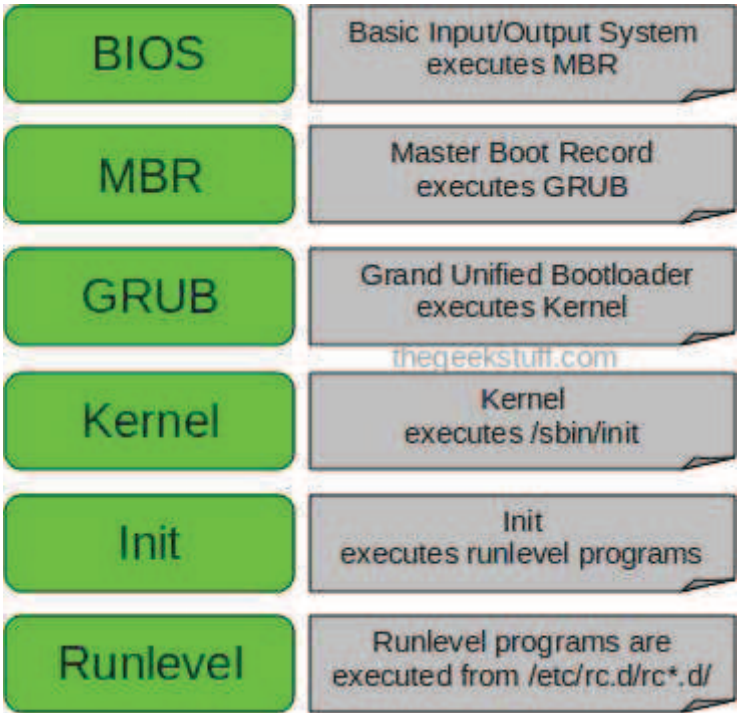
Chapter 2

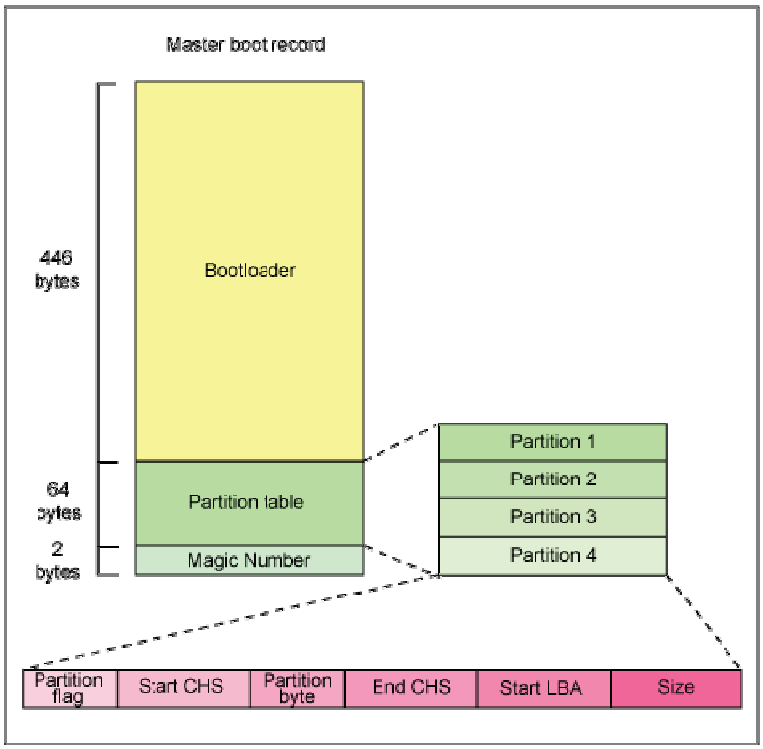
Operate running systems

Boot Sequence

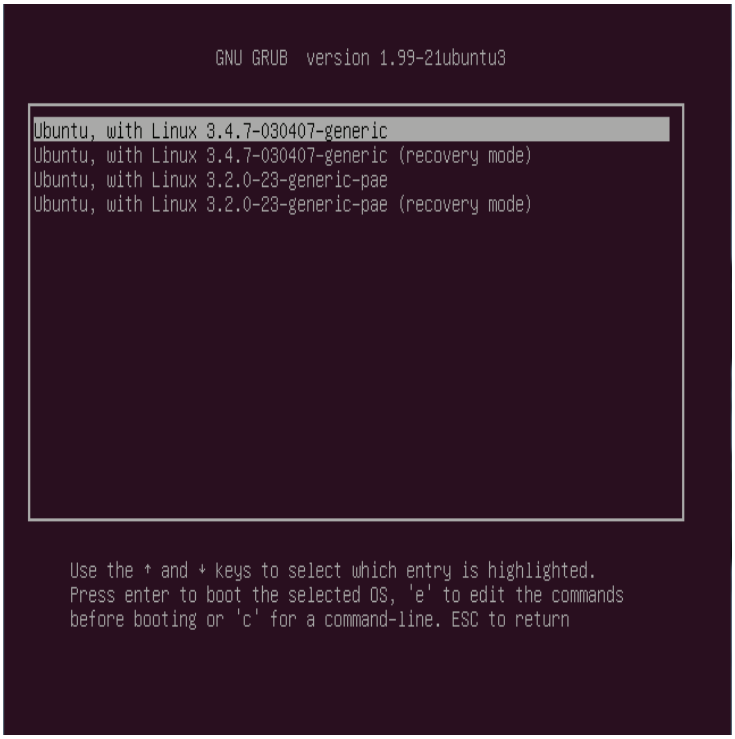


ls /var/log

- Bios
- MBR --> 512 byte
- GRUB



[root@rajaopenldap1 log]# vim /etc/grub.conf



[root@rajaopenldap1 log]# locate vmlinuz

/boot/.vmlinuz-2.6.32-431.20.3.el6.i686.hmac

/boot/.vmlinuz-2.6.32-431.23.3.el6.i686.hmac

/boot/.vmlinuz-2.6.32-431.29.2.el6.i686.hmac

/boot/.vmlinuz-2.6.32-504.1.3.el6.i686.hmac

/boot/.vmlinuz-2.6.32-504.el6.i686.hmac

/boot/vmlinuz-2.6.32-431.20.3.el6.i686

/boot/vmlinuz-2.6.32-431.23.3.el6.i686

/boot/vmlinuz-2.6.32-431.29.2.el6.i686

/boot/vmlinuz-2.6.32-504.1.3.el6.i686

/boot/vmlinuz-2.6.32-504.el6.i686

- Kernel
- init
- runlevel

Run Levels

cat /etc/inittab

inittab is only used by upstart for the default runlevel.

#

ADDING OTHER CONFIGURATION HERE WILL HAVE NO EFFECT ON YOUR SYSTEM.

#

System initialization is started by /etc/init/rcS.conf

#

Individual runlevels are started by /etc/init/rc.conf

#

Ctrl-Alt-Delete is handled by /etc/init/control-alt-delete.conf

#

```
# Terminal gettys are handled by /etc/init/tty.conf and /etc/init/serial.conf,
# with configuration in /etc/sysconfig/init.
#
# For information on how to write upstart event handlers, or how
# upstart works, see init(5), init(8), and initctl(8).
#
# Default runlevel. The runlevels used are:
#   0 - halt (Do NOT set initdefault to this)
#   1 - Single user mode
#   2 - Multiuser, without NFS (The same as 3, if you do not have networking)
#   3 - Full multiuser mode
#   4 - unused
#   5 - X11
#   6 - reboot (Do NOT set initdefault to this)
#

id:5:initdefault:
```

```
SV:123456:respawn:/command/svscanboot
[root@rajaopenldap1 log]#

[root@rajaopenldap1 log]# ps -aux | more

USER        PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root          1  0.0  0.1   2948  1328 ?        Ss   19:55   0:04 /sbin/init
root          2  0.0  0.0      0     0 ?        S    19:55   0:00 [kthreadd]
root          3  0.0  0.0      0     0 ?        S    19:55   0:00 [migration/0]
root          4  0.0  0.0      0     0 ?        S    19:55   0:00 [ksoftirqd/0]
root          5  0.0  0.0      0     0 ?        S    19:55   0:00 [stopper/0]
root          6  0.0  0.0      0     0 ?        S    19:55   0:02 [watchdog/0]
root          7  0.0  0.0      0     0 ?        S    19:55   0:01 [events/0]
```

root 8 0.0 0.0 0 0 ? S 19:55 0:00 [cgroup]

root 9 0.0 0.0 0 0 ? S 19:55 0:00 [khelper]

root 10 0.0 0.0 0 0 ? S 19:55 0:00 [netns]

root 11 0.0 0.0 0 0 ? S 19:55 0:00 [async/mgr]

root 12 0.0 0.0 0 0 ? S 19:55 0:00 [pm]

root 13 0.0 0.0 0 0 ? S 19:55 0:00 [sync_supers]

root 14 0.0 0.0 0 0 ? S 19:55 0:00 [bdi-default]

root 15 0.0 0.0 0 0 ? S 19:55 0:00 [kintegrityd/0]

root 16 0.1 0.0 0 0 ? S 19:55 0:06 [kblockd/0]

root@rajaopenldap1 rc5.d]# ls -l

total 0

lrwxrwxrwx 1 root root 17 Nov 1 2014 K00ipmievd -> ../init.d/ipmievd

lrwxrwxrwx 1 root root 22 Mar 5 2014 K01bmc-watchdog -> ../init.d/bmc-watchdog

lrwxrwxrwx 1 root root 14 Nov 1 2014 K01ctdb -> ../init.d/ctdb

lrwxrwxrwx 1 root root 14 Nov 1 2014 K01luci -> ../init.d/luci

lrwxrwxrwx. 1 root root 21 Oct 28 2012 K01modclusterd -> ../init.d/modclusterd

lrwxrwxrwx. 1 root root 16 Oct 30 2012 K01nagios -> ../init.d/nagios

lrwxrwxrwx 1 root root 15 Nov 1 2014 K01numad -> ../init.d/numad

lrwxrwxrwx. 1 root root 15 Oct 28 2012 K01ricci -> ../init.d/ricci

lrwxrwxrwx. 1 root root 16 Apr 18 2013 K01smartd -> ../init.d/smartd

lrwxrwxrwx 1 root root 14 Aug 2 2014 K02npcd -> ../init.d/npcd

lrwxrwxrwx. 1 root root 16 Oct 30 2012 K02puppet -> ../init.d/puppet

lrwxrwxrwx. 1 root root 16 Oct 30 2012 K03kannel -> ../init.d/kannel

[root@rajaopenldap1 rc5.d]# cd ../init.d/

```
[root@rajaopenldap1 init.d]# ls
abrt-ccpp        foghorn        netcf-transaction  rpcsvcgssd
abrtd            functions      netconsole         rstatd
abrt-oops        gatherer       netfs              rsyslog
acpid            gfs2           netlabel           rusersd
.
.
.
```

Sample:

```
[root@rajaopenldap1 init.d]# cat crond
#!/bin/sh
#
# crond          Start/Stop the cron clock daemon.
#
# chkconfig: 2345 90 60
# description: cron is a standard UNIX program that runs
user-specified \
#              programs at periodic scheduled times. vixie cron
adds a \
```

```
#                 number of features to the basic UNIX cron, including better \
#                 security and more powerful configuration options.

### BEGIN INIT INFO
# Provides: crond crontab
# Required-Start: $local_fs $syslog
# Required-Stop: $local_fs $syslog
# Default-Start:  2345
# Default-Stop: 90
# Short-Description: run cron daemon
# Description: cron is a standard UNIX program that runs user-specified
#             programs at periodic scheduled times. vixie cron adds a
#                 number of features to the basic UNIX cron, including better
#                 security and more powerful configuration options.
### END INIT INFO
```

```
[ -f /etc/sysconfig/crond ] || {
   [ "$1" = "status" ] && exit 4 || exit 6
}

RETVAL=0
prog="crond"
exec=/usr/sbin/crond
lockfile=/var/lock/subsys/crond
config=/etc/sysconfig/crond

# Source function library.
. /etc/rc.d/init.d/functions

[ $UID -eq 0 ] && [ -e /etc/sysconfig/$prog ] && .
/etc/sysconfig/$prog

start() {
   if [ $UID -ne 0 ] ; then
      echo "User has insufficient privilege."
      exit 4
   fi
```

```
    [ -x $exec ] || exit 5
    [ -f $config ] || exit 6
    echo -n $"Starting $prog: "
    daemon $prog $CRONDARGS
    retval=$?
    echo
    [ $retval -eq 0 ] && touch $lockfile
}

stop() {
    if [ $UID -ne 0 ] ; then
        echo "User has insufficient privilege."
        exit 4
    fi
    echo -n $"Stopping $prog: "
        if [ -n "`pidfileofproc $exec`" ]; then
                killproc $exec
                RETVAL=3
        else
                failure $"Stopping $prog"
        fi
```

```
    retval=$?
    echo
    [ $retval -eq 0 ] && rm -f $lockfile
}

restart() {
    rh_status_q && stop
    start
}

reload() {
        echo -n $"Reloading $prog: "
        if [ -n "`pidfileofproc $exec`" ]; then
                killproc $exec -HUP
        else
                failure $"Reloading $prog"
        fi
        retval=$?
        echo
}
```

```
force_reload() {
        # new configuration takes effect after restart
   restart
}

rh_status() {
   # run checks to determine if the service is running or use generic status
   status -p /var/run/crond.pid $prog
}

rh_status_q() {
   rh_status >/dev/null 2>&1
}



case "$1" in
   start)
      rh_status_q && exit 0
      $1
      ;;
```

```
  stop)
    rh_status_q || exit 0
    $1
    ;;
  restart)
    $1
    ;;
  reload)
    rh_status_q || exit 7
    $1
    ;;
  force-reload)
    force_reload
    ;;
  status)
    rh_status
    ;;
  condrestart|try-restart)
    rh_status_q || exit 0
    restart
    ;;
```

```
  *)
    echo $"Usage: $0 {start|stop|status|restart|condrestart|try-restart|reload|force-reload}"
    exit 2
esac
exit $?

[root@rajaopenldap1 init.d]#
```

service start | stop | restart |...

```
/etc/init.d/httpd restart
service httpd restart
```

tty

```
ps -aux  | grep tty
Warning: bad syntax, perhaps a bogus '-'? See /usr/share/doc/procps-3.2.8/FAQ
root     3447  0.0  0.0   2004   476 tty2     Ss+  20:01   0:00 /sbin/mingetty /dev/tty2
```

root 3449 0.0 0.0 2004 480 tty3 Ss+ 20:01 0:00 /sbin/mingetty /dev/tty3

root 3455 0.0 0.0 2004 476 tty4 Ss+ 20:01 0:00 /sbin/mingetty /dev/tty4

root 3464 0.0 0.0 2004 476 tty5 Ss+ 20:01 0:00 /sbin/mingetty /dev/tty5

root 3468 0.0 0.0 2004 480 tty6 Ss+ 20:01 0:00 /sbin/mingetty /dev/tty6

root 3509 1.3 3.3 51496 34332 tty1 Ss+ 20:02 1:24 /usr/bin/Xorg :0 -br -verbose -audit 4 -auth /var/run/gdm/auth-for-gdm-rLXR0g/database -nolisten tcp vt1

shells

[root@rajaopenldap1 init.d]# cat /etc/shells

/bin/sh

/bin/bash

/sbin/nologin

/bin/tcsh

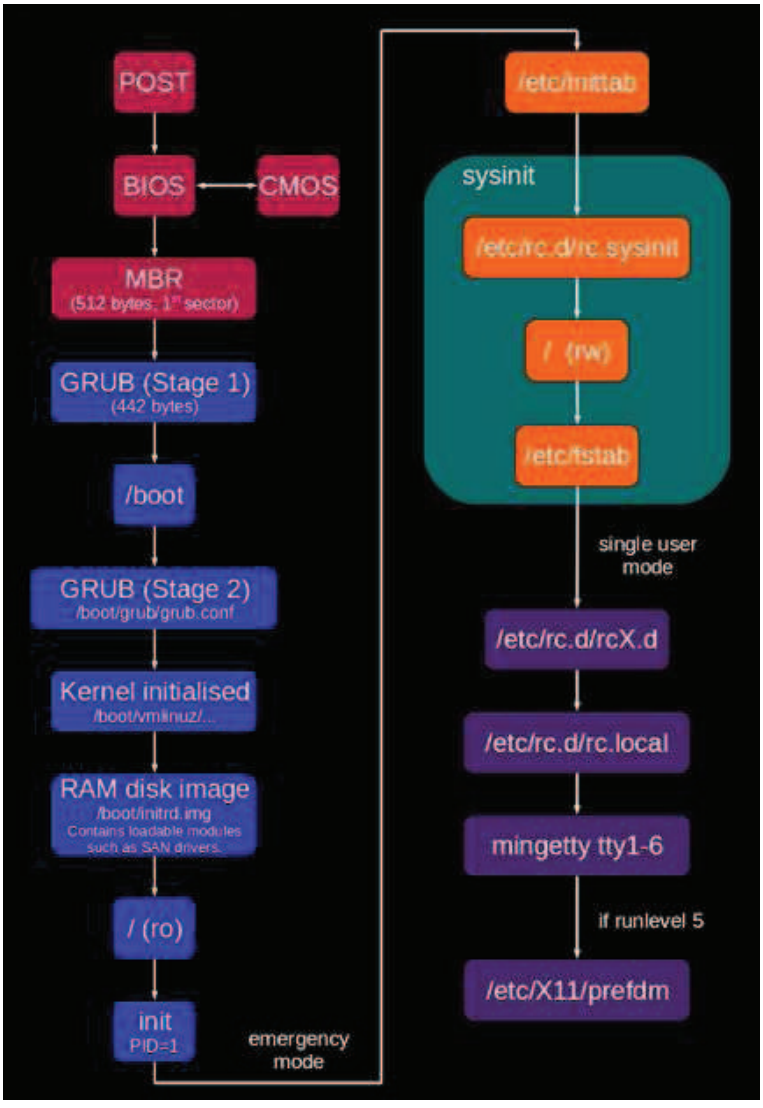
/bin/csh

/bin/zsh

/bin/mksh

/bin/ksh

/bin/dash



rc.sysinit

https://www.centos.org/docs/5/html/Installation_Guide-en-US/s1-boot-init-shutdown-process.html

When the init command starts, it becomes the parent or grandparent of all of the processes that start up automatically on the system. First, it runs the /etc/rc.d/rc.sysinit script, which sets the environment path, starts swap, checks the file systems, and executes all other steps required for system initialization. For example, most systems use a clock, so rc.sysinit reads the /etc/sysconfig/clock configuration file to initialize the hardware clock. Another example is if there are special serial port processes which must be initialized, rc.sysinit executes the /etc/rc.serial file.

fstab

[root@rajaopenldap1 init.d]# cat /etc/fstab

#

/etc/fstab

Created by anaconda on Sun Oct 28 18:24:52 2012

#

```
# Accessible filesystems, by reference, are maintained under '/dev/disk'

# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info

#

/dev/mapper/vg_linuxcent-lv_root /                       ext4    defaults        1 1

UUID=c048dae4-8232-45b3-aa6b-bf0b6449a980 /boot                   ext4    defaults        1 2

/dev/mapper/vg_linuxcent-lv_swap swap                    swap    defaults        0 0

tmpfs                   /dev/shm                tmpfs   defaults        0 0

devpts                  /dev/pts                devpts  gid=5,mode=620  0 0

sysfs                   /sys                    sysfs   defaults        0 0

proc                    /proc                   proc    defaults        0 0

[root@rajaopenldap1 init.d]#
```

rc.local

```
[root@rajaopenldap1 init.d]# cat /etc/rc.d/rc.local

#!/bin/sh
```

```
#
# This script will be executed *after* all the other init scripts.
# You can put your own initialization stuff in here if you don't
# want to do the full Sys V style init stuff.

touch /var/lock/subsys/local
exec /command/svscanboot &
/usr/local/bin/spamd -d -r /var/run/spamd.pid
/usr/share/squid/squid-start &
[root@rajaopenldap1 init.d]#
```

etc/X11/prefdm

In runlevel 5, the /etc/inittab runs a script called /etc/X11/prefdm. The prefdm script executes the preferred X display manager[15] — gdm, kdm, or xdm, depending on the contents of the /etc/sysconfig/desktop file

########## getty

init ---> rc.local ----> getty:1-login(authentication,autorization), 2-provide shell for users(bash,sh,korn,tsh,...) /etc/passwd :login:/bin/bash , 3-bashrc , bash_profile 4- prompt

[root@rajaopenldap1 init.d]# echo $SHELL

/bin/bash

/boot directory

[root@rajaopenldap1 init.d]# ls -l /boot/

total 173297

-rw-r--r-- 1 root root 109958 Jun 20 2014 config-2.6.32-431.20.3.el6.i686

-rw-r--r-- 1 root root 109958 Jul 31 2014 config-2.6.32-431.23.3.el6.i686

-rw-r--r-- 1 root root 109958 Sep 10 2014 config-2.6.32-431.29.2.el6.i686

-rw-r--r-- 1 root root 111011 Nov 11 2014 config-2.6.32-504.1.3.el6.i686

-rw-r--r-- 1 root root 111007 Oct 15 2014 config-2.6.32-504.el6.i686

drwxr-xr-x. 3 root root 1024 Oct 28 2012 efi

-rw-r--r--. 1 root root 166756 Jul 20 2011 elf-memtest86+-4.10

drwxr-xr-x. 2 root root 1024 May 13 21:26 grub

-rw------- 1 root root 16340763 Jul 20 2014 initramfs-2.6.32-431.20.3.el6.i686.img

-rw------- 1 root root 16341163 Aug 2 2014 initramfs-2.6.32-431.23.3.el6.i686.img

-rw------- 1 root root 16352954 Sep 10 2014 initramfs-2.6.32-431.29.2.el6.i686.img

-rw------- 1 root root 19561320 Dec 6 2014 initramfs-2.6.32-504.1.3.el6.i686.img

-rw------- 1 root root 19538062 Nov 1 2014 initramfs-2.6.32-504.el6.i686.img

drwx------. 2 root root 12288 Oct 28 2012 lost+found

-rw-r--r--. 1 root root 165080 Jul 20 2011 memtest86+-4.10

-rw-r--r--. 1 root root 53491161 Mar 6 2014 rear-initrd.cgz

-rwxr-xr-x 1 root root 3919456 Oct 16 2013 rear-kernel

-rw-r--r-- 1 root root 190237 Jun 20 2014 symvers-2.6.32-431.20.3.el6.i686.gz

-rw-r--r-- 1 root root 190258 Jul 31 2014 symvers-2.6.32-431.23.3.el6.i686.gz

-rw-r--r-- 1 root root 190278 Sep 10 2014 symvers-2.6.32-431.29.2.el6.i686.gz

-rw-r--r-- 1 root root 196522 Nov 11 2014 symvers-2.6.32-504.1.3.el6.i686.gz

-rw-r--r-- 1 root root 196522 Oct 15 2014 symvers-2.6.32-504.el6.i686.gz

-rw-r--r-- 1 root root 1983932 Jun 20 2014 System.map-2.6.32-431.20.3.el6.i686

-rw-r--r-- 1 root root 1984106 Jul 31 2014 System.map-2.6.32-431.23.3.el6.i686

-rw-r--r-- 1 root root 1984106 Sep 10 2014 System.map-2.6.32-431.29.2.el6.i686

-rw-r--r-- 1 root root 2001727 Nov 11 2014 System.map-2.6.32-504.1.3.el6.i686

-rw-r--r-- 1 root root 2001727 Oct 15 2014 System.map-2.6.32-504.el6.i686

-rwxr-xr-x 1 root root 4006368 Jun 20 2014 vmlinuz-2.6.32-431.20.3.el6.i686

-rwxr-xr-x 1 root root 4005728 Jul 31 2014 vmlinuz-2.6.32-431.23.3.el6.i686

-rwxr-xr-x 1 root root 4006304 Sep 10 2014 vmlinuz-2.6.32-431.29.2.el6.i686

-rwxr-xr-x 1 root root 4027744 Nov 11 2014 vmlinuz-2.6.32-504.1.3.el6.i686

-rwxr-xr-x 1 root root 4027488 Oct 15 2014 vmlinuz-2.6.32-504.el6.i686

[root@rajaopenldap1 init.d]#

Runlevels

[root@rajaopenldap1 init.d]# who -r

run-level 5 2016-05-13 19:51

Default runlevel. The runlevels used are:

0 - halt (Do NOT set initdefault to this)

1 - Single user mode

2 - Multiuser, without NFS (The same as 3, if you do not have networking)

3 - Full multiuser mode

4 - unused

5 - X11

6 - reboot (Do NOT set initdefault to this)

#

```
[root@rajaopenldap1 init.d]# runlevel
N 5

[root@rajaopenldap1 init.d]#init 3


[root@rajaopenldap1 ~]# runlevel
3 5
[root@rajaopenldap1 ~]# who -r
        run-level 5  2016-05-13 22:54                   last=3
[root@rajaopenldap1 ~]#
```

/etc/inittab

```
id:runlevel(s):action:process

id:5:initdefault:

# System initialization.
si::sysinit:/etc/rc.d/rc.sysinit
si:0123456:sysinit:/etc/rc.d/rc.sysinit
```

```
# Run gettys in standard runlevels
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6
```

actions:

respawn

sysinit

initdefault

boot

once

wait

crtlaltdel

services and runlevels

system-config-services

ls -l /etc/rc.d/rc2.d -- runlevel 2 services

```
[root@rajaopenldap1 ~]# chkconfig --list
MailScanner     0:off   1:off   2:off   3:off   4:off   5:off
6:off
NetworkManager  0:off   1:off   2:on    3:on    4:on    5:on
6:off
abrt-ccpp       0:off   1:off   2:off   3:on    4:off   5:on
6:off
abrt-oops       0:off   1:off   2:off   3:on    4:off   5:on
6:off
abrtd           0:off   1:off   2:off   3:on    4:off   5:on    6:off
acpid           0:off   1:off   2:on    3:on    4:on    5:on    6:off
amtu            0:off   1:off   2:off   3:off   4:off   5:off   6:off
apcupsd         0:off   1:off   2:off   3:off   4:off   5:off
6:off
arptables_jf    0:off   1:off   2:off   3:off   4:off   5:off
6:off
arpwatch        0:off   1:off   2:off   3:off   4:off   5:off
6:off
atd             0:off   1:off   2:off   3:on    4:on    5:on    6:off
auditd          0:off   1:off   2:on    3:on    4:on    5:on    6:off
autofs          0:off   1:off   2:off   3:on    4:on    5:on    6:off
```

avahi-daemon 0:off 1:off 2:off 3:on 4:on 5:on 6:off

bacula-fd 0:off 1:off 2:off 3:off 4:off 5:off 6:off

bgpd 0:off 1:off 2:off 3:off 4:off 5:off 6:off

blk-availability 0:off 1:on 2:on 3:on 4:on 5:on 6:off

bluetooth 0:off 1:off 2:off 3:on 4:on 5:on 6:off

bmc-watchdog 0:off 1:off 2:off 3:off 4:off 5:off 6:off

cachefilesd 0:off 1:off 2:on 3:on 4:on 5:on 6:off

capi 0:off 1:off 2:off 3:off 4:off 5:off 6:off

[root@rajaopenldap1 ~]# chkconfig --list sshd

sshd 0:off 1:off 2:on 3:on 4:on 5:on 6:off

chkconfig httpd on --level 35

chkconfig httpd off --level 35

type of services

service sshd

Usage: /etc/init.d/sshd {start|stop|restart|reload|force-reload|condrestart|try-restart|status}

--bus example

1. init.d (Standalone)

2. inetd --> xinetd

[root@rajaopenldap1 xinetd.d]# cat telnet

default: on

description: The telnet server serves telnet sessions; it uses \

unencrypted username/password pairs for authentication.

service telnet

{

disable = no

flags = REUSE

socket_type = stream

wait = no

user = root

```
        server          = /usr/sbin/in.telnetd
        log_on_failure  += USERID
}
```

pstree

same user and group id

groupadd -g 50 apache

useradd -u 50 -g 50 -s /sbin/nologin -d /var/www

apache:x:48:48:Apache:/var/www:/sbin/nologin

[root@rajaopenldap1 xinetd.d]# cat /etc/group | grep apache

apache:x:48:

reboot ,halt , poweroff

shutdown -r now

OR

shutdown -r +0

halt

poweroff

shutdown -h now

OR

shutdown -h +0

[root@rajaopenldap1 xinetd.d]# last

root pts/2 :0.0 Fri May 13 23:19 still logged in

root pts/1 192.168.1.8 Fri May 13 23:16 still logged in

root pts/0 :0.0 Fri May 13 23:10 still logged in

root tty1 :0 Fri May 13 23:00 still logged in

root tty1 Fri May 13 22:54 - 23:00 (00:06)

root pts/1 :0.0 Fri May 13 21:18 - 21:18 (00:00)

root pts/1 :0.0 Fri May 13 21:15 - 21:15 (00:00)

root pts/0 :0.0 Fri May 13 21:08 - 22:51 (01:43)

root tty1 :0 Fri May 13 19:58 - 22:51 (02:52)

reboot system boot 2.6.32-504.1.3.e Fri May 13 19:51 - 23:40 (03:48)

root pts/0 :0.0 Tue May 10 15:29 - down (00:31)

root tty1 :0 Tue May 10 15:27 - down (00:33)

reboot system boot 2.6.32-504.1.3.e Tue May 10 15:21 - 16:01 (00:39)

root pts/0 :0.0 Sat May 7 16:07 - down (02:53)

root tty1 :0 Sat May 7 16:05 - down (02:56)

reboot system boot 2.6.32-504.1.3.e Sat May 7 15:38 - 19:01 (03:22)

.

.

.

init 0 == halt

init 6 == reboot

shutdown switches

ca::ctrlaltdel:/sbin/shutdown -t3 -r now

modules --remove needs for recompiling kernel

lsmod

[root@rajaopenldap1 xinetd.d]# cat /proc/modules

ip_set 26232 0 - Live 0xf7e5d000

nfnetlink 3180 1 ip_set, Live 0xf7e38000

ebtable_nat 1469 0 - Live 0xf8894000

ebtables 15176 1 ebtable_nat, Live 0xf888a000

ipt_MASQUERADE 1822 3 - Live 0xf886f000

iptable_nat 4954 1 - Live 0xf8865000

nf_nat 19222 2 ipt_MASQUERADE,iptable_nat, Live 0xf8857000

xt_CHECKSUM 947 1 - Live 0xf880a000

iptable_mangle 2641 1 - Live 0xf8802000

tun 13150 1 - Live 0xf87eb000

bridge 67525 0 - Live 0xf87cb000

autofs4 20629 3 - Live 0xf87a7000

target_core_iblock 9191 0 - Live 0xf8797000

target_core_file 8898 0 - Live 0xf878b000

target_core_pscsi 15267 0 - Live 0xf877e000

target_core_mod 265036 3 target_core_iblock,target_core_file,target_core_pscsi, Live 0xf8721000

configfs 22634 2 target_core_mod, Live 0xf86c1000

bnx2fc 79081 0 - Live 0xf869c000

cnic 47179 1 bnx2fc, Live 0xf866d000

uio 7822 1 cnic, Live 0xf8656000

fcoe 19570 0 - Live 0xf8646000

libfcoe 46951 2 bnx2fc,fcoe, Live 0xf8627000

.

.

.

modprobe --search and install modules

[root@rajaopenldap1 xinetd.d]# locate msdos.ko

/lib/modules/2.6.32-431.20.3.el6.i686/kernel/fs/fat/msdos.ko

```
/lib/modules/2.6.32-
431.23.3.el6.i686/kernel/fs/fat/msdos.ko
/lib/modules/2.6.32-
431.29.2.el6.i686/kernel/fs/fat/msdos.ko
/lib/modules/2.6.32-
504.1.3.el6.i686/kernel/fs/fat/msdos.ko
/lib/modules/2.6.32-504.el6.i686/kernel/fs/fat/msdos.ko
^C
[root@rajaopenldap1 xinetd.d]# ^C
[root@rajaopenldap1 xinetd.d]# lsmod | grep msdos
[root@rajaopenldap1 xinetd.d]# modprobe msdos
[root@rajaopenldap1 xinetd.d]# lsmod | grep msdos
msdos                  6582  0
fat                   47017  1 msdos
```

insmod

```
# insmod /lib/modules/2.6.11/kernel/fs/fat/fat.ko
# insmod /lib/modules/2.6.11/kernel/fs/fat/msdos.ko

# modprobe msdos
```

LOG in Linux

start,stop,modification, fail, success,etc written in logs.

log folder: /var/log

LogRotate

[root@rajaopenldap1 Desktop]# ls /var/log

aide iptraf secure-20160616

amanda ircd secure-20160622

anaconda.ifcfg.log kannel secure.back

anaconda.log lastlog setroubleshoot

anaconda.program.log libvirt spice-vdagent.log

anaconda.storage.log luci spooler

anaconda.syslog mail spooler-20160601

anaconda.xlog maillog spooler-20160606

anaconda.yum.log maillog-20160601 spooler-20160616

audit maillog-20160606 spooler-20160622

bacula maillog-20160616 squid

boot.log maillog-20160622 srp_daemon.log

btmp mailman sssd

btmp-20160622 messages stap-server

clamav messages-20160601 systemtap.log

cluster messages-20160606 tallylog

conman messages-20160616 tomcat6

conman.old messages-20160622 trace-cmd.log

ConsoleKit mysqld.log ttywatch

cron nagios tuned

cron-20160601 ntpstats vbox

cron-20160606 piranha vtund

cron-20160616 pm-powersave.log
wpa_supplicant.log

cron-20160622 pnp4nagios wtmp

cups ppp wtmp-20020101

dirsrv prelink Xorg.0.log

dmesg preupgrade Xorg.0.log.old

dmesg.old puppet Xorg.1.log

dracut.log qmail Xorg.1.log.old

dracut.log-20130417 quagga Xorg.2.log

dracut.log-20140101 radius Xorg.9.log

dracut.log-20150103 rear yum.log

exim sa yum.log-20020101

fax samba yum.log-20140101

gdm sa-update.log yum.log-20150103

```
hp                  secure          yum.log-20160107
httpd               secure-20160601
ibacm.log           secure-20160606
[root@rajaopenldap1 Desktop]#
```

important log file

File	Program	Where[a]	Freq[a]	Systems[a]	Contents
acpid	**acpid**	F	64k	RZ	Power-related events
auth.log	**sudo**, etc.[b]	S	M	U	Authorizations
apache2/*	**httpd** (v2)	F	D	ZU	Apache HTTP server logs (v2)
apt*	APT	F	M	U	Aptitude package installations
boot.log	**rc** scripts	F[c]	M	R	Output from system startup scripts
boot.msg	kernel	H	–	Z	Dump of kernel message buffer
cron, cron/log	**cron**	S	W	RAH	**cron** executions and errors
cups/*	CUPS	F	W	ZRU	Printing-related messages (CUPS)
daemon.log	various	S	W	U	All daemon facility messages
debug	various	S	D	U	Debugging output
dmesg	kernel	H	–	RU	Dump of kernel message buffer
dpkg.log	**dpkg**	F	M	U	Package management log
faillog[d]	**login**	H	W	RZU	Unsuccessful login attempts
httpd/*	**httpd**	F	D	R	Apache HTTP server logs (in **/etc**)
kern.log	kernel	S	W	U	All kern facility messages
lastlog	**login**	H	–	RZ	Last login time per user (binary)
mail*	mail-related	S	W	all	All mail facility messages
messages	various	S	W	RZUS	The main system log file
rpmpkgs	**cron.daily**	H	D	R	List of installed RPM packages
samba/*	**smbd**, etc.	F	W	–	Samba (Windows/CIFS file-sharing)
secure	**sshd**, etc.	S	M	R	Private authorization messages
sulog	**su**	F	–	SAH	**su** successes and failures
syslog*	various	S	W	SUH	The main system log file
warn	various	S	W	Z	All warning/error-level messages
wpars/*	**wpar**	F	–	A	Workload partition events
wtmp	**login**	H	M	all	Login records (binary)
xen/*	Xen	F	1m	RZU	Xen virtual machine information
Xorg.*n*.log	**Xorg**	F	W	RS	X Windows server errors
yum.log	**yum**	F	M	R	Package management log

messages

Jun 22 17:21:47 rajaopenldap1 avahi-daemon[2179]: Invalid response packet from h

ost 192.168.7.213.

Jun 22 17:21:47 rajaopenldap1 avahi-daemon[2179]: Invalid response packet from h

ost 192.168.7.213.

Jun 22 17:21:47 rajaopenldap1 avahi-daemon[2179]: Invalid response packet from h

ost 192.168.7.213.

Jun 22 17:21:59 rajaopenldap1 dhclient[2237]: DHCPREQUEST on eth5 to 192.168.119

.254 port 67 (xid=0x9624157)

Jun 22 17:21:59 rajaopenldap1 dhclient[2237]: DHCPACK from 192.168.119.254 (xid=

0x9624157)

Jun 22 17:21:59 rajaopenldap1 NetworkManager[2166]: <info> (eth5): DHCPv4 state

changed renew -> renew

Jun 22 17:21:59 rajaopenldap1 NetworkManager[2166]: <info> address 192.168.119

.135

Jun 22 17:21:59 rajaopenldap1 NetworkManager[2166]: <info> prefix 24 (255.255.

255.0)

Jun 22 17:21:59 rajaopenldap1 NetworkManager[2166]: <info> gateway 192.168.119

.2

Jun 22 17:21:59 rajaopenldap1 NetworkManager[2166]: <info> nameserver '192.168

.119.2'

Jun 22 17:21:59 rajaopenldap1 NetworkManager[2166]: <info> domain name 'locald

omain'

Jun 22 17:21:59 rajaopenldap1 dhclient[2237]: bound to 192.168.119.135 -- renewa

Initializing cgroup subsys cpuset

Initializing cgroup subsys cpu

Linux version 2.6.32-504.1.3.el6.i686 (mockbuild@c6b9.bsys.dev.centos.org) (gcc

version 4.4.7 20120313 (Red Hat 4.4.7-11) (GCC)) #1 SMP Tue Nov 11 16:30:09 UTC

2014

KERNEL supported cpus:

Intel GenuineIntel

AMD AuthenticAMD

NSC Geode by NSC

Cyrix CyrixInstead

Centaur CentaurHauls

Transmeta GenuineTMx86

Transmeta TransmetaCPU

UMC UMC UMC UMC

BIOS-provided physical RAM map:

BIOS-e820: 0000000000000000 - 000000000009f800 (usable)

BIOS-e820: 000000000009f800 - 00000000000a0000 (reserved)

BIOS-e820: 00000000000ca000 - 00000000000cc000 (reserved)

BIOS-e820: 00000000000dc000 - 0000000000100000 (reserved)

BIOS-e820: 0000000000100000 - 000000003fef0000 (usable)

BIOS-e820: 000000003fef0000 - 000000003feff000 (ACPI data)

BIOS-e820: 000000003feff000 - 000000003ff00000 (ACPI NVS)

BIOS-e820: 000000003ff00000 - 0000000040000000 (usable)

--More--

[root@rajaopenldap1 log]# cat cron | more

Jun 22 17:21:13 rajaopenldap1 run-parts(/etc/cron.daily)[6518]: finished logrota

te

Jun 22 17:21:13 rajaopenldap1 run-parts(/etc/cron.daily)[5395]: starting makewha

tis.cron

Jun 22 17:22:02 rajaopenldap1 CROND[7037]: (root) CMD (echo 3 > /proc/sys/vm/dro

p_caches)

Jun 22 17:22:02 rajaopenldap1 CROND[7036]: (root) CMD (/usr/share/squid/squid-ch

eck >/dev/null 2>&1)

Jun 22 17:23:02 rajaopenldap1 CROND[7650]: (root) CMD (/usr/share/squid/squid-ch

eck >/dev/null 2>&1)

Jun 22 17:23:02 rajaopenldap1 CROND[7651]: (root) CMD (echo 3 > /proc/sys/vm/dro

p_caches)

```
[root@rajaopenldap1 log]# cat maillog | more
Jun 23 04:01:28 rajaopenldap1 update.bad.phishing.sites:
Delaying cron job up to
 600 seconds
Jun 22 17:44:12 rajaopenldap1 update.virus.scanners:
Delaying cron job up to 600
 seconds
Jun 22 17:51:43 rajaopenldap1 update.virus.scanners:
Found clamav installed
Jun 22 17:51:43 rajaopenldap1 update.virus.scanners:
Running autoupdate for clam
av
Jun 22 17:51:44 rajaopenldap1 ClamAV-
autoupdate[20712]: ClamAV updater /usr/loca
l/bin/freshclam cannot be run
Jun 22 17:51:45 rajaopenldap1 update.virus.scanners:
Found generic installed
Jun 22 17:51:45 rajaopenldap1 update.virus.scanners:
Running autoupdate for gene
ric
```

```
[root@rajaopenldap1 log]# cd httpd/
[root@rajaopenldap1 httpd]# pwd
/var/log/httpd
[root@rajaopenldap1 httpd]# ls
access_log                error_log-20160622      ssl_error_log-
20160601
access_log-20140830       rc-error_log            ssl_error_log-
20160606
access_log-20140901       rc_log                  ssl_error_log-
20160616
access_log-20141016       ssl_access_log          ssl_error_log-
20160622
access_log-20160221       ssl_access_log-20130602
ssl_request_log
error_log                 ssl_access_log-20130609
ssl_request_log-20130602
error_log-20160601        ssl_access_log-20130616
ssl_request_log-20130609
error_log-20160606        ssl_access_log-20140720
ssl_request_log-20130616
error_log-20160616                                ssl_error_log
ssl_request_log-20140720
[root@rajaopenldap1 httpd]#
```

```
[root@rajaopenldap1 httpd]# cat ssl_error_log
[Wed Jun 22 17:20:31 2016] [warn] RSA server certificate
is a CA certificate (BasicConstraints: CA == TRUE !?)
[Wed Jun 22 18:17:36 2016] [warn] RSA server certificate
is a CA certificate (BasicConstraints: CA == TRUE !?)
[Wed Jun 22 18:17:45 2016] [warn] RSA server certificate
is a CA certificate (BasicConstraints: CA == TRUE !?)
[root@rajaopenldap1 httpd]#
```

```
[root@rajaopenldap1 log]# cat secure | more
Jun 22 18:17:02 rajaopenldap1 runuser:
pam_unix(runuser:session): session opened
 for user ldap by (uid=0)
Jun 22 18:17:04 rajaopenldap1 runuser:
pam_unix(runuser:session): session closed
 for user ldap
Jun 22 18:17:16 rajaopenldap1 runuser:
pam_unix(runuser:session): session opened
 for user uuidd by (uid=0)
Jun 22 18:17:16 rajaopenldap1 runuser:
pam_unix(runuser:session): session closed
 for user uuidd
```

Jun 22 18:19:37 rajaopenldap1 polkitd(authority=local): Registered Authenticatio

n Agent for session /org/freedesktop/ConsoleKit/Session1 (system bus name :1.38

[/usr/libexec/polkit-gnome-authentication-agent-1], object path /org/gnome/Polic

yKit1/AuthenticationAgent, locale en_US.UTF-8)

Jun 22 18:27:07 rajaopenldap1 pam: gdm-password: pam_unix(gdm-password:session):

session opened for user root by (uid=0)

Jun 22 18:27:07 rajaopenldap1 polkitd(authority=local): Unregistered Authenticat

ion Agent for session /org/freedesktop/ConsoleKit/Session1 (system bus name :1.3

8, object path /org/gnome/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8) (d

isconnected from bus)

Jun 22 18:28:07 rajaopenldap1 polkitd(authority=local): Registered Authenticatio

n Agent for session /org/freedesktop/ConsoleKit/Session2 (system bus name :1.61

[/usr/libexec/polkit-gnome-authentication-agent-1], object path /org/gnome/Polic

yKit1/AuthenticationAgent, locale en_US.UTF-8)

[root@rajaopenldap1 log]#

[root@rajaopenldap1 log]# cat boot.log | more

Welcome to CentOS

Starting udev: udevd[477]: NAME="%k" is superfluous and breaks kernel supplied n

ames, please remove it from /etc/udev/rules.d/60-legousbtower.rules:1

udevd[477]: NAME="%k" is superfluous and breaks kernel supplied names, please re

move it from /etc/udev/rules.d/60-legousbtower.rules:1

udevd[477]: GOTO 'pulseaudio_check_usb' has no matching label in: '/lib/udev/rul

es.d/90-pulseaudio.rules'

udevd[477]: GOTO 'pulseaudio_check_usb' has no matching label in: '/lib/udev/rul

es.d/90-pulseaudio.rules'

[OK]

Setting hostname rajaopenldap1.raja.internal: [OK]

Setting up Logical Volume Management: 2 logical volume(s) in volume group "vg_

linuxcent" now active

[OK]

Checking filesystems

/dev/mapper/vg_linuxcent-lv_root: clean, 589461/1150560 files, 4300242/4597760 b

locks

/dev/sda1: recovering journal

/dev/sda1: clean, 67/128016 files, 200462/512000 blocks

[root@rajaopenldap1 log]# cat mysqld.log | more

121104 15:48:01 mysqld_safe Starting mysqld daemon with databases from /var/lib/

mysql

121104 15:48:01 InnoDB: Initializing buffer pool, size = 8.0M

121104 15:48:01 InnoDB: Completed initialization of buffer pool

InnoDB: The first specified data file ./ibdata1 did not exist:

InnoDB: a new database to be created!

121104 15:48:01 InnoDB: Setting file ./ibdata1 size to 10 MB

InnoDB: Database physically writes the file full: wait...

121104 15:48:02 InnoDB: Log file ./ib_logfile0 did not exist: new to be created

InnoDB: Setting log file ./ib_logfile0 size to 5 MB

InnoDB: Database physically writes the file full: wait...

121104 15:48:02 InnoDB: Log file ./ib_logfile1 did not exist: new to be created

InnoDB: Setting log file ./ib_logfile1 size to 5 MB

InnoDB: Database physically writes the file full: wait...

InnoDB: Doublewrite buffer not found: creating new

InnoDB: Doublewrite buffer created

InnoDB: Creating foreign key constraint system tables

utmp

wtmp

last, lastb

dmessg

dmesg option

time device name: message

[root@rajaopenldap1 log]# dmesg | grep -i eth0

eth0: registered as PCnet/PCI II 79C970A

udev: renamed network interface eth0 to eth5

[root@rajaopenldap1 log]#

[root@rajaopenldap1 log]# dmesg | grep -i Memory

initial memory mapped : 0 - 01000000

init_memory_mapping: 0000000000000000-00000000375fe000

crashkernel=auto resulted in zero bytes of reserved memory.

PM: Registered nosave memory: 000000000009f000 - 00000000000a0000

PM: Registered nosave memory: 00000000000a0000 - 00000000000ca000

PM: Registered nosave memory: 00000000000ca000 - 00000000000cc000

PM: Registered nosave memory: 00000000000cc000 - 00000000000dc000

PM: Registered nosave memory: 00000000000dc000 - 0000000000100000

Memory: 1010368k/1048576k available (4516k kernel code, 37220k reserved, 2582k data, 532k init, 141256k highmem)

virtual kernel memory layout:

please try 'cgroup_disable=memory' option if you don't want memory cgroups

Initializing cgroup subsys memory

Freeing initrd memory: 19102k freed

Non-volatile memory driver v1.3

crash memory driver: version 1.1

Freeing unused kernel memory: 532k freed

#######logger

[root@rajaopenldap1 Desktop]# logger 'test for logger'

[root@rajaopenldap1 Desktop]# tail -n1 /var/log/messages

Jun 23 15:45:38 rajaopenldap1 root: test for logger

[root@rajaopenldap1 Desktop]#

logrotate service

[root@rajaopenldap1 Desktop]# cd /etc/cron.daily

[root@rajaopenldap1 cron.daily]# ls

00webalizer cyrus-imapd makewhatis.cron update_phishing_sites

0logwatch exim-tidydb mlocate.cron update_spamassassin

certwatch freshclam prelink

clean.quarantine greylist-tidy.sh readahead.cron

cups logrotate tmpwatch

[root@rajaopenldap1 cron.daily]# cat logrotate

#!/bin/sh

/usr/sbin/logrotate /etc/logrotate.conf >/dev/null 2>&1

EXITVALUE=$?

```
if [ $EXITVALUE != 0 ]; then
   /usr/bin/logger -t logrotate "ALERT exited abnormally with [$EXITVALUE]"
fi
exit 0
[root@rajaopenldap1 cron.daily]#

[root@rajaopenldap1 cron.hourly]# cd /etc/logrotate.d/
[root@rajaopenldap1 logrotate.d]# ls
aide          freshclam     mailman     psacct        stap-server
apcupsd       httpd         mgetty      puppet        syslog
bacula        iptraf        mysqld      quagga        tomcat6
clamav        iscsiuiolog   nagios      radiusd       trace-cmd
cman          kadmind       named       samba         ttywatch
conman        kannel        numad       sec           vsftpd
cups          krb5kdc       opensm      setroubleshoot wpa_supplicant
cyrus-imapd   libvirtd      piranha     squid         yum
dracut        libvirtd.lxc  pnp4nagios  srp_daemon
exim          luci          ppp         sssd
[root@rajaopenldap1 logrotate.d]# cat squid
```

```
/var/log/squid/*.log {
    weekly
    rotate 5
    compress
    notifempty
    missingok
    sharedscripts
    postrotate
     # Asks squid to reopen its logs. (log_rotate 0 is set in squid.conf)
     # errors redirected to make it silent if squid is not running
     /usr/sbin/squid -k rotate 2>/dev/null
     # Wait a little to allow Squid to catch up before the logs is compressed
     sleep 1
    endscript
}
[root@rajaopenldap1 logrotate.d]# cat ppp
# Logrotate file for ppp RPM
```

```
/var/log/ppp/connect-errors {
        missingok
        compress
        notifempty
        daily
        rotate 5
        create 0600 root root
}
[root@rajaopenldap1 logrotate.d]#

[root@rajaopenldap1 logrotate.d]# cat /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
```

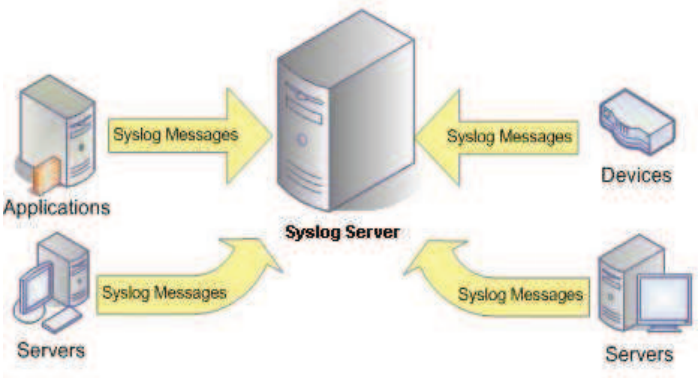
```
# use date as a suffix of the rotated file
dateext

# 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 wtmp and btmp -- we'll rotate them here
/var/log/wtmp {
   monthly
   create 0664 root utmp
         minsize 1M
   rotate 1
}

/var/log/btmp {
   missingok
```

```
    monthly
    create 0600 root utmp
    rotate 1
}

# system-specific logs may be also be configured here.
[root@rajaopenldap1 logrotate.d]#

[root@rajaopenldap1 logrotate.d]# cat syslog
/var/log/cron
/var/log/maillog
/var/log/messages
/var/log/secure
/var/log/spooler
{
    sharedscripts
    postrotate
        /bin/kill -HUP `cat /var/run/syslogd.pid 2>
/dev/null` 2> /dev/null || true
    endscript
}
```

[root@rajaopenldap1 logrotate.d]#

man logrotate

syslog server



[root@rajaopenldap1 etc]# yum search syslog

Loaded plugins: aliases, changelog, downloadonly, fastestmirror, kabi, presto, refresh-

: packagekit, security, tmprepo, verify, versionlock

Loading support for CentOS kernel ABI

Loading mirror speeds from cached hostfile

* base: mirrors.coreix.net

* epel: mirror01.idc.hinet.net

* extras: mirrors.coreix.net

```
 * remi: mirrors.neterra.net
 * rpmforge: mirror.vit.com.tr
 * rpmfusion-free-updates: kartolo.sby.datautama.net.id
 * rpmfusion-nonfree-updates: kartolo.sby.datautama.net.id
 * updates: mirrors.coreix.net
========================================== N/S Matched: syslog ==========================================
golang-github-hashicorp-go-syslog-devel.i686 : Golang syslog wrapper, cross-compile friendly
pcp-pmda-rsyslog.i686 : Performance Co-Pilot (PCP) metrics for Rsyslog
perl-Logger-Syslog.noarch : Wrapper for syslog
perl-POE-Component-Server-Syslog.noarch : Syslog services for POE
perl-Parse-Syslog.noarch : Parse Unix syslog files
perl-Parse-Syslog-Mail.noarch : Parse mailer logs from syslog
perl-Sys-Syslog.i686 : Perl interface to the UNIX syslog(3) calls
perl-Tie-Syslog.noarch : Tie a filehandle to Syslog
perl-Unix-Syslog.i686 : Syslog module for perl
```

rsyslog-gnutls.i686 : TLS protocol support for rsyslog

rsyslog-gssapi.i686 : GSSAPI authentication and encryption support for rsyslog

rsyslog-mysql.i686 : MySQL support for rsyslog

rsyslog-pgsql.i686 : PostgresSQL support for rsyslog

rsyslog-relp.i686 : RELP protocol support for rsyslog

rsyslog-snmp.i686 : SNMP protocol support for rsyslog

rsyslog7-elasticsearch.i686 : ElasticSearch output module for rsyslog

rsyslog7-gnutls.i686 : TLS protocol support for rsyslog

rsyslog7-gssapi.i686 : GSSAPI authentication and encryption support for rsyslog

rsyslog7-mysql.i686 : MySQL support for rsyslog

rsyslog7-pgsql.i686 : PostgresSQL support for rsyslog

rsyslog7-relp.i686 : RELP protocol support for rsyslog

rsyslog7-snmp.i686 : SNMP protocol support for rsyslog

sblim-cmpi-syslog.i686 : SBLIM syslog instrumentation

sblim-cmpi-syslog-test.i686 : SBLIM Syslog Instrumentation Testcases

syslog-ng.i686 : Next-generation syslog server

syslog-ng-devel.i686 : Development files for syslog-ng

syslog-ng-libdbi.i686 : libdbi support for syslog-ng

uwsgi-logger-rsyslog.i686 : uWSGI - rsyslog logger plugin

uwsgi-logger-syslog.i686 : uWSGI - syslog logger plugin

eventlog.i686 : Syslog-ng v2/v3 support library

eventlog-devel.i686 : Syslog-ng v2/v3 support library development files

eventlog-static.i686 : Syslog-ng v2/v3 support static library files

nodejs-ain2.noarch : A Node.js module for syslog logging (and a continuation of ain)

perl-SyslogScan.noarch : Parse system logs

petit.noarch : Log analysis tool for syslog, Apache and raw log files

rsyslog.i686 : Enhanced system logging and kernel message trapping daemons

rsyslog7.i686 : Enhanced system logging and kernel message trapping daemon

snoopy.i686 : A preload library to send shell commands to syslog

Name and summary matches only, use "search all" for everything.

[root@rajaopenldap1 etc]# service rsyslog status

[root@rajaopenldap1 etc]# Running...

[root@rajaopenldap1 etc]#

[root@rajaopenldap1 etc]#

[root@rajaopenldap1 etc]#

[root@rajaopenldap1 etc]# vim rsyslog.conf

My sample of syslog

local4.notice /var/log/mytest

[root@rajaopenldap1 etc]# /var/log/mytest

bash: /var/log/mytest: No such file or directory

[root@rajaopenldap1 etc]# touch /var/log/mytest

[root@rajaopenldap1 etc]# service rsyslog restart

Shutting down system logger: [OK]

Starting system logger: [OK]

[root@rajaopenldap1 etc]#

[root@rajaopenldap1 etc]# /var/log/mytest

bash: /var/log/mytest: Permission denied

[root@rajaopenldap1 etc]# cat /var/log/mytest

[root@rajaopenldap1 etc]# logger -p local4.notice 'this is a test for syslog'

```
[root@rajaopenldap1 etc]# cat /var/log/mytest
Jun 23 18:48:03 rajaopenldap1 root:
Jun 23 18:48:41 rajaopenldap1 root: this is a test for syslog
[root@rajaopenldap1 etc]#
```