

syslog - centralized logging

David Morgan

© David Morgan 2004

A logging system

- Conforming programs emit categorized messages
- Messages are candidates for logging
- syslog handles the logging
 - performed by syslogd
 - per /etc/syslog.conf

© David Morgan 2004

Historical rationale - Then

- Some programs logged messages to one file
- Some programs logged to another
- Some programs logged to STDERR
- Some wrote to a pipe

© David Morgan 2004

Historical rationale - Now

- Programs themselves don't log messages
- They write them to syslog instead
- syslog manages logging centrally
 - decides which messages to log
 - decides where to log them to

© David Morgan 2004

Programs emit messages... ...you read them

- API calls to standard library functions
 - `openlog()` - identifies this program and its “facility” at program start
 - `syslog()` - provides a message, tagged with a “priority”
 - `closelog()` - closes logging before program terminates
- or “logger,” equivalent access from shell
- Of direct concern only to programmers
- Others write config files and read log file results

© David Morgan 2004

Programs emit messages... ...examples

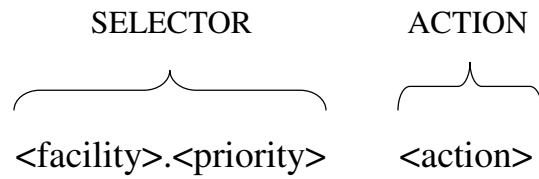
- “Normally, `dhcpcd` will log all output using the `syslog` (3) function with the log facility set to `LOG_DAEMON`.” man page for `dhcpcd` (8) dynamic host configuration protocol daemon
- Messages from `/var/log/messages`
 - Jul 24 13:19:25 brain kernel: eth1: NE2000 found at 0x300, using IRQ 3
 - Aug 3 15:33:03 brain PAM_pwddb[25812]: (login) session opened for user david by (uid=0)
 - Jul 31 20:23:31 brain ftpd[16423]: FTP LOGIN REFUSED (access denied) FROM cras1p66.navix.net [207.91.10.69], anonymous
 - Jul 26 17:01:23 brain httpd: httpd shutdown succeeded

© David Morgan 2004

/etc/syslog.conf

Entries, called rules, determine messages' handling

Rule format:



© David Morgan 2004

/etc/syslog.conf

<facility>.<priority>	<action>
auth	write to a file
authpriv	write to a terminal
cron	by tty device
daemon	by user
kern	write to a remote syslog
lpr	(via UDP to port 514)
mail	
news	
syslog	
user	
uucp	
local0 - local7	
*	

↑ higher priority ↓

© David Morgan 2004

/etc/syslog.conf rule example

```
mail.info /var/adm/info
```

The disposition of any messages issued

- by programs whose facility is “mail,”
- as having priority “info” or higher

shall be to write those messages into the file
/var/adm/info.

© David Morgan 2004

Standard /etc/syslog.conf

```
kern.* /dev/console
*.info;mail,news,authpriv.none /var/log/messages
authpriv.* /var/log/secure
*.emerg *
uucp,news.crit /var/log/messages
```

© David Morgan 2004

What happens?

- Each message is tested against every rule
- For each rule
 - does the message's facility match the rule's?
 - does the message's priority match or exceed the rule's?
 - if so, "log" the message as defined by rule's action

© David Morgan 2004

Syntax wrinkles

- * all facilities or all priorities
- = makes priority restrictive/single
- ! makes priority inverse/ignored
- none no priority

© David Morgan 2004

Multiple selectors, facilities

- separate selectors with ;
- separate facilities with ,
- selectors overwrite their predecessors

S E L E C T O R S

*.=info ; mail, news.none <action>

F A C I L I T I E S

“Log all messages of priority ‘info,’ but not if their facility is ‘mail’ or ‘news’ ”

© David Morgan 2004

Action (logging) destinations

- /var/log/messages that file
- /dev/tty6 that terminal
- root,bclinton terminals where those users are logged in
- @loghost syslog daemon on machine loghost

© David Morgan 2004

Important log files in /var/log

- cron
- dmesg boot messages
- lastlog user logins
- log.smb
- maillog mail traffic
- messages genl purpose
- news
- secure login attempts
- sendmail
- uucp
- wtmp current activity
- xferlog ftp transfers

© David Morgan 2004

Viewing log files dynamically

```
tail -f <name of log file>
```

© David Morgan 2004

Logfile rotation and management

- cron
 - /etc/crontab
 - /etc/cron.daily
 - /etc/cron.daily/logrotate
- logrotate
 - /etc/logrotate.conf
 - /etc/logrotate.d

© David Morgan 2004