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
  - Archiving log files

```
#!/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
/usr/bin/touch logfile
/bin/kill –signal pid
/usr/bin/gzip logfile.1
```

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

Finding Log Files

- Ways and locations
  - Common directory
    - /var/log, /var/adm
  - Read software configuration files
    - Ex: /usr/local/etc/apache22/httpd.conf

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

syslog.conf(5)

Under /var/log in FreeBSD (1)

- You can see that under /var/log …

```
npbsd1:/var/log -lwhsu- ls
all.log           auth.log.3.bz2    maillog.2.bz2     sendmail.st.0
all.log.0.bz2     auth.log.4.bz2    maillog.3.bz2     sendmail.st.1
all.log.1.bz2     auth.log.5.bz2    maillog.4.bz2     sendmail.st.2
all.log.2.bz2     auth.log.6.bz2    maillog.5.bz2     sendmail.st.3
all.log.3.bz2     auth.log.7.bz2    maillog.6.bz2     sendmail.st.4
all.log.4.bz2     console.log       maillog.7.bz2     setuid.today
all.log.5.bz2     cron              messages          setuid.yesterday
all.log.6.bz2     cron.0.bz2        messages.0.bz2    slip.log
all.log.7.bz2     cron.1.bz2        messages.1.bz2    sudo.log
amd.log           cron.2.bz2        messages.2.bz2    sudo.log.0.gz
amd.log.0.bz2     cron.3.bz2        messages.3.bz2    sudo.log.1
amd.log.1.bz2     debug.log         messages.4.bz2    userlog
amd.log.2.bz2     dmesg.today       messages.5.bz2    wtmp
amd.log.3.bz2     dmesg.yesterday   mount.today       wtmp.0
amd.log.4.bz2     lastlog           mount.yesterday   wtmp.1
auth.log          lpd-errs          pf.today          xferlog
auth.log.0.bz2    maillog           ppp.log
auth.log.1.bz2    maillog.0.bz2     security
auth.log.2.bz2    maillog.1.bz2     sendmail.st
```

Lots of logs

Under /var/log in FreeBSD (2)

- Logs – because of syslogd

syslogd(8)

```
bsd2:~ -lwhsu- cat /etc/syslog.conf | grep -v ^#
*.err;kern.warning;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
ftp.info                                                /var/log/xferlog
cron.*                                                  /var/log/cron
*.=debug                                                /var/log/debug.log
*.emerg                                                 *
!startslip
*.*                                                     /var/log/slip.log
!ppp
*.*                                                     /var/log/ppp.log
!sudo
*.*                         /var/log/sudo.log
console.info                                            /var/log/console.log
*.*                                                     /var/log/all.log
*.*                                                     @loghost
```

Under /var/log in FreeBSD (3)

- Logs are rotated – because newsyslog facility

newsyslog.conf(5)
newsyslog(8)

  - In crontab

```
bsd2:~ -lwhsu- grep newsyslog /etc/crontab
0       *       *       *       *       root    newsyslog
```

  - newsyslog.conf

```
bsd2:/usr/src/etc -lwhsu- cat newsyslog.conf | grep -v ^#
/var/log/all.log                        600  7     *    @T00  J
/var/log/amd.log                        644  7     100  *     J
/var/log/auth.log                       600  7     100  *     JC
/var/log/console.log                    600  5     100  *     J
/var/log/cron                           600  3     100  *     JC
/var/log/daily.log                      640  7     *    @T00  JN
/var/log/debug.log                      600  7     100  *     JC
/var/log/kerberos.log                   600  7     100  *     J
/var/log/lpd-errs                       644  7     100  *     JC
/var/log/maillog                        640  7     *    @T00  JC
/var/log/messages                       644  5     100  *     JC
/var/log/monthly.log                    640  12    *    $M1D0 JN
/var/log/pflog                          600  3     100  *     JB    /var/run/pflogd.pid
/var/log/ppp.log        root:network    640  3     100  *     JC
/var/log/security                       600  10    100  *     JC
/var/log/sendmail.st                    640  10    *    168   B
/var/log/slip.log       root:network    640  3     100  *     JC
/var/log/weekly.log                     640  5     1    $W6D0 JN
/var/log/wtmp                           644  3     *    @01T05 B
/var/log/xferlog                        600  7     100  *     JC
```

Vendor Specifics

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

```
linux1 [/etc/logrotate.d] -lwhsu- cat mail
/var/log/mail/maillog /var/log/mail/mail.info  /var/log/mail.warn /var/log/mail.err {
missingok
monthly
size=100M
rotate 4
create 0640 root security
nocompress
}
```

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

utmp(5)

Syslog

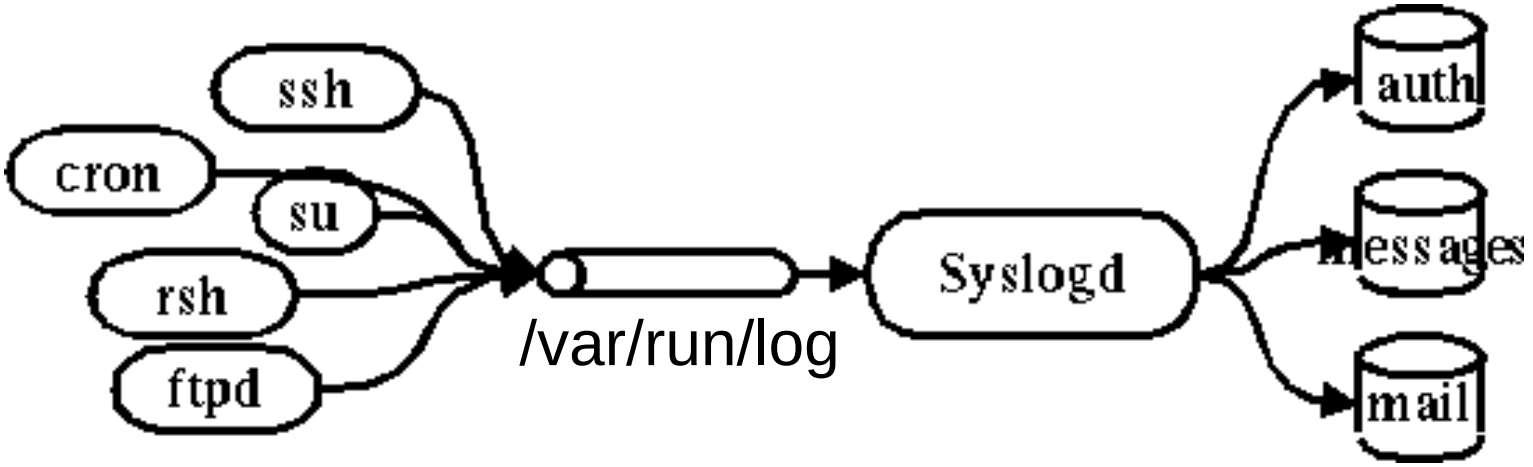
Syslog – The system event logger (1)

- 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

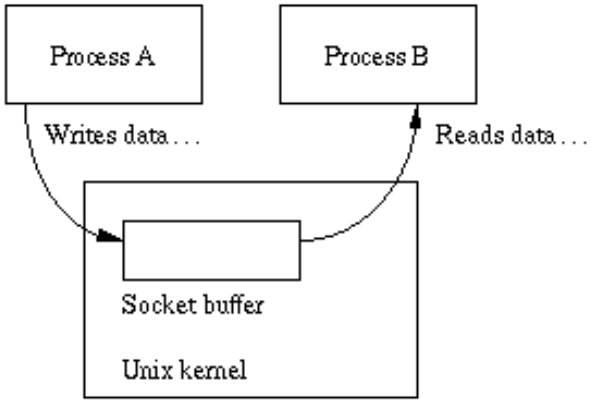
syslog(3)

logger(1)

Syslog –
The system event logger (2)




```
lwbsd:~ -lwhsu- ls -l /var/run/log
srw-rw-rw-  1 root  wheel  - 0 Nov 26 12:01 /var/run/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)

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

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"

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)

- Example:

```
*.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

```
Dec  2 07:12:09 lwbsd sudo:    lwhsu : TTY=pts/2 ; PWD=/z ; USER=root ; COMMAND=/bin/mkdir dump
Dec  2 07:12:13 lwbsd sudo:    lwhsu : TTY=pts/2 ; PWD=/z ; USER=root ; COMMAND=/usr/sbin/chown lwhsu dump
Dec  2 07:12:31 lwbsd sudo:    lwhsu : TTY=pts/2 ; PWD=/usr/home/lwhsu ; USER=root ; COMMAND=/sbin/dump 0uLf - /
Dec  2 07:12:47 lwbsd kernel: lock order reversal:
Dec  2 07:12:47 lwbsd kernel: 1st 0xffffffff38c67a28
Dec  2 07:12:48 lwbsd kernel: bufwait (bufwait) @ /usr/src/sys/kern/vfs_bio.c:2443
Dec  2 07:12:48 lwbsd kernel: 2nd 0xffffff01bd83f430 snaplk (snaplk) @ /usr/src/sys/ufs/ffs/ffs_snapshot.c:2224
Dec  2 07:12:48 lwbsd kernel: KDB: stack backtrace:
Dec  2 07:12:48 lwbsd kernel: db_trace_self_wrapper() at db_trace_self_wrapper+0x2a
Dec  2 07:12:48 lwbsd kernel: _witness_debugger() at _witness_debugger+0x49
Dec  2 07:12:48 lwbsd kernel: witness_checkorder() at witness_checkorder+0x7e6
Dec  2 07:12:48 lwbsd kernel: __lockmgr_args() at __lockmgr_args+0xc59
Dec  2 07:12:48 lwbsd kernel: ffs_copyonwrite() at ffs_copyonwrite+0x15e
Dec  2 07:12:48 lwbsd kernel: ffs_geom_strategy() at ffs_geom_strategy+0x158
Dec  2 07:12:48 lwbsd kernel: bufwrite() at bufwrite+0x108
Dec  2 07:12:48 lwbsd kernel: ffs_update() at ffs_update+0x196
Dec  2 07:12:48 lwbsd kernel: ffs_fsync() at ffs_fsync+0x18
Dec  2 07:12:48 lwbsd kernel: ufs_remove() at ufs_remove+0xe4
Dec  2 07:12:48 lwbsd kernel: VOP_REMOVE_APV() at VOP_REMOVE_APV+0x93
Dec  2 07:12:48 lwbsd kernel: kern_unlinkat() at kern_unlinkat+0x245
Dec  2 07:12:48 lwbsd kernel: syscall() at syscall+0x1dd
Dec  2 07:12:48 lwbsd kernel: Xfast_syscall() at Xfast_syscall+0xab
Dec  2 07:12:48 lwbsd kernel: --- syscall (10, FreeBSD ELF64, unlink), rip = 0x80071593c, rsp = 0x7fffffffe388, rbp =
0x800908d80 ---
Dec  2 07:13:46 lwbsd sshd[72206]: error: PAM: authentication error for illegal user hadar from 81.246.26.179
Dec  2 07:15:50 lwbsd sshd[76073]: error: PAM: authentication error for illegal user hadar from 88.63.75.242
Dec  2 07:20:15 lwbsd sshd[84588]: error: PAM: authentication error for illegal user hadassah from 200.62.142.212
```

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

```
!sudo
*.*                                    /var/log/suduo.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 *.cs.nctu.edu.tw
    –a 140.113.209.0/24
  - rc.conf

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