Lab 10: Monitoring System Performance
The purpose of this lab is to explore the various ways to monitor a unix system. It includes knowing where log files are kept and how to find information within them, as well as how to use the cron facility to setup your own monitoring services.

Supplies

- VMWare Server 1.05 or higher
- Benji VM

Preconfiguration

- NA

Forum

If you get stuck on one of the steps below don't beat your head against the wall. Use the forum to ask for assistance or post any valuable tips and hints once you have finished. Forum is at: http://simms-teach.com/forum/viewforum.php?f=13

Part One: Monitoring Log Files
The syslog daemon is a daemon that handles collecting information and error messages from various services (programs) and logging them in various log files, usually in the directory, /var/log. The /etc/syslog.conf can be used to tell the syslog daemon how you want to collect this logging information.

1. Log on as *root*.
2. Change directory to */var/log*:
   cd /var/log
3. Use the ls command to determine how many log files are active in this directory. Notice that log files are rotated.
   How many backups are there of each log file?
   How often are these log files backed up (rotated)?
4. Use the ls -l command to determine which log files are most heavily used.
   What is the most heavily used log file?
5. Run the following command on the log files:
   file * | more

Note that most logs are either empty or have ASCII text in them. Which two logs are **data** files and cannot be viewed as text?

6. Look for the oldest *wtmp* file. Use that file as an argument to the who command:
   who wtmp.? | more
   What does this file tell you?
7. View the file, */etc/logrotate.conf*. In this file, find where it controls the number and frequency of logfile rotations.
8. Let's add a new log entry to catch all system notices, and we'll log these notices to the file */var/log/notices*. Add the following line to the */etc/syslog.conf* file: ***.=notice /var/log/notices**
9. Create the new log file:
   > /var/log/notices
10. Now restart the syslog services:
    service syslog restart
    You may get a notification that both the syslogd and the klogd stopped and started successfully. In any case proceed to the next step.
11. Switch to another console screen and log in as **root**
12. Switch to another console screen and log in as **cis191**.
    After logging in as guest, attempt to **su** to superuser, but do not type the correct password.
13. Now check the "notices" log file. What is there?

Part Two: Using cron

In this procedure you will create a cron file as root to perform a regular backup schedule of the /home file system. The schedule will include a level 0 backup every Sunday at 3:00 AM, and a level 1 backup every day, except Sunday, at 1:00 AM

1. Log in as root.
2. Make a backup directory off of / that contains two subdirectories, one for level0 backups and one for level1 backups:
   cd /; mkdir -p backup/level0 backup/level1
3. Remove any existing cron jobs from root's crontable:
   crontab -r
4. In root's home directory, create a file called *cron*.
5. The first line in the file should perform the level 0 backup.
6. The second line in the file should perform the level 1 backup.
7. All dump files created should show a timestamp in the file name (hint: use the date command).
8. Initially (for testing purposes) set the level 0 backup to run a few minutes in the future. Schedule a level 1 backup to run each minute for six minutes following the level 0 backup.
9. Register your file *cron* with the crontab command using **crontab cron** and check it with the **crontab -l** command.
10. Test your cron job and validate the results mailed to you.
11. Update your cron job to meet the original scheduling criteria at the beginning of this section.
12. You may not be able to run this cron job, if your system is not running at these hours. Be sure this cron job is registered and shows with the **crontab -l** command as this is what you will turn in.

To Turn in

Create a lab10 file that shows:

- /etc/syslog.conf
- /var/log/notices
- /etc/dumpdates
- one of the dump results emailed to you
- the output of `crontab -l`

Review your work in lab10 before submitting to make sure you have covered each area of the grading rubric. Then submit your work using:

`scp lab10 cis191@opus.cabrillo.edu:lab10.`*`lastname`*

Grading rubric (30 points)

5 points for including all five deliverables
5 points for correctly modifying /etc/syslog.conf
5 points for capturing root and failed logins in your custom logfile
5 points for correct dump commands in your cron job
5 points for correct cron job scheduling
5 points for email showing dump results from cron job