



# Syslog

---

---

CIS 68C1

UNIX System Administration

# Syslog

- Syslog – A System Logging Facility
  - ✗ Two key functions
    - ✗ Provides a logging facility for programs
    - ✗ Give administrators control over logging
  - ✗ Flexible
    - ✗ Allows messages to be sorted and prioritized
    - ✗ Messages can be routed to various destinations
      - ✗ Log files
      - ✗ Terminals
      - ✗ Other hosts for centralized network logging

# Syslog

- Syslog's Primary Components
  - ✗ The **syslogd** logging daemon
    - ✗ Started at boot time
    - ✗ Configuration file: **/etc/syslog.conf**
  - ✗ Library of programmer's functions
    - ✗ Programmers use these functions to submit log entries
    - ✗ Write to **/dev/log**
  - ✗ The **logger** utility
    - ✗ Command line utility to submit log messages

# Syslog

## □ How Syslog Works

- ✘ Programmers write programs to log messages via **syslog**
  - ✘ The syslog programmers functions write messages to **/dev/log**
  - ✘ Programmer chooses the severity level of messages
- ✘ Syslog daemon
  - ✘ Consults the configuration file **/etc/syslog.conf**
  - ✘ Reads messages from **/dev/log**
  - ✘ Routes messages to the specified destination(s)

# Syslog

- /etc/syslog.conf
  - ✗ Controls how syslog handles messages
  - ✗ Simple text file with each line formatted as:
    - ✗ *selector* <tab> *action*
  - ✗ The *selector* selects which messages will be logged
    - ✗ *selector* is actually the pair *facility.priority*
      - ✗ *facility*           the program sending the message
      - ✗ *priority*         the severity level of the message
      - ✗ Values for *facility* and *priority* are predefined
  - ✗ The *action* describes how messages will be logged

# Syslog

## □ /etc/syslog.conf

### ✘ The *selector*

- ✘ Special values can be used in a *selector*

\* All possible values

none No values

- ✘ Multiple *facilities* with the same *priority* can be separated by commas

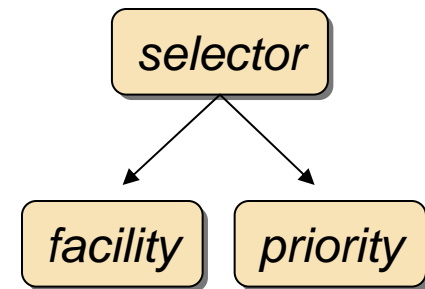
- ✘ Multiple *selectors* can be combined with a semicolon

- ✘ Red Hat Linux allows adding prefixes to the *priority*

= This priority only

! Except this priority and higher

!= All except this priority



# Syslog

- /etc/syslog.conf - *facility*

| Facility        | Messages from   |
|-----------------|---|
| kern            | The kernel  |
| user            | User processes (default)  |
| mail            | The <b>sendmail</b> daemon and other mail software                |
| cron            | The <b>cron</b> daemon  |
| authpriv, auth  | Security and authorization commands (auth is deprecated)          |
| lpr             | The BSD printing system   |
| ftp             | The FTP daemon  |
| daemon          | Other system daemons  |
| local0 – local7 | Local messages  |
| syslog          | Internal messages from <b>syslogd</b>                             |
| mark            | Causes <b>syslogd</b> to generate timestamps at regular intervals |
| *               | All facilities except <b>mark</b>                                 |

*Some common predefined syslog facilities (see also: man syslog.conf)*

# Syslog

- /etc/syslog.conf - *priority*
  - ✗ Eight *priority* levels are ordered from high to low
  - ✗ Message is logged if its priority is at least as severe as the priority specified in /etc/syslog.conf

| Priority | Description  | Priority    |
|----------|--|-------------|
| emerg    | Emergency / Panic situations                           | 0 = Highest |
| alert    | Urgent situations                                      | 1           |
| crit     | Critical conditions                                    | 2           |
| err      | All other error conditions                             | 3           |
| warning  | Warning messages                                       | 4           |
| notice   | Attention messages – situation needs further diagnosis | 5           |
| info     | Informational messages                                 | 6           |
| debug    | For syslog and other debugging purposes                | 7 = Lowest  |

*The predefined syslog priority levels (see also: man syslog.conf)*

# Syslog

- /etc/syslog.conf - **action**
  - ✗ **syslogd** writes messages to location specified by **action**
  - ✗ Only a single **action** may be specified per line

| Action                 | Description   |
|------------------------|---|
| <i>filename</i>        | Writes message to a file <i>filename</i> on the local machine ( <i>filename</i> must exist and be a full path; <b>syslogd</b> will not create it) |
| @ <i>hostname</i>      | Forwards message to <b>syslogd</b> on <i>hostname</i> (which must be resolvable via /etc/hosts, NIS, DNS, etc.)                                   |
| @ <i>ipaddr</i>        | Forwards message to the host at IP address <i>ipaddr</i>  |
| <i>user1,user2,...</i> | Writes message on listed users' TTY(s) if logged in   |
| <i>fifo</i>            | Writes message to a FIFO (a named pipe)   |
| *                      | Writes message to all logged in users   |

*Choices of syslog actions*

# Syslog

## □ Example /etc/syslog.conf

```
# Selector                                Action
#
# Only kernel messages to the console; avoids clutter
kern.*                                    /dev/console

# Log anything (except mail) of level info or higher
# Don't log private authentication messages!
*.info;mail.none;authpriv.none          /var/log/messages

# The authpriv file has restricted access
authpriv.*                                /var/log/secure
mail.*                                    /var/log/maillog
cron.*                                    /var/log/cron
# uucp & news errors of level crit and higher
uucp,news.crit                            /var/log/spooler

# lpr messages < err go to user's tty; >= err go to admin's TTY
lpr.!err                                  /dev/tty
lpr.err                                    admin

# Everybody gets emergency messages, plus log them on another host
*.emerg                                    *
*.emerg                                    @logger-host
```

# Syslog

## □ Example Syslog Messages

```
Nov 15 03:39:15 caplap su(pam_unix)[1606]: authentication failure;  
logname=cappella uid=500 euid=0 tty= ruser=cappella rhost= user=root  
Nov 15 03:40:27 caplap gnome-name-server[1746]: starting  
Nov 15 03:41:36 caplap su(pam_unix)[1607]: session closed for user root  
Nov 15 03:51:05 caplap -- cappella[1111]: LOGIN ON tty3 BY cappella  
Nov 15 05:30:38 caplap login(pam_unix)[1811]: session closed for user cappella  
Nov 15 05:30:39 caplap Font Server[1069]: terminating  
Nov 15 05:30:53 caplap xinetd[832]: Exiting...  
Nov 15 05:30:53 caplap automount[752]: shutting down, path = /net  
Nov 15 05:30:55 caplap rpc.statd[585]: Caught signal 15, un-registering and  
exiting.
```



# Syslog

- Strategies and Considerations
  - ✗ Message quantity
    - ✗ Determined by configuration in `/etc/syslog.conf`
    - ✗ Determines number of log files and message destination
  - ✗ Centralized network logging
    - ✗ Required for log manageability
    - ✗ Added protection against hacks to local log files
    - ✗ Logging host should be stable, secure system
  - ✗ Security
    - ✗ Log files can be hacked
    - ✗ Anyone can use syslog facility to fake messages
    - ✗ Messages are not guaranteed to be sent (via UDP)
    - ✗ Firewalls should not allow incoming syslog messages