Network Administration Lab
Experiment#4
Periodic Processes Management & Logging

Dr. Ahmed Awad & Eng.Ibrahim Amryeh

October 6, 2020

1 Objectives

The purpose of this experiment is to deal with periodic processes to schedule some administrative tasks on periodic basis. Thereafter, it aims to practice managing syslog messages.

2 Overview

2.1 Periodic Process

When a process has to be executed following a time schedule, it is said to be a **periodic process**. Such processes are widely used in network and system administration. Such tasks might include: periodic checking for network connectivity, periodic updates, periodic email checking, and others.
Cron is one of the most commonly used periodic processes in Linux. It is a daemon whose objective is to run commands on a predetermined schedule. It has been used for simple reminders on Linux system. Besides, it is used for file system cleanup from the different junk files.
Cron tasks are typically implemented in a configuration file named **crontab**. This file contains a list of command lines and the times at which they have to be invoked. Each line contains the following format:

minute hour dom month week command

a. Minute: The minute in which the command will be executed. Its options are between 0-59

b. Hour: The hour in which the command will be executed. Its options are between 0-23.

c. The day of month (dom): The day in which the command will be executed. Its options are between 0-31.

d. Month: The month in which the command will be executed. Its options are between 1-12.

e. Week: The day of the week in which the command will be executed. Its options are between 0-6 (0 represents Sunday).

2.2 Log files & Syslog

The purpose of logging is to hint towards the resolution of configuration problems. Therefore, periodic logging of events is a crucial task of a network administrator. However, rotating log files is required as they grow large very quickly, specially for busy services.
Syslog forms a comprehensive logging system whose objective is to standarize the logging process through sorting the log messages by their source, importance, and destination. Syslogd daemon (rsyslogd in newer versions of Linux) is typically responsible for capturing syslog messages when necessary. This daemon reads its configuration file and then performs logging. Cron process can be exploited as well for critical syslog message generation.

3 Procedure

3.1 Crontab Configuration

a. Make sure that Cron has been installed in your Linux machine. **How can you do such check?**

b. Install Cron if it does not exist. Show all the steps needed for installation.

c. Open the crontab file. **What command do you use for this purpose?**

d. Open the crontab using geditor. **Whad do you need to do?**

e. What does the command **crontab -l** do?

f. What permissions does the crontab file have?

g. Which users have permissions to schedule cron tasks? **Justify your answer?**

3.2 Implementing Periodic Tasks

a. Implement a periodic process that creates a file every 1 minute. The name of the file should be the time in which it will be created. Stop this process after 5 executions and show the files that have been created.

b. Modify the above task that you have created so that it runs every 2 minutes only on Sundays. Make sure that your process works fine and then stop it.

c. Modify the above task that you have created so that it runs only on every system reboot. Make sure that your process works fine and then stop it.

d. Write a periodic process that pings the gateway of your machine on every 12 am and 12 pm on everyday of the week. The ping should be logged into a file named **ping.log** under /var/log directory.

e. What does the command **service cron status** do?

3.3 Log files

a. Where can you find most of the log files in Linux?

b. Show some examples of log files in your machine. Is their naming convention consistent? Justify your answer?

c. What does the command **lastlog** do?

d. What does log files rotation mean? Is it possible to implement it using cron? How?

e. Write a bash shell script that removes all the log files under the directory **/var/log** that have not been accessed in a week.

3.4 Syslog messages

a. Show the basic information related to syslog daemon running on your machine.

b. Write a bash shell script that generates a syslog message if your machine has been pinged.

c. Generate a syslog message by your machine whose destination is your neighboring machine and make sure that this message has been captured by the neighboring machine.