

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

"Implementing SYSLOG Daemon in z/OS"

Hands-on Lab Guide

(z/OS CS SYSLOG Daemon and CRON Exercises)



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

Revision date -

Thursday, 19 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 for Configuring SYSLOG Daemon for z/OS	- 4 -
<i>Specific Lab Diagram for SYSLOG Daemon.....</i>	<i>- 5 -</i>
Part 1: Configuring a SYSLOG Daemon Configuration File.....	- 5 -
Part 2: Refresh SYSLOG Daemon to Use Your Configuration and Verify	- 7 -
End of SYSLOGD Lab.....	- 9 -

Part 0: Lab Description for Configuring SYSLOG Daemon for z/OS

Each student ZOS (MVS) system has two TCP/IP stacks running in it. The “maintenance” 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 test TCP/IP stack.

The student test 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.

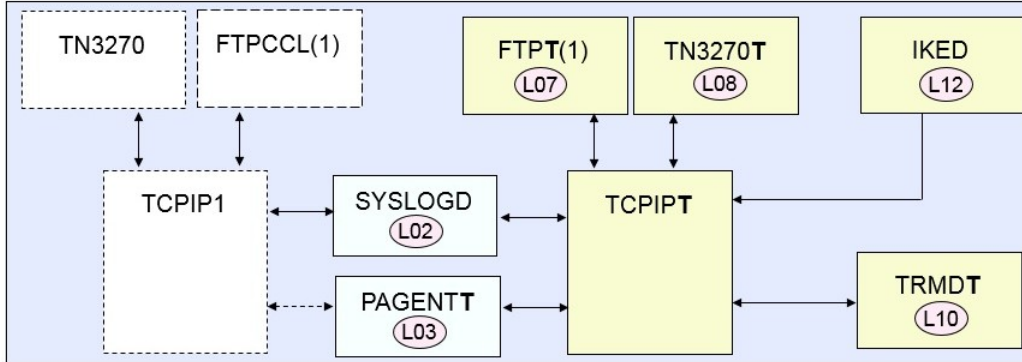
Your Lab Instructor has provided you with your TEAM name, your MVS system number, your USERID, and your PASSWORD. If you do not yet have this information, please advise the Instructor. Please review the lab diagram.

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.

Specific Lab Diagram for SYSLOG Daemon



As the diagram above shows, your z/OS system (ZOSn or MVSn) should run with a UNIX SYSLOG Daemon. In our case, we are using a daemon for local processes only. The SYSLOG Daemon captures messages from UNIX processes that you will be using. You are to configure this SYSLOG Daemon environment, replace the instructor version of a configuration file with your own version, and test your own version.

The lab is divided into several sections:

- *Part 1: Configuring a syslog.conf file in UNIX System Services (USS) or in the Open MVS (OMVS) environment.*
- *Part 2: Refreshing the running z/OS SYSLOG Daemon process to read your new configuration file and verify your work. Examine the CRON Daemon process.*

Part 1: Configuring a SYSLOG Daemon Configuration File

1. Log into your MVS system, if you are not already logged on, using the TCPIP1 “maintenance” address of **192.168.20.8n**.
2. Enter SDSF when you see the READY prompt:
 - a. **ISPF D.LOG**
3. At the command line issue the command to see the running UNIX (“OMVS”) processes on MVS:
 - a. **/D OMVS,A=ALL**
4. Browse through the display until you find the SYSLOG Daemon job. Answer these questions:
 - a. **What is the Job Name of the SYSLOG Daemon?** (You need this information later.)

 - b. **What address space is it running in?**

 - c. **Which UNIX owner is associated with the SYSLOG Daemon?**

 - d. **What is the UNIX Process ID of the SYSLOG Daemon?**

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

5. Move into the OMVS shell from the SDSF log:
 - a. **TSO OMVS**
 6. Issue the command to verify that you are in your user directory (/u/usernx):
 - a. **pwd**
 7. Switch to SuperUser mode:
 - a. **su**
 8. Review the contents of the /etc/rc file from which we started SYSLOGD at OMVS initialization:
 - a. **cat /etc/rc**
 9. Use PF7 (F7) and PF8 (F8) to browse up and down through the displayed file to find the SYSLOGD entry. How did SYSLOGD obtain the job name that you saw on the MVS console?
-
10. Issue the command to look at the running UNIX processes from within the UNIX environment and look for the syslog daemon process:
 - a. **ps -ef** (you will see output something like this)
OMVSKERN 17104904 1 - Aug 13 ? 1:12 /usr/sbin/syslogd -c -i -u -f /etc/syslog.conf
 11. Write down here the UNIX Process ID (PID) of the running SYSLOGD. You will need it later. (In our example above, the PID is "17104904".)
-
12. What significance do the following parameters have?
 - a. **"-c"** parameter: _____
 - b. **"-i"** parameter: _____
 - c. **"-u"** parameter: _____
 - d. **"-f"** parameter: _____Review the lecture materials if necessary.
 13. SYSLOGD should be running prior to the completion of TCP/IP initialization. You should **not** stop the SYSLOG Daemon or useful messages may be lost. Instead you should replace the running configuration file with a new one and then send a UNIX "sighup" signal to the running process so that it will re-read the new configuration file.
 14. Copy the sample SYSLOGD configuration file into your own directory and rename it to "syslogt.conf":
 - a. **cp /usr/lpp/tcpip/samples/syslog.conf syslogt.conf**
 15. Edit the new syslogt.conf member:
 - a. **oedit syslogt.conf**
 - i. You can ignore any "TRUNCATION" warnings.
 16. At the bottom of the file comment out the line **"*.err /var/log/%Y/%m/%d/errors"** by placing a comment character of **"#"** in front of the line. The result should look as follows:
 - a. **# *.err /var/log/%Y/%m/%d/errors**
 - i. We are building our logs to have permanent names; in our labs we are not using the "Year"/"Month"/"Day" convention that is evident in the sample.
 17. Add a line below the line you commented out. You want to record all messages for SYSLOGD in the /var/CSLOG/subdirectory:
***,* /var/CSLOG/syslogall.log**
 18. Above this line insert two more lines for logging that you will use in some future lab exercises. You will initially comment out these two lines:
local4.* /var/CSLOG/ipsec.log

local4.none;*. * /var/CSLOG/syslogall.log

- a. **local4.*** is a special facility class that IPSEC logs into.
 - b. **local4.none** indicates that we should not be logging IPsec into the syslogall.log, since we are already logging IPsec messages in a separate location. We don't want "double logging" in this case. In some cases you might find double logging desirable.
19. **Close** and **File** the new syslogt.conf file with a **PF3 (F3)**.

Part 2: Refresh SYSLOG Daemon to Use Your Configuration and Verify

1. Replace the running copy of SYSLOG Daemon's configuration file with your version:
 - a. **cp syslogt.conf /etc/syslog.conf**
2. Return to the system log:
 - a. Enter **exit** twice
 - b. **Enter**
3. Cause SYSLOGD to reread its configuration file:
 - a. **/F SYSLOGDC,RESTART**
F SYSLOGDC,RESTART
FSUM1254 SYSLOGDC MODIFY COMMAND ACCEPTED
FSUM1252 SYSLOGDC RECONFIGURATION COMPLETE
 - b. Prior to z/OS V1.11 it was necessary to use a unix SIGHUP command to cause SYSLOGD to reread its configuration file, "kill -1 <pid>".
4. Return to OMVS:
 - a. **TSO OMVS**
 - b. **su**
5. Issue the command to see the running SYSLOG daemon:
 - a. **ps -ef**
6. Is the PID number the same or different from what it was before?
 - a. _____
7. Why is it important for SYSLOGD to continue to execute when the configuration file is refreshed?

8. Next switch to the /var directory, under which the new log directory (CSLOG) was to be created.
 - a. **cd /var**
9. List the contents of this directory:
 - a. **ls -al**
 - b. Do you find the directory named "CSLOG"? _____
 - i. If you do, then the "-c" parameter did its job and created the new directory.
10. Move into CSLOG to see if the log file or files were created.
 - a. **cd CSLOG**
 - b. **ls -al**
11. Browse the contents of syslogall.log:

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

- a. **obrowse syslogall.log**
 - i. Notice how the restart of SYSLOG Daemon is recorded into the new UNIX log file.
12. Exit from browsing the file:
 - a. **PF3**
13. Exit from superuser status
 - a. **exit**
14. Exit from the OMVS shell:
 - a. **exit**
15. Return to the SDSF screen:
 - a. **Enter**
16. Stop the TCPIPT stack
 - a. **/P TCPIPT**
17. After you see the stack ENDED in the messages, restart the stack you stopped.
 - a. **/S TCPIPT**
18. Return to OMVS:
 - a. **TSO OMVS**
 - b. **su**
 - c. **cd /var/CSLOG**
19. Browse through the contents of “syslogall.log”:
 - a. **obrowse syslogall.log**
 - b. What do you notice? **What types of messages are now in the log?**

20. Exit out of the file:
 - a. **PF3**
21. Now discover whether there is a CRON process in place to manage the SYSLOG Daemon logs:
 - a. **ps -ef**
22. Do you find CRON as a running process? (/usr/sbin/cron)
 - a. _____
23. Review the line of the /etc/rc file that shows how we started the CRON Daemon at OMVS initialization:
 - a. **cat /etc/rc | grep cron**
24. View the running CRONTABS file placed into /usr/spool/cron by OMVSKERN:
 - a. **crontab -l -u OMVSKERN**
 - b. **NOTE:** *In z/OS V1R11 the management and automation of SYSLOG Daemon were vastly simplified, but your shop may currently be using CRON Daemon and scripts to manage logs.*
 - i. *Best Practices for SYSLOG Daemon management recommend the use of the Archiving functions that were introduced in z/OS V1R11.*
25. **IMPORTANT:** You should advise the person who manages the logs for you of the increased logging output generated with Security Policies so that monitoring and adjusting of log sizes and archiving can be arranged. In case the administrator in charge of SYSLOGD management is unaware of the usability changes made to SYSLOGD in z/OS V1R11, let them know of these improvements so that they may read up on in the IP Configuration Guide and in the IP System Administrator’s Guide.
26. Exit from superuser mode and the OMVS Shell.
 - a. **exit**
 - b. **exit**

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

c. **Enter**

27. Do **NOT** issue the command to archive the SYSLOG Daemon log files.

a. If you did want to archive the command would be

/F SYSLOGDC,ARCHIVE

i. Note, the messages would tell you that this SYSLOGD configuration file has not been defined for Archiving (“0 FILES”):

```
F SYSLOGDC,ARCHIVE
```

```
FSUM1254 SYSLOGDC MODIFY COMMAND ACCEPTED
```

```
FSUM1260 SYSLOGDC ARCHIVE COMPLETE FOR 0 FILES
```

b. Remember again that:

i. ***Best Practices for SYSLOG Daemon management recommend the use of the Archiving functions that were introduced in z/OS V1R11 but we are not using the function in this class.***

28. You have successfully completed the SYSLOG Daemon lab. (SYSLOGD is one of the pre-requisites for Policy Agent.)

End of SYSLOGD Lab

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

