

# 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

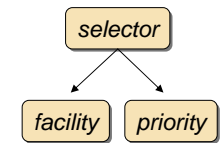
- ✗ Programmers write programs to log messages via **syslog**
  - ✗ The syslog programmers functions write messages to **/dev/log**
  - ✗ Programmer chooses the severity level of messages
- ✗ Syslog daemon
  - ✗ Consults the configuration file **/etc/syslog.conf**
  - ✗ Reads messages from **/dev/log**
  - ✗ 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

## □ 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