

Syslog and Log Rotate

yihshih

Log files

❑ Execution information of each services

- sshd log files
- httpd log files
- ftpd log files

❑ Purpose

- For post tracking
- Like insurance

```
ad3: WARNING - READ_DMA UDMA ICRC error (retrying request) LBA=96553119
ad3: WARNING - READ_DMA UDMA ICRC error (retrying request) LBA=96553119
ad3: FAILURE - READ_DMA status=51<READY,DSC,ERROR> error=84<ICRC,ABORTED>
LBA=96553119
g_vfs_done():ad3s1a[READ(offset=49435164672, length=36864)]error = 5
vnode_pager_getpages: I/O read error
vm_fault: pager read error, pid 850 (cp)
ad3: WARNING - READ_DMA UDMA ICRC error (retrying request) LBA=96556319
ad3: WARNING - READ_DMA UDMA ICRC error (retrying request) LBA=96556319
ad3: FAILURE - READ_DMA status=51<READY,DSC,ERROR> error=84<ICRC,ABORTED>
LBA=96556319
g_vfs_done():ad3s1a[READ(offset=49436803072, length=36864)]error = 5
vnode_pager_getpages: I/O read error
vm_fault: pager read error, pid 850 (cp)
```

Logging Policies

❑ Common schemes

- Throw away all log files
- Rotate log files at periodic intervals
- Archiving log files



```
#!/bin/sh
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

Under /var/log in FreeBSD (1)

❑ You can see that under /var/log ...

```
zfs[/var/log] -wutzh- ls
./                lastlog          maillog.7.bz2    sendmail.st
../              lpd-errs        messages         sendmail.st.0
auth.log          maillog          messages.0.bz2   sendmail.st.1
cron              maillog.0.bz2   messages.1.bz2   sendmail.st.2
cron.0.bz2        maillog.1.bz2   messages.2.bz2   sendmail.st.3
cron.1.bz2        maillog.2.bz2   mount.today      setuid.today
cron.2.bz2        maillog.3.bz2   mount.yesterday  wtmp
debug.log         maillog.4.bz2   pf.today         xferlog
dmesg.today       maillog.5.bz2   ppp.log
dmesg.yesterday  maillog.6.bz2   security
```

Lots of logs

Under /var/log in FreeBSD (2)

❑ Logs – because of syslogd

```
bsd5[~] -wutzh- cat /etc/syslog.conf | grep -v ^#
*. *                               /var/log/all.log
*. *                               @loghost
*.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                                 *
console.info                           /var/log/console.log
!sudo
*. *                                    /var/log/sudo.log
```

Under /var/log in FreeBSD (3)

❑ Logs are **rotated** – because **newsyslog** facility

- In crontab

```
chbsd [/etc] -wutzh- grep newsyslog /etc/crontab
0 * * * * root newsyslog
```

- newsyslog.conf

```
chbsd [/etc] -wutzh- cat /etc/newsyslog.conf
# logfilename      [owner:group] mode count size when flags [pid_file] [sig_num]
/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/maillog   640 7 * @T00 JC
/var/log/messages  644 5 100 * JC
/var/log/monthly.log 640 12 * $M1D0 JN
/var/log/security  600 10 100 * JC
/var/log/sendmail.st 640 10 * 168 B
```

newsyslog.conf(5)
newsyslog(8)

Vendor Specifics

❑ FreeBSD

- newsyslog utility
- /etc/newsyslog.conf

❑ Red Hat

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

```
linux1[/etc/logrotate.d] -wutzh- 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



Syslog

Syslog –

The system event logger (1)

❑ Two main functions

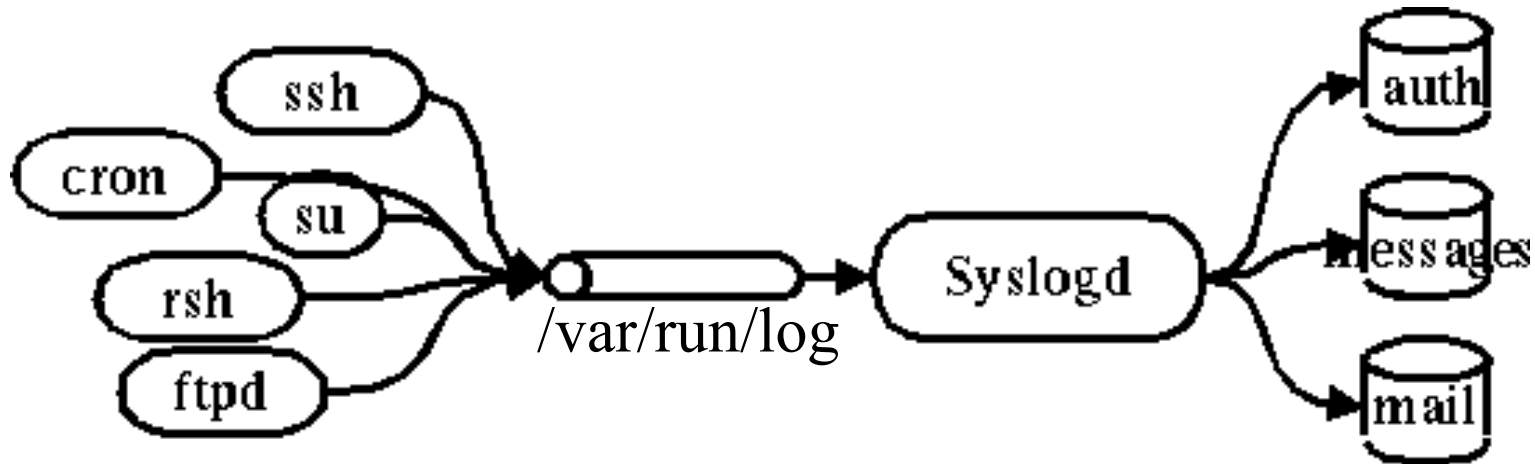
- To release programmers from the tedious of writing log files
- To put administrators in control of logging

❑ Three parts:

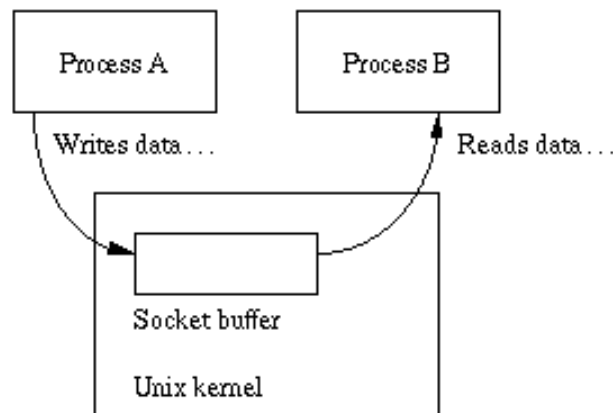
- `syslogd`, `/etc/syslog.conf`
 - The logging daemon and configure file
- `openlog()`, `syslog()`, `closelog()`
 - Library routines to use `syslogd`
- `logger`
 - A user command that use `syslogd` from shell

Syslog –

The system event logger (2)



```
zfs[~] -wutzh- ls -al /var/run/log
srw-rw-rw- 1 root wheel 0 Nov 21 17:07 /var/run/log=
```



Configuring syslogd (1)

❑ Basic format

- The configuration file `/etc/syslog.conf` controls syslogd's behavior
- *selector* <Tab> *action*
 - **Selector: facility.level**
 - **Facility:** 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	Level	Approximate meaning
kern	The kernel	emerg	Panic situations
user	User processes (the default if not specified)	alert	Urgent situations
mail	sendmail and other mail-related software	crit	Critical conditions
daemon	System daemons	err	Other error conditions
auth	Security and authorization-related commands	warning	Warning messages
lpr	The BSD line printer spooling system	notice	Things that might merit investigation
news	The Usenet news system	info	Informational messages
uucp	Reserved for UUCP, which doesn't use it	debug	For debugging only
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)

❑ 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

```
Aug 28 20:00:00 chbsd newsyslog[37324]: logfile turned over due to size>100K
Aug 28 20:01:45 chbsd sshd[37338]: error: PAM: authentication error for root from 204.16.125.3
Aug 28 20:01:47 chbsd sshd[37338]: error: PAM: authentication error for root from 204.16.125.3
Aug 28 20:07:15 chbsd sshd[37376]: error: PAM: authentication error for root from 204.16.125.3
Aug 28 20:07:17 chbsd sshd[37376]: error: PAM: authentication error for root from 204.16.125.3
Aug 30 09:47:49 chbsd sudo: wutzh : TTY=ttyp4 ; PWD=/usr/home/wutzh ; USER=root ; COMMAND=
Aug 30 22:02:02 chbsd kernel: arp: 140.113.215.86 moved from 00:d0:b7:b2:5d:89 to 00:04:e2:10:
Aug 30 22:05:13 chbsd kernel: arp: 140.113.215.86 moved from 00:04:e2:10:11:9c to 00:d0:b7:b2:
Sep 1 14:50:11 chbsd kernel: arplookup 0.0.0.0 failed: host is not on local network
Sep 3 13:16:29 chbsd sudo: wutzh : TTY=ttyp4 ; PWD=/usr/ports ; USER=root ; COMMAND=/usr/b
Sep 3 13:18:40 chbsd sudo: wutzh : TTY=ttyp4 ; PWD=/usr/ports ; USER=root ; COMMAND=/usr/l
Sep 3 13:25:06 chbsd sudo: wutzh : TTY=ttyp4 ; PWD=/usr/ports ; USER=root ; COMMAND=/usr/l
Sep 3 13:27:09 chbsd kernel: arp: 140.113.215.86 moved from 00:d0:b7:b2:5d:89 to 00:04:e2:10:
Sep 3 13:27:14 chbsd kernel: arp: 140.113.215.86 moved from 00:04:e2:10:11:9c to 00:d0:b7:b2:
Sep 3 15:27:05 chbsd sudo: wutzh : TTY=ttyp4 ; PWD=/usr/ports ; USER=root ; COMMAND=/usr/l
Sep 3 15:27:10 chbsd sudo: wutzh : TTY=ttyp4 ; PWD=/usr/ports ; USER=root ; COMMAND=/usr/l
Sep 3 15:27:25 chbsd sudo: wutzh : TTY=ttyp4 ; PWD=/usr/ports ; USER=root ; COMMAND=/usr/l
```

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	<i>varies</i>	The kernel

FreeBSD Enhancement (1)

❑ 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`
- Use `-ss` option to prevent `syslogd` from opening its network port
- `rc.conf`

```
syslogd_enable="YES"
```

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

Debugging syslog

❑ logger

- It is useful for submitting log from shell

❑ For example

- Add the following line into `/etc/syslog.conf`

```
local5.warning          /tmp/evi.log
```

- Use **logger** to verify

➤ `logger(1)`

```
# logger -p local5.warning "test message"  
# cat /tmp/evi.log  
Nov 22 22:22:50 zfs wutzh: test message
```

Using syslog in programs

```
#include <syslog.h>

int main() {
    openlog("mydaemon", LOG_PID, LOG_DAEMON);
    syslog(LOG_NOTICE, "test message");
    closelog();
    return 0;
}
```

```
zfs[~] -wutzh- tail -1 /var/log/messages
Nov 22 22:40:28 zfs mydaemon[4676]: test message
```