

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

"Implementing Policy Agent in z/OS: Basic Setup"

Hands-on Lab Guide

(Policy Agent Exercises)



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

Revision date -

Friday, 20 June 2025

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

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

PART 0: LAB DESCRIPTION (CONFIGURING POLICY AGENT FOR QOS POLICY)....	- 4 -
SPECIFIC LAB DESCRIPTION: POLICY AGENT.....	- 4 -
PART 1: ANALYZING THE POLICY AGENT (PAGENT) PROCEDURE	- 6 -
PART 2: CREATING MAIN POLICY AGENT CONFIGURATION FILE PROCEDURE...	- 8 -
PART 3: INITIALIZING AND OPERATING THE POLICY AGENT PROCEDURE.....	- 11 -
END OF PAGENT LAB	- 13 -

Part 0: Lab Description (Configuring Policy Agent for QoS Policy)

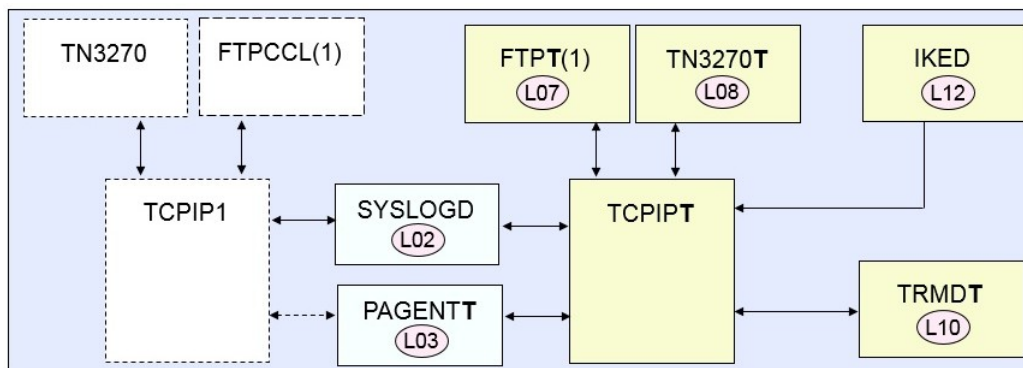
Each student ZOS (MVS) system has two TCP/IP stacks running in it. The basic TCPIP stack belonging to the instructors is named TCPIP1. The TN3270 procedure that has affinity to the instructor TCPIP1 is named TN3270. The FTP procedure that has affinity to TCPIP1 is named FTPCCL(1).

In our labs you use TCPIP1 for basic maintenance on ZOS until you 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 stack.

The student TCP/IP stack is named TCPIPT. The students customize this 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 TCPIPT.

Specific Lab Description: Policy Agent

Each team on a single ZOS (MVS) system will create its own Policy Agent configuration file (pagent.conf).



In this diagram you see TCPIP1 and some of its associated procedures. These procedures are used for maintenance of z/OS in general.

The TCPIPT stack is already running. Some of the labs require you to manipulate the configuration of this stack.

The remaining procedures represent part of what you, the students, configure in this course: SYSLOGD, PAGENT (named PAGENTT), TRMD (named TRMDT).

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

SYSLOGD has already been built for you by the time you are ready for this lab. Note how SYSLOGD is used by the entire z/OS image. Messages from both TCP/IP stacks are managed by SYSLOGD.

Note how Policy Agent (PAGENT -- with jobname of PAGENTT in our labs) can be used by the entire z/OS image. However, the configuration files for PAGENT indicate that PAGENT is to manage policies only for TCPIPT.

In a later lab you will configure TRMD. TRMD is a daemon – with jobname TRMDT in our lab – that is tied to a single TCP/IP stack. It is used mainly by Intrusion Detection Services (IDS) and by IKED.

In this lab you will configure the Policy Agent (PAGENT) procedure to manage QOS policies for the TCPIPT stack and to install priority queuing definitions for the QDIO OSAs.

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 USER3.

The lab is divided into several sections:

- ***Part 1: Analyzing the Policy Agent (PAGENT) Procedure***
- ***Part 2: Creating the Main Policy Agent Configuration File (pagent.conf).***
- ***Part 3: Initializing and Operating the Policy Agent procedure***

Part 1: Analyzing the Policy Agent (PAGENT) Procedure

1. Create a PCOMM session to connect to TN3270 at TCPIP1 on your assigned MVS system.
 - a. You should be telnetting into TCPIP1 on some MVS system at **192.168.20.8n** (where “n” is the suffix of the MVS/ZOS system).
 - b. Team1x telnets as User1x to TCPIP1 in MVS1 at **192.168.20.81**
 - c. Team 2x telnets as User2x to TCPIP1 in MVS2 at **192.168.20.82**
 - d. Team 3x telnets as User3x to TCPIP1 in MVS3 at **192.168.20.83**
 - e. Team 4x telnets as User4x to TCPIP1 in MVS4 at **192.168.20.84**
 - f. Team 5x telnets as User5x to TCPIP1 in MVS5 at **192.168.20.85**
 - g. Team 6x telnets as User6x to TCPIP1 in MVS6 at **192.168.20.86**
 - h. Team 7x telnets as User7x to TCPIP1 in MVS7 at **192.168.20.87**
 - i. Team 8x telnets as User8x to TCPIP1 in MVS8 at **192.168.20.88**
 - j. Team 9x telnets as User9x to TCPIP1 in MVS9 at **192.168.20.89**
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**
4. Go into SDSF with
 - a. **ISPF D.LOG**
5. Verify that the following procedures are running by issuing the command “/D A,L” from the SDSF command line (don’t use quotation marks):
 - a. SYSLOGDC (SYSLOG Daemon for this MVS)
 - b. TCPIP1 (this is the stack you telnetted into)
 - c. TN3270 (this is the TN3270 proc associated with TCPIP1)
 - d. FTPCCL(1) (this is the FTP proc associated with TCPIP1 – without TLS)
 - e. **TCPIPT** (this is the stack into which PAGENTT will install policies)
6. From the SDSF console, start the current version of Policy Agent:
 - a. In the response to the “/D A,L” in the previous step, if PAGENTT is already started bring it down with /P PAGENTT.
 - b. **/S PAGENTT**
 - c. Look for the message that tells you what type of policy has been loaded into the TCPIPT stack: **EZZ8771I**. (You will probably see more than one policy type – perhaps QoS, or AT-TLS (TTLS) policy, or even IPSec policy.)
7. From the SDSF command line enter the command to look at the contents of the running procedure (“display active jobs”):
 - a. **PF3**
 - b. **DA**
 - c. What **RACF userid** is associated with the OMVS segment that PAGENTT requires for successful startup (OWNER)?

-
8. From the Active Jobs display, issue the command to **select** PAGENTT:

- a. Place an “S” next to the procedure name and **Enter**:

NP	JOBNAME	StepName	ProcStep	JobID	Owner
s	PAGENTT	PAGENTT	PAGENT	STC04393	TCPIP

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

PF10 will move to the right in the log and PF11 will move to the left.

9. Answer the following questions about the procedure:
 - a. Write down here **the path and name of the main PAGENT configuration file:** _____
 - b. Where is Policy Agent logging its messages?

 - c. What is the symbolic name of the Language Environment data definition card in the JCL? ("**_CEE_ENVFILE=**")

 - d. What are **the path and the name of the Language Environment file (STDENV DD file)**?

10. Use **PF3 (F3)** to exit the view of the PAGENTT procedure.
11. On the command line enter the following to view the IBM Sample of the PAGENTT procedure:
 - a. **=3.4**
 - b. Specify a dataset name of '**SYS1.TCPIP.SEZAINST**' (without quotation marks) and press **ENTER**.
 - c. On the DSLIST screen place a **B** (for browse) next to the dataset and **Enter**.
 - i. This dataset contains the IBM samples for various z/OS Communications Server TCP/IP functions.
 - d. View the contents of the PAGENT sample procedure by entering '**S PAGENT**' (without quotation marks) on the command line.
12. Answer the following questions for the IBM sample of the Policy Agent procedure:
 - a. Does the basic procedure include a pointer to the symbolic name of the Language Environment file? ("**_CEE_ENVFILE=**")

 - b. Does the basic procedure indicate where Policy Agent is to log its messages?

 - c. Does the basic procedure indicate where Policy Agent is to find its Main Configuration File?

 - d. Does the basic procedure give you information on how to code the location of the PAGENT logging and of the Main Configuration File directly on the PAGENT EXEC statement?

 - e. Name the five environment variables that you might include in the STDENV file:

 - f. If you do not name the configuration file on the EXEC statement or in the STDENV file, what default does PAGENT take?
 - i. Configuration file default: _____
 - g. If you do not name the location of logging for PAGENT, what default does PAGENT take?
 - i. Log messages in _____

13. Name several differences in our customized version of the PAGENT procedure and the default sample found in SYS1.TCPIP.SEZAINST:
-
-
-
14. Exit from the view of the sample PAGENT procedure.
- a. **PF3 (F3)**
 - b. **PF3 (F3)**
 - c. **PF3 (F3)**
15. **For our labs you will use our customized version of the PAGENT procedure because we are using only one PROCLIB to which students have no WRITE access.**
- a. You will be modifying only configuration and environment files and thus will not need to store new procedures in the PROCLIB.

Part 2: Creating Main Policy Agent Configuration File Procedure

In this part of the lab you are going to reconfigure the Main Policy Agent Configuration file and then cause PAGENTT to re-read the new version.

1. Move into the OMVS shell from the ISPF Command line in order to configure Policy Agent:
 - a. **TSO OMVS**
2. Verify with the UNIX command *pwd* that your current directory is */u/usernx/*.
Examples:
 - a. Userid **user21** is positioned in **/u/user21 on MVS2**
 - b. Userid **user22** is positioned in **/u/user22 on MVS2**
 - c. Userid **user23** is positioned in **/u/user23 on MVS2**
 - d. Userid **user31** is positioned in **/u/user31 on MVS3**
 - e. Userid **user32** is positioned in **/u/user32 on MVS3**
 - f. Userid **user33** is positioned in **/u/user33 on MVS3**
 - g. Userid **user41** is positioned in **/u/user41 on MVS4**
 - h. Userid **user42** is positioned in **/u/user42 on MVS4**
 - i. Userid **user43** is positioned in **/u/user43 on MVS4**
 - j. Userid **user51** is positioned in **/u/user51 on MVS5**
 - k. Userid **user52** is positioned in **/u/user52 on MVS5**
 - l. Userid **user53** is positioned in **/u/user53 on MVS5**
 - m. Userid **user61** is positioned in **/u/user61 on MVS6**
 - n. Userid **user62** is positioned in **/u/user62 on MVS6**
 - o. Userid **user63** is positioned in **/u/user63 on MVS6**
 - p. Userid **user71** is positioned in **/u/user71 on MVS7**
 - q. Userid **user72** is positioned in **/u/user72 on MVS7**
 - r. Userid **user73** is positioned in **/u/user73 on MVS7**
 - s. Userid **user81** is positioned in **/u/user81 on MVS8**

- t. Userid **user82** is positioned in **/u/user82 on MVS8**
 - u. Userid **user83** is positioned in **/u/user83 on MVS8**
 - v. Userid **user91** is positioned in **/u/user91 on MVS9**
 - w. Userid **user92** is positioned in **/u/user92 on MVS9**
 - x. Userid **user93** is positioned in **/u/user93 on MVS9**
3. Switch to SuperUser mode:
 - a. **su**
4. Examine the STDENV file to see what its contents are:
 - a. **obrowse /etc/PAGT1/pagentt.env**
PAGENT_CONFIG_FILE=/etc/PAGT1/pagentt.conf
PAGENT_LOG_FILE=/tmp/pagentt.log
LIBPATH=/usr/lib
TZ=EST5EDT4
 - b. Observe how we have specified the **PAGENT_CONFIG_FILE** and the **PAGENT_LOG_FILE** variables. However, you saw in a previous step that **we customized our PAGENT JCL to override certain values.**
 - i. In our MVS JCL **we are overriding the location of the PAGENT_LOG_FILE and routing PAGENT messages to SYSLOGD.**
5. Exit from this view of the Language Environment file where you saw that, although we have it coded, in fact, we are using only the default LIBPATH and the TimeZone variable. (Our JCL has overridden the configuration file specification and the log file specification in this file.)
 - a. **PF3 (F3)**
6. Review the UNIX TCP/IP “Samples” directory to see the many types of PAGENT policy files in text format that are available to you if you decide to code policies without the help of z/OS Configuration Assistant:
 - a. **cd /usr/lpp/tcpip/samples**
 - b. **ls -al pag***
 - c. Do you see many sample files for getting started with an LDAP repository (“ldif” files)? _____
 - d. Do you see many samples for getting started using text files (“conf” files)? _____
 - e. Do you see the Main Pagent Configuration File? _____ This is the file you will begin your PAGENT configuration with.
7. Exit back to your own user directory (where “**nx**” is your team number):
 - a. **cd /u/user**nx**/**
8. Copy the PAGENT Main Configuration File into your directory and **rename** it:
 - a. **cp /usr/lpp/tcpip/samples/pagent.conf pagentt.conf**
 - i. (notice the **double “t”** in the first field of the renamed file)
9. NOTE: In this exercise we are using only one file for this Policy Agent exercise, the IBM sample Main Configuration File – which includes QoS policies, which we will leave in place.
10. Edit the new pagent.conf member:
 - a. **oedit pagentt.conf**
11. First quickly look through the file, noting the excellent instructions given there! (Sometimes the instructions in a configuration file are easier to understand than those in the IP Configuration Guide. You should always examine both resources before configuring.) Ignore the “Truncation” warning.
 - a. **PF8 (F8)** to page forward; **PF7 (F7)** to page backward in the file.
12. Make note of all the possible definition types that could be included (for Sysplex Monitoring, etc). We will not code all these parts.

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

- a. We are coding only some QoS policies and the policies that load the OSA QDIO Adapter with the OSA queue priority TOS byte settings.
13. Add the following line to set loglevel:
 - a. **LogLevel 31**
14. Add the following line at the appropriate place in the file. In this exercise we are using only one file for this Policy Agent exercise: the IBM sample Main Configuration File – which includes QoS policies and the QDIO OSA TOS byte values – and which will also be the TCP Image file.
 - a. **TcpImage <Student TCP Procname> FLUSH PURGE 600**
15. Next find the section in the file that deals with setting the priorities for the queues in a QDIO OSA. From the command line enter:
 - a. **f SetSubNetPrioTosMask**
16. Replicate the example given.
 - a. Use “**rr**” on the first line to be replicated and “**rr**” on the last line.
17. Uncomment the section you just copied.

BE CAREFUL: You **MUST** delete the last column of each setting of the priorities so as not to set a VLAN User priority. Ultimately the example and YOUR CODING should look as follows, with the example still commented out (with the #-sign in column 1) and your version uncommented:

```
# example: SetSubNetPrioTosMask
# {
#   SubnetTosMask    11100000
#   PriorityTosMapping 1 1110000 7 <<delete VLAN User Pri.
#   PriorityTosMapping 1 1100000 6 <<delete VLAN User Pri.
#   PriorityTosMapping 2 1010000 5 <<delete VLAN User Pri.
#   PriorityTosMapping 2 1000000 4 <<delete VLAN User Pri.
#   PriorityTosMapping 3 0110000 3 <<delete VLAN User Pri.
#   PriorityTosMapping 3 0100000 2 <<delete VLAN User Pri.
#   PriorityTosMapping 4 0010000 1 <<delete VLAN User Pri.
#   PriorityTosMapping 4 0000000 0 <<delete VLAN User Pri.
# }
SetSubNetPrioTosMask
{
  SubnetTosMask    11100000
  PriorityTosMapping 1 1110000
  PriorityTosMapping 1 1100000
  PriorityTosMapping 2 1010000
  PriorityTosMapping 2 1000000
  PriorityTosMapping 3 0110000
  PriorityTosMapping 3 0100000
  PriorityTosMapping 4 0010000
  PriorityTosMapping 4 0000000
}
```
18. **Browse** through the rest of the file to find the Policy Rules and Actions. Leave these QOS Rules and Actions in place.
 - a. **PF7 (F7) and PF8 (F8)** – for backwards and forwards in the file
19. **Close** and **File** the new pagentt.conf file with a **PF3 (F3)**.
20. Copy your version of the pagentt.conf file into the /etc/PAGT1/ directory, thus overlaying the current copy of the configuration file that is already running:
 - a. **cp pagentt.conf /etc/PAGT1/**
21. Exit from Superuser mode in the UNIX shell.

- a. **exit**
- 22. Exit from the UNIX shell itself:
 - a. **exit**
 - b. **ENTER**
 - c. **PF3**
- 23. Return to the SDSF log (command “=**D.LOG**”)

Part 3: Initializing and Operating the Policy Agent procedure

1. Next enter the command to cause the Policy Agent to re-read the entire configuration file:
 - a. **/F PAGENTT,REFRESH**
 - b. With the resulting message (EZZ8771I) you should see that the QoS policy has been installed into TCPIPT.
EZZ8771I PAGENT CONFIG POLICY PROCESSING COMPLETE FOR TCPIPT : **QOS**
2. Next enter the command to cause Policy Agent to re-read only changed files:
 - a. **/F PAGENTT,UPDATE**
 - b. **Note the difference in Message EZZ88771I now:**
EZZ8771I PAGENT CONFIG POLICY PROCESSING COMPLETE FOR TCPIPT : **NONE**
3. Return to the OMVS shell:
 - a. **TSO OMVS**
4. Switch again into superuser so that you may browse the SYSLOG Daemon log to see what was recorded about PAGENTT:
 - a. **su**
5. Review the tail end of the log file from the UNIX shell:
 - a. **tail -100 /var/CSLOG/syslogall.log** (or /var/syslogall.log – depending on where your SYSLOG daemon is currently writing output.)
 - i. If you do not see the answers for the questions we ask you next, please browse the log:
 - 1) **obrowse /var/CSLOG/syslogall.log**
 - b. Use **PF7** and **PF8** to move up and down through the file.
 - i. **Do you see evidence of the two MODIFY commands?** _____
6. Exit out of the syslog file and review the configuration again.
 - a. **PF3** if you were in browse mode.
 - b. **obrowse pagentt.conf**
 - i. **Loglevel at which PAGENTT was started:** _____
 - ii. This is a very low log level. This is why there are not many messages in the syslog file. With a higher log level many more messages will be logged in syslog. When you implement security items and increase the pagent log level you must make sure your syslog is customized with large enough space so that messages are not lost.
 - c. **PF3** to exit browse.
7. Use the **pasearch** command to display “policy object information” (“c”) for the QoS policies (“q”) installed into TCPIPT (“-p <stackname>”):
 - a. **pasearch -p TCPIPT -cq**
8. Is the QoS policy stored locally or was it retrieved from a Central Policy Agent Server? _____

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

9. Do you remember, from which file did PAGENTT read the QoS policy RULES and ACTIONS?
 - a. Circle response: QoS Policy File or the base configuration file?
10. Is PAGENTT reading the policies from an LDAP Server? _____
11. Are the policies to be flushed and purged? _____
12. Then issue the pasearch command (with “-qA”) in order to see only the Active QoS policies that have been installed in the TCPIP1 and then the TCPIPT stack:
 - a. **pasearch -qA -p TCPIP1 > myqA1**
 - i. TCPIP1 is not named in the pagentt.conf file; therefore:
EZZ8437I pasearch Command: Parameter Error 51
 - b. **pasearch -qA -p TCPIPT > myqAT**
13. Browse myqAT and you see a consolidated list of the running policies.
 - a. **obrowse myqAT**
14. Find the rule named “ftpd”:
 - a. **f ftpd** (on the ISPF command line)
15. What is the name of the ACTION that matches this RULE?

16. How many Policy ACTIONS are associated with this RULE?

17. During what time frame is the rule active?

18. Which networking interfaces does this rule apply to?

19. Are there any restrictions on the Source or Destination IP addresses that this rule is using?

20. What are the source ports for this policy? _____
21. Which protocol does this rule apply to? TCP or UDP? (Protocols are defined in the /etc/protocol or the ‘sys1.tcpip.sezainst(proto)’ file. The file sample is in /usr/lpp/tcpip/samples/protocol.)

22. When was the policy last created and when was it last updated?

23. Exit from this view of the QoS policies and from the OMVS shell:
 - a. **PF3 (F3)**
 - b. **exit**
 - c. **exit**
 - d. **ENTER**
24. Move to SDSF:
 - a. **=D.LOG**
25. Query the existing log, debug, and trace levels of PAGENTT:
 - a. **/F PAGENTT,QUERY**
26. Raise the log and debug levels of PAGENTT temporarily:
/F PAGENTT,LOGLEVEL,LEVEL=127
 - a. **Open the IP Diagnosis manual and the IP Configuration Reference determine the meaning of DEBUG LEVEL 31:**

- b. **Open the IP Diagnosis manual and the IP Configuration Reference and determine the meaning of LOGLEVEL 127:**
-

27. Return to OMVS to view the results:
- a. **TSO OMVS**
 - b. **su**
 - c. **obrowse /var/CSLOG/syslogall.log ... or ... /var/syslogall.log**
28. Compare the problem determination information with enhanced PAGENT logging and debug levels and without. **Do you think you would want to run constantly with the enhanced levels?** _____
- a. **Why or why not?** _____
-
29. You have finished the Basic Policy Agent lab. You are now prepared for the more complicated Policy Agent labs!

End of PAGENT Lab

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

