when linux system starts it starts with pid 1 or systemd

many of these process started as daemons(which run as background processes they are just listening and waiting for incoming connections

They are started from systemd and one of the process started by systemd is bash its a login environment where user can enter and when user launches commands they always known as process. Every thing you run on linux box is process and all these processes have process id(pid)

When user launches from bash environment it is specific case of processes and they are called JOBS

users should have access to manage his own jobs and that is why user can manage these jobs from shell, using jobs command

if we are talking about jobs we are talking about specific jobs launched by specific user

Kernel threat is a process started by kernel and you can see it on process list

jobs --- to list all the jobs

sleep 50 & -- bg

sleep 50 --fg

to come out ctrl+z

fg 1(job no)

ps -- you can list the processes related to your account

sample output

```
  PID TTY          TIME CMD
49042 pts/0    00:00:00 su
```

ps aux | head

```
[root@server10 ~]# ps aux | head
USER        PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root          1  0.0  0.5 126556  5816 ?        Ss   14:06   0:02 /usr/lib/systemd/systemd --switched-root --system
 --deserialize 21
root          2  0.0  0.0      0     0 ?        S    14:06   0:00 [kthreadd]
root          3  0.0  0.0      0     0 ?        S    14:06   0:00 [ksoftirqd/0]
root          7  0.0  0.0      0     0 ?        S    14:06   0:00 [migration/0]
root          8  0.0  0.0      0     0 ?        S    14:06   0:00 [rcu_bh]
root          9  0.0  0.0      0     0 ?        S    14:06   0:00 [rcuob/0]
root         10  0.0  0.0      0     0 ?        S    14:06   0:00 [rcuob/1]
root         11  0.0  0.0      0     0 ?        S    14:06   0:00 [rcuob/2]
root         12  0.0  0.0      0     0 ?        S    14:06   0:00 [rcuob/3]
[root@server10 ~]#
```

TTY ? IS FOR BACKGROUND PROCESSES

STATUS S = SLEEPING

ps aux | grep syslog

syslog is generic log daemon which takes care of the logging of the system

ps -ef | head

```
[root@server10 ~]# ps -ef | head
UID         PID   PPID  C STIME TTY          TIME CMD
root          1      0  0 14:06 ?        00:00:02 /usr/lib/systemd/systemd --switched-root --system --deserialize 2
1
root          2      0  0 14:06 ?        00:00:00 [kthreadd]
root          3      2  0 14:06 ?        00:00:00 [ksoftirqd/0]
root          7      2  0 14:06 ?        00:00:00 [migration/0]
root          8      2  0 14:06 ?        00:00:00 [rcu_bh]
root          9      2  0 14:06 ?        00:00:00 [rcuob/0]
root         10      2  0 14:06 ?        00:00:00 [rcuob/1]
root         11      2  0 14:06 ?        00:00:00 [rcuob/2]
root         12      2  0 14:06 ?        00:00:00 [rcuob/3]
[root@server10 ~]#
```

ps fax --- used to see parent child relations in graphical way

Understanding Memory Usage

m

Many server do not have enough RAM Memory. Solution to use RAM in smart way is swap. Swap is a memory that can be addressed by linux kernel as RAM but it is on HARDDISK and the result is slow.

Linux has two memories active/inactive memory the process which are not active is moved to swap(inactive memory) that makes linux memory usage bit more efficient

Cache

Cache is important to speed up linux system, the idea behind this is when user request file from harddisk the file is placed in RAM and that's take lot of time even for fast ssd harddisks for that reason linux tries to keep the file in CACHE as long as possible.

For cache also linux applies active/inactive memory

Free -m

```
[root@server10 ~]# free -m
              total        used        free      shared  buff/cache   available
Mem:            977         589          72           5         316         148
Swap:          2047          11        2036
[root@server10 ~]#
```

Cat /proc/meminfo

```
HugePages_Free:        0
HugePages_Rsvd:        0
HugePages_Surp:        0
Hugepagesize:       2048 kB
DirectMap4k:       94080 kB
DirectMap2M:      954368 kB
[root@server10 ~]# grep ctive /proc/meminfo
Active:           299164 kB
Inactive:         304680 kB
Active(anon):     241000 kB
Inactive(anon):   251760 kB
Active(file):      58164 kB
Inactive(file):    52920 kB
[root@server10 ~]#
```

Understanding Performance Load

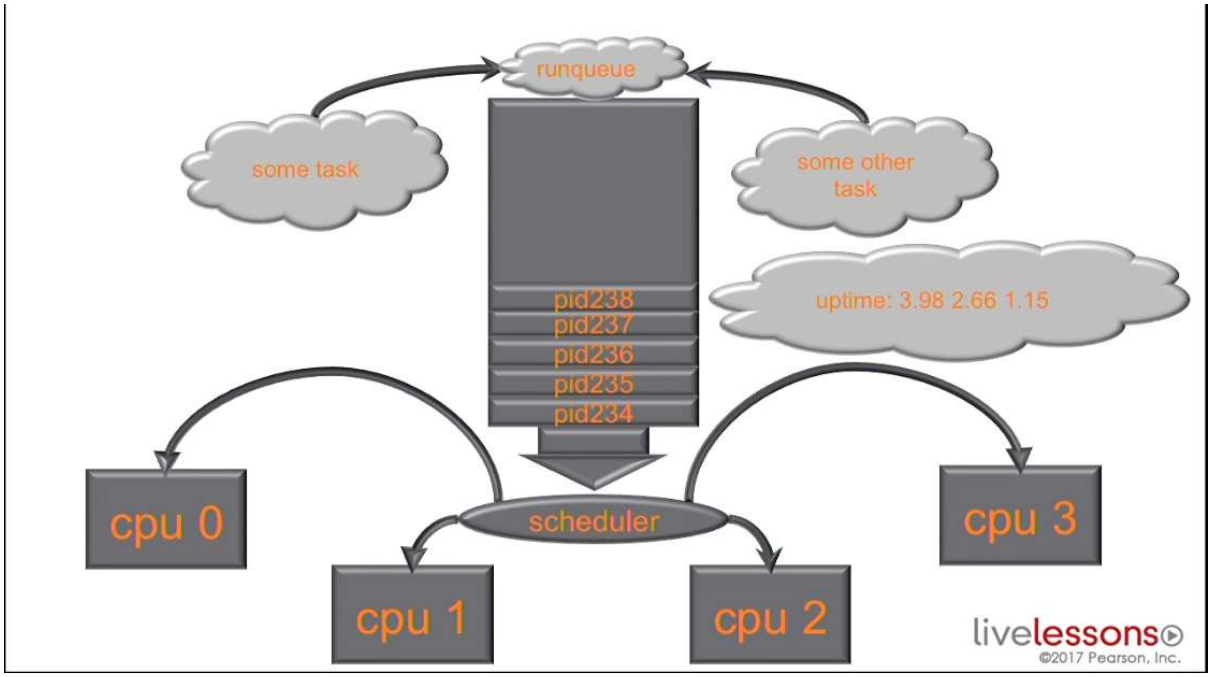
Runqueue is part of linux kernel which is taking care runnable tasks

Scheduler is also kernel component

Scheduler places the pid in diff cpu cores

Performance load parameters can be requested using

Uptime cmd



Uptime : 3.98 2.05 1.05 these are values of load for last 1 min, 5 min, 15 min these values depends on no of cpus. In this case server cpu=4 in last one min the system is very busy using almost 4 cpus

3.98 indicates temporary peak in last 1 min

```
[root@server10 ~]# uptime
 16:19:44 up  2:13,  2 users,  load average: 0.03, 0.04, 0.06
[root@server10 ~]#
```

lscpu | less ---- give the information no of cpus

Monitoring system activity with top cmnd

Zombie process are process lost connection with parent processes

Kill -9 pid --- to kill the process not nicely(wont clear the screen)

Kill -15 pid --- to kil the process nicely(clear the screen)

Pidof dd – easy way to find pids

Kill pid --- to stop the process

Killall processname

Understanding priorities and niceness

RealTime Process- these processes have high priority they are generally called as kernel threats processes

Normal Process: these process have priority numbers ex 20 30

Nice: it is used to change the priority of the processes by its range -20 to 19 in linux lower the number higher the priority

As an admin RealTime process are not dealed because they all are happening internal space

Only root user can increase the priorities and normal users decrease the priorities

renice -5 pid

renice 5 pid