LPIC-1 102-400 – Lesson 11 – Lab

*** Enter into your Lab environment as root**

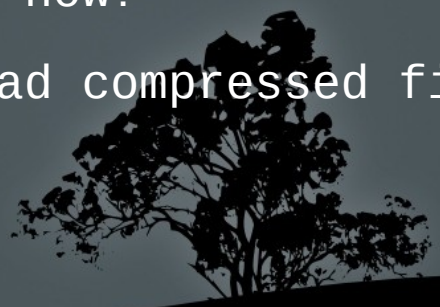
- **# ps aux | egrep -i "(syslog|klogd)"** # what do you see?
- **# view /etc/rsyslog.conf** # examine configuration in both CentOS and Debian
- **# ls -la /etc/rsyslog.d** # look into **ryslog.d**
- **# vi /etc/rsyslog.conf** # Add this line at the end of
  # rsyslog.conf
  daemon.* /var/log/daem.log
  :wq
- **# systemctl restart rsyslog** # restart rsyslog to re-read the configuration
- **# view /var/log/daem.log** # check the new log file
- **# logger -p daemon.info "mysql dying \ painfully"** # send some message

Lesson 11 – Lab

- **# logger -p daemon.info -t mysql "mysql \ still dying painfully"** # send another message
- **# view /var/log/daem.log** # check the logs
- **# logger -p user.info "Testing by root" 1** send some message as root
- **# su – user1** # login as **user1**
- **$ logger -p user.info "Testing by user1"** # send a message as **user1**
- **$ logger -t bug -p user.info "Testing by \ user1"** # change the message tag with '**bug:**'
- **$ exit** # exit back to root
- **# grep Testing -r /var/log** # find logs containing 'Testing'
- **# grep user1 -r /etc/rsyslog.*** # find logs containing **user1**

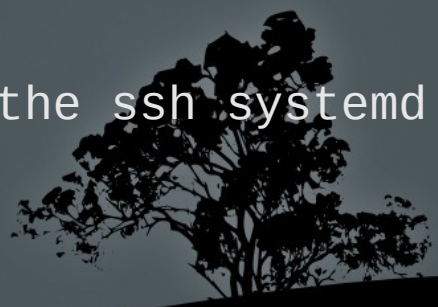
Lesson 11 – Lab

- **# find /var/log -type f -ls; | sort -k11 | less** # find and sort all logs alphabetically
- **# vi /etc/logrotate.conf** # check the logrotate configuration
- **# tail -f /var/log.messages** # follow **messages** (launch tail in another shell using screen)
- **# logger -p lpr.notice -t printer "Printer is no more"** # send a message using the **lpr** facility
- **# tail /var/log/messages** # check if the message appeared in the logs
- **# less /var/log/auth.log.3.gz** # can you read a compressed file?
- **# zless /var/log/auth.log.3.gz** # how about now?
- **# view /var/log/auth.log.3.gz** # can you read compressed files with view?



Lesson 11 – Lab

- **# grep cron.daily /var/log/syslog*** # find daily cron logs
- **# zgrep cron.daily /var/log/syslog*** # include compressed files too
- **# head -n20 /var/log/syslog** # show top 20 lines of **syslog**
- **# tail -n20 /var/log/syslog** # show bottom 20 lines of **syslog**
- **# file /var/log/[bw]tmp** # show binary session files
- **# last** # show last logins
- **# lastb** # show last failed logins
- **# systemctl restart ssh.service**
- **# journalctl -xe** # show most recent messages, with extra information, from **journald** database
- **# journalctl -u ssh** # check messages from the ssh systemd unit



License