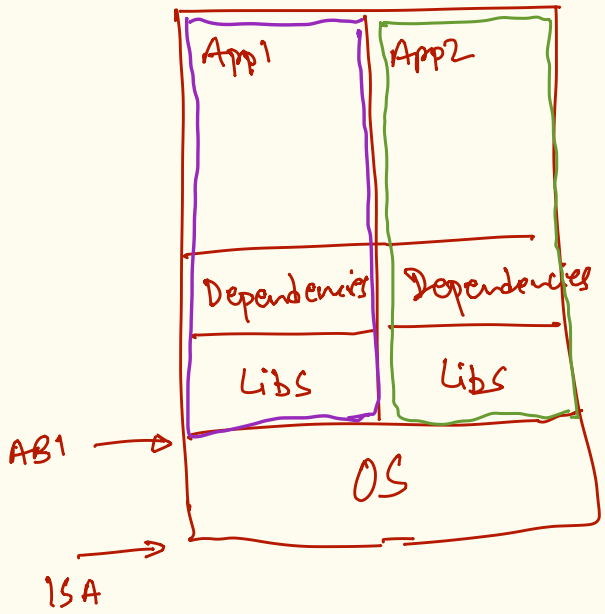
CS 744 Lecture 25

containerization

- namespaces — mechanism to isolate/restrict view/access to system resources objects.
- cgroups — "limit" usage of resources deterministic
- chroot / image files — setup repository of fs dependencies.
- capabilities. — restrict the actions/services that appl^n^s. are allowed.

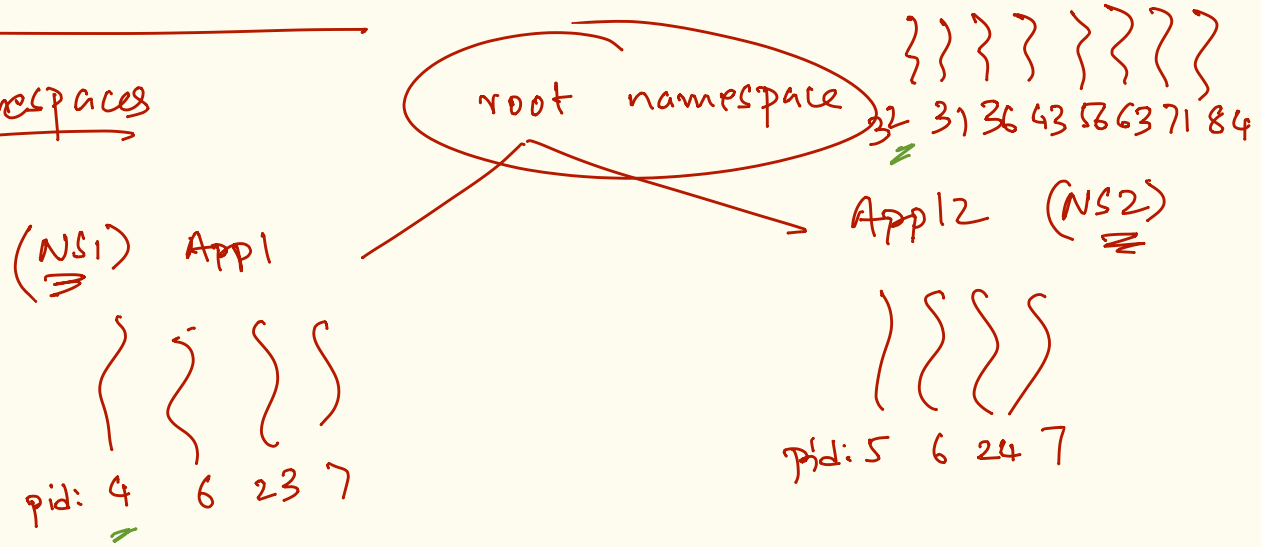


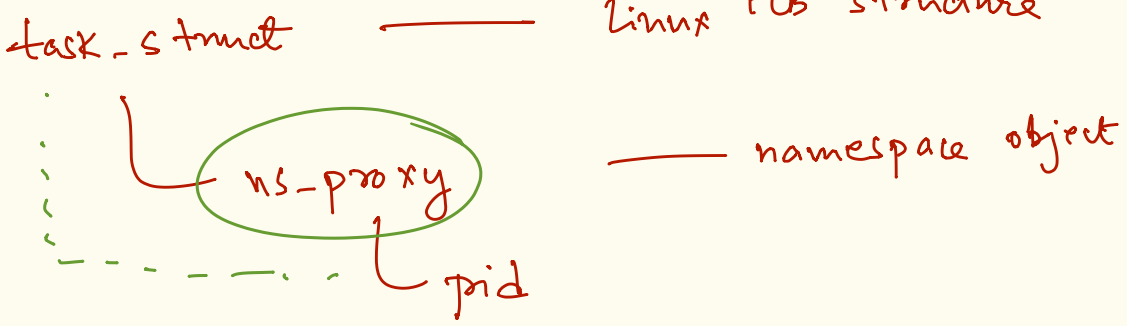
* traditionally, the OS enables the "process-view".

* application-view (group of processes & resources)
  - set of processes of the appl^n.
  - set of tools / files / mount points / devices
  - dependencies
  - n/w endpoints (IP addr, ...)

---

* namespaces





typical Linux namespaces —

- pid
- mount
- proc
- time
- uts
- net
- ipc

system calls / syscall arguments to set/store/use namespaces.

- eg: fork — clone
  - arguments
    - NEW_UTS
    - NEW_PID
    - NEW_USER
  - via system call args.
- unshare — enters NS of a existing process
- setns — sets/ NS of a process

② cgroup — control group — of processes.

resources of

resources

- memory —
- cpu — access, how much?
- network
- mount, files, disk

- every process - belongs to a cgroup.

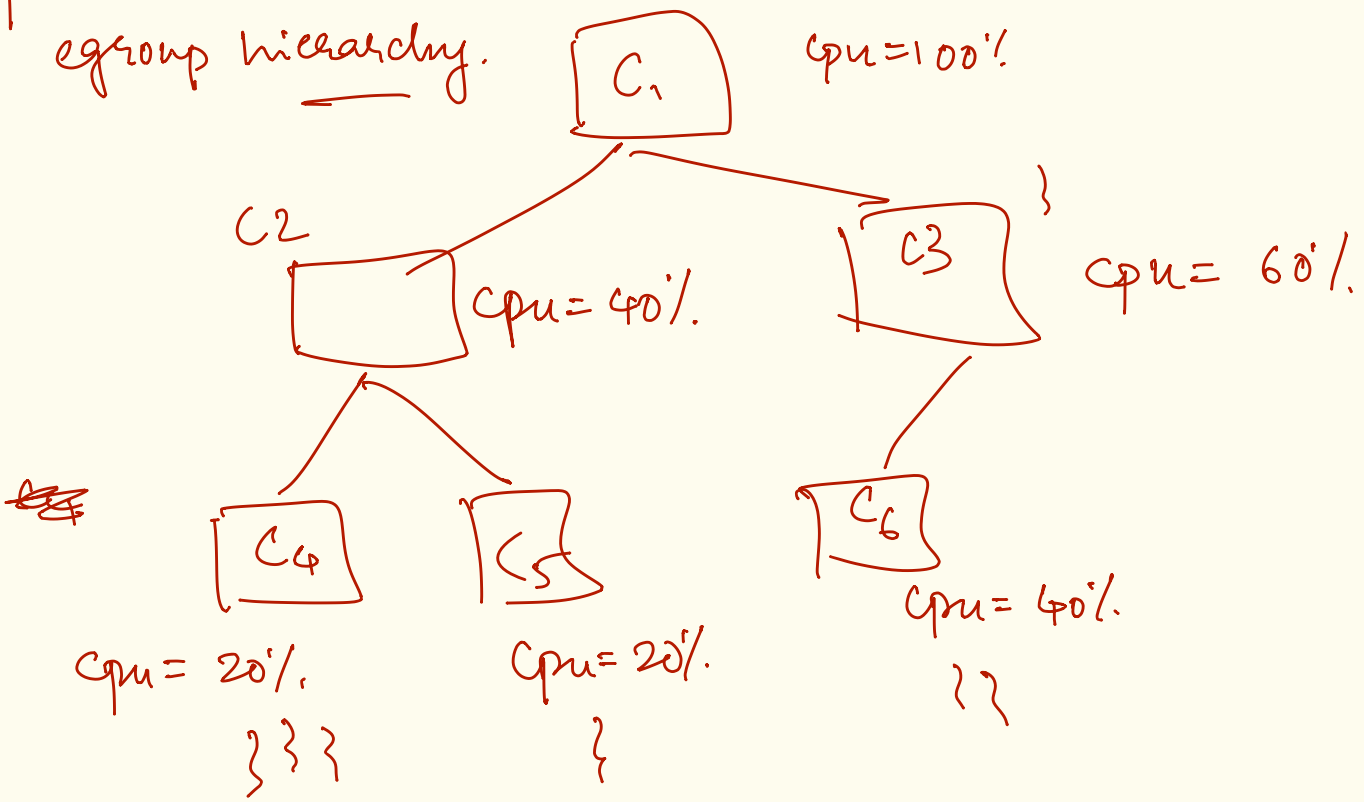
- all OS resource actions are modulo resource limit & access settings.

task_struct

css_set ~ points to cgroup object that this proces belongs to.

cgroup
cgroup_subsys } structs of (Linux) OS of accounting & usage..

per resource cgroup hierarchy.



③ ldd — list dynamic dependencies.

ldd
- lists the (shared) object / library dependencies required by a program.
- a program / application to execute has to have these dependencies available at the default / listed path for its loading.

chroot
- a (UNIX) mechanism / tool that changes the (working) root directory to a specified path.
- all new executions treat specified path as root.

---

chroot + ldd : enable a localized file & file directories "namespace", which can store all dependencies relative to a local / per app path.

- each such bundle is a complete set of files w/ correct directory ordering relative to root directory
  - a simple, per-application image. (file).
    container

⊛ Dockerfile is a file that contains instructions to create a Docker container image.

⊛ docker uses the image file along with the tools ldd, chroot, namespaces, cgroup to create / execute a container!