z/OSMF Hands-On Lab: Choose your own, Parts I, II, and III

Lab Exercise:

Configuration Assistant for z/OS Communications Server

Session ID’s:

15604: Wednesday 10:00am
15815: Thursday 1:30pm
15814: Friday 11:15am

Estimated Lab Time: 30 minutes

Speaker Names: Kim Bailey and Lin Overby
Enterprise Networking Solutions Design and Strategy
Abstract:

This hands-on lab will provide an opportunity to learn about using some of the functions and features of the Configuration Assistant in z/OSMF first hand.

This session is intended as a user experience session, and will be useful to systems programmers that focus on z/OS TCP/IP network administration that want to experience using the Configuration Assistant to create configuration for a Policy-based networking technology; or, for administrators that have been using the Configuration Assistant on Windows, are planning to migrate to z/OSMF and want to become familiar with the web interface.

As a reminder: With z/OS V2R1, the Configuration Assistant is no longer provided as a Window’s download. Users must use the Configuration Assistant with z/OSMF.

The Configuration Assistant for z/OS Communications Server is a management application that helps users configure the Policy-based networking technologies of z/OS Communications Server:

- **IP Security (IPSec)**
  - IP Filter Rules
  - VPN Tunnels
- **Network Security Services (NSS)**
  - Required for IKEv2 for certificate services
  - Also used for remote security services with a DataPower appliance
- **Defense Manager Daemon (DMD)**
  - Setup to user IPSec defensive filters
- **Application Transparent TLS (AT-TLS)**
  - Support for the TLS/SSL protocol as an extension of the TCP/IP stack’s TCP transport layer
- **Intrusion Detection Services (IDS)**
  - TCP/IP can detect signature events (ex: scans and attacks) that can cause misuse of system resources
- **Policy-based Routing (PBR)**
  - Configure TCP/IP to route traffic based upon criteria other than destination IP address
- **Qualities of Service (QoS)**
  - Provides settings to allow the TCP/IP stack to provide advanced controls for tuning the performance of the traffic it’s servicing
The z/OS Management Facility (z/OSMF) provides a web-based, graphical interface with systems management applications that plug-in. These applications are targeted toward system programmers on z/OS. Configuration Assistant for z/OS Communications Server is one of the application plug-ins to z/OSMF.

This session is not intended to provide instruction or education for the following, and it assumes that users have some basic understanding of the TCP/IP networking technologies on z/OS. Other Share sessions may be more appropriate for a technology introduction or deep-dive.

- Understanding the Policy-based networking technologies (IPSecurity, NSS, DMD, AT-TLS, PBR, IDS, QoS)
- Setup up Policy-based networking environment (Policy Agent, IKE, NSS, Syslogd, etc)
- TCP/IP profile setup in support of IPSec or AT-TLS
Using the Configuration Assistant:

This lab helps you to become familiar with using the Configuration Assistant as a plug-in to z/OSMF

Lab Hints and Tips:

- Do not use the browser “back” button selection. Use the breadcrumbs!
- While using the Configuration Assistant, feel free to use the comprehensive helps and tutorials to learn more about the technology being configured.
- As with all the labs in this session, all the teams will be working with the same z/OSMF instance. Each team will be given a unique id to work with.
- Each team will have their own configuration backing store to save the configuration created during the session.

Configuration Assistant Lab

This lab provides one main task and one optional task.

Main Task: Helps you to briefly explore the technology perspectives and reusable resources, and then takes you through the creation of an IPSec filter rule and the generation of policy.

Optional Task: Once you complete the Main task, the optional task provides a quick exploration of the “Tools” menu.

Feel free to explore the technologies other than IPSec after you complete the session.
Exercise instructions:

Here are the steps you will perform in this lab:

__ 1. Logon to z/OSMF
   __ a. Launch the Mozilla Firefox browser
   __ b. Point Browser to z/OSMF – enter the following URL
       https://mvs1.centers.ihost.com/zosmf/
   __ c. Enter the User ID (SHARAnn) and password assigned to your workstation.

__ 2. Begin using the Configuration Assistant
   __ a. Expand the Configuration Category in the Left Navigation Tree
   __ b. Click on Configuration Assistant

__ 3. Open the configuration backing store for your session
   __ a. Use the perspective selection to switch between each perspective
   __ b. Create z/OS Images in the systems table
   __ c. Create the TCP/IP stacks in the systems table

__ 4. Explore the IPSec (IP Security Perspective) Reusable Resources
   __ a. Become familiar with the IPSec technology perspective reusable resources
   __ b. Traffic Descriptors
   __ c. Security Levels
   __ d. Requirement Maps
   __ e. Address Groups

__ 5. Define IPSec reusable resources for use in your Connectivity Rule (Filter Rule)
   __ a. Create a Traffic Descriptor
   __ b. Create a Requirement Map
   __ c. Create an Address Group
   __ d. Create a Connectivity Rule

__ 6. Generate and Install the policy configuration (for the Policy Agent)
   __ a. Select “Install Configuration Files”
   __ b. View the generated policy
c. Perform the Install

Refer to Section 7 for the Optional Task of exploring the Tools button actions.
1. Logon to zOSMF

Step 1: Log in to z/OSMF

- Launch the Mozilla Firefox browser
  - Note: If browser asks to add exception for certificate, do so
- Point Browser to z/OSMF – enter the following url
  - https://mvs1.centers.ihost.com/zosmf/
  - Note: Ignore and close the warning message
    - IZUG809W Unsupported Web browser version or level found: "3.6.13 (.NET CLR 3.5.30729)". Some z/OSMF functions might not be available if you continue.
- Login with SHARE userid/pw as provided by the lab instructor
  - Each workstation has been assigned a unique z/OS User ID
    - SHARAnn (where nn is 01 - 20)
    - Password: to be provided
- Each User ID has been authorized to all the z/OSMF applications (Plug-ins)

Note: All screen captures in the handout show the ID SHARA20, your browser will be slightly different to reflect the User ID that you were given.
2. Begin Using the Configuration Assistant

**Step 2a:** Expand the Configuration Category in the Left Navigation Tree and Click on Configuration Assistant
**Step 2b: Selecting and Opening the Configuration Backing Store**

The next panel is the first panel that opens is the main panel of the Configuration Assistant. Here you will see drop-down selection box and an Open button.

Also shown is a table with a set of links. Feel free to click on the links and view What’s New (in this release), Getting Starting (new users), etc.

Use the selection box to select your configuration backing store for the session which is the name of your user Id and the day of this lab (however in this document the backing store is called ShareDemo), for example, if your user id is SHARA01 and this is the lab session on Wednesday, then your backing store will be SHARA01_WEDNESDAY. Please only open your backing store. You will work with your backing store during your session with the Configuration Assistant.

The configuration backing store contains representations of the z/OS system images and TCP/IP stacks along with the configuration resources defined to those stacks that you define during your session.

Click on “Open” to begin configuring your TCP/IP stacks with the policy-based networking technologies.

![Welcome to V2R1 Configuration Assistant for z/OS Communications Server](image-url)
3. Become Familiar with the TCP/IP Technologies you can Configure with the Configuration Assistant

The Configuration Assistant presents each TCP/IP technology in a “Perspective”, which provides the following:

- A separate view for configuring each of the policy-based networking technologies: IPSec (IP Security), AT-TLS (Application Transparent TLS), IDS (Intrusion Detection Services), PBR (Policy-based Routing), DMD (Defense Manager Daemon), NSS (Network Security Services).
- The systems table where the images and stacks to be configured are displayed is a key feature in each technology perspective. The system table spans all technology perspectives.

Step 3a: Switching between perspectives

When the backing store is opened, if it is a new backing store, the default perspective is IPSec; otherwise, it is the last perspective being configured when the backing store was saved. Take some time to switch between technology perspectives and come back to IPSec.
**Step 3b: Create z/OS System Images and TCP/IP Stacks in the systems table**

Add the z/OS system images and TCP/IP stacks that you want to configure to the systems table. The same systems table spans all technology perspectives.

Use the table “**Actions**” menu and select “**Add a z/OS Image**”.

This lab requires only one z/OS Image and Stack, but feel free to add more to practice.
Fill in the panel to define the z/OS system image. Use the panel Help link to learn more about the properties of the image. You can choose your own names; however, it may be more difficult to track since the examples will not match.

Select the “Ok” button to complete the image.

A popup dialog will appear to ask if a stack should be created, select the “Proceed” button.

Popup dialog asking to create the stack. Select “Proceed”.

Proceed to the Next Step?

Connectivity rules are configured for each TCP/IP stack. To continue with configuration you need to add a TCP/IP stack to the new z/OS system image. Do you want to add a TCP/IP stack now?

Cancel  Proceed
**Step3c: Create the TCP/IP stack**

Fill in the properties of the TCP/IP stack for image ZOS1 and select the “Ok” button.

You will see another dialog asking to begin configuring the stack with IPSec rules, select the “Cancel” button.
You will be sent back to the systems table where a new z/OS system image and TCP/IP stack are displayed.

A new image and stack are now in the systems table.
4. IPSec Reusable Resources

**Step 4a. Learn about reusable resources, specifically those for IPSec**

Now that you’ve created the TCP/IP stacks you want configure, the next step is to create your IPSec connectivity rules. But first, it’s important to understand the **reusable resources** the Configuration Assistant provides to help you with creating your rules.

**Reusable resources** help define the properties of your rules, and the value they provide is that they can be reused in rules for a single stack or across stacks. Each policy-based technology has its own set of reusable resources, and they are not shared across technologies.

For technology perspectives that have **reusable resources**, the Configuration Assistant presents these as tabs within the perspective beside the Systems table. This session will focus only on the **IPSec** reusable resources, but when complete, feel free to explore the other technologies.

The **IPSec** technology perspective has five types of reusable resources:

<table>
<thead>
<tr>
<th>Reusable Resource Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic Descriptors</td>
<td>Define the traffic you want to protect, using properties such as the TCP/IP port and jobname.</td>
</tr>
<tr>
<td>Security Levels</td>
<td>• For VPN tunnels, define the authentication and encryption methods used to protect the traffic.</td>
</tr>
<tr>
<td></td>
<td>• For basic filer rules, the security level is permit or deny.</td>
</tr>
<tr>
<td>Requirement Maps</td>
<td>Compound resource used to map one or more Traffic Descriptors to a Security Level. (What is protected and how)</td>
</tr>
<tr>
<td>Address Groups</td>
<td>Defines the IP Addresses or subnets that are the endpoints of the communication for connectivity rules.</td>
</tr>
<tr>
<td>Reusable (Connectivity) Rules</td>
<td>Define the rule once and reuse it across multiple stacks.</td>
</tr>
</tbody>
</table>
• Click on the tabs for each reusable resource.

• As reusable resources are created, they are added to a table. Each type of reusable resource has its own table. All reusable resources, except Reusable Rules, have predefined resources (IBM-provided) created.
Step 4b: View Predefined Traffic Descriptors

- Click on the “Traffic Descriptors” tab
- Select the Traffic Descriptor “FTP-Server” and click on the link. The default action is Modify. (Alternatively, select the button for “FTP-Server” and use the table Actions menu to Modify.)
  - Notice the Description of “FTP-Server” and other Traffic Descriptors shows (VERIFY). This indicates that IBM has provided this Traffic Descriptor, and it should be verified to determine if it should be modified.
- Select the table Actions menu and issue the “View Details”
Step 4c: View Predefined Security Levels

- Click on the “Security Levels” tab
- Select one of the Security Levels pointed to below with the “red arrows”.
  - Select the table Actions menu “View Details” option to view the details of the security level. Do this for each of the security levels pointed to with the red arrows.
  - Notice that the predefined security levels can’t be modified, but they can be copied.

Select a predefined security level. Select the table Actions menu “View Details” option to view the details of the security level. Do this for each of the security levels pointed to with the red arrows.
Step 4d: View Requirement Maps

- Click on the “Requirement Maps” tab
- Select the Filtering Requirement Map. Select the table Actions menu “View Details” option to view the details of the requirement maps. Then select the Trusted_Internet_Zone requirement map.
  - Notice that the predefined requirement maps can’t be modified, but they can be copied!
  - Notice how the Requirement Maps contain predefined traffic descriptors and security levels.

Select a predefined requirement map. Select the table Actions menu View Details
Step 4e: View Address Groups

- Click on the "Address Groups" tab
- Select the predefined address group All_IPv4_Addresses. Select the table Actions menu “View Details” option to view the details of the address group.
5. Define Reusable Resources for use in Connectivity Rules

Now that reusable resources have become more familiar, you will create some so they can be used in Connectivity Rules.

- In the IPSec technology, users can configure two basic types of Connectivity Rules, IP Filters and IP Tunnels. To determine the type of rule needed, first think about the systems and applications you want to protect and how you want to protect them. For example, consider (Note: These only provide one aspect in each case; however, there are certainly others to consider):

**IP Filtering:**

- Do you want to ensure that only traffic that you “Permit” is able to enter or leave your system and all other traffic should not be serviced (“Denied”)? If so, you’ll want to create some filter rules.

**IP Tunnels:**

- Do you want to have secure communications to another system(s)? For example, you recently acquired a new business having two systems that require communication with your z/OS systems. You’re not sure about all of the types of traffic that will flow, but some of it will be sensitive, so you decide to use IPSec VPN dynamic tunnels to secure the data using encryption.

The tasks under IPSec for this lab session will focus on the IP Filtering and create a filter rule to allow access to a test application “Testtool” in your enterprise, but only from the test systems (“Permit” the test systems). The Testtool application uses the TCP protocol and listens on port 100 and the test systems are in subnet 201.100.10.0/29. Two administrator from systems 9.100.2.2 and 9.100.2.3 can also access the application.

**Disclaimer:** This IP filter rule created in this lab is a simplistic example used only for the purpose of demonstrating how to create a rule in the Configuration Assistant. No real-world application of this specific example is intended.
**Step 5a:** First, create the Traffic Descriptor

- From the table **Actions** menu, select **New** to create a new traffic descriptor

- One important feature to note is the **Save** button. Notice that it is “grayed”. This is because changes to the configuration have not yet been made. Once a resource, such as a traffic descriptor is created, the **Save** button will become active.

  - If the **Save** button is gray, that means that you haven’t created any resources to save. Once you do, the **Save** button is active. Then after the button is pushed, it becomes gray again.

  - Users are encouraged to save changes periodically throughout the session (keep in mind this is a web-based connection!). Saving your backing store actually writes the changes to disk.
A traffic descriptor can contain more than one type of traffic that you want to pair with a security level. Select **New** to define the traffic type for Testtool.

Select **New** and **TCP** to define the traffic type for Testtool

(Expands to allow for selecting a protocol)
Testtool is a server application that uses the TCP protocol and listens on port 100, so it receives connections from clients (connection direction is inbound). Fill in the properties and click “Ok”.

Properties of the traffic type: TCP, ports, connection direction
The traffic type for Testtool has been created, so click “Ok” to complete the traffic descriptor. In this example the traffic descriptor only contains one traffic type, but a traffic descriptor can contain more than one traffic type.
Congratulations a new traffic descriptor has been created!
You will be positioned at the newly created resource.
Now that a resource has been created, notice the **Save** button is active.
Click “Save”
Notice that after clicking “Save”, you will be prompted to record in the “History Log”. This is optional, although the Config Assistant will record all saves automatically.
**Step 5b: Create the Requirement Map**

Since we’re creating a filter rule to “Permit” and “Deny” access to the Testtool application, we’ll use those predefined **Security levels**. This means that next we’ll create our requirement map.

- Remember that a requirement map maps the traffic descriptor to a security level.
- Select the Requirement Maps tab and use the table **Actions** menu to select **New**.
Fill-in the properties of the Requirement Map. Select on the Traffic Descriptor in editable table an click. A list of the traffic descriptors will be show (see next panel figure). Select Testtool. Click on the Security Level and select Permit.

Notice the “Deny” for All_Other_Traffic. This will deny all other traffic for the connectivity rule.

Hint: You’ll need to “double click” in the rows of the editable table.
Add the traffic descriptor **Testtool**.

Click **“Ok”**
Congratulations a new Requirement Map has been created!

![New Requirement Map]

<table>
<thead>
<tr>
<th>Name Filter</th>
<th>Description Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSH-Server</td>
<td>IBM supplied: RSH - Remote Shell Server</td>
</tr>
<tr>
<td>SMTP</td>
<td>IBM supplied: Simple Mail Transfer Protocol (SMTP) Server</td>
</tr>
<tr>
<td>SNMP-Agent</td>
<td>IBM supplied: Simple Network Management Protocol (SNMP) Agent traffic</td>
</tr>
<tr>
<td>SNMP-Manager</td>
<td>IBM supplied: Simple Network Management Protocol (SNMP) Manager</td>
</tr>
<tr>
<td>SNTP</td>
<td>IBM supplied: Simple Network Time Protocol (SNTP) Server</td>
</tr>
<tr>
<td>PerfilTesttool</td>
<td>A testing application</td>
</tr>
<tr>
<td>TN3270-Clien</td>
<td>(VERIFY) IBM supplied: TN3270 Client traffic</td>
</tr>
<tr>
<td>TN3270-Server</td>
<td>(VERIFY) IBM supplied: TN3270 Server traffic</td>
</tr>
<tr>
<td>Trace_Route_IP-V4</td>
<td>IBM supplied: IP-V4 ICMP - Trace Route traffic</td>
</tr>
<tr>
<td>Trace_Route_IP-V6</td>
<td>IBM supplied: IP-V6 ICMP - Trace Route traffic</td>
</tr>
<tr>
<td>Web</td>
<td>IBM supplied: Web Server traffic</td>
</tr>
<tr>
<td>Web-SSL</td>
<td>IBM supplied: Web Secure SSL traffic</td>
</tr>
</tbody>
</table>

Total: 39, Selected: 1

New Requirement Map
Step 5c: Create an Address Group

An address group allows for defining the IP addresses and subnets that define the endpoints for the connectivity rule when protecting your Testtool application.

Select the Address Groups reusable resource tab. Use the table Actions menu and select “New” to begin creating an address group.

Recall that we need to permit the test systems and administrator to access Testtool. This is subnet 201.100.10.0/29 and IP addresses 9.100.2.2 and 9.100.2.3.
Add the following to the editable table: 201.100.10.0/29, and IP addresses 9.100.2.2 and 9.100.2.3.

Click “Ok”
Congratulations a new address group, “TestandAdmin” has been created!
Now that reusable resources have been created (traffic descriptors, address groups, and requirement maps), these will become the components of the connectivity rule. Reusable resources don’t actually result in any TCP/IP policy configuration! It is only when the connectivity rule is created that configuration can be generated for the stack.

**Step 5d:** Create a Connectivity Rule for the Testtool application
First, from the Systems table, select the TCP/IP stack. Then, select “Rules…” from the Actions menu to begin configuring this stack with IPSec connectivity rules.

A wizard will assist with creating the rule.
Click "New" to begin creating a connectivity rule
Several types of connectivity rules are supported for IP Security, but the “Typical” rule allows for configuring basic filter rules and tunnels.

Use the radio button to select “Typical”.

Click “Next”
The rule to protect Testool is a basic filtering rule, so use the radio button to select “Filtering only”. We’re only concerned about local traffic since Testtool runs on this stack, so ensure local traffic is checked.

Click “Next”
When creating the filter rule, the **local and remote data endpoints** refer to the IP addresses and/or networks that are the endpoints for communication. The **local data endpoint** refers to this stack.

Since our Testtool is a server application that issues a socket bind() to INAddr_Any (all IP addresses) and listens for incoming connections, we'll protect **All_IPV4_Addresses** for the “**Local data endpoint**” selection.

For the “**Remote data endpoint**”, select the **TestandAdmin** address group that was created to ensure the intended users can access the Testtool application.

Click “**Next**”

Now that the communication endpoints have been defined for the connectivity rule, next a requirement map is needed. A new requirement map can be created or one that is already existing can be used.

Select the requirement map, PermitTestool, that was just created. Once selected, the traffic descriptor(s) and security level that comprise PermitTestool is shown.

Click “Next”
Select the “Finish” button to complete the connectivity rule.
Congratulations you have a new connectivity rule, **TestToolRule**, for Image ZOS1, TCP/IP stack TCPIP1!
Now you can perform additional actions on the rule, such as:

- **View Details** to view the details of the rule
- Optionally, under the column “**Name**”, click on the “**TestToolRule**” link. From here you can modify the rule or you can use the table **Actions** menu to modify.

When complete, click on the “**Close**” button and return to the view of the **Systems table**.
6. Generating and Installing the Configuration

Now that the rule is created, configuration must be generated and installed so that the Policy Agent (Pagent) can read the new configuration and install the new rule into the TCP/IP stack.

Select the TCP/IP stack, TCPIP1 and click on the Actions menu.
Step 6a: Select “Install Configuration Files”.

With this action, the Configuration Assistant will generate the IPSec policy and prepare it for installation (saving to disk or FTP).
The following displays the entry that represents the IPSec policy that will be generated for stack TCPIP1, and provides information about when the install (save to disk or FTP) for this policy has occurred (see the table columns).

Click on the entry TCPIP1 and the table **Actions** menu.

<table>
<thead>
<tr>
<th>Stack</th>
<th>Configuration</th>
<th>File Name</th>
<th>Host Name</th>
<th>Last Install</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCPIP1</td>
<td>IP Security Policy</td>
<td>/etc/dt教材/v2n1/ZOS1/TCPIP1/ipsPol</td>
<td></td>
<td>Never</td>
<td>Needs inst</td>
</tr>
</tbody>
</table>
Step 6b: Before clicking on install, view the policy configuration that will be generated if you are curious!
**Step 6c:** Use the **Actions** menu to select **Install**
The install panel is launched.

**Install file name:** The Install file name can be changed. Both Unix file names and MVS datasets are supported.

**Installation method:** Files may be saved locally or can be FTP’d to another system. Note: Since this is a “demo” system, you won’t be able to save the file, so just click “Close”
7. Optional Exercise

7.1 Exploring the “Tools” button

The tools button provides access to tasks that occur outside of the technology perspectives. These tasks relate to the Configuration Assistant as a whole and apply consistently across perspectives.

We’ll take a quick look at all tasks except for Log Level. This is serviceability setting that you may be directed to change by IBM Service based upon the need for servicing the product.

Step 7.1a: Tools button

The Tools button is in the right corner of the panel for each technology perspective.

Click on the drop-down arrow on the button to display the Actions.
Step 7.1b: Manage Backing Stores

The Manage Backing Stores task is new in z/OS V2R1. A new panel has been developed to assist with improved backing store management.

From each perspective, access the Tools drop-down menu on the right of the panel.

Click on “Manage Backing Stores”
Displays all of the backing stores.

Notice the **Status** and **Time Last Updated** columns and that the backing store in use is "current".

- A status of "Available" indicates that the backing store is free for use. A status of "Locked" indicates the backing store is in use by another user.

Next click on the table **Actions** menu.
View the tasks available from the Actions menu.

(Note: since this is a live system environment with other users, please don't complete any of the Actions. Thanks!)

Notice the Refresh button. You may want to refresh to update the list of backing stores to see if anything changed.
Step 7.1c: History and Preferences

Click on “History”
The History selection takes you to the History Log. Here the events of your session are recorded. You can control whether you are prompted to comment for the event; however, the Configuration Assistant will automatically record certain events such as Saving the backing store or performing an **Install** automatically.

During your session certain events are important to record. Saves are important since this actually saves the resources you have created during your session to disk.

Notice that some events have no comment this is because the user did not comment, but the Config Assistant still recorded the event.
Next, select “Preferences”
Preferences allow you to control when you receive the prompt for recording a comment to the History Log. For example, if you don’t want to enter comments then you may want to disable the comment settings.

Take a moment to view the options.

![Preferences screenshot]
End of exercise

This completes the prepared lab session tasks. Please feel free to explore other features of the Configuration Assistant.

We are open to comments for improving the user experience provided by the Configuration Assistant.
Thank You
Additional Information

**Additional information**

- **z/OS Management Facility website**
- **IBM z/OS Management Facility education modules in IBM Education Assistant**
  - [http://publib.boulder.ibm.com/infocenter/ieduasst/stg1r0/index.jsp](http://publib.boulder.ibm.com/infocenter/ieduasst/stg1r0/index.jsp)
  - Scroll down to z/OS Management Facility
- **IBM Publications Center**
  - Program Directory for z/OS Management Facility (GI11-9847)
  - IBM z/OS Management Facility Configuration Guide (SA38-0657)
  - IBM z/OS Management Facility Programming (SA32-1066)
  - IBM z/OS V2R1.0 Management Facility License Information (GC52-1386)
- **IBM z/OS Management Facility Information center**