CST8177 – Linux II

midterm, system services, logs

Todd Kelley
kelleyt@algonquincollege.com

Today's Topics

- quota command
- system services
- syslog
- logger command line utility

Quota

- individual users can check their individual quota
- "quota" command
  - block usage and limits
  - inode usage and limits
  - remainder on grace period if over soft limit

System Services: examples

- We've seen several system services by now
- NTP service: keeps clock accurate
  - ntpd : the daemon
  - /etc/ntp.conf : the daemon config file
  - /etc/init.d/ntpd : the SysVinit script
  - ntpd daemon itself IS the client (of an ntp server)
  - ntpd logs to /var/log/messages

System Services: examples

- SSH service: logins with Putty.exe or ssh
  - sshd : the daemon (SSH server)
  - /etc/ssh/sshd_config : the daemon config file
  - /etc/init.d/sshd : the SysVinit script
  - client program: putty.exe, ssh, scp, and more
  - daemon logs its messages to /var/log/secure
  - client manpage: man ssh
  - daemon manpage: man sshd
  - daemon config file manpage: man 5 sshd_config
  - client config file manpage: man 5 ssh_config
- If we stop the sshd daemon, noone can log in over SSH

System Services: daemons

- daemon:
  - a program, launched at boot time usually
    - /etc/init.d/* : the SysVinit scripts for starting, stopping, restarting, getting status of daemons
  - doesn't terminate – it keeps providing the service
  - many daemons, but not all, take requests from a corresponding client program
  - examples:
    - sshd : secure shell daemon, serves the ssh client
    - httpd : web server daemon, serves web browser client
    - crond : cron daemon, no client
    - ntpd: a client that provides a system service and uses an ntp server

System Services: config files

- System Service Daemons have config files
- Normally maintained somewhere in /etc/
- Often end in ".conf"
- Default config file comes with install package
- System administrators customize them
- Config files control various parameters
  - some parameters apply to many services:
    - how should logging be done
    - what port should the service listen on
  - some are specific to an individual service:
    - ntpd: which ntp server should be used
    - sshd: which version(s) of SSH protocol to use

config files (cont'd)

- Often config files have many comments in them
- # is a common comment character
  - usually lines beginning with # are ignored
- Various possible options will be "commented out"
- Those options can be activated by "uncommenting" them

config files (cont'd)

- From /etc/ssh/sshd_config

```
# Logging
# obsoletes QuietMode and FascistLogging
SyslogFacility AUTH
#SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
```

config files (cont'd)

To comment out this line
SyslogFacility AUTH
it becomes
#SyslogFacility AUTH

and to uncomment this line
#SyslogFacility AUTHPRIV
it becomes
SyslogFacility AUTHPRIV

System Services: clients

- So far in your work with computers you've seen more of the clients than the servers.
- Examples of clients you use all the time
  - ssh, putty.exe
  - Web Browser
  - Explorer (Windows Networking)
  - ftp
  - DHCP (example: network connection at Algonquin)
- Each of these clients requires a server to be running at the "other end"

System Services: logging

- Daemons need a place where they can send their output
- Most daemons use the syslog logging service
- Centralized logs are easier to manage
- syslog is itself a daemon
  - daemon : syslogd
  - config file : syslog.conf
  - client program: logger command line utility, as well as all the other daemons
- daemons send their messages to syslog, and syslog puts those messages in an appropriate place, usually a file under /var/log/

Syslog config: /etc/syslog.conf

- Contents of /etc/syslog.conf is a set of rules

- Every rule consists of two fields:

selector action

- Every selector has two parts:

facility.priority

Syslog Facilities

- auth : authorization
- authpriv : private authorization
- cron : crond
- daemon : other misc daemons
- kern : the kernel
- lpr : printer
- mail : email
- news : usenet news
- syslog : syslog itself
- user : user messages
- uucp : unix to unix copy
- local0 through local7 : local use
- * : all of the above

Syslog Priorities

- In order of increasing priority:
  - debug : debug level messages
  - info : normal information
  - notice : normal but significant, unusual
  - warning : not an error, but action should be taken
  - err : error condition, non-urgent failure
  - crit : critical condition, failure in primary system
  - alert : action needed immediately
  - emerg : panic, system unusable, notify all
  - * : all of the above
  - none: none of the above for the given facility

Syslog actions

- Absolute pathname of a file
  - put the message (log entry) in that file
  - dash in front means omit syncing on every entry
- Terminal or Console : ex /dev/console
  - write the message on that screen
- @hostname : remote machine
  - send the message to syslog on the remote machine
- username
  - write the message on that user's terminal
- * : everyone logged in
  - write the message on everyone's screen
- named pipe (fifo) : useful for debugging