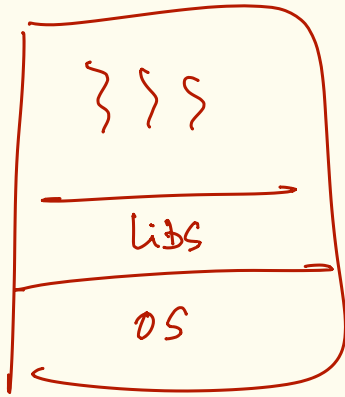
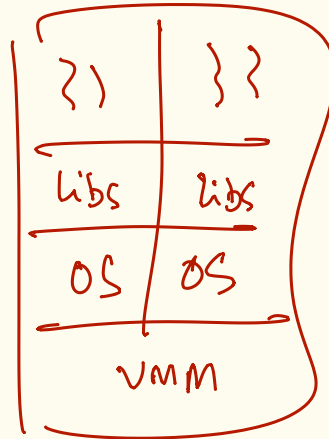
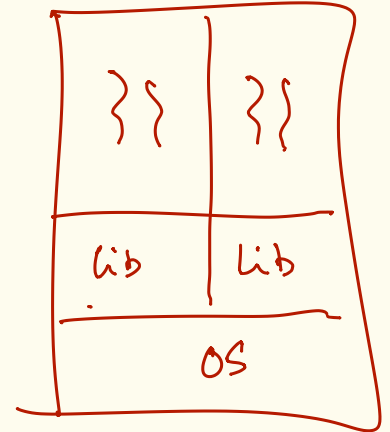


Containers

process-view

system-view
w/
VMsprocess-group
abstraction

⊗ application-view

↖ (container)

- ~ root fs
- ~ dependencies - libraries & tools
- ~ device endpoints
- ~ resources ~~isolation~~ layout

4 main primitives that support containers.-

- (i) namespaces
- (ii) cgroups
- (iii) chroot & image file / FS
- (iv) capabilities & secure computing

(i) namespaces

~ is a (linux) mechanism to provide isolated views of system resources/objects.

~ process namespace

↳ NS1 ~ pid 11, 23, 46, 87

NS2 ~ pid 11, 43, 84, 87,
5

~ typical linux namespaces

~ pid

~ mount

~ proc

~ time

~ uts

~ net

~ user

~ ipc

usage / access

- new system calls /
system call flags

e.g: fork - clone

NEWPID

NEWUSER

NEWUTS

~ unshare ~ change ^{to} the
NS of a

~ ~~new~~

process
& execute
commands