Chapter 11
Syslog and Log Files

Log files

- Execution information of each services
  - sshd log files
  - httpd log files
  - ftpd log files
- Purpose
  - For post tracking
  - Like insurance

Logging Policies

- Common schemes
  - Throw away all log files
  - Rotate log files at periodic intervals

```
#!/bin/sh
/usr/bin/cd /var/log
/bin/mv logfile.2.gz logfile.3.gz
/bin/mv logfile.1.gz logfile.2.gz
/bin/mv logfile logfile.1
/bin/cat /dev/null > logfile
/bin/kill –signal pid
/usr/bin/gzip logfile.1
```

  - Archiving log files

```
0 3 * * * /usr/bin/tar czvf /backup/logfile.`/bin/date +\%Y\%m\%d`.tar.gz /etc
```

Finding Log Files

- Ways and locations
  - Common directory
    - **/var/log, /var/adm**
  - Read software configuration files
    - **Ex: httpd.conf**

      TransferLog /home/www/logs/access.log
  - See /etc/syslog.conf

Under /var/log in FreeBSD (1)

You can see that under /var/log …

```
tytsai@tybsd:/var/log> ls
Xorg.0.log          cron.1.gz          maillog.2.gz       sendmail.st        setuid.yesterday
Xorg.0.log.old      cron.2.gz          maillog.3.gz       sendmail.st.0      slip.log
auth.log            cron.3.gz          maillog.4.gz       sendmail.st.1      userlog
auth.log.0.gz       cvsup.log          maillog.5.gz       sendmail.st.2      world.log
auth.log.1.gz       dmesg.today        maillog.6.gz       sendmail.st.3      wtmp
auth.log.2.gz       dmesg.yesterday    maillog.7.gz       sendmail.st.4      wtmp.0
auth.log.3.gz       lastlog            messages           sendmail.st.5      wtmp.1
auth.log.4.gz       lpd-errs           messages.0.gz      sendmail.st.6      xdm.log
auth.log.5.gz       maillog            mount.today        sendmail.st.7
cron                maillog.0.gz       ppp.log            sendmail.st.8
cron.0.gz           maillog.1.gz       security           setuid.today
tytsai@tybsd:/var/log>
```

That is because syslogd …

```
*.err;kern.debug;auth.notice;mail.crit          /dev/console
*.notice;authpriv.none;kern.debug;lpr.info;mail.crit;news.err   /var/log/messages
security.*                                      /var/log/security
auth.info;authpriv.info                         /var/log/auth.log
mail.info                                       /var/log/maillog
lpr.info                                        /var/log/lpd-errs
cron.*                                          /var/log/cron
*.emerg                                         *
```

Under /var/log in FreeBSD (2)

Why it rotates? That is because the newsyslog facility …

```
tytsai@tybsd:/etc> grep newsyslog crontab
0       *       *       *       *       root    newsyslog
tytsai@tybsd:/etc>
```

newsyslog.conf

```
# logfilename          [owner:group]    mode count size when  flags
/var/log/cron                          600  3     100  *     Z
/var/log/amd.log                       644  7     100  *     Z
/var/log/auth.log                      600  7     100  *     Z
/var/log/lpd-errs                      644  7     100  *     Z
/var/log/maillog                       640  7     *    @T00  Z
/var/log/sendmail.st                   640  10    *    168   B
/var/log/messages                      644  5     100  *     Z
/var/log/all.log                       600  7     *    @T00  Z
```

Vendor Specifics

- FreeBSD
  - newsyslog utility
  - /etc/periodic

```
tytsai@linux3:/etc/logrotate.d> less amd
/var/log/amd.log {
    create 0640 root security
    daily
    rotate 10
    notifempty
    missingok
    compress
}
```

- Red Hat
  - logrotate utility
  - /etc/logrotate.conf, /etc/logrotate.d directory

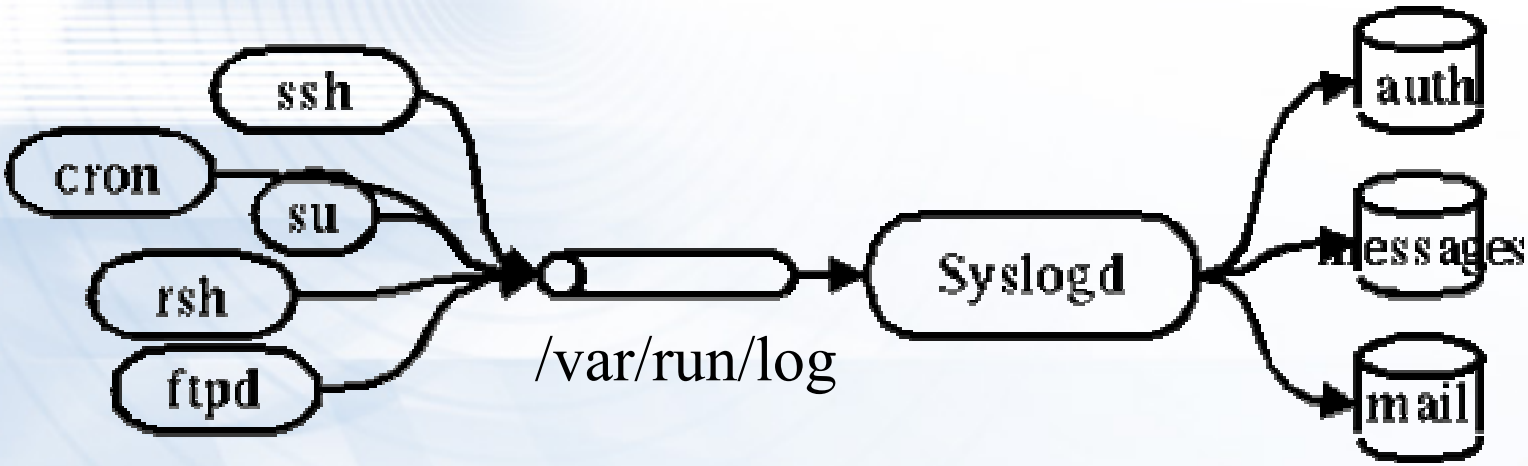
Files Not to Manage

- You can manage most log files yourself, except…
  - /var/log/lastlog (/var/adm/lastlog)
    - **Record of each user's last login**
  - /var/run/utmp (/etc/utmp)
    - **Record of each user that is currently logged in**

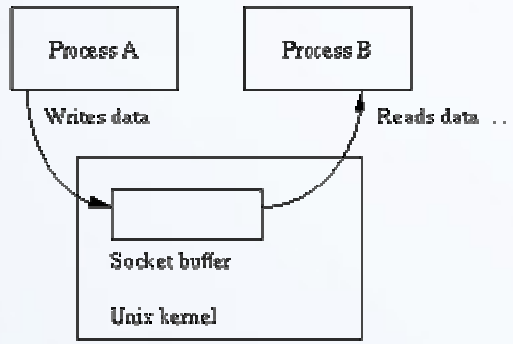
Syslog – The system event logger (1)

- Two main functions
  - To release programmers from the tedious of writing log files
  - To put administrators in control of logging
- Three parts:
  - syslogd, /etc/syslog.conf
    - **The logging daemon and configure file**
  - openlog, syslog(), closelog()
    - **Library routines to use syslogd**
  - logger
    - **A user command that use syslogd from shell**

Syslog – The system event logger (2)




```
tytsai@tybsd:/var/run> ls -al | grep log
srw-rw-rw-   1 root  wheel       0 Nov  7 15:12 log=
```



Configuring syslogd (1)

- Basic format
  - *selector* <Tab> *action*
    - Selector: program.level
      - **Program: the program that sends the log message**
      - **Level: the message severity level**
    - Action: tells what to do with the message
  - Ex:
    - **mail.info /var/log/maillog**

Configuring syslogd (2)

- selector
  - Syntax: facility.level
    - **Facility and level are predefined (see next page)**
  - Combined selector
    - **facility.level**
    - **facility1,facility2.level**
    - **facility1.level;facility2.level**
    - ***.level**
  - Level indicate the minimum importance that a message must be logged
  - A message matching any selector will be subject to the line's action

Configuring syslogd (3)

Facility	Programs that use it
kern	The kernel
user	User processes (the default if not specified)
mail	**sendmail** and other mail-related software
daemon	System daemons
auth	Security and authorization-related commands
lpr	The BSD line printer spooling system
news	The Usenet news system
uucp	Reserved for UUCP, which doesn't use it
cron	The **cron** daemon
mark	Timestamps generated at regular intervals
local0-7	Eight flavors of local message
syslog[a]	**syslogd** internal messages
authpriv[a]	Private authorization messages (should all be private, really)
ftp[a]	The FTP daemon, **ftpd**
*	All facilities except "mark"

Level	Approximate meaning
emerg	Panic situations
alert	Urgent situations
crit	Critical conditions
err	Other error conditions
warning	Warning messages
notice	Things that might merit investigation
info	Informational messages
debug	For debugging only

Configuring syslogd (4)

- Action
  - filename
    - **Write the message to a local file**
  - @hostname
    - **Forward the message to the syslogd on hostname**
  - @ipaddress
    - **Forwards the message to the host at that IP address**
  - user1, user2
    - **Write the message to the user's screen if they are logged in**
  - *
    - **Write the message to all user logged in**

Configuring syslogd (5)

> Ex:

```
*.emerg                                          /dev/console
*.err;kern,mark.debug;auth.notice;user.none      /var/adm/console.log
*.info;kern,user,mark,auth.none                  @loghost
*alert;kern.crit;local0,local1,local2.info       root
```

lpr.err ➔ /var/adm/console.log
@loghost

Level
emerg
alert
crit
err
warning
notice
info
debug

Configuring syslogd (6)

- Output of syslogd

```
Sep 20 15:28:24 tybsd /kernel: pid 8052 (conftest), uid 0: exited on signal 6 (core dumped)
Sep 28 15:38:48 tybsd sshd[22574]: error: PAM: Authentication failure
Sep 28 15:38:50 tybsd sshd[22574]: error: PAM: Authentication failure
Oct  1 14:13:03 tybsd sshd[27154]: error: PAM: Authentication failure
Oct  2 17:36:31 tybsd login: ROOT LOGIN (root) ON ttyv0
Oct  2 17:36:35 tybsd shutdown: power-down by root:
Oct  2 17:36:38 tybsd syslogd: exiting on signal 15
Oct  4 08:50:47 tybsd /kernel: Copyright (c) 1992-2004 The FreeBSD Project.
Oct  4 08:50:47 tybsd /kernel: Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993,
Oct  4 08:50:47 tybsd /kernel: The Regents of the University of California. All rights reserved.
Oct  4 08:50:47 tybsd /kernel: FreeBSD 4.10-STABLE #2: Mon Sep 20 14:02:22 CST 2004
Oct  4 08:50:47 tybsd /kernel: root@tybsd.csie.nctu.edu.tw:/usr/obj/usr/src/sys/TYBSD
Oct  4 08:50:47 tybsd /kernel: Timecounter "i8254"  frequency 1193182 Hz
Oct  4 08:50:47 tybsd /kernel: CPU: Mobile Intel(R) Pentium(R) 4 - M CPU 1.80GHz (1798.49-MHz 686-
```

Software that use syslog

Program	Facility	Levels	Description
amd	daemon	err-info	NFS automounter
date	auth	notice	Sets the time and date
ftpd	daemon	err-debug	FTP daemon
gated	daemon	alert-info	Routing daemon
halt/reboot	auth	crit	Shutdown programs
inetd	daemon	err, warning	Internet super-daemon
login/rlogind	auth	crit-info	Login programs
lpd	lpr	err-info	BSD line printer daemon
named	daemon	err-info	Name server (DNS)
nnrpd	news	crit-notice	INN news readers
ntpd	daemon, user	crit-info	Network time daemon
passwd	auth	err	Password-setting program
popper	local0	notice, debug	Mac/PC mail system
sendmail	mail	alert-debug	Mail transport system
su	auth	crit, notice	Switches UIDs
sudo	local2	alert, notice	Limited **su** program
syslogd	syslog, mark	err-info	Internal errors, timestamps
tcpd	local7	err-debug	TCP wrapper for **inetd**
cron	cron, daemon	info	System task-scheduling daemon
vmunix	kern	*varies*	The kernel

FreeBSD Enhancement (1)

- Facility name
  - FreeBSD allows you to select messages based on the name of the program

```
!named
*.*                                /var/log/named.log
```

- Severity level

Selector	Meaning
mail.info	Selects mail-related messages of info priority and higher
mail.>=info	Same meaning as mail.info
mail.=info	Selects only messages at info priority
mail.<=info	Selects messages at info priority and below
mail.<info	Selects all priorities lower than info
mail.>info	Selects all priorities higher than info

FreeBSD Enhancement (2)

- Restriction log messages from remote hosts
  - syslogd –a *.csie.nctu.edu.tw –a 140.113.209.0/24
  - rc.conf

```
syslogd_flags="-a 140.113.209.0/24:* -a 140.113.17.0/24:*"
```