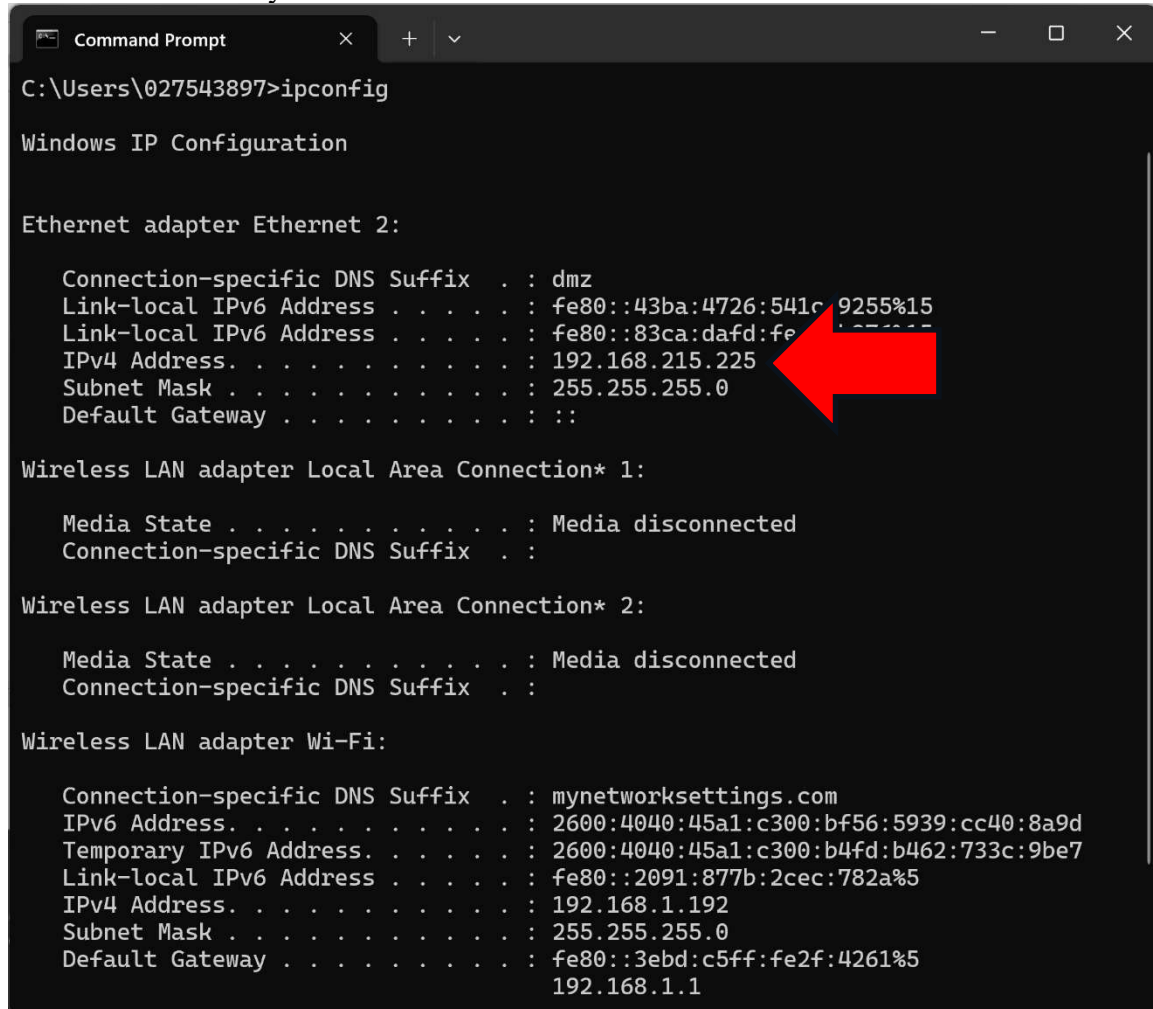
24. Click on the **Actions** pull-down and notice all the different options available.
- a. You will be adding your z/OS system in a later lab.



Configuring PCOMM

Use your lab diagrams for this task.

1. At your workstation, open a command window and issue the command to determine what your IP address is:
 - a. **Start >>> Windows System >>> Command Prompt**
 - b. Enter **ipconfig**
 - c. Press **ENTER** key



```
C:\Users\027543897>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix  . : dmz
    Link-local IPv6 Address . . . . . : fe80::43ba:4726:541c:9255%15
    Link-local IPv6 Address . . . . . : fe80::83ca:dafd:fe80::877b:2cec%5
    IPv4 Address. . . . . : 192.168.215.225
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : ::

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

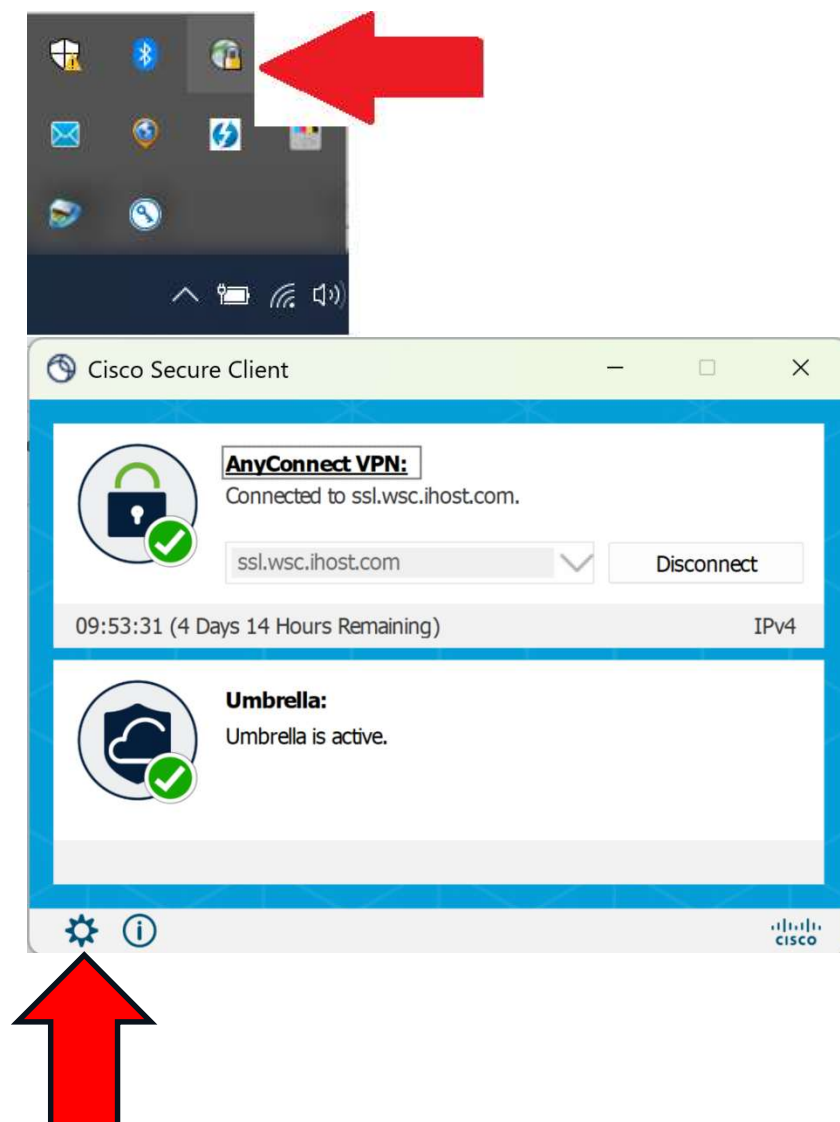
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

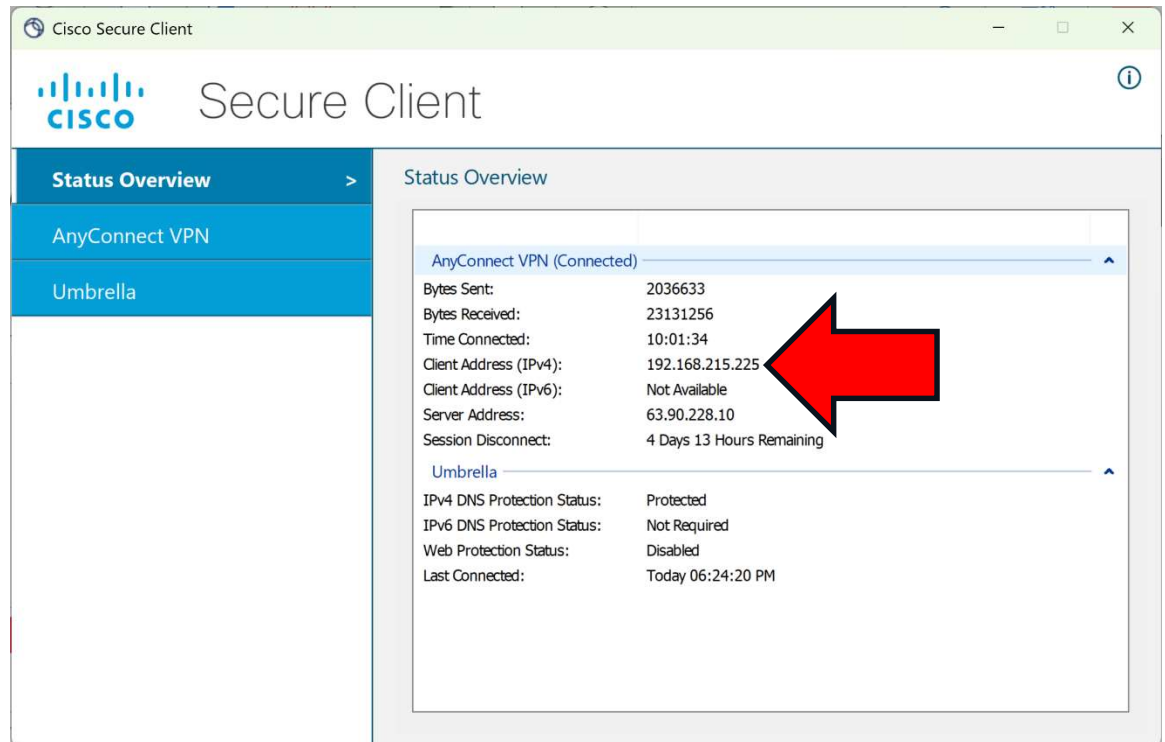
    Connection-specific DNS Suffix  . : mynetworksettings.com
    IPv6 Address. . . . . : 2600:4040:45a1:c300:bf56:5939:cc40:8a9d
    Temporary IPv6 Address. . . . . : 2600:4040:45a1:c300:b4fd:b462:733c:9be7
    Link-local IPv6 Address . . . . . : fe80::2091:877b:2cec:782a%5
    IPv4 Address. . . . . : 192.168.1.192
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::3ebd:c5ff:fe2f:4261%5
                                192.168.1.1
```

- i. Write down here the IPv4 address of your workstation (DNS Suffix = dmz).
- ii. **NOTE:** The IP Address is the one associated with the Local Cisco AnyNet Connect VPN endpoint.

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent



Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent



2. Create a PCOMM session to connect to TN3270 at TCPIP1 (the “maintenance” TCP/IP stack) on your assigned MVS system.
 - a. Find Personal Communications on your desktop or in the START menu of your system. Initialize it and **CONFIGURE** a new session:
 - i. For **zSeries** host
 - ii. Using a **LAN** Interface.
 - iii. With **TN3270** connection
 - b. Create a new session with these **SESSION PARAMETER** specifications:
 - i. Identify a **Session Size of 27 x 132**
 - c. Establish the **LINK PARAMETERS** ... as follows:
 - i. Host IP Addr **192.168.20.8n** (where “n” is the suffix of your MVS)
 - ii. Port number **23**
3. Click on **OK** and you should see the TN3270 Logon (“Message 10”) screen.
4. Customize the appearance of the Emulator Session:
 - a. **Edit >>> Preferences >>> Appearance >>> Window Setup >>>**
 - b. On the Window Setup Screen
 - i. Leave or make **checkmarks** only in **Session Profile** and **Session Dimensions**.
 - ii. Select **OK**.
 - c. **File >>> Save as... >>> <session profile name of MVS_nWIDE>**
 - i. “n” represents the suffix of the MVS you are connecting with.
 - ii. Select **Save**.
 - d. You should see that the top bar of emulator screen reflects this session name.
5. When you see the TN3270 logon (“Message 10”) screen from the TN3270 server, provide your userid with the logon command that has been built for this system. (The logon command in this system is “TSO”).)

- a. **TSO <userid>**
6. On the ISPF signon screen, provide the password you were given in class.
 - a. **<password>**
 - b. Press 3270 keyboard's **ENTER** key (= **Windows 'Ctrl' key**)
7. When you see the READY prompt, enter ...
 - a. **ISPF D.LOG**
 - i. This takes you to a view of the MVS console for your image.
 - ii. You will be working with this a lot in future labs.

Part 2: Reviewing the z/OS Environment at Your MVS Image

1. From the MVS log enter the command to see how many TCP/IP stacks are currently running:
 - a. **/D TCPIP**
 - b. You should see two stacks:
 - i. TCPIP1 (maintenance stack)
 - ii. TCPIPT (student production stack)
2. Security logging can consume much log space in UNIX. Ensure that there is a separate zFS file system mounted at the UNIX director “/var”:
 - a. **/D OMVS,F**
 - i. Look for file name for your MVS_n that starts with “USSZFS.MVS_n.VxRx.VAR...” mounted at /MVS_n/var
 - ie. ZFS 19 ACTIVE RDWR 12/03/2020 L=32
NAME=USSZFS.MVS2.V3R1.VAR..ZFS 22.05.52 Q=0
PATH=/MVS2/var
OWNER=MVS2 AUTOMOVE=U CLIENT=N
 - z/OSMF is installed in this path by default.
3. From the command line enter the commands to view the IBM TCP/IP samples dataset:
 - a. **=3.4**
 - b. At the DSNNAME field of the next panel enter:
 - i. **SYS1.TCPIP.SEZAINST**
 - c. Press **ENTER**
 - d. Use the Tab key to move to the left of the dataset name and enter “**B**”.
4. Look for the member named: **EZARACF**
 - a. Select it with “**S**” next to the name.
 - b. Page through it noting all the examples for the RACF permissions that are necessary to protect the network and the MVS system when TCP/IP functions are implemented.
5. Exit from the EZARACF member:
 - a. **PF3 (F3)** until you return to the Data Set List Utility panel.
6. Change the DSNNAME field to start browsing the contents of the Student Datasets:
 - a. **USER.CS**
 - b. Press **ENTER**
7. Among others you should see:

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

- a. **USER.CS.ENVVARS** (for LE environment variable files – VB)
 - b. **USER.CS.SOURCE** (for your jobs)
 - c. **USER.CS.TCPPARMS** (for your IP configuration members)
8. Place a “**B**” next to the **USER.CS.SOURCE** dataset name to view the members in it.
9. The instructors have provided you with some datasets for use later in the Certificate Creation lab (where nx is your team suffix number (21,31,41...)):
 - a. **GBGCACnx**
 - b. **GBGCASnx**
 - c. **GBGCLInx**
 - d. **GBGRGCnx**
 - e. **GBGRGSnx**
 - f. **GBGSRVnx**
 - g. **GBGXCEnx**
 - h. **GBGXDEnx**
 - i. **GBGX12nx**
10. Exit from the view of **USER.CS.SOURCE**.
 - a. **PF3**
11. Place a “**B**” next to the **USER.CS.TCPPARMS** dataset name to view the members in it.
12. The instructors have provided you with the following datasets (where **n** is your MVS number (2,3,4,5,6,7) and **nx** is your team suffix number (21,31,41...)):
 - a. **DATnA** TCPDATA file
 - b. **FTPCLSnx** Sample client FTP Data file from SYS1.TCPIP.SEZAINST
 - c. **FTPSECnx** Sample server FTP Data file from SEZAINST
 - d. **TCPnA** TCP/IP profile
 - e. **TCPnAIPS** TCP/IP profile to be customized for IP Filter/IPsec support
 - f. **TLSOFFnx** Obeyfile for disabling the stack for AT-TLS
 - g. **TLSOnnx** Obeyfile for enabling the stack for AT-TLS
 - h. **TNnA** TN3270 profile
 - i. **TNnATTLS** TN3270 profile for AT-TLS
13. Exit from the view of **USER.CS.TCPPARMS**.
 - a. **PF3**
14. Now move to the MVS Console “Active Applications” View:
 - a. **=D.DA** (from the Command Line)
15. At the command line enter the following to display only the running applications that start with the letter “T”:
 - a. **PREFIX T***
16. Enter a question Mark “?” next to the TCPIPT procedure:
 - a. **? TCPIPT** TCPIPT TCPIP STC04699 TCPIP
 - b. Press **ENTER**
17. Select the JESJCL view of the running procedure:
 - a. **“S”**
 - b. Press **ENTER**
18. Examine the manner in which we have used **Variables** and **System Symbolics** in our started procedure:
 - a. **TCPIPT PROC PARMS='CTRACE(CTIEZB00)',**

- PROF=TCP&CL1.A,DATA=DAT&CL1.A,**
- b. **XX CS=SYS1**
- c. **XX* CS=USER**
- d. **IEFC653I SUBSTITUTION JCL -
PARMS='CTRACE(CTIEZB00)',PROF=TCP2A,DATA= DAT2A,CS=SYS1**
- 19. Notice that our startup for TCPIPT uses the **System Symbolic**:
 - a. **&CL1** (it stands for the MVS SYSID defined in SYS1.PARMLIB(IEASYMxx))
 - i. It resolves to the last digit of your MVS or ZOS name.
- 20. Notice that we have defined our own Variable called **“CS”**:
 - a. **CS=SYS1**
 - b. **CS=USER**
- 21. We have defined our own Variable called **“PROF”**:
 - a. **PROF=TCP&CL1.A**
- 22. We have defined our own Variable called **“DATA”**:
 - a. **DATA=DAT&CL1.A,**
- 23. TN3270T is set up the same way.
- 24. We can initialize either TN3270T or TCPIPT in one of two ways:
 - a. **S TCPIPT,CS=SYS1**
 - b. **S TCPIPT,CS=USER**
- 25. The two initializations pick up their configuration dataset members either from:
 - a. **‘SYS1.CS.TCPPARMS’** or
 - b. **‘USER.CS.TCPPARMS’**
- 26. Their PROFILE and TCPDATA files then resolve to:
 - a. MVS1:
 - i. **TCP1A , DAT1A**
 - b. MVS2:
 - i. **TCP2A , DAT2A**
 - c. MVS3:
 - i. **TCP3A , DAT3A**
 - d. MVS4:
 - i. **TCP4A , DAT4A**
 - e. MVS5:
 - i. **TCP5A , DAT5A**
 - f. MVS6:
 - i. **TCP6A , DAT6A**
 - g. MVS7:
 - i. **TCP7A , DAT7A**
 - h. MVS8:
 - i. **TCP8A , DAT8A**
 - i. MVS9:
 - i. **TCP9A , DAT9A**
- 27. Currently we are running the procedures using the SYS1.CS.TCPPARMS members. But in the later labs you will be using these variables and symbolics to pick up your version vs. the instructor version of the lab procedures.
 - a. Now you should understand why you found TnA, TCPnA, and DATnA in your TCPPARMS dataset.

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

28. Go back to the log view of the Console:
 - a. **PF3 (F3)** and **=D.LOG**
29. Issue the command to see your network addresses for the Student TCPIPT stack:
 - a. **/D TCPIP,TCPIPT,NETSTAT,HOME**
 - b. **NOTE:** In some labs you will be using addresses **192.168.20.9n** and **192.168.20.1ab** on the Student stack (TCPIPT).
 - i. **192.168.20.1ab** = a static VIPA (**VLINK1**)
 - ii. A dynamic VIPA name starts “**VIPL**” with the IP address expressed in hexadecimal in the final digits

Part 3: Reviewing the UNIX Environment at Your MVS Image

1. On the command line enter the command to proceed to the UNIX environment:
 - a. **TSO OMVS**
2. Discover what UNIX Identity you have:
 - a. **id**
 - i. Are you a superuser? _____
 - ii. What is your UNIX identity? _____
3. Switch into Superuser mode:
 - a. **su**
4. Issue the command to discover your UNIX identity now:
 - a. **id**
 - i. What is your UNIX identity now? _____
5. Look at your running UNIX environment:
 - a. **env**
 - b. The TimeZone variable (TZ) has been set, but it is only valid for the SHELL environment. It does not affect the timezone in other processes.
6. View the mounted files from the UNIX perspective to ensure that you have a separate logging file system on “/var”:
 - a. **df**
 - b. Do you see a mount for /MVS_n/var? _____
7. Discover what your UNIX home directory is:
 - a. **pwd**
 - i. Name of directory: _____
8. Display the UNIX processes that are running:
 - a. **ps -ef**
9. Verify that SYSLOG Daemon is already running in the list from the previous command or issue the following command:
 - a. **ps -ef | grep syslog**
 - b. What is the Process ID (PID) of the Syslog Daemon? _____
10. Exit from the OMVS shell:
 - a. Enter **exit** (twice)
 - b. Press **ENTER**
11. Exit out of TSO.
 - a. Press **PF3**

End of Environment Lab



Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent