Syslog & xinetd

Stephen Pilon

Syslog and Log Files

- What create log files?
- Logging Policies
  - Throw away all data immediately
  - Reset log files at periodic intervals
  - Rotate log files, keeping data for a fixed time
  - Compress and archive logs to tape or other permanent media

Syslog and Log Files

- Automate the maintenance of log files with cron
- Throwing away log files
  - DON'T
- Rotate log files

Syslog and Log Files

```
#!/bin/sh
cd /var/log
mv logfile.2 logfile.3
mv logfile.1 logfile.2
mv logfile logfile.1
cat /dev/null > logfile
chmod 600 logfile
```

Syslog and Log Files

- Most Linux distributions supply a program called logrotate
- Some daemons keep their log files open all the time

Syslog and Log Files

- Linux Log Files
  - /var/log
  - /var/adm
  - syslog

Syslog and Log Files

- Kernel logging
  - Kernel stores logs entries in internal buffer
  - dmesg redirects its output to /var/log/dmesg
    - /var/log/boot.msg on SUSE
  - klogd
- Startup script logging
  - initlog on RHEL

Syslog and Log Files

- Logrotate: Manage log files
  - runs with cron
  - /etc/logrotate.conf
  - /etc/logrotate.d

Syslog and Log Files

- Syslog: The system event logger
  - written by Eric Allman
  - comprehensive logging system
  - can sort by source and importance
  - can route to a variety of destinations
    - log files
    - users' terminals

Syslog and Log Files

- Alternatives to syslog
  - syslog-ng (syslog, next generation)
    - SUSE default
  - SDSC Secure Syslog
    - from San Diego Supercomputing Center
    - high-performance syslog

Syslog and Log Files

- Syslog architecture
  - syslogd, the logging daemon (along with it config file, /etc/syslog.conf)
  - openlog, library routines that submit messages to syslogd
  - logger, a user-level command that submits log entries from the shell

Syslog and Log Files

- Configuring syslogd
  - /etc/syslog.conf
  - selector <Tab> action
    - mail.info /var/log/maillog
  - selectors identify the program that is sending the log message
    - facility.level

Syslog and Log Files

- Syslog security levels
  - emerg — Panic situations
  - alert — Urgen situations
  - crit — Critical conditions
  - err — Other error conditions
  - warning — Warning messages
  - notice — Things that might merit investigation
  - info — Informational messages
  - debug — For debugging only

Syslog and Log Files

- In syslog.conf – levels indicate the minimum level importance that a message must have in order to be logged.

Syslog and Log Files

A basic configuration for a stand-alone machine

```
#emergencies: tell everyone who is logged on
*.emerg                 *
#important messages
*.warning;daemon,auth.info;user.none    /var/log/messages
#printer errors
lpr.debug               /var/log/lpd-errs
```

Syslog and Log Files

Network client

```
# Forward important messages to the central logger
*.warning;lpr,local1.none          @netloghost
daemon,auth.info                   @netloghost
```

XINETD AND INETD: MANAGE DAEMONS

- Daemons that manage other daemons
- inetd comes from the UNIX world
- Most Linux distributions have migrated to xinetd
  - Created by Panos Tsirigotis

XINETD AND INETD: MANAGE DAEMONS

- xinetd
  - Souped-up alternative to inetd
  - Incorporates security features
  - Better log management features
  - More flexible configuration language

XINETD AND INETD: MANAGE DAEMONS

- Work with daemons that provide services over the network
- Attach themselves to the network ports that would normally be managed by the daemons
- Some daemons rely upon RPC

XINETD AND INETD: MANAGE DAEMONS

- Configuring xinetd
  - Configuration file is traditionally /etc/xinetd.conf

XINETD AND INETD: MANAGE DAEMONS

```
defaults
{
    instances               = 60
    log_type                = SYSLOG authpriv
    log_on_success          = HOST PID
    log_on_failure          = HOST
    cps                     = 25 30
}
```

XINETD AND INETD: MANAGE DAEMONS

```
service ftp
{
        socket_type             = stream
        protocol                = tcp
        wait                    = no
        user                    = root
        server                  = /usr/sbin/wu.ftpd
        server_args             = -a
        instances               = UNLIMITED
        only_from               = 128.138.0.0/16
        log_on_success          += DURATION
}
```

XINETD AND INETD: MANAGE DAEMONS

- Log directly to file or syslog
- Can provide some interesting services
  - forwarding requests to an internal host

XINETD AND INETD: MANAGE DAEMONS

- /etc/services
  - Used by several standard library routines that map between service names and port numbers
  - Comes configured

XINETD AND INETD: MANAGE DAEMONS

```
tcpmux          1/tcp           # TCP port multiplexer
echo            7/tcp
echo            7/udp
...
ssh             22/tcp          # SSH Remote Login Protocol
ssh             22/udp          # SSH Remote Login Protocol
smtp            25/tcp  mail
rlp             39/udp resource
...
```

portmap: map RPC services to TCP and UDP ports

- Maps RPC service numbers to the TCP/IP ports on which their servers are listening
- If the portmap daemon dies, all the services that rely on it must be restarted