

# Linux System Administration

---

Arnon Rungsawang

*fenganr@ku.ac.th*

**M**assive **I**nformation & **K**nowledge **E**ngineering

Department of Computer Engineering

Faculty of Engineering

Kasetsart University, Bangkok, Thailand.

# Outline

---

- Monitor the system
- Process management
- Filesystems and storage devices
- User info
- Creating a new system user account
- Operating as root
- RPM: adding, updating software
- CRON: Scheduling a task
- System log files
- FIND: using the find command
- Finding files in the system
- Managing time
- Simple mail reader
- Text terminal configuration
- System hardware information
- PERL administration/maintenance

# Monitoring the system (1)

## ■ Basic command line:

<code>ps tree</code>	Process and parent-child relationships.
<code>ps -aux</code>	Process status.
<code>top</code>	Show top process.
<code>vmstat</code>	Monitor virtual memory.
<code>free</code>	Display amount of free and used memory in the file system. Also “ <code>cat /proc/meminfo</code> ”.
<code>cat /proc/sys/vm /freepages</code>	Display virtual memory “free pages”.
<code>cat /proc /filesystems</code>	Display file systems currently in use.

# Monitoring the system

## pstree

```
[arnon@godzilla tmp]$ pstree
init-+-apmd
  |-atd
  |-automount
  |-cron
  |-identd---identd---3*[identd]
  |-inetd-+-2*[in.telnetd---login---bash---vim]
    |-in.telnetd---login---bash---pstree
    |-in.telnetd---login---bash-+-bnr2---bnr2---12*[bnr2]
      |-3*[hp---2*[hp]]
      \-hp
    \-in.telnetd---login---bash
  |-kflushd
  |-klogd
  |-kpiod
  |-kswapd
  |-kupdate
  |-lockd---rpciod
  |-mdrecoveryd
  |-6*[mingetty]
  |-8*[nfsd]
  |-portmap
  \-rpc.mountd
```

# Monitoring the system

## ps aux

```
[arnon@godzilla tmp]$ ps aux
```

USER	PID	%CPU	%MEM	VSZ	RSS	TTY	STAT	START	TIME	COMMAND
root	1	0.0	0.0	1120	68	?	S	Feb19	0:04	init [3]
root	2	0.0	0.0	0	0	?	SW	Feb19	0:00	[kflushd]
root	3	0.0	0.0	0	0	?	SW	Feb19	0:00	[kupdate]
root	4	0.0	0.0	0	0	?	SW	Feb19	0:00	[kpiod]
root	5	0.0	0.0	0	0	?	SW	Feb19	0:01	[kswapd]
root	6	0.0	0.0	0	0	?	SW<	Feb19	0:00	[mdrecoveryd]
bin	332	0.0	0.0	1212	216	?	S	Feb19	0:00	portmap
root	346	0.0	0.0	0	0	?	SW	Feb19	0:00	[lockd]
root	347	0.0	0.0	0	0	?	SW	Feb19	3:06	[rpciod]
root	356	0.0	0.0	1156	0	?	SW	Feb19	0:00	[rpc.statd]
root	370	0.0	0.0	1104	0	?	SW	Feb19	0:00	[apmd]
root	385	0.0	0.0	1268	0	?	SW	Feb19	0:00	[ypbind]
root	391	0.0	0.0	1288	120	?	S	Feb19	0:00	[ypbind]
root	420	0.0	0.0	1208	44	?	S	Feb19	0:00	/usr/sbin/automou
root	472	0.0	0.0	1172	164	?	S	Feb19	0:00	syslogd -m 0
root	481	0.0	0.0	1412	168	?	S	Feb19	0:00	klogd
nobody	495	0.0	0.0	1292	320	?	S	Feb19	0:00	identd -e -o
nobody	498	0.0	0.0	1292	320	?	S	Feb19	0:00	identd -e -o
nobody	499	0.0	0.0	1292	320	?	S	Feb19	0:00	identd -e -o
nobody	501	0.0	0.0	1292	320	?	S	Feb19	0:00	identd -e -o

# Monitoring the system

## top

```
[arnon@godzilla tmp]$ top
```

```
7:21pm up 10 days, 18:37, 5 users, load average: 0.31, 0.32, 0.17
```

```
85 processes: 82 sleeping, 3 running, 0 zombie, 0 stopped
```

```
CPU states: 2.6% user, 4.3% system, 0.0% nice, 0.7% idle
```

```
Mem: 517256K av, 514192K used, 3064K free, 21432K shrd, 10616K buff
```

```
Swap: 136512K av, 4404K used, 132108K free 452124K cached
```

PID	USER	PRI	NI	SIZE	RSS	SHARE	STAT	LIB	%CPU	%MEM	TIME	COMMAND
664	arnon	13	0	376	360	304	S	0	4.5	0.0	0:30	hp
698	arnon	16	0	1004	1004	764	R	0	3.6	0.1	0:00	top
1	root	0	0	120	68	52	S	0	0.0	0.0	0:04	init
2	root	0	0	0	0	0	SW	0	0.0	0.0	0:00	kflushd
3	root	0	0	0	0	0	SW	0	0.0	0.0	0:00	kupdate
4	root	0	0	0	0	0	SW	0	0.0	0.0	0:00	kpiod
5	root	0	0	0	0	0	SW	0	0.0	0.0	0:01	kswapd
6	root	-20	-20	0	0	0	SW<	0	0.0	0.0	0:00	mdrecoveryd
332	bin	0	0	248	216	176	S	0	0.0	0.0	0:00	portmap
346	root	0	0	0	0	0	SW	0	0.0	0.0	0:00	lockd
347	root	0	0	0	0	0	SW	0	0.0	0.0	3:07	rpciod
356	root	0	0	88	0	0	SW	0	0.0	0.0	0:00	rpc.statd
370	root	0	0	64	0	0	SW	0	0.0	0.0	0:00	apmd
385	root	0	0	84	0	0	SW	0	0.0	0.0	0:00	ypbind
391	root	0	0	176	116	100	S	0	0.0	0.0	0:00	ypbind

# Monitoring the system

## vmstat, free, freepage, filesystem

```
[arnon@godzilla tmp]$ vmstat
```

```
procs          memory  swap          io  system          cpu
 r  b  w  swpd  free  buff  cache  si  so  bi  bo  in  cs  us  sy  id
 2  0  0  4404 3056 10484 452020  0  0  1  0  0  2  3  4  1
```

```
[arnon@godzilla tmp]$ free
```

```
total      used      free      shared  buffers  cached
Mem:      517256  514600    2656     21032   10488   452324
-/+ buffers/cache: 51788  465468
Swap:    136512  4404     132108
```

```
[arnon@godzilla tmp]$ cat /proc/sys/vm/freepages
```

```
256  512  768
```

```
[arnon@godzilla tmp]$ cat /proc/filesystems
```

```
ext2
nodev  proc
nodev  nfs
nodev  smbfs
      iso9660
nodev  autofs
nodev  devpts
```

```
[arnon@godzilla tmp]$
```

# Monitoring the system (2)

---

## ■ Basic command line:

<code>uname -a</code>	Print system information.
<code>uptime</code>	Tell how long the system has been running. Also number of users and system's load average.
<code>w</code>	Show who is logged on and what they are doing.
<code>/sbin/lsmmod</code>	List all currently loaded kernel modules.
<code>/sbin/runlevel</code>	Display the system's currently runlevel.
<code>hostname</code>	Display the system's name.

# Monitoring the system

## uname, uptime, w, ...

```
[arnon@godzilla tmp]$ uname -a
Linux godzilla.cpe.ku.ac.th 2.2.14-5.0 #2 Fri Oct 26 04:13:33 ICT 2001 i686 unknown
[arnon@godzilla tmp]$ uptime
 7:43pm up 10 days, 19:00,  5 users,  load average: 0.15, 0.12, 0.09
[arnon@godzilla tmp]$ w
 7:43pm up 10 days, 19:00,  5 users,  load average: 0.14, 0.12, 0.09
USER      TTY      FROM          LOGIN@  IDLE   JCPU   PCPU   WHAT
arnon     pts/0    louis         Tue10am 0.00s  1.08s  0.02s  w
arnon     pts/1    louis         Wed 3pm 4:36   1:18   0.54s  -bash
search    pts/2    mammoth       Mon 3pm 30:45  0.44s  0.31s  vim .././inclu
search    pts/3    mammoth       23Feb 2 5:43   3.64s  3.42s  vim service.cpp
b41tas    pts/4    jin           5:41pm 1:07m  0.10s  0.06s  -bash
[arnon@godzilla tmp]$ /sbin/lsmmod
Module          Size Used by
[arnon@godzilla tmp]$ /sbin/runlevel
N 3
[arnon@godzilla tmp]$ hostname
godzilla.cpe.ku.ac.th
[arnon@godzilla tmp]$
```

# Process management

---

- Identify the process
  - `pstree -p`
  - `ps -auxw`
  - `top`
- Kill the process
  - `kill <process-id-number>`
    - If hangs give a stronger signal:  
`kill -9 <process-id-number>`
  - `killall <command-name>`
- See all signal: `/usr/include/bits/signum.h`

## pstree, kill, killall

```
[arnon@godzilla tmp]$ pstree -p
init(1)-+-apmd(370)
  |-atd(513)
  |-automount(420)
  |-crond(527)
  |-identd(495)---identd(498)-+-identd(499)
  |                               |-identd(501)
  |                               \-identd(502)
  ...
```

```
[arnon@godzilla tmp]$ kill -9 495
kill: (495) - Not owner
[arnon@godzilla tmp]$ killall identd
identd(495): Operation not permitted
identd(498): Operation not permitted
identd(499): Operation not permitted
identd(501): Operation not permitted
identd(502): Operation not permitted
identd: no process killed
[arnon@godzilla tmp]$
```

# Semaphores

- Some processes may use semaphores (shared memory)
- Identify the semaphores
  - `ipcs -q` list share queues.
  - `ipcs -m` shared memory.
  - `ipcs -s` list semaphores.
- Remove the semaphores
  - `ipcrm -s <ipcs id>`

```
[arnon@godzilla tmp]$ ipcs -m
```

```
----- Shared Memory Segments -----
```

key	shmid	owner	perms	bytes	nattch	status
0x00000000	341504	nobody	600	46084	27	dest

# ulimit

---

- Display the limits of a shell.
- Can be set for the number of open files and processes, memory and virtual memory etc.

```
[arnon@godzilla tmp]$ ulimit -a
core file size (blocks)      1000000
data seg size (kbytes)      unlimited
file size (blocks)          unlimited
max memory size (kbytes)    unlimited
stack size (kbytes)         8192
cpu time (seconds)          unlimited
max user processes          2048
pipe size (512 bytes)       8
open files                   1024
virtual memory (kbytes)     2105343
```

# Filesystems and Storage Devices (1)

## ■ Hard Drive Info

<code>df -k</code>	Report filesystem disk space usages. ( <code>-k</code> report in Kbytes)
<code>du -sh</code>	Calculates file space usage for a given directory. (and everything under it) ( <code>-s</code> option summarizes)
<code>mount</code>	Displays all mounted devices, their mount point, filesystem, and access. Used with command line arguments to mount file system.
<code>cat /proc/swaps</code>	Display swap partition(s) size, type and quantity used.
<code>cat /proc/ide /hda/&lt;anyfile&gt;</code>	Display disk information held by kernel.

# Filesystem and storage devices

## df, mount, /proc/swap, ...

```
[arnon@godzilla tmp]$ df -k
```

Filesystem	1k-blocks	Used	Available	Use%	Mounted on
/dev/hda2	2016044	1704052	209580	89%	/
/dev/hda3	7590060	2610240	4594260	36%	/godzilla01
trex:/trex	38464340	4190860	32319576	11%	/misc/trex

```
[arnon@godzilla tmp]$ du -sh
```

```
286M .
```

```
[arnon@godzilla tmp]$ mount
```

```
/dev/hda2 on / type ext2 (rw,usrquota)
```

```
none on /proc type proc (rw)
```

```
none on /dev/pts type devpts (rw,gid=5,mode=620)
```

```
/dev/hda3 on /godzilla01 type ext2 (rw,nosuid,nodev,usrquota)
```

```
/dev/hdd1 on /godzilla02 type ext2 (rw,nosuid,nodev,usrquota)
```

```
/dev/hdb1 on /godzilla03 type ext2 (rw,nosuid,nodev,usrquota)
```

```
automount(pid420) on /misc type autofs (rw,fd=5,pgrp=420,minproto=2,maxproto=3)
```

```
trex:/trex on /misc/trex type nfs (rw,addr=192.168.33.115)
```

```
[arnon@godzilla tmp]$ cat /proc/swap
```

Filename	Type	Size	Used	Priority
/dev/hda1	partition	136512	3716	-1

```
[arnon@godzilla tmp]$ cat /proc/ide/hda/model
```

```
WDC AC310100B
```

```
[arnon@godzilla tmp]$ cat /proc/ide/hda/capacity
```

```
19807200
```

# Filesystems and Storage Devices (2)

---

- Add an extra hard drive.
  - Enter the drive into the partition table
    - **fdisk /dev/<drive>**
  - Create file system
    - **mkfs -t ext2 /dev/<drive>**
  - Mount the drive
    - **mount -t ext2 /dev/<drive's device name> /<home2 or some suitable directory>**

# Linux IDE naming conventions

Device	Description	Configuration
/dev/hda	1 <sup>st</sup> (Primary) IDE controller	Master
/dev/hdb	1 <sup>st</sup> (Primary) IDE controller	Slave
/dev/hdc	2 <sup>nd</sup> (Secondary) IDE controller	Master
/dev/hdd	2 <sup>nd</sup> (Secondary) IDE controller	Slave

Note: SCSI disks are label /dev/sda, sdb, etc ...

- See full list of disks and partition
  - **cat /proc/partitions**
- See linux devices
  - Kernel 2.4 (RedHat 7.1+)
    - **cat /usr/src/linux-2.4/Documentation/devices.txt**
  - Kernel 2.2 (RedHat 7.0-)
    - **cat /usr/src/linux/Documentation/devices.txt**

# /etc/fstab file

- To make the drive a permanent member of system and mount upon system boot.

- Example: /etc/fstab file

/dev/sdb6	/	ext2	defaults	1 1
/dev/sdb1	/boot	ext2	defaults	1 2
/dev/cdrom	/mnt/cdrom	iso9660	noauto,user,users,ro	0 0
/dev/fd0	/mnt/floppy	auto	noauto,owner	0 0
none	/proc	proc	defaults	0 0
none	/dev/pts	devpts	gid=5,mode=620	0 0
/dev/sdb5	swap	swap	defaults	0 0
/dev/sdc1	/home2	ext2	defaults	1 2

- Check file system created

- **fsck /dev/<drive's device name>**

# Mounting other file systems (1)

---

- CD-ROM
  - Mount
    - **mount -t iso9660 /dev/cdrom /mnt/cdrom**
  - Un-mount
    - **umount /dev/cdrom**
- Floppy disk
  - Mount
    - **mount /dev/fd0 /mnt/floppy**
  - Un-mount
    - **umount /dev/fd0**
- Ramdisk
  - Mount
    - **mount /dev/ram /mnt/ramd**
  - Un-mount
    - **umount /dev/ram**

# Mounting other file systems (2)

---

- Windows partition
  - Mount
    - **mount /dev/<drive's device name> /mnt/win**
  - Un-mount
    - **umount /mnt/win**

# Increase open files limit

---

- Kernel configuration for max number of files.
  - **cat /proc/sys/fs/file-max**
- Number of files presently open.
  - **cat /proc/sys/fs/file-nr**
- Set max file limit
  - **echo <size> > /proc/sys/fs/file-max**
- Kernel 2.2 configuration for max number of inodes.
  - **cat /proc/sys/fs/inodes-max**
- To change max number of inodes.
  - **echo <size> > /proc/sys/fs/inode-max**

# System crash and disk check upon boot (1)

---

- The system will check if the disk was unmounted cleanly.
- See the following message

```
Unexpected inconsistency; Run fsck Manually
...
***An error occurred during the file system check.
***Dropping you to a shell; the system will reboot
...
.
Give root password for maintenance
(or type Control-D for normal startup):
```

# System crash and disk check upon boot (2)

---

- Enter the root password and run fsck

```
(repair file system)1# fsck -A -y
...
..
.
*****FILE SYSTEM WAS MODIFIED*****
...
..
.
(repair file system)2# exit
```

# Journalled Filesystem EXT3

---

- Convert from ext2 to ext3
  - **Tune2fs -j /dev/<drive's device name>**
- Configuration file in “/etc/fstab” changes from ext2 to ext3

# User info (1)

---

## ■ commands

who	Display currently logged in users. Use “ <code>who -uH</code> ” for idle time and terminal info.
users	Show all users logged in.
w	Display currently logged in users and processes they are running.
whoami	Display user id.
groups	Display groups you are part of. Use “ <code>groups user-id</code> ” to display groups for given user.
set	Display all environment variables in your current environment.

# who, users, w, whoami, groups, ...

```
[arnon@godzilla arnon]$ who
arnon pts/0 Feb 26 10:06
arnon pts/1 Feb 27 15:01
search pts/2 Feb 25 15:35
search pts/3 Mar 1 20:13
[arnon@godzilla arnon]$ users
arnon arnon search search
[arnon@godzilla arnon]$ w
 8:59pm up 10 days, 20:16, 4 users, load average: 0.15, 0.15, 0.17
USER  TTY  FROM          LOGIN@  IDLE  JCPU  PCPU  WHAT
arnon pts/0 louis          Tue10am 2:46 14.39s 1.08s -bash
arnon pts/1 louis          Wed 3pm 0:00s 31.40s 0.03s w
search pts/2 mammoth       Mon 3pm 5:00 0.17s 0.10s -bash
search pts/3 mammoth       8:13pm 6:48 1.00s 0.88s vim service.cpp
[arnon@godzilla arnon]$ whoami
arnon
[arnon@godzilla arnon]$ groups
teacher
[arnon@godzilla arnon]$ set
BASH=/bin/bash
BASH_ENV=/trex/home/teacher/arnon/.bashrc
BASH_VERSION=1.14.7(1)
...
```

# User info (2)

---

## ■ commands

id	Display user and all group ids. Use “ <i>id user-id</i> ” to display info for another user id.
last	Show listing of last logged in users.
history	Shell command to display previously entered commands.

# id, last, history

```
[arnon@godzilla arnon]$ id
uid=5001(arnon) gid=500(teacher) groups=500(teacher)
[arnon@godzilla arnon]$ last
search pts/3 mammoth Fri Mar 1 20:13 still logged in
b41tas ftpd686 jin.cpe.ku.ac.th Fri Mar 1 19:13 - 19:34 (00:20)
b41tas ftpd628 jin.cpe.ku.ac.th Fri Mar 1 18:30 - 18:45 (00:15)
b41tas ftpd616 jin.cpe.ku.ac.th Fri Mar 1 18:25 - 18:28 (00:03)
b41tas ftpd593 jin.cpe.ku.ac.th Fri Mar 1 17:49 - 18:13 (00:23)
b41tas ftpd586 jin.cpe.ku.ac.th Fri Mar 1 17:47 - 17:56 (00:08)
b41tas pts/4 jin Fri Mar 1 17:41 - 20:15 (02:33)
b41tas pts/4 jin Fri Mar 1 11:18 - 13:01 (01:42)
```

```
wtmp begins Fri Mar 1 08:34:04 2002
```

```
[arnon@godzilla arnon]$ history
```

```
1208 cd
1209 who
1210 users
1211 w
1212 whoami
1213 groups
1214 su -
```

```
...
```

# Create a new system user account (1)

---

- Command line method
  - Add a user to the system.
    - **useradd**
  - Will grant the user read/write privileges to the floppy (/dev/fd0) upon creation of user by adding user to group floppy.
    - **useradd -G floppy**
  - Delete user from system. Purges user from /etc/password, group and shadow files.
    - **userdel**
  - Delete user and remove his home directory from the system. Other file will remain.
    - **userdel -r**
  - Assign a password to the user.
    - **passwd**

# Create a new system user account

## Command line method

```
[root@godzilla /root]# useradd
usage: useradd [-u uid [-o]] [-g group] [-G group,...]
             [-d home] [-s shell] [-c comment] [-m [-k template]]
             [-f inactive] [-e expire ] [-p passwd] [-n] [-r] name
useradd -D [-g group] [-b base] [-s shell]
             [-f inactive] [-e expire ]
[root@godzilla /root]# useradd -u 1234 -g 100 -d /home/toto toto
[root@godzilla /root]# passwd toto
Changing password for user toto
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully
[root@godzilla /root]# groups toto
toto : users
[root@godzilla /root]# usermod -G wheel toto
[root@godzilla /root]# groups toto
toto : users wheel
[root@godzilla /root]# userdel -r toto
[root@godzilla /root]#
```

# Create a new system user account (2)

## ■ File Editing Method

- Create user entry in `/etc/passwd`.

- `<user>:x:<uid>:<gid>:<name>:<directory home>:/bin/bash`

- Create group in `/etc/group`.

- `<group>:x:<gid>`

```
[arnon@godzilla arnon]$ head /etc/passwd
```

```
root:x:0:0:root:/root:/bin/bash
```

```
bin:x:1:1:bin:/bin:
```

```
daemon:x:2:2:daemon:/sbin:
```

```
...
```

```
[arnon@godzilla arnon]$ head /etc/group
```

```
root:x:0:root
```

```
bin:x:1:root,bin,daemon
```

```
daemon:x:2:root,bin,daemon
```

# Create a new system user account (3)

---

- Create home directory.
  - **mkdir <directory home>**
- Copy default files.
  - **cp -pR /etc/skel/. <directory home>**
  - **chown -R <user>.<group> <directory home>**
- Use the commands “pwconv” and “grpconv” to synchronize the shadow files.
- Assign a passwd
  - **passwd <user>**

# Operating as root (System Administrator)

---

- Shell/command mode
  - Switch user account to root.
    - **su -**  
Then enter the root password.
- GUI mode
  - Allow console to be accessed by another user from the same system.
    - **xhost +localhost**
  - Switch user account to root.
    - **su -**  
then enter the root password.
  - Set environment variable for GUI sessions.
    - **export DISPLAY=:0.0**
  - Launch GUI application.
    - **xinit**

# RPM - RedHat Package Manager (1)

- The rpm command is used to manage software application and system modules.

RPM Command	Description
rpm -qilp <i>program_package-ver.rpm</i>	Query for information on package and list destination of files to be installed by the package.
rpm -Uvh <i>program_package-ver.rpm</i>	Upgrade the system with the RPM package.
rpm -ivh <i>program_package-ver.rpm</i>	New install.
rpm -Fvh <i>program_package-ver.rpm</i>	Freshen install. Remove all files of older version.

# RPM - RedHat Package Manager (2)

---

RPM Command	Description
<code>rpm -q <i>program_package</i></code>	Query system RPM database (/var/lib/rpm), to see if package is installed.
<code>rpm -qi <i>program_package</i></code>	Query system RPM database for info/description on package (if installed).
<code>rpm -ql <i>program_package</i></code>	List all files on the system associated with the package.
<code>rpm -qf <i>file</i></code>	Identify the package to which this file belong.

# RPM - RedHat Package Manager (3)

---

RPM Command	Description
<code>rpm -e <i>program_package</i></code>	Uninstall package from your system.
<code>rpm -qa</code>	List all packages on your system. Use this with grep to find families of packages.
<code>rpm -K --nogpg *.rpm</code>	Non sure if RPM downloaded ok? Verify md5 sum.

# RPM - RedHat Package Manager (4)

RPM Flag	Description
--nodeps	RPM flag to force install even if dependency requirement are not met.
--force	Overwrite of other packages allowed.
--notriggers	Don't execute script which are triggered by the installation of this package.
--root <i>/directory-name</i>	Use the system chrooted at <i>/directory-name</i> . This means the database will be read or modified under <i>/directory-name</i> . (Used by developers to maintain multiple environments)
--ignorearch	Allow installation even if the architectures of the binary RPM and host don't match. This is often required for RPM's which were assembled incorrectly.

# CRON - Scheduling a task

---

- Add shell script to have run hourly, daily, weekly or monthly into the appropriate directory.
  - /etc/cron.hourly/
  - /etc/cron.daily/
  - /etc/cron.weekly/
  - /etc/cron.monthly/

```
[root@godzilla cron.daily]# cat inn-cron-expire  
#!/bin/sh  
/sbin/chkconfig innd && su - news -c "/usr/bin/news.daily delayrm"  
[root@godzilla cron.daily]#
```

# System log files (1)

---

- System messages.
  - /var/log/messages
- Logging by PAM of network access attempts.
  - /var/log/secure
- Log of system boot.
  - /var/log/dmesg
  - Also see command “*dmesg*”.
- Log of system init process.
  - /var/log/boot.log
- File transfer log
  - /var/log/xferlog.1

## /var/log/messages

```
[root@godzilla log]# less /var/log/messages
```

```
...  
Mar  1 21:14:14 godzilla PAM_pwdb[1731]: (su) session opened for user root by  
arnon(uid=5001)  
Mar  1 21:14:55 godzilla PAM_pwdb[1731]: (su) session closed for user root  
Mar  1 21:15:09 godzilla PAM_pwdb[1759]: (su) session opened for user root by  
arnon(uid=5001)  
Mar  1 21:15:32 godzilla useradd[1785]: new user: name=toto, uid=1234, gid=100,  
home=/home/toto, shell=/bin/bash  
Mar  1 21:15:55 godzilla PAM_pwdb[1786]: password for (toto/1234) changed by  
(arnon/0)  
Mar  1 21:16:17 godzilla usermod[1790]: add `toto' to group `wheel'  
Mar  1 21:16:17 godzilla usermod[1790]: add `toto' to shadow group `wheel'  
Mar  1 21:19:16 godzilla userdel[1794]: delete user `toto'  
Mar  1 21:19:16 godzilla userdel[1794]: delete `toto' from group `wheel'  
Mar  1 21:19:16 godzilla userdel[1794]: delete `toto' from shadow group `wheel'  
Mar  1 21:23:19 godzilla PAM_pwdb[1759]: (su) session closed for user root  
Mar  1 22:01:29 godzilla PAM_pwdb[2126]: (su) session opened for user root by  
arnon(uid=5001)  
...
```

## /var/log/secure

```
[root@godzilla log]# less /var/log/secure
```

```
...  
Feb 27 21:52:40 godzilla login: LOGIN ON 4 BY g43pain FROM lucifer  
Feb 27 22:22:28 godzilla in.telnetd[28478]: connect from 192.168.33.176  
Feb 27 22:22:45 godzilla login: LOGIN ON 5 BY search FROM tweetybird  
Feb 28 00:46:24 godzilla in.telnetd[28668]: connect from 192.168.33.176  
Feb 28 00:46:33 godzilla login: LOGIN ON 4 BY search FROM tweetybird  
Feb 28 18:56:20 godzilla in.telnetd[30592]: connect from 192.168.33.172  
Feb 28 18:56:35 godzilla login: LOGIN ON 6 BY b42bms FROM nautilus  
Mar 1 11:18:08 godzilla in.telnetd[32698]: connect from 192.168.33.178  
Mar 1 11:18:10 godzilla login: LOGIN ON 4 BY b41tas FROM jin  
Mar 1 17:41:39 godzilla in.telnetd[532]: connect from 192.168.33.178  
Mar 1 17:41:41 godzilla login: LOGIN ON 4 BY b41tas FROM jin  
Mar 1 17:47:46 godzilla in.ftpd[586]: connect from 192.168.33.178  
Mar 1 17:49:25 godzilla in.ftpd[593]: connect from 192.168.33.178  
Mar 1 18:25:05 godzilla in.ftpd[616]: connect from 192.168.33.178  
Mar 1 18:30:25 godzilla in.ftpd[628]: connect from 192.168.33.178  
Mar 1 19:13:17 godzilla in.ftpd[686]: connect from 192.168.33.178  
Mar 1 20:13:56 godzilla in.telnetd[873]: connect from 192.168.33.118  
Mar 1 20:13:59 godzilla login: LOGIN ON 3 BY search FROM mammoth  
...
```

## /var/log/dmesg

```
[root@godzilla log]# less /var/log/dmesg
Linux version 2.2.14-5.0 (root@godzilla.cpe.ku.ac.th) (gcc version egcs-2.91.66
19990314/Linux (egcs-1.1.2 release)) #2 Fri Oct 26 04:13:33 ICT 2001
Detected 503549883 Hz processor.
Console: colour VGA+ 80x25
Calibrating delay loop... 501.35 BogoMIPS
Memory: 517212k/524224k available (1008k kernel code, 416k reserved, 5544k data,
 44k init, 0k bigmem)
Dentry hash table entries: 262144 (order 9, 2048k)
Buffer cache hash table entries: 524288 (order 9, 2048k)
Page cache hash table entries: 131072 (order 7, 512k)
VFS: Diskquotas version dquot_6.4.0 initialized
L1 I Cache: 64K L1 D Cache: 64K
L2 Cache: 512K
CPU: AMD AMD-K7(tm) Processor stepping 02
Checking 386/387 coupling... OK, FPU using exception 16 error reporting.
Checking 'hlt' instruction... OK.
POSIX conformance testing by UNIFIX
PCI: PCI BIOS revision 2.10 entry at 0xfd9e1
PCI: Using configuration type 1
PCI: Probing PCI hardware
PCI: Enabling I/O for device 00:00
```

## /var/log/xferlog

```
[root@godzilla log]# less /var/log/xferlog
```

```
Fri Mar 1 17:56:02 2002 464 jin.cpe.ku.ac.th 651960320 /godzilla02/video/disc01
```

```
.DAT b_o r b41tas ftp 0 * i
```

```
Fri Mar 1 17:58:21 2002 57 jin.cpe.ku.ac.th 86489388 /godzilla02/video/disc01.D
```

```
AT b_o r b41tas ftp 0 * c
```

```
Fri Mar 1 18:30:58 2002 1 jin.cpe.ku.ac.th 1570 /misc/trex/home/bstudent/b41/b4
```

```
1tas/project/serior/ESHEEP/src/include/user.h b_o r b41tas ftp 0 * c
```

```
Fri Mar 1 19:19:01 2002 329 jin.cpe.ku.ac.th 719580332 /godzilla02/video/disc02
```

```
.DAT b_o r b41tas ftp 0 * c
```

```
[root@godzilla /root]# less /var/log/xferlog.2
```

```
Wed Feb 13 02:03:28 2002 1 mammoth.cpe.ku.ac.th 452 /godzilla01/home/project/sea  
rch/WORMS_PROJECT/dworms-0.2/conf/dworms.conf b_o r search ftp 0 * c
```

```
Wed Feb 13 02:04:06 2002 1 mammoth.cpe.ku.ac.th 2486 /godzilla01/home/project/se  
arch/WORMS_PROJECT/WORM-1.0-final/conf/worm.conf b_o r search ftp 0 * c
```

# System log files (2)

- Requires the use of the `lastlog` command to examine contents.
  - `/var/log/lastlog`
  - See command “`lastlog`” for print the last login of system users.
- Log from sendmail daemon.
  - `/var/log/maillog`

```
[root@godzilla log]# lastlog
```

```
...
postgres                **Never logged in**
b41ratc                  4      trex    Fri Dec 21 18:10:32 +0700 2001
b42dan                   3      trex    Sat Jan 26 23:20:35 +0700 2002
usenet                   2      trex    Wed Jan 16 11:29:05 +0700 2002
g41act                   0      trex    Mon Nov 19 11:00:21 +0700 2001
papers                   0      lucifer Wed Jan  2 03:34:09 +0700 2002
search                   3      mammoth Fri Mar  1 20:13:59 +0700 2002
spider                   tty2   Fri Nov 30 13:26:31 +0700 2001
...
```

# Logrotate - Rotate log files (1)

---

- When system and server generate log files, if unchecked they will grow large enough to burden the system and application.
- The *logrotate* program will periodically backup the log file by renaming it.
- Also allow to set the limit for the number of logs or their size.
- The configuration file.
  - /etc/logrotate.conf
- The directory for configuration script.
  - /etc/logrotate.d/

## /etc/logrotate.conf

---

```
[root@godzilla log]# less /etc/logrotate.conf
# see "man logrotate" for details
# rotate log files weekly
weekly
# keep 4 weeks worth of backlogs
rotate 4
# create new (empty) log files after rotating old ones
create
# uncomment this if you want your log files compressed
#compress
# RPM packages drop log rotation information into this directory
include /etc/logrotate.d
# no packages own lastlog or wtmp -- we'll rotate them here
/var/log/wtmp {
    monthly
    create 0664 root utmp
    rotate 1
}
```

## /etc/logrotate.d/apache

---

```
[root@godzilla log]# less /etc/logrotate.d/apache
/var/log/httpd/access_log /var/log/httpd/agent_log /var/log/httpd/error_log /var
/log/httpd/referer_log {
    missingok
    sharedscripts
    postrotate
        /bin/kill -HUP `cat /var/run/httpd.pid 2>/dev/null` 2> /dev/null || true
    endscript
}
```

# Using the find command (1)

---

- Form of command.
  - *find path operations*
- Example:
  - Search and list all files from current directory and down for the string ABC.
    - **find ./ -name "\*" -exec grep -H ABC {} \;**
  - Find all files of given type from current directory on down.
    - **find ./ -name "\*.conf" -print**

# Using the find command (2)

---

## ■ Example:

- Find all user files larger than 5Mb.
  - **find /home -size +5000000c -print**
- Find all files owned by a user (defined by user id number. See /etc/passwd) on the system.
  - **find / -user 501 -print**
- Find all suid and setgid executables.
  - **find / \(-perm -400 -o -perm -2000\) -type f -exec ls -ldb {} \;**
  - **find / -type f -perm +6000 -ls**

# Using the find command (3)

---

- Example:
  - Find all world writable directories.
    - **find / -perm -0002 -type d -print**
  - Find all world writable files.
    - **find / -perm -0002 -type f -print**
    - **find / -perm -2 ! -type l -ls**
  - Find files with no user.
    - **find / -nouser -o -nogroup -print**
  - Find files modified in the last two days.
    - **find / -mtime 2 -o -ctime 2**

# Finding/Location files

---

locate/slocate	Find location/list of files which contain a given partial name.
which	Find executable file location of command given. Command must be in path.
whereis	Find executable file location of command given and related files.
rpm -qf <i>file</i>	Display name of RPM package from which the file was installed.

Note: The script `/etc/cron.daily/updatedb.cron` generates the index for the **locate** command. It will generate the database `/var/lib/locatedb`.

# Finding/Location files

## locate, which, whereis, ...

```
[root@godzilla /root]# locate traceroute
/usr/doc/kde/HTML/en/knu/knu-traceroute.gif
/usr/man/man8/traceroute.8.gz
/usr/sbin/traceroute6
/usr/sbin/traceroute
/usr/share/GXedit/traceroute.scr
/godzilla02/temp/spider_data_dont_delete/source/www.cs.washington.edu/lab+traceroute.html
/godzilla02/temp/spider_data_dont_delete/source/www.cc.gatech.edu/hw+traceroute.html
/godzilla02/temp/spider_data_dont_delete/source/www.mit.edu/handouts+h13-traceroute-sols.html
/godzilla02/temp/spider/worker/web.mit.edu/handouts+h13-traceroute-sols.html
/godzilla02/temp/spider/worker/www.mit.edu/handouts+h13-traceroute-sols.html
/godzilla02/temp/spider/worker3/www.cs.washington.edu/lab+traceroute.html
[root@godzilla /root]# which traceroute
/usr/sbin/traceroute
[root@godzilla /root]# whereis traceroute
traceroute: /usr/sbin/traceroute /usr/man/man8/traceroute.8.gz
[root@godzilla /root]#
```

# Managing Time

- Set System Time
  - Print the time returned by the remote host.
    - **rdate -p *hostname***
  - Set the system time to the returned time.
    - **rdate -s *hostname***
  - Set the hardware clock
    - **hwclock**

```
[root@godzilla /root]# rdate -p mike.cpe.ku.ac.th
[mike.cpe.ku.ac.th]  Fri Mar  1 22:52:33 2002
[root@godzilla /root]# rdate -s mike.cpe.ku.ac.th
[root@godzilla /root]# date
Fri Mar  1 22:52:36 ICT 2002
[root@godzilla /root]# rdate -s -p mike.cpe.ku.ac.th;hwclock --systohc;date
[mike.cpe.ku.ac.th]  Fri Mar  1 22:57:14 2002
Fri Mar  1 22:57:15 ICT 2002
[root@godzilla /root]#
```

# Simple mail reader

Mail command	Description
?	List commands (Help).
h	Print mail headers.
h <i>n</i>	Print mail headers starting with message number <i>n</i> .
q	Quit.
t	Type current message.
t <i>n</i>	Type out message <i>n</i> to the console.
n	Type out next message.
d	Delete the active message.
d <i>n</i>	Delete message number <i>n</i> .
d <i>start-end</i>	Delete message number <i>start</i> to <i>end</i> .

# Text Terminal Configuration (1)

---

- Print the file name of the terminal connected to standard input.

- `tty`

```
[root@godzilla /root]# tty
```

```
/dev/pts/6
```

# Text Terminal Configuration (2)

- Text terminal configuration commands
  - Print all current settings in human-readable form

- stty -all

```
[root@godzilla /root]# stty -all
```

```
speed 9600 baud; rows 55; columns 126; line = 0;
```

```
intr = ^C; quit = ^\; erase = ^?; kill = ^U; eof = ^D; eol = <undef>;  
eol2 = <undef>; start = ^Q; stop = ^S; susp = ^Z;
```

```
rprnt = ^R; werase = ^W; lnext = ^V; flush = ^O; min = 1; time = 0;
```

```
-parenb -parodd cs8 -hupcl -cstopb cread -clocal -crtscts
```

```
-ignbrk -brkint -ignpar -parmrk -inpck -istrip -inlcr -igncr icrnl ixon -  
ixoff -iuclc -ixany -imaxbel
```

```
opost -olcuc -ocrnl onlcr -onocr -onlret -ofill -ofdel nl0 cr0 tab0 bs0 vt0  
ff0
```

```
isig icanon iexten echo echoe echok -echonl -noflsh -xcase -tostop -  
echoprnt echoctl echoke
```



# Text Terminal Configuration (4)

- Clear text terminal
  - clear
- Reset text terminal
  - reset
- Terminal control characters

Description	Control Character	C format
Linefeed	cntl-j	\n
Backspace	cntl-h	
Carriage Return	cntl-m	\r
Escape Character	cntl-v	
Repaint screen	cntl-r	
Stop screen scroll	cntl-s	
Resume screen scroll	cntl-q	

# Text Terminal Configuration (5)

---

- Note:

- When typing a “`cntl-m`” is just like hitting the “Enter” key. If you want to enter the “`cntl-m`” as part of the `stty` command then prefix it with “`cntl-v`” so that the “`cntl-m`” “escaped” from acting as a terminal directive but instead acts as command input.
- Check terminal type: `echo $TERM`
- Set terminal type: `export TERM=xterm`

# Hardware Info

---

Command	Description
lsdev	List devices and info on system hardware.
/sbin/lspci	List all PCI devices (result of probe). Also “lspci -vvx” and “cat /proc/pci”.
cat /proc/interrupts	List IRQ’s used by system.
cat /proc/ioports	List I/O ports used by system.
cat /proc/dma	List DMA channels and device used by system.
cat /proc/cpuinfo	List info about CPU.

# Hardware Info

```
[root@godzilla /root]# lsdev
```

```
Device          DMA  IRQ  I/O Ports
```

```
-----  
cascade         4    2  
dma              0080-008f  
dma1             0000-001f  
dma2             00c0-00df  
eth0            10   d800-d87f  
fpu             13   00f0-00ff  
ide0             14   01f0-01f7 03f6-03f6 ffa0-ffa7  
ide1             15   0170-0177 0376-0376 ffa8-ffaf
```

```
...
```

```
[root@godzilla /root]# lspci
```

```
00:00.0 Host bridge: Advanced Micro Devices [AMD] AMD-751 [Irongate] System Controller (rev 23)
```

```
00:01.0 PCI bridge: Advanced Micro Devices [AMD] AMD-751 [Irongate] AGP Bridge (rev 01)
```

```
00:04.0 ISA bridge: VIA Technologies, Inc. VT82C686 [Apollo Super] (rev 1b)
```

```
00:04.1 IDE interface: VIA Technologies, Inc. VT82C586 IDE [Apollo] (rev 06)
```

```
...
```

# PERL Administrator/ Maintenance (1)

---

- At some point you will be required to administer the installation of PERL modules.
- Installation can be done.
  - Manually
    - Un-zip/Un-tar modules:  
`tar xzf yourmodules.tar.gz`
    - Built with PERL makefile:  
`perl Makefile.PL`  
`make`
    - Install:  
`make install`

# PERL Administrator/ Maintenance (2)

---

- Automatically

```
#perl -MCPAN -e shell
```

```
...
```

```
..
```

```
cpan> install URI
```

```
...
```

```
..
```

```
cpan> i /PerlMagick/
```

```
Distribution J/JC/JCRISTY/PerlMagick-5.36.tar.gz
```

```
Module Image::Magick (J/JC/JCRISTY/PerlMagick-5.36.tar.gz)
```

```
cpan> install Image::Magick
```

```
...
```

```
cpan> install Image::Info
```

```
...
```

```
cpan> install IO::String
```

```
IO::String is up to date.
```

```
cpan> help
```

Any  
questions  
?

