System Configurations

@qazwsxedcrfvtg14

Outline

- Basic Information
- System Administration
- Network Configuration
- System Logs
- System Debug

Outline

- Basic Information
- System Administration
- Network Configuration
- System Logs
- System Debug

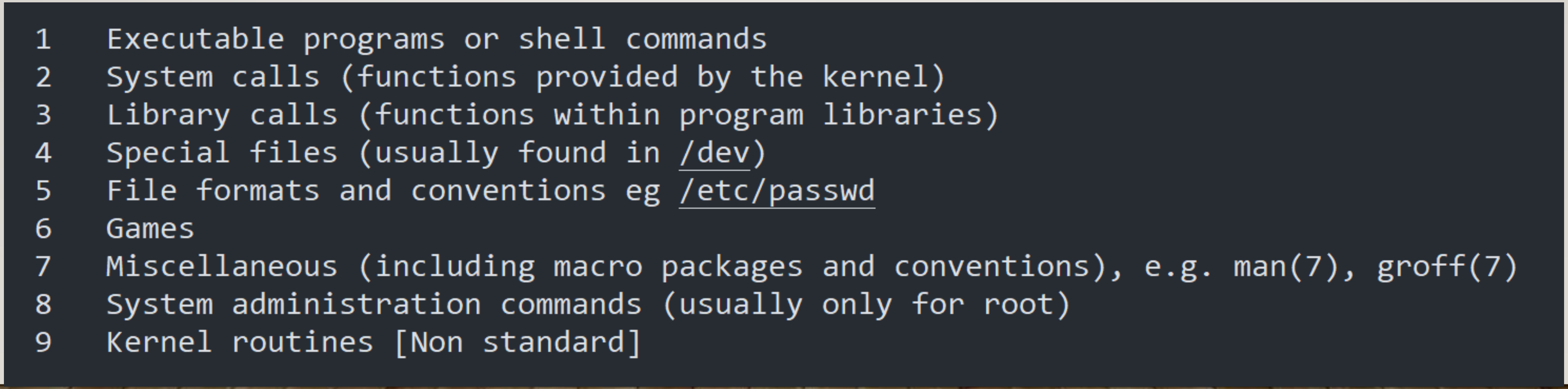
man

- Manuals
- Read manuals

```
$ man [section] page

$ man man

$ man 7 hier

$ man passwd

$ man 5 passwd
```

man

- Sections
  - `man man`



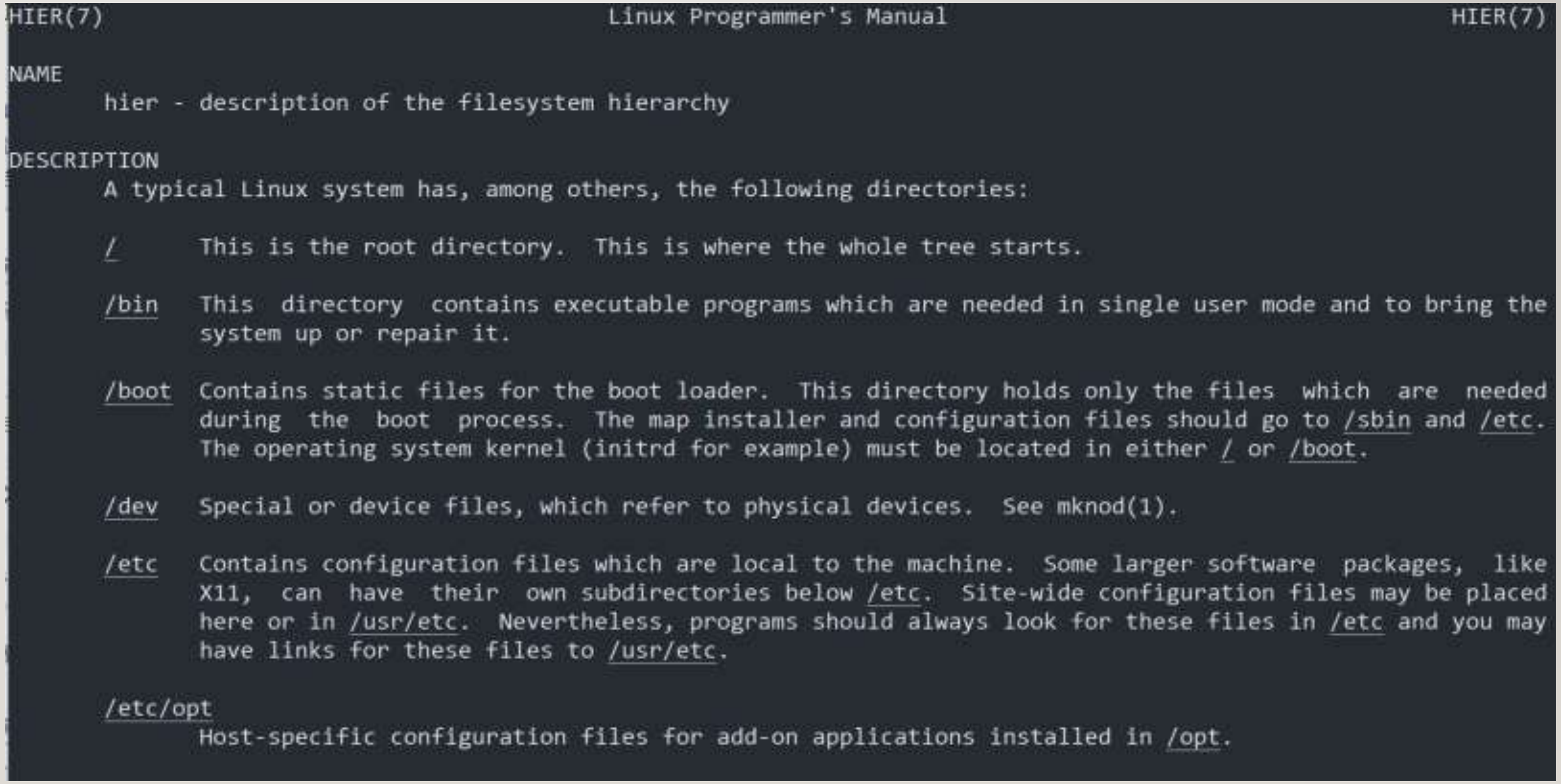
```
1   Executable programs or shell commands
2   System calls (functions provided by the kernel)
3   Library calls (functions within program libraries)
4   Special files (usually found in /dev)
5   File formats and conventions eg /etc/passwd
6   Games
7   Miscellaneous (including macro packages and conventions), e.g. man(7), groff(7)
8   System administration commands (usually only for root)
9   Kernel routines [Non standard]
```

FHS - Filesystem Hierarchy Standard

- Defines directory structures for UNIX-like operating systems
- Maintained by Linux Foundation
- May be slightly different on different distributions

FHS

- man hier
- man 7 hier
- Official Page



```
HIER(7)                         Linux Programmer's Manual                         HIER(7)

NAME
       hier - description of the filesystem hierarchy

DESCRIPTION
       A typical Linux system has, among others, the following directories:

       /      This is the root directory.  This is where the whole tree starts.

       /bin   This  directory  contains executable programs which are needed in single user mode and to bring the
              system up or repair it.

       /boot  Contains static files for the boot loader.  This directory holds only the files  which  are  needed
              during  the  boot  process.  The map installer and configuration files should go to /sbin and /etc.
              The operating system kernel (initrd for example) must be located in either / or /boot.

       /dev   Special or device files, which refer to physical devices.  See mknod(1).

       /etc   Contains configuration files which are local to the machine.  Some larger software  packages,  like
              X11,  can  have  their  own subdirectories below /etc.  Site-wide configuration files may be placed
              here or in /usr/etc.  Nevertheless, programs should always look for these files in /etc and you may
              have links for these files to /usr/etc.

       /etc/opt
              Host-specific configuration files for add-on applications installed in /opt.
```

Directory Structure

Directory Structure	
/	Root directory, the whole tree starts.
/bin	Essential binaries bringing the system up
/boot	Static files for the boot loader
/dev	Devices
/etc	Configuration files
/home	Home directories for users
/lib	Shared libraries, kernel modules

Directory Structure

Directory Structure	
/mnt	Temporary mount points for mounting storage devices
/proc	Information about system
/root	Home directory for root
/sbin	Essential system binaries
/srv	Site-specific data
/tmp	Temp files
/usr	Read-only user data, see second hierarchy

Directory Structure

Directory Structure	
/var	Variable files, or another aspect, log files
/var/cache	Application cache data
/var/lib	Variable state information(e.g. database)
/var/local	Variable data for /usr/local
/var/lock	Lock files
/var/log	Log files
/var/tmp	Temp files preserved between reboots

FHS - Filesystem Hierarchy Standard

- Sometimes, the “meaning” of these directories are vague:
  - They varies between different distributions
  - The location of some files are unexpected
- Use `which` command is a convenient way for you to locate the files
- Use `find` command is also a good choice!

Outline

- Basic Information
- System Administration
- Network Configuration
- System Logs
- System Debug

New machine

- When you log in to a new machine, or maybe a corrupted one, here is a great command for you to figure out the situation and get some basic information.
- You may read this short article.

Configuration Files

- Host-specific configuration files are usually stored in `/etc`.
- Larger software packages may store configuration files in their own subdirectories in `/etc`.

Configuration Files

- /etc/passwd: the password file
  - One line for each user account
  - Seven fields, delimited by ":"
  - [login_name]:[password]:[UID]:[GID]:[username/comment]:[user's homedir]:[user command interpreter (shell)]
- Wait … where is the password?

/etc/shadow – shadowed password file

- nine fields
- login name
- encrypted passwords
- date of last password change
- minimum password age
- maximum password age
- password warning period
- password inactivity period
- account expiration date
- reserved field

Configuration Files

- Why shadow?
  - `-rw-r--r-- 1 root root 2.6K 12月 16 02:47 /etc/passwd`
  - `-rw-r----- 1 root shadow 1.7K 12月 16 03:09 /etc/shadow`
- A funny article

Configuration Files

- `/etc/group`: The user group file
  - group name
  - password
  - GID
  - user list

Configuration Files

- `getent passwd [username]`
- `getent group [username]`

Configuration Files

- /sbin/sysctl - configure kernel parameters at runtime
  - `$ sysctl -a   # list all variables`
  - `$ sysctl [variable]   # read some variable`
  - `$ sysctl -w [variable[=value]] [...]   # write some variable`

Configuration Files

- `sudo` - Execute a command as another user
- Policy configured via `visudo` and stored in `/etc/sudoers`

Systemd

- Systemd - a system and service manager for Linux operating systems
- The main command to control systemd is systemctl

```
systemctl status      # Show system status
systemctl             # Show all running units
systemctl --failed    # List failed units
systemctl start xxx   # Start a unit
systemctl stop xxx    # Stop a unit
systemctl restart xxx # Restart a unit
systemctl reload xxx  # Ask a unit to reload config file(s)
systemctl status xxx  # Show the status of a unit
```

Systemd

- Why Arch moved to systemd?

Outline

- Basic Information
- System Administration
- Network Configuration
- System Log
- System Debug

Network Configuration

- `/etc/hostname:` Local hostname configuration file
  - Set during boot; stored in kernel
  - Change it during runtime: hostnamectl
- `/etc/hosts`: Static table lookup for hostnames
  - IP_address canonical_hostname [aliases ...]
  - Useful when DNS isn't running, e.g. during system bootup
- `/etc/resolv.conf`: Resolver configuration file
  - Configuration for DNS, a trusted source of DNS information

Network Configuration

- Network interfaces … ?
  - Varies significantly between different distributions
  - Debian, Ubuntu: `/etc/network/interfaces`
  - CentOS: `/etc/sysconfig/network-scripts/ifcfg-<interface-name>`
  - ArchLinux (our workstations): /etc/systemd/network/*
  - FreeBSD (our workstation, too): /etc/rc.conf

Outline

- Basic Information
- System Administration
- Network Configuration
- System Log
- System Debug

System Log

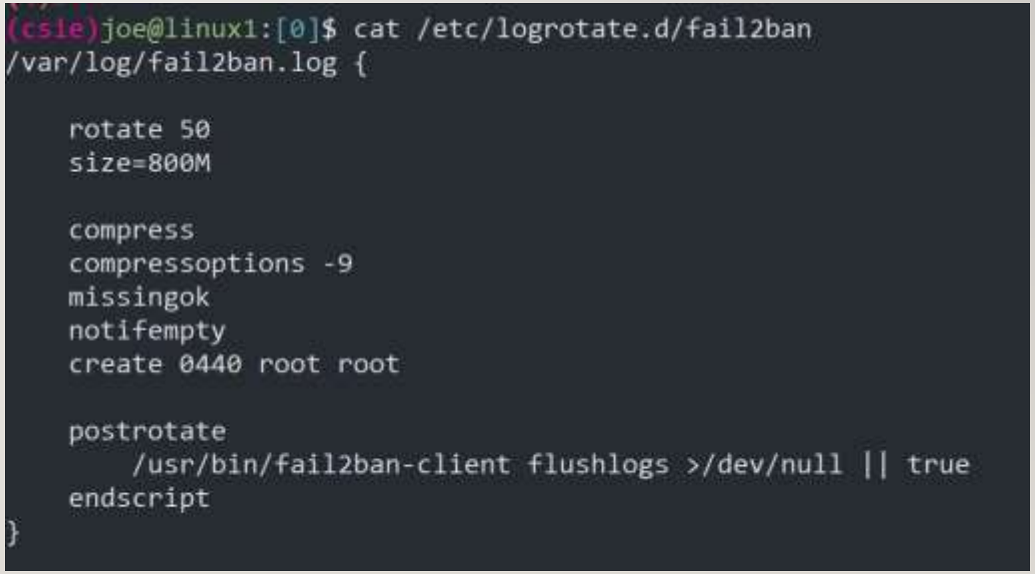
- `/var/log` is the most possible location for logs you need
- System logs: `dmesg, lastlog, wtmp, faillog`, etc.
- Still other possible location and format for different logs, so that you may not find all the logs easily.

System Log

- `systemd-journald`: Powerful new-era system logging tool
  - A system service collecting and storing logging data
  - The collected log are stored in `/var/log/journal`
  - You can’t read these files directly, but use the command `journalctl`
  - `May 20 01:43:43 linux1 sshd[17637]: Accepted publickey for joe from 127.0.0.0 port 56892 ssh2: RSA SHA256:____`

System Log

- `logrotate`: rotates, compresses, and mails system logs
- Backup the logs for you to trace the activities before (if you need to)
- Reduce disk usage by compressing the log into archive
- Delete useless logs (often too old) by implementing log rotation



```
(csie)joe@linux1:[0]$ cat /etc/logrotate.d/fail2ban
/var/log/fail2ban.log {

    rotate 50
    size=800M

    compress
    compressoptions -9
    missingok
    notifempty
    create 0440 root root

    postrotate
        /usr/bin/fail2ban-client flushlogs >/dev/null || true
    endscript
}
```

Outline

- Basic Information
- System Administration
- Network Configuration
- System Log
- System Debug

System Debug

- file
- gdb
- ldd
- ps
- lsof
- strace
- …

It’s your time!

- https://www.csie.ntu.edu.tw/~joe/lab9/main
- https://www.csie.ntu.edu.tw/~joe/lab9/main2
- Try to find what did this program do
- Hint:
  - input is a string
  - `strace -f`
  - `system call: exec*, open*, read, write`
  - `ignore open so file.`