

CYBR 4423

Unix/Linux Administration

Process

Basic Concepts

A program is a structured set of commands stored in an executable file on a Linux file system. A program can be executed to create a process

A process is an instance of a computer program being executed, or running in memory and on the CPU
It can be running in the foreground or the background.

A service (or a daemon) is a background process, without direct user interaction

Once started, services run continuously in the background and are ready for incoming requests and send responses.

A (user) job is a process, but often it refers to a user session process usually started from a shell

Process Structure

Processes ID

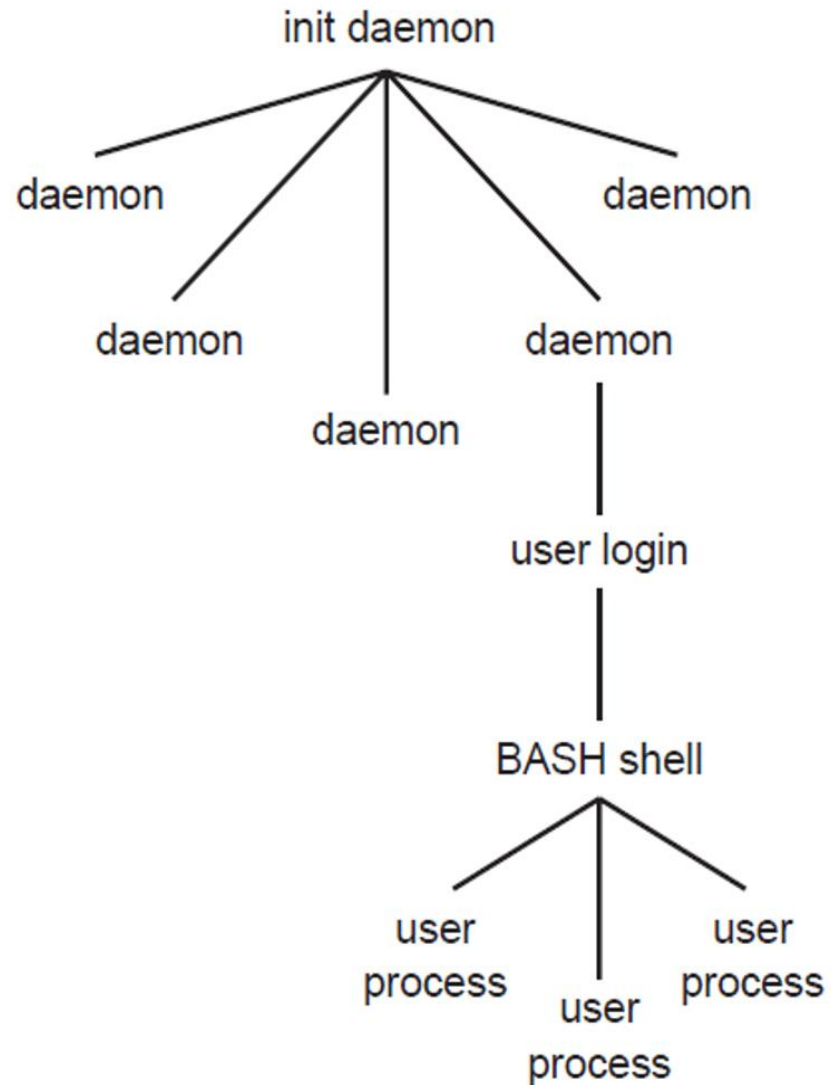
Each process is identified by a process id (PID)

Processes are hierarchical

The root process is the "init" process, which starts essential system process during the system startup

Process identification

The "init" process has PID of 1



Process Monitoring

"ps" command

Get a snap shot of the current running processes

"pstree" command

Showing processes in a hierarchical format

"pgrep" command

Search for processes

[Pgrep 1](#)

pgrep Command

pgrep looks through the currently running processes and lists the process IDs which matches the selection criteria to stdout. All the criteria have to match.

For example: **pgrep -u root sshd** will only list the processes called sshd AND owned by root.

On the other hand: **pgrep -u root,daemon** will list the processes owned by root OR daemon.

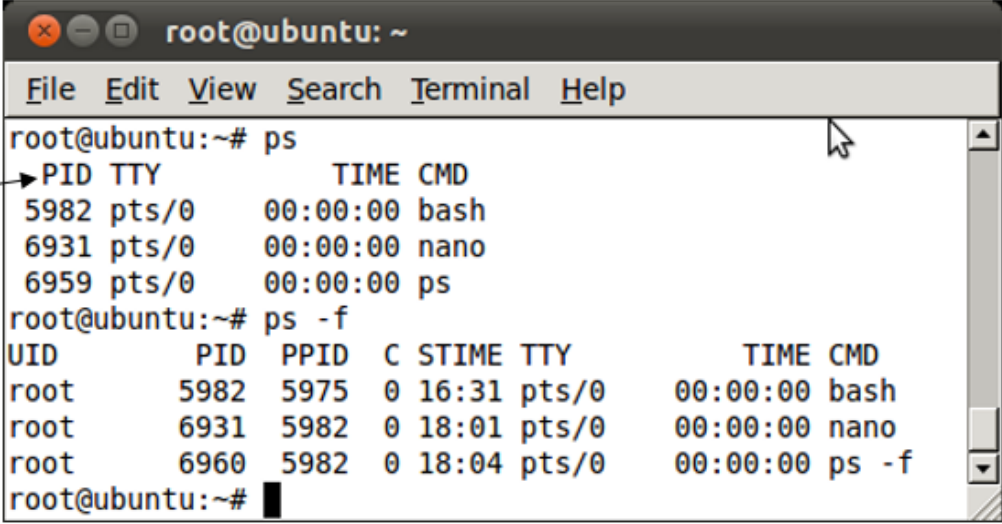
pkill will send the specified signal (by default SIGTERM) to each process instead of listing them on stdout.

ps (Process Status)

Common options

-A or -e show all processes
-f show more information

TTY: terminal.
pts/0: current
terminal.



```
root@ubuntu: ~  
File Edit View Search Terminal Help  
root@ubuntu:~# ps  
→ PID TTY          TIME CMD  
   5982 pts/0        00:00:00 bash  
   6931 pts/0        00:00:00 nano  
   6959 pts/0        00:00:00 ps  
root@ubuntu:~# ps -f  
UID          PID    PPID  C STIME TTY          TIME CMD  
root         5982    5975  0 16:31 pts/0        00:00:00 bash  
root         6931    5982  0 18:01 pts/0        00:00:00 nano  
root         6960    5982  0 18:04 pts/0        00:00:00 ps -f  
root@ubuntu:~#
```

More examples

Dynamic Process Monitoring

GUI

Gnome system monitor

Menu -> System -> Administration -> System Monitor -> Process tab

"top" command

Press O (upper case) to select sorting column (by default sorted by % CPU)

Press space bar to refresh; press s to change refresh interval

Press c to display absolute path for commands (last column)

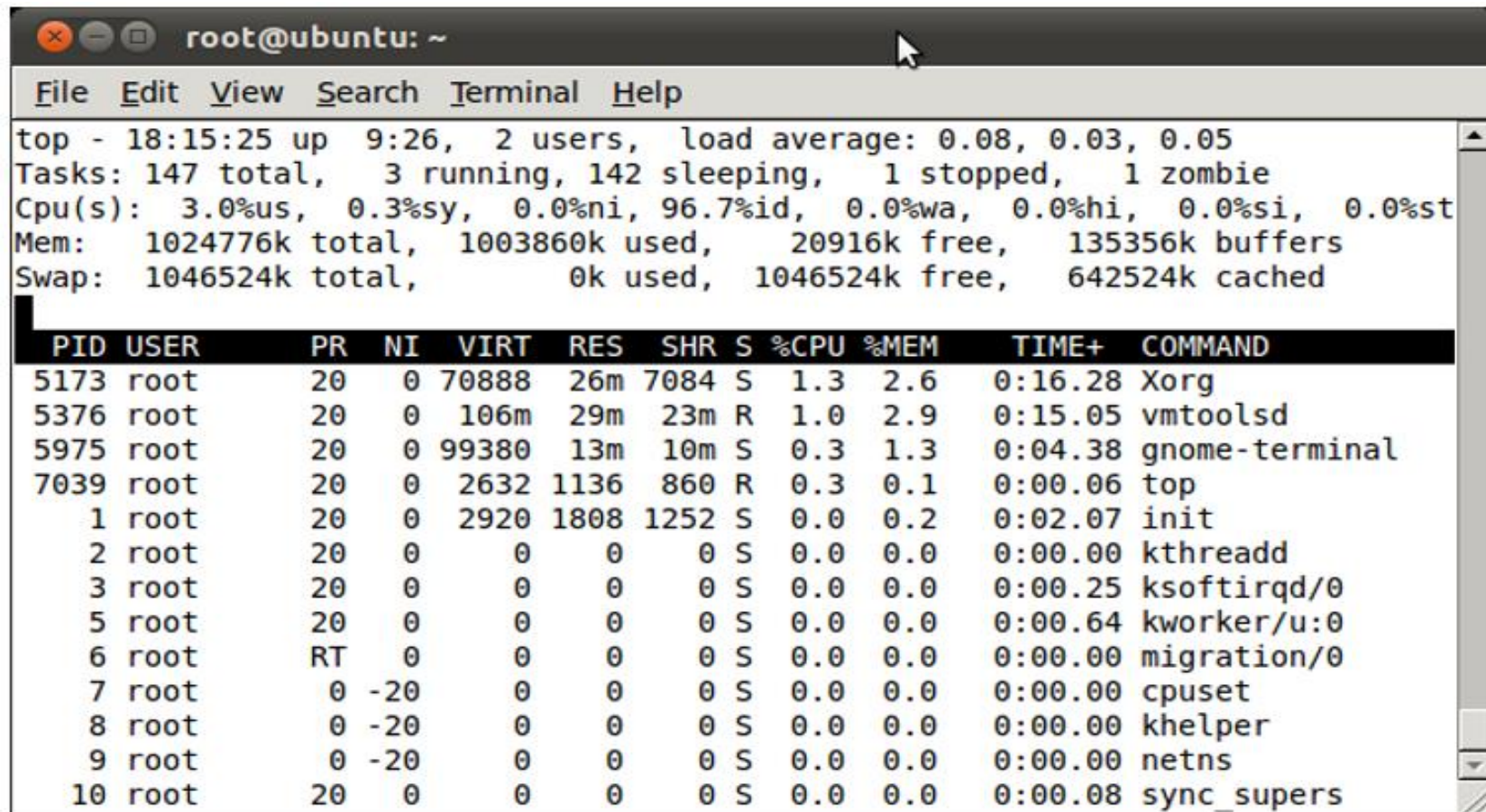
Press k to kill a process (need PID)

Press h for help

Press q to quit

Top Command

How to Run Top Command



```
root@ubuntu: ~
File Edit View Search Terminal Help
top - 18:15:25 up 9:26, 2 users, load average: 0.08, 0.03, 0.05
Tasks: 147 total, 3 running, 142 sleeping, 1 stopped, 1 zombie
Cpu(s): 3.0%us, 0.3%sy, 0.0%ni, 96.7%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Mem: 1024776k total, 1003860k used, 20916k free, 135356k buffers
Swap: 1046524k total, 0k used, 1046524k free, 642524k cached

  PID USER      PR  NI  VIRT  RES  SHR  S  %CPU  %MEM    TIME+  COMMAND
 5173 root        20   0 70888  26m 7084 S   1.3   2.6   0:16.28 Xorg
 5376 root        20   0 106m  29m 23m R   1.0   2.9   0:15.05 vmtoolsd
 5975 root        20   0 99380  13m 10m S   0.3   1.3   0:04.38 gnome-terminal
 7039 root        20   0  2632 1136  860 R   0.3   0.1   0:00.06 top
    1 root        20   0  2920 1808 1252 S   0.0   0.2   0:02.07 init
    2 root        20   0     0     0     0 S   0.0   0.0   0:00.00 kthreadd
    3 root        20   0     0     0     0 S   0.0   0.0   0:00.25 ksoftirqd/0
    5 root        20   0     0     0     0 S   0.0   0.0   0:00.64 kworker/u:0
    6 root        RT   0     0     0     0 S   0.0   0.0   0:00.00 migration/0
    7 root         0 -20     0     0     0 S   0.0   0.0   0:00.00 cpuset
    8 root         0 -20     0     0     0 S   0.0   0.0   0:00.00 khelper
    9 root         0 -20     0     0     0 S   0.0   0.0   0:00.00 netns
   10 root        20   0     0     0     0 S   0.0   0.0   0:00.08 sync_supers
```


Job Control

Running a program in the background

Use the "&" at the end of the command (a space is required to before "&")
Press "ctrl-z" to stop the current running program and puts it in background
Use "bg" command + program

Bring a program to foreground

Use the "fg" command + [job id]

Terminate (kill) a process or a job

Use the "kill" command (kill [PID])
Press "ctrl-c" when running a program

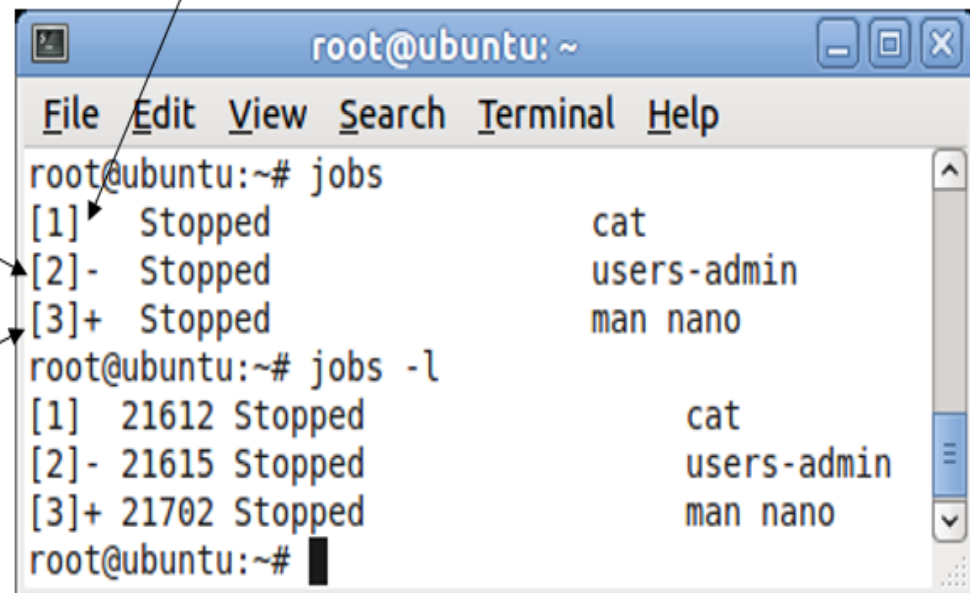
jobs Command

The "jobs" command lists running jobs started by the current session (bash)

'-' identifies the job that would become the default if the current default job were to exit; this job can also be represented as "%-".

'+' identifies the job that would be used as default for the "fg" or "bg" commands; this job can also be represented as "%+" or "%%";

Job id



```
root@ubuntu: ~  
File Edit View Search Terminal Help  
root@ubuntu:~# jobs  
[1] Stopped cat  
[2]- Stopped users-admin  
[3]+ Stopped man nano  
root@ubuntu:~# jobs -l  
[1] 21612 Stopped cat  
[2]- 21615 Stopped users-admin  
[3]+ 21702 Stopped man nano  
root@ubuntu:~#
```

Service/Daemon

A service is also called a daemon (Disk And Execution Monitor)

a process or collection of processes that wait for an external event to trigger an action on the part of the program.

Examples of common services are the SSH, Apache Web Server, FTP Server, OpenLDAP server, etc.

2 types of daemons:

Signal-controlled daemons. These are always activated when a corresponding task exists.

Interval-controlled daemons. These are always activated at certain intervals.

inet

The inetd (Internet daemon) daemon and its replacement xinetd (extended Internet daemon; xinetd.org) are called super servers or service dispatchers

It starts other daemons, such as smbd (Samba) and vsftpd (FTP), as necessary.

It listens for network connections. When one is made, they identify a server daemon based on the port the connection comes in on and start the daemon.

Service port file

/etc/services



Managing Services

For each daemon, there is a script file in `"/etc/init.d/"`. Each script can be controlled and run with the following command:

`[script file name] + command (start, stop, restart, etc.)`

For example, "apache2" is the script file name

`/etc/init.d/apache2 start`

Use "service" (`/usr/sbin/service`) command to manage services

"service --status-all" shows all services and their status

"service [service script file name] + command

`service apache2 start`

Parameter	Description
start	Starts the service.
stop	Stops the service.
reload (or restart)	Reloads the configuration file of the service, or stops the service and starts it again.

sleep Command

The sleep instruction suspends the calling process for at least the specified number of seconds (the default)

```
sleep 10
```

Applications

- Timer

- Background process

Shell Startup Files

~/.profile

executed by the command interpreter for login shells (the shell which a user uses to login)

This file is not read by bash, if ~/.bash_profile or ~/.bash_login exists.

~/.bashrc

executed by bash for non-login or remote shells

used for setting up user shell environments

Summary

Key concepts

Program, process, service/daemon, job

Foreground, background

Key commands

ps, pstree, top, jobs, pgrep

fg, bg, kill, sleep

&

service

ctrl-c, ctrl-z

Login

	System Wide	User specific
Login shell	/etc/profile /etc/profile.d/*	~/.profile
Non-login shell	N/A	
Bash non-login	/etc/	~/.bashrc
	N/A	

Startup Files

/etc/profile



~/.profile

~/.bashrc

<http://blog.flowblok.id.au/2013-02/shell-startup-scripts.html>

System Daemons

Some important daemons include the following:

inetd

syslogd. Logs system messages in the directory /var/log/
(start script is /etc/init.d/syslog; configuration file is
/etc/syslog.conf).

Service and Process

exec

start up sequence and config - .gconf .bashrc, .bash_profile

- init daemon
- start up, boot
- booting and shutting down
- sleep, write a timer app
- core system service
- event log

Inetd

Inet.conf

Etc/services



cron

cron. Starts other processes at specified times (system-wide files: /etc/crontab and in /etc/cron.*; user-specific files are in /var/spool/cron/tabs/).

Session Commands

Exit a shell (terminal)

`exit`

`login, logout`

`reboot`

`shutdown now`

System Startup

Init

/sbin/init

/etc/init/rc-sysinit.conf

Also looks for /etc/inittab

A replacement of system V /etc/rc

.bashrc

.xinitrc

This script overrides the default script that gets called when you log into the X Window System.

.Xdefaults

This file This file contains defaults that you can specify for X Window System applications.

Who -r

Who -b

Runlevel

wait



Init process

Linux Init Process

Types

System core process

Init

Active process

Daemon

Initctl list

Process Status

Status

Running

Sleeping

Suspended

Stopped