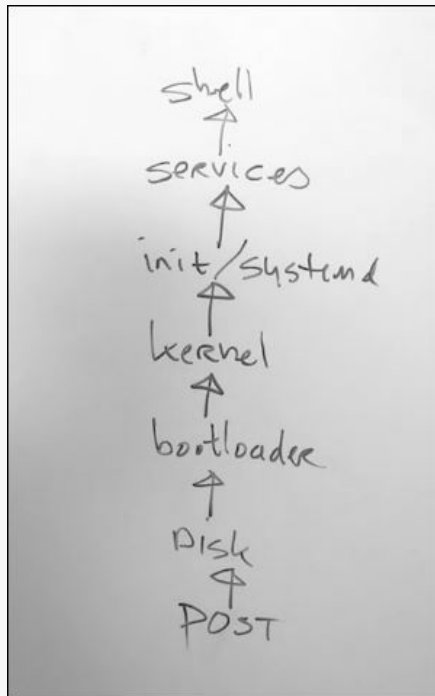


Boot order



Process Properties w/ ps

PID- Process ID-Virtual Memory Size-
VCZ- Residence Memory Size-Console
RSS- Process running on
TTY

ps aux Find SSHD service running on
| grep system
sshd

ps -ef Parent Process ID
| less
(PPID)

ps -e -o pid,args --forest

Process Properties w/ ps

PID- Process ID-Virtual Memory Size-
VCZ- Residence Memory Size-Console
RSS- Process running on
TTY

ps Find SSHD service running on
aux | system
grep
sshd

Process Properties w/ ps (cont)

ps -ef | less Parent Process ID
(PPID)

ps -e -o pid,args -- Show relation between
forest | less parent and child
processes

ps aux --sort Sorting process memory
pmem

Systemd

/usr/lib/systemd Main config dir

systemctl -t help List available unit
types

ls /usr/lib/systemd/syst- List available
em/*socket socket service

Socket: ListenStr- Listen on TCP
eam=22 port 22

Service can be dead and socket can still
listening, reducing resource to run service

systemctl show sshd = List all options
man systemd.directives can be included
in service

systemctl set-property Modify unit file
httpd.service Memory- httpd
Limit=500m

Target Group of unit file
systemctl get-default Default target

systemctl set-default Set default to
multi-user.target multi.user

When boot systemd.unit=rescue.target

systemctl list-units List all current
units

Linux Log

Make dir "journal" in /var/log make journal consistently

vim /etc/systemd/journ- change storage=auto to
ald.conf make journalctl consis-
tently

Managing Shell Jobs

sleep 600 then Ctrl+Z Start job in
or sleep 600 & background

fg Move last bg job
to foreground

jobs Show current jobs

Cron jobs

/etc/cron.d/ Main dir to put
file for
scheduling (used
by rpm)

minute hour Crontab syntax
dayofmonth month
dayofweek username
command

crontab -e Open crontab for
current user

/10 1-5 /bin/logger Run logger every
10 minute on
weekdays

cat /var/log/cron | grep Verify schedule
CRON cron jobs

Libraries, RPM

ldd Show all libraries the command
/usr/bin/ldd need
passwd

rpm -qa | List all installed packages
grep (query all) and see if httpd is
httpd installed

rpm -qi Provide info about package
httpd



By nhatalog0605

Published 25th September, 2018.

Last updated 6th April, 2020.

Page 1 of 3.

Sponsored by **Readable.com**

Measure your website readability!

<https://readable.com>

Libraries, RPM (cont)

<code>rpm -ql http</code>	Provide list of files installed from package
<code>rpm -qc httpd</code>	List configuration file (c)
<code>rpm -qd httpd</code>	List documentation about package (d)
<code>rpm -qpi filename</code>	Provide info about uninstalled package
<code>rpm -qp --scripts filename</code>	Find which scripts are executed if package is installed
<code>rpm -qf /etc/nanorc</code>	Find out which package the file coming from

Configuring GRUB2 Boot Loader

Press ESC after boot	Stop booting process
Rescue kernel	Boot w/ minimal modules
Press e	Edit
Take out "rhgb" "-quiet"	See what's happen upon boot
Edit /etc/default/grub	Permanent boot modifications
/boot/grub2/grub.cfg	Determine everything when system boot
<code>grub2-mkconfig -o /boot/grub2/grub.cfg</code>	Write a new GRUB config
<code>systemd.unit=rescue.target</code>	Start booting at rescue mode
<code>systemd.unit=emergency.target</code>	Boot at minimal
<code>mount -o remount,rw /</code>	Put root file system in read,write mode

Configuring GRUB2 Boot Loader (cont)

<code>rd.break</code>	Break in boot procedure at the end of init params
<code>chroot /sysroot</code>	Set root file system to /sysroot
<code>echo b > /proc/sysrq-trigger</code>	Crash and reset
<code>touch .autorelabel</code>	on CentOS

Rsyslog

<code>systemctl status rsyslog</code>	Check status of Rsyslog
---------------------------------------	-------------------------

`vim /etc/rsyslog.conf`

<code>facility</code>	authpriv, kern, mail
<code>priority</code>	.emerg, .crit, .debug
<code>kern.* /dev/console</code>	Log from kern with all priority written to /dev/console
<code>mail.* -/var/log/maillog</code>	Written not in realtime (-)
<code>.emerg :omusrmsg:</code>	Every user will receive emergency message on console
<code>*.crit /var/log/critical</code>	Save message with critical priority or higher to /var/log/critical
<code>logger -p crit</code>	Write log with crit priority
<code>/etc/cron.daily/logrotate</code>	
<code>logrotate.conf</code>	

Install software

<code>tar xvf filename -C /tmp</code>	Decompress tar file verbose (v), x (extract) f(file) to /tmp dir
<code>file filename</code>	Find info about compressed file
<code>gunzip filename</code>	Decompress file
<code>tar czvf etc.tar /etc/</code>	Create tarball (c) and compress (z)
<code>gunzip filename</code>	Unzip file
<code>-p</code>	preserver permission while decompress, compress

Process Signals

Within top, press k	PID, 15(sigterm)
<code>kill 14053</code>	Kill process 14053
<code>killall dd</code>	Kill all process w/name dd
<code>kill -9 14321</code>	Kill process 14321 w/ signal 9 (kill)
<code>kill \$(pidof dd)</code>	Kill all dd process, similar to killall
<code>kill -l</code>	List of kill signal

SELinux Booleans

<code>getsebool -a</code>	List of all current booleans
<code>setsebool ftpd_a-non_write on</code>	Switch on to anonymous writing on ftp

SELinux

<code>getenforce</code>	Current mode of SELinux
<code>setenforce Permissive</code>	Change to Permissive mode



By **nhatalog0605**

cheatography.com/nhatalog0605/

Published 25th September, 2018.
Last updated 6th April, 2020.
Page 2 of 3.

Sponsored by **Readable.com**
Measure your website readability!
<https://readable.com>

SELinux (cont)

cd /etc/sysconfig/
selinux Disable or enable
SELinux

Systemd timers, at

/usr/lib/systemd/s-
ystem Dir for unit file and
timers

systemctl status atd Check at daemon
status

at 11:00, Ctrl+d to start job at 11
start job

atq Current jobs
running w/ at

atrm *jobnumber* Remove job

SELinux Labels

man semanage-fco-
ntext man page for
setting context

semanage fcontext -a Setting SELinux to
-t httpd_sys_content_t allow Apache read
"/web(/.*)?" from /web

ls -lZd /web

restorecon -Rv /web

semanage port -a -t Allow Apache
http_port_t -p tcp 444 listen to port 444

SEAlert

less /var/log/mes-
sages Look for sealrt
sages

sealrt -l *code* Troubleshoot
sealrt

Kernel Modules

lsmod | less List modules

modprobe cdrom Load cdrom
module

modinfo cdrom Info about
module

/etc/modprobe.d

echo options cdrom Create
autoclose=1 > cdrom.conf to
cdrom.conf automatically
apply option

/proc Interface to
modify linux
kernel

echo 1 > /proc/sys/ip-
v6/conf/all/disabl-
e_ipv6 Disable ipv6 on
runtime

echo net.ipv6.conf.a-
ll.disable_ipv6 = 1 > Disable ipv6
etc/sysctl.d/ipv6.conf persistently

sysctl -a List all tools

Yum

yum search Search for package
package

yum info Info about package
package

yum provides Provide package info
*/filename

yum remove Remove package
package

yum Download the package to
downloader analyse
package

yum list Get information about
package

yum install Install from the repo

yum update Compare packages and
update if suitable

Process Priority

RT Real time process, part
of the kernel

Within top, press r

nice -n 5 dd Run dd command with
if/dev/zero nice value of 5 and
of=/dev/null & priority of 25

renice -n 5 Change priority of
14053 process id 14053

Changing top Display Properties

Press f Changing top window and
sorting

Press z Color top window

Press Write to config file
W

Managing Processes

```
top - 17:36:45 up 9 min, 2 users, load average: 0.05, 0.21, 0.20
Tasks: 184 total, 1 running, 183 sleeping, 0 stopped, 0 zombie
MiB Mem: 1282336 total, 443768 free, 729932 used, 318616 buff/cache
MiB Swap: 1003516 total, 1003516 free, 0 used, 955988 avail Mem

  PID USER      PR  NI  VIRT  RES  SHR  S  CPU% MEM%   TIME+  COMMAND
 2386 student    20   0 3811472 194736 54756 S  0.7 10.3  0:10.26 gnome-shell
1226 root       20   0 241888 40592 12512 S  0.2 2.2  0:03.79 X
3093 root     20   0 161972 2308 1576 R  0.3 0.1  0:00.81 top
1 root       20   0 128164 6796 4120 S  0.0 0.4  0:01.76 systemd
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  0:00.07 ksoftirqd/0
5 root       20   0 0 0 0 S  0.0 0.0  0:00.00 worker/0:0H
6 root       20   0 0 0 0 S  0.0 0.0  0:00.02 worker/u2:0
7 root       20   0 0 0 0 S  0.0 0.0  0:00.00 migration/0
8 root       20   0 0 0 0 S  0.0 0.0  0:00.00 rcu_bh
9 root       20   0 0 0 0 S  0.0 0.0  0:00.34 rcu_sched
10 root      20   0 0 0 0 S  0.0 0.0  0:00.00 rcu-dm
```

Load average: last min, last 5 mins, last 15 mins

Press 1 to see number of CPU cores

Zombie task: Tasks lost communication w/
parent process

CPU: US process started by users, SY
process relay directly to hardware, ni (nice)
process w/ adjusted priority, id (idle) CPU
time, wa(waiting) for harddisk.

S for status, R for running, S for sleeping
VIRT virtual mem, RES resident mem
process really using, SHR sharing mem to
share with other processes

top -u student: process started by user



By **nhatlong0605**

cheatography.com/nhatlong0605/

Published 25th September, 2018.

Last updated 6th April, 2020.

Page 3 of 3.

Sponsored by **Readable.com**

Measure your website readability!

<https://readable.com>