Log Management
SysLog

TZNOG-5 2017 - Dodoma, SNS

Syslog

- Syslog is an old, old protocol
  - **sys**tem **log**
- Used to send log messages from a device (router, switch, server) to a log collection server
- Uses UDP to send packets over the network
  - what do you think about using UDP?

Examples

- The things you have been looking at in /var/log/syslog or /var/log/messages are delivered locally by syslog
- Formatting is a little different depending on the source of the log message, but the idea is the same

```
May 12 22:05:51 noc cups-lpd[20129]: Unable to get command line from client!
May 12 22:07:24 noc cups-lpd[21357]: Connection from 192.168.2.74 (IPv4 192.168.2.74)
May 12 22:15:01 noc sudo:     inst : TTY=unknown ; PWD=/u1/home/inst ; USER=root ; COMMAND=/u2/apb-auto-backup/cron-script
May 12 22:16:15 noc cups-lpd[21357]: Unable to get command line from client!
May 12 22:16:15 noc cups-lpd[31293]: Connection from 192.168.2.74 (IPv4 192.168.2.74)
May 12 22:16:18 noc cups-lpd[31293]: Unable to get command line from client!
```

Syslog Facility, Priority

- Each message sent to a syslog server has some text, a **facility** and a **level**
  - facilities are things like **auth**, **daemon**, **ftp**, **mail**, **local0**, **local1**, ..., **local7**
  - levels are things like emerg, alert, err, warning, notice, info, debug
- We will choose facility **local7** this time

Syslog Security

- Introducing rsyslog or syslog-ng
- The syslog protocol is old, and is really insecure (no authentication!)
  - really, really old!
- You don’t want everybody in the world to be able to send you log messages. *Why?*

Syslog Security

- On FreeBSD, by default, syslogd will not accept messages over the network
- We can specify the -a option to allow network access from a specific network only
  - syslogd -a 196.200.220.0/24
- Not all syslogd implementations are as flexible
- Check /etc/rsyslog.d/50-default.conf

Configuring syslogd

- syslogd is configured on most UNIX-like systems using /etc/rsyslog.conf
  - lines specify a priority/level pattern, and what to do with messages that match it
- on Ubuntu, other settings are configured in /etc/default/ (as you might expect)

Starting and Stopping

- The traditional way to tell syslogd to re-read rsyslog.conf is to send it a HUP signal
  - killall -HUP rsyslogd
  - On Ubuntu you can run
    - Sudo service rsyslog reload
- On Ubuntu one can also restart the whole process using:
  - Sudo services rsyslog restart

Syslog on Equipments

- To tell a cisco switch or router to send log messages to a syslog server, we specify a server address and a facility
  - logging facility local7
  - logging 196.200.220.251

Exercise

- Configure your host/server/router
- Check messages are arriving
- Configure your server
- Make sure logs are being rotated
- Do stuff to make log messages appear (e.g. change the router configuration)