Managing Shell Jobs

sleep 600 then Ctrl+Z or sleep 600 &	Start job in background
fg	Move last bg job to foreground
jobs	Show current jobs

Process Properties w/ ps

PID-VCZ-RSS-TTY	Process ID-Virtual Memory Size-Residence Memory Size-Console Process running on
ps aux | grep sshd	Find SSHD service running on system
ps -ef | less (PPID)	Parent Process ID
ps -e -o pid,args --forest	

Process Properties w/ ps

PID-VCZ-RSS-TTY	Process ID-Virtual Memory Size-Residence Memory Size-Console Process running on
ps aux | grep sshd	Find SSHD service running on system
ps -ef | less (PPID)	Parent Process ID

Process Properties w/ ps (cont)

ps -e -o pid,args --forest | less	Show relation between parent and child processes
ps aux --sort pmem	Sorting process memory

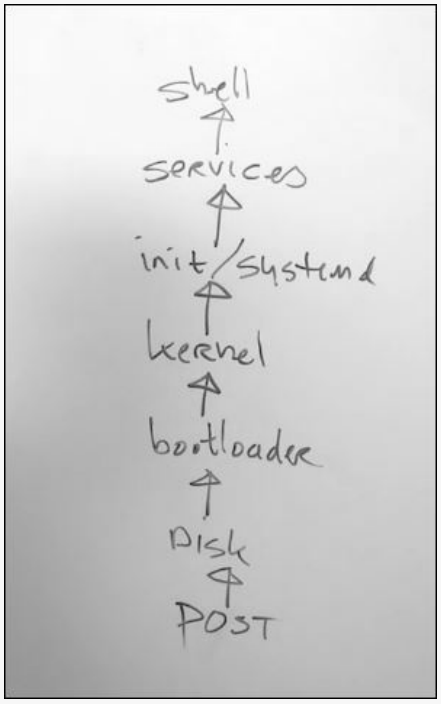
Cron jobs

/etc/cron.d/	Main dir to put file for scheduling (used by rpm)
minute hour dayofmonth month dayofweek username command	Crontab syntax
crontab -e	Open crontab for current user
/10 1-5 /bin/logger	Run logger every 10 minute on weekdays
cat /var/log/cron | grep CRON	Verify schedule cron jobs

Linux Log

Make dir "journal" in /var/log	make journal consistently
vim /etc/systemd/journald.conf	change storage=auto to make journalctl consistently

Boot order



Systemd

/usr/lib/systemd	Main config dir
systemctl -t help	List available unit types
ls /usr/lib/systemd/system/*socket	List available socket service
Socket: ListenStream=22	Listen on TCP port 22
Service can be dead and socket can still listening, reducing resource to run service	

Systemd (cont)

systemctl show sshd = man systemd.directives	List all options can be included in service
systemctl set-property httpd.service Memory-Limit=500m	Modify unit file htttpd
Target	Group of unit file
systemctl get-default	Default targart
systemctl set-default multi-user.target	Set default to multi.user
When boot systemd.unit=rescue.target	
systemctl list-units	List all current units

Process Signals

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

Install software

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

Libraries, RPM

ldd /usr/bin/-passwd	Show all libraries the command need
rpm -qa | grep httpd	List all installed packages (query all) and see if httpd is installed
rpm -qi httpd	Provide info about package
rpm -ql http	Provide list of files installed from package
rpm -qc httpd	List configuration file (c)
rpm -qd httpd	List documentation about package (d)
rpm -qpi filename	Provide info about uninstalled package

Libraries, RPM (cont)

rpm -qp --scripts filename	Find which scripts are executed if package is installed
rpm -qf /etc/nanorc	Find out which package the file coming from

Rsyslog

systemctl status rsyslog	Check status of Rsyslog
vim /etc/rsyslog.conf	
facility	authpriv, kern, mail
priority	.emerg, .crit, .debug
kern.* /dev/console	Log from kern with all priority written to /dev/c-onsole
mail.* -/var/-log/maillog	Written not in realtime (-)
*.emerg :omusrmsg:	Every user will receive emergency messsage on console
*.crit /var/l-og/critical	Save message with critical priority or higher to /var/log/-critical
logger -p crit Critical Situation	Write log with crit priority
/etc/cron.daily/logrotate	
logrotate.conf	

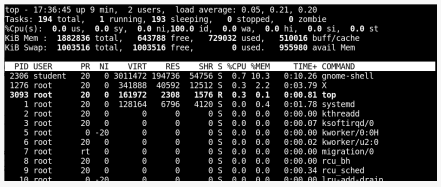
Configuring GRUB2 Boot Loader

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
grub2-mkconfig -o /boot/grub2/grub.cfq	Write a new GRUB config
systemd.unit=rescue.target	Start booting at rescue mode
systemd.unit=emergency.target	Boot at minimal
mount -o remount,rw /	Put root file system in read,write mode
rd.break	Break in boot procedure at the end of init params
chroot /sysroot	Set root file system to /sysroot
echo b > /proc/sysrq-trigger	Crash and reset
touch .autorelabel	on CentOS

SELinux Booleans

getsebool -a	List of all current booleans
setsebool ftpd_anon_write on	Switch on to anonymous writing on ftp

Managing Processes



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

Changing top Display Properties

Press f	Changing top window and sorting
Press z	Color top window
Press W	Write to config file

Process Priority

RT	Real time process, part of the kernel
Within top, press r	
nice -n 5 dd if/dev/zero of=/dev/null &	Run dd command with nice value of 5 and priority of 25
renice -n 5 14053	Change priority of process id 14053

Yum

yum search *pacckage*	Search for package
yum info *package*	Info about package
yum provides */filename	Provide package info
yum remove *package*	Remove package
yum downloader *package*	Download the package to analyse
yum list	Get information about package
yum install	Install from the repo
yum update	Compare packages and update if suitable

Systemd timers, at

/usr/lib/systemd/system	Dir for unit file and timers
systemctl status atd	Check at daemon status
at 11:00, Ctrl+d to start job	start job at 11
atq	Current jobs running w/ at
atrm *jobnumber*	Remove job

Kernel Modules

lsmod | less	List modules
modprobe cdrom	Load cdrom module
modinfo cdrom	Info about module
/etc/modprobe.d	
echo options cdrom autoclose=1 > cdrom.conf	Create cdrom.conf to automatically apply option
/proc	Interface to modify linux kernel
echo 1 > /proc/sys/ipv6/conf/all/disable_ipv6	Disable ipv6 on runtime
echo net.ipv6.conf.all.disable_ipv6 = 1 > etc/sysctl.d/ipv6.conf	Disable ipv6 persistently
sysctl -a	List all tools

SELinux

getenforece	Current mode of SELinux
setenforce Permissive	Change to Permissive mode
cd /etc/sysconfig/selinux	Disable or enable SELinux

SELinux Labels

man semanage-fcontext	man page for setting context
semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"	Setting SELinux to allow Apache read from /web
ls -lZd /web	
restorecon -Rv /web	
semanage port -a -t http_port_t -p tcp 444	Allow Apache listen to port 444

SEAlert

less /var/log/messages	Look for sealert
sealrt -l *code*	Troubleshoot sealert