

Architecture Masterclass



Nigel Poulton

Author & Trainer

@nigelpoulton | www.nigelpoulton.com

Waffle waffle waffle...



Overview/ Summary



Docker Architecture: Big Picture

Kernel Internals

Docker Magic

Containers on Windows

Recap



Up Next:

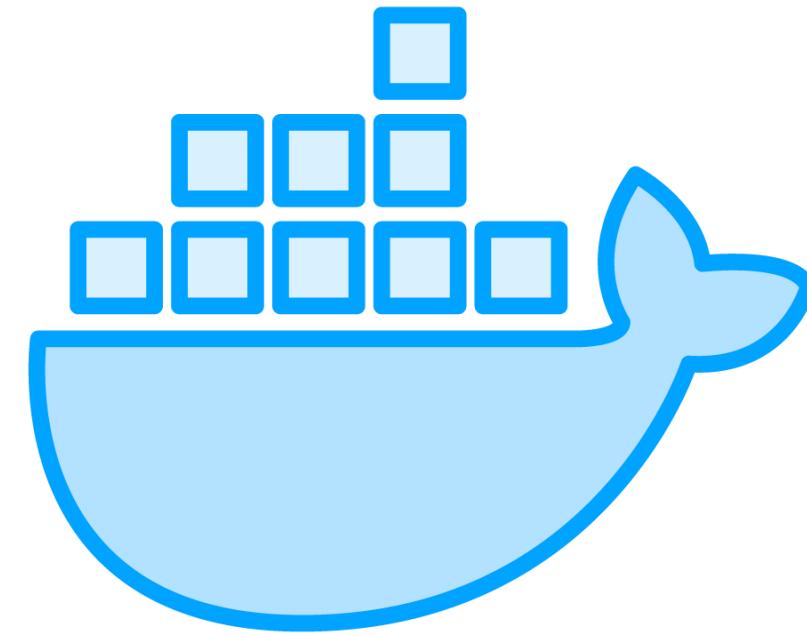
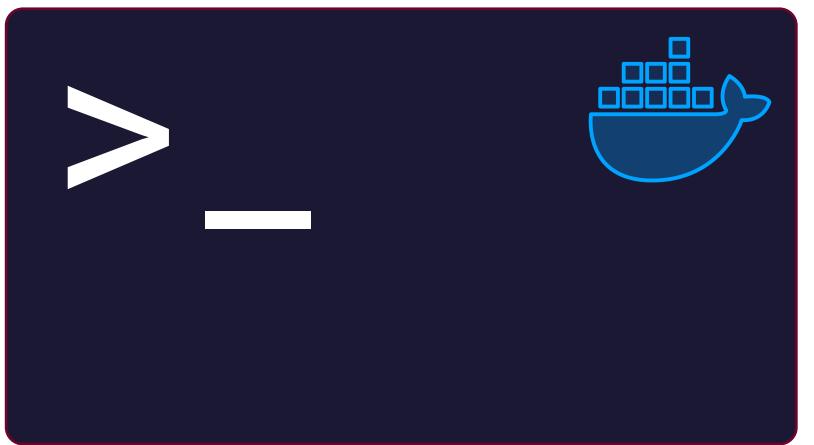
Docker Architecture: Big Picture



Docker Architecture: Big Picture





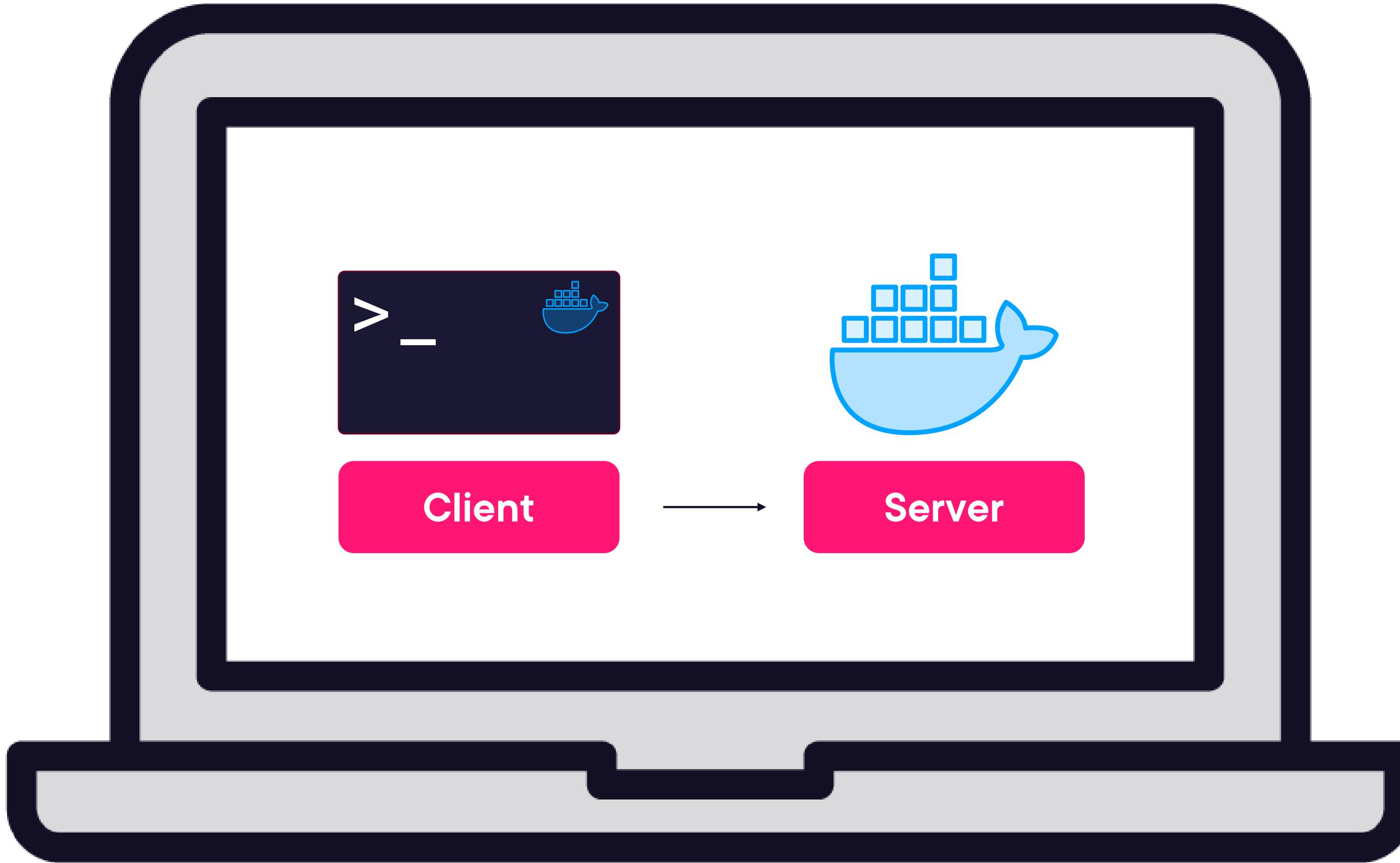


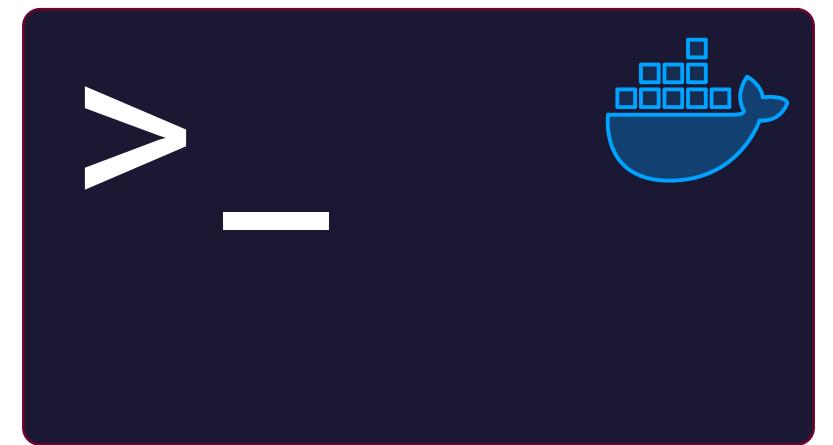
Client



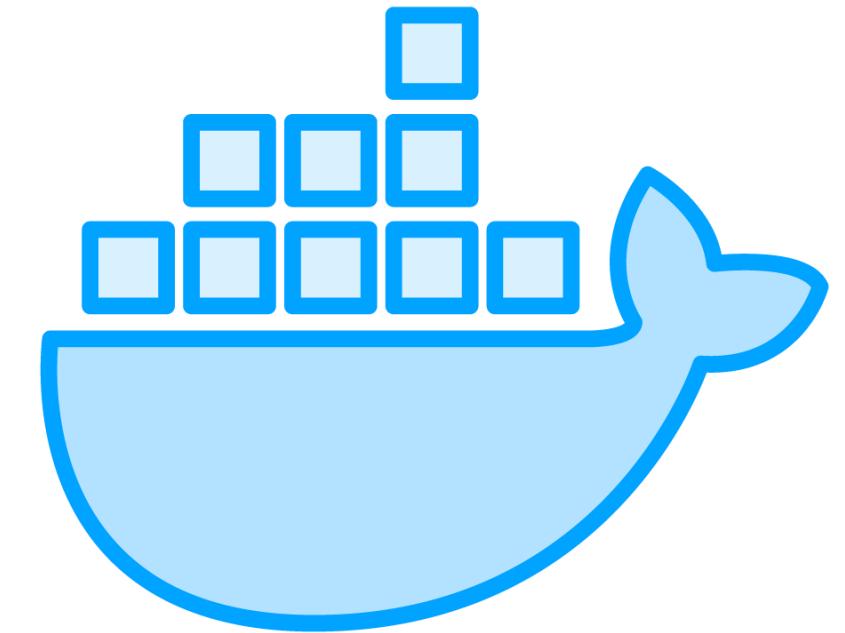
Server



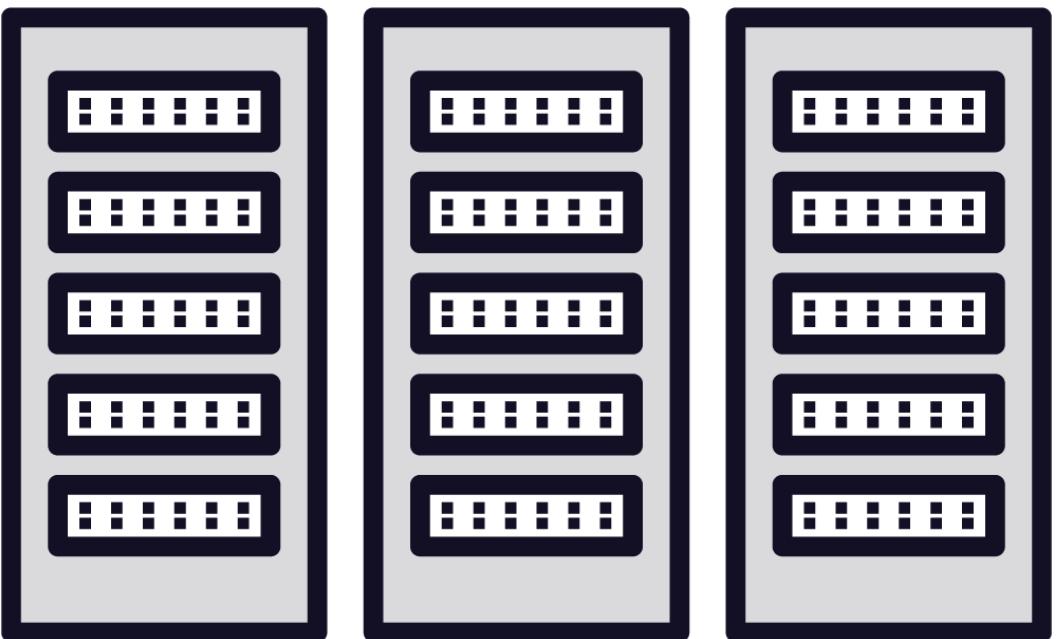
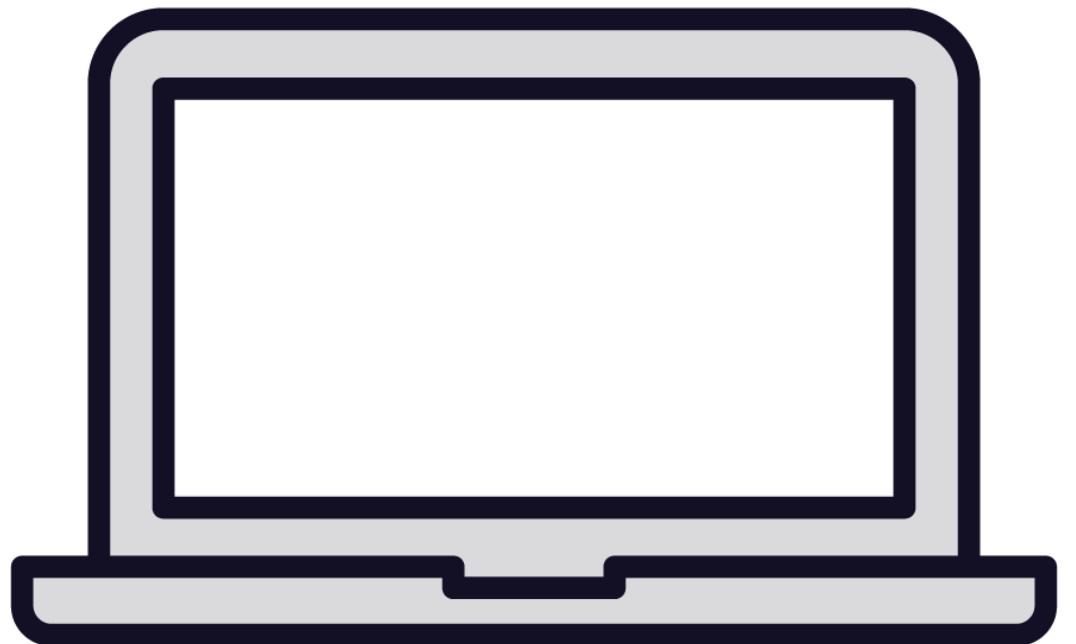


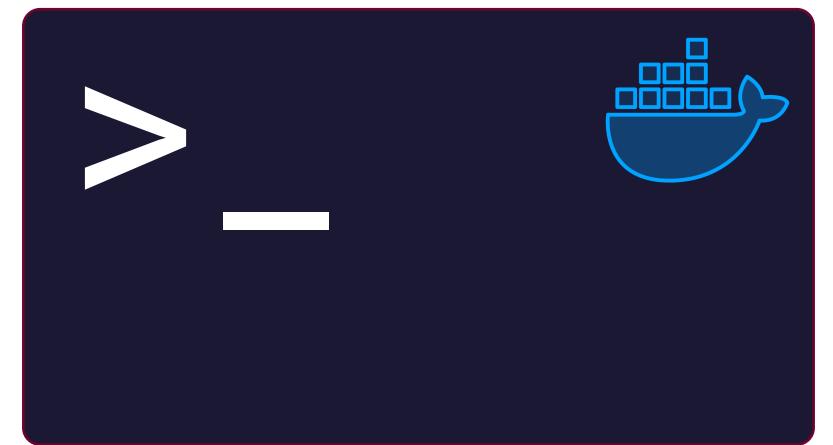


Client



Server



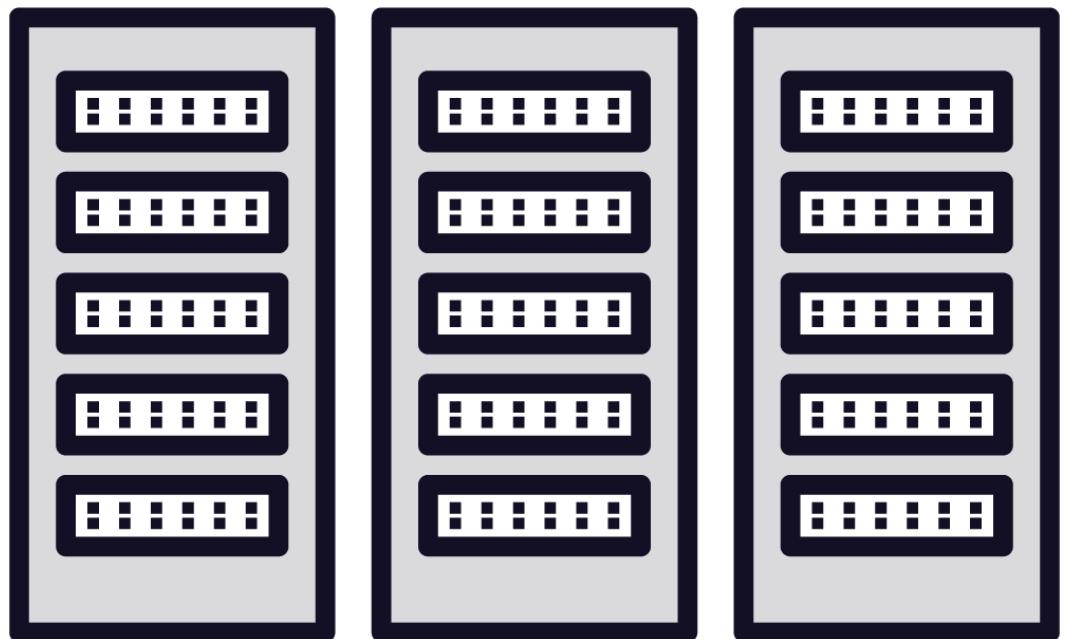
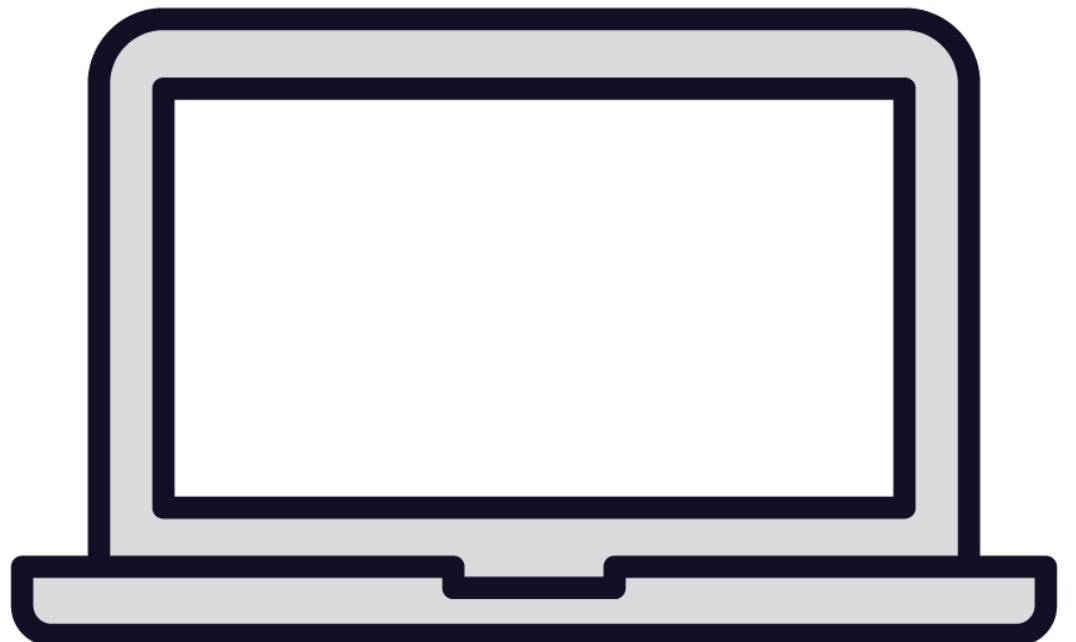
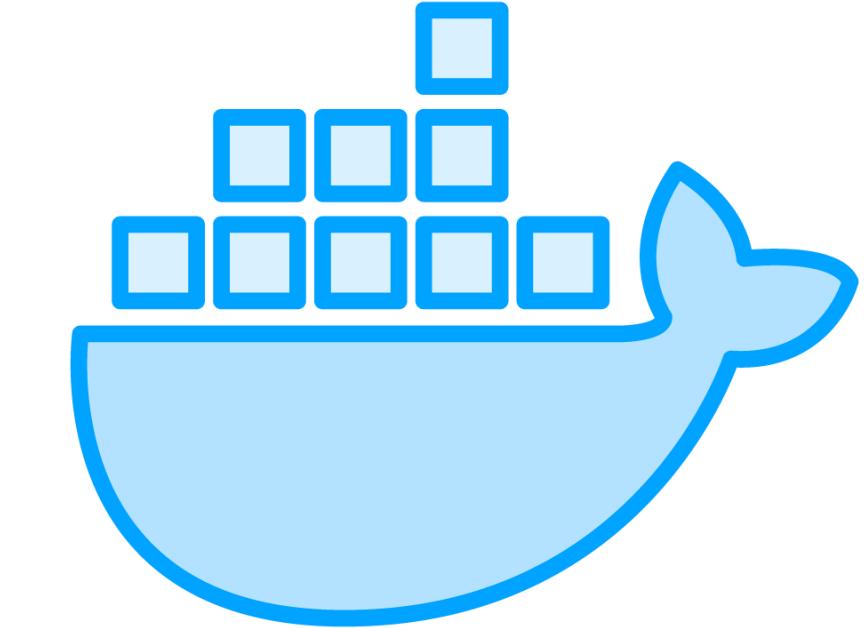


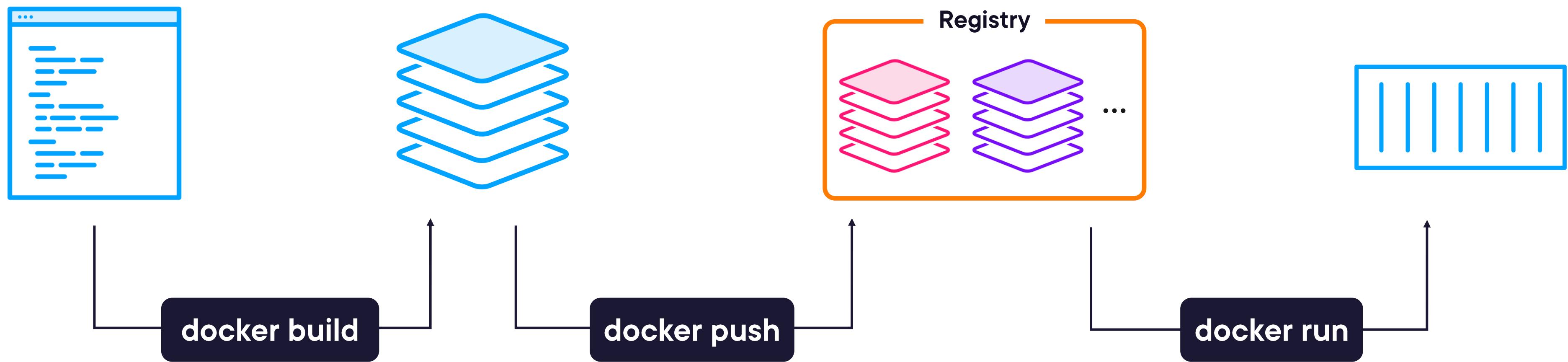
Client

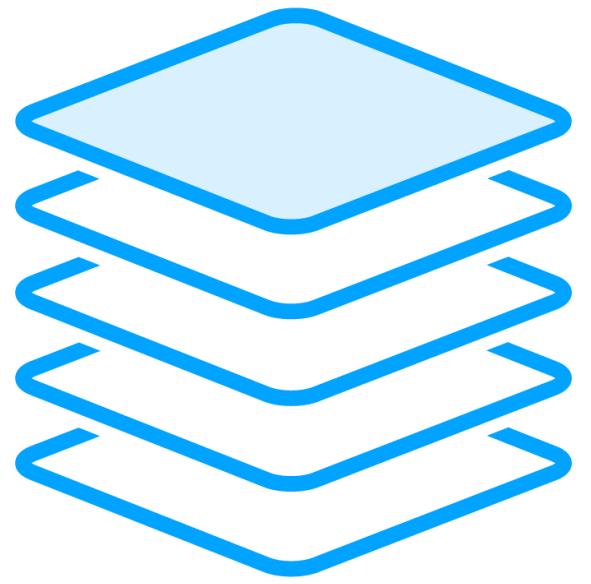
POST



{API}

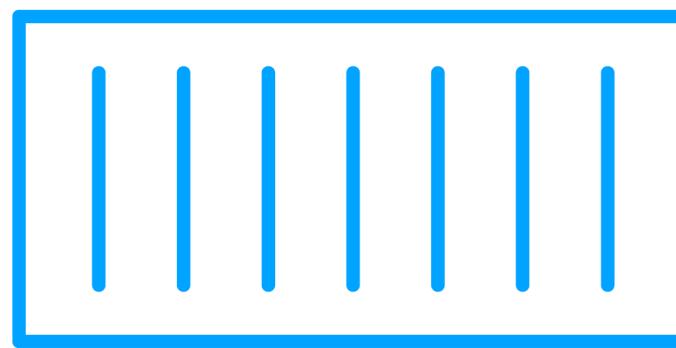






docker build

OCI image



docker run

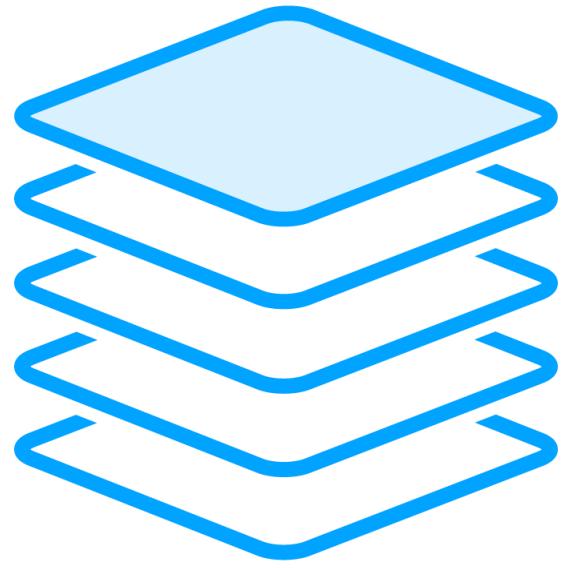
OCI container



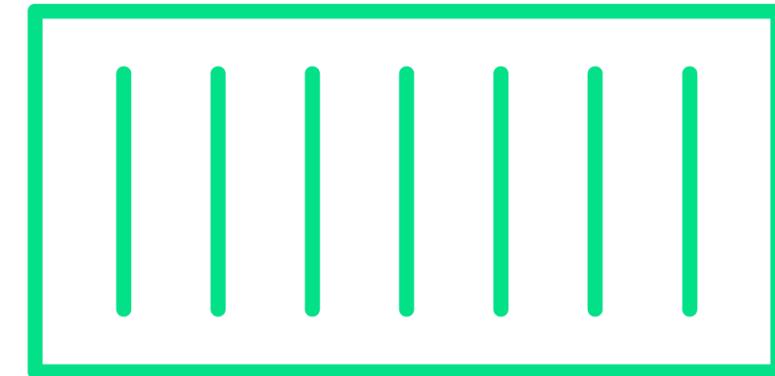
Open Container Initiative (OCI)

Standards body for low-level container-related standards.



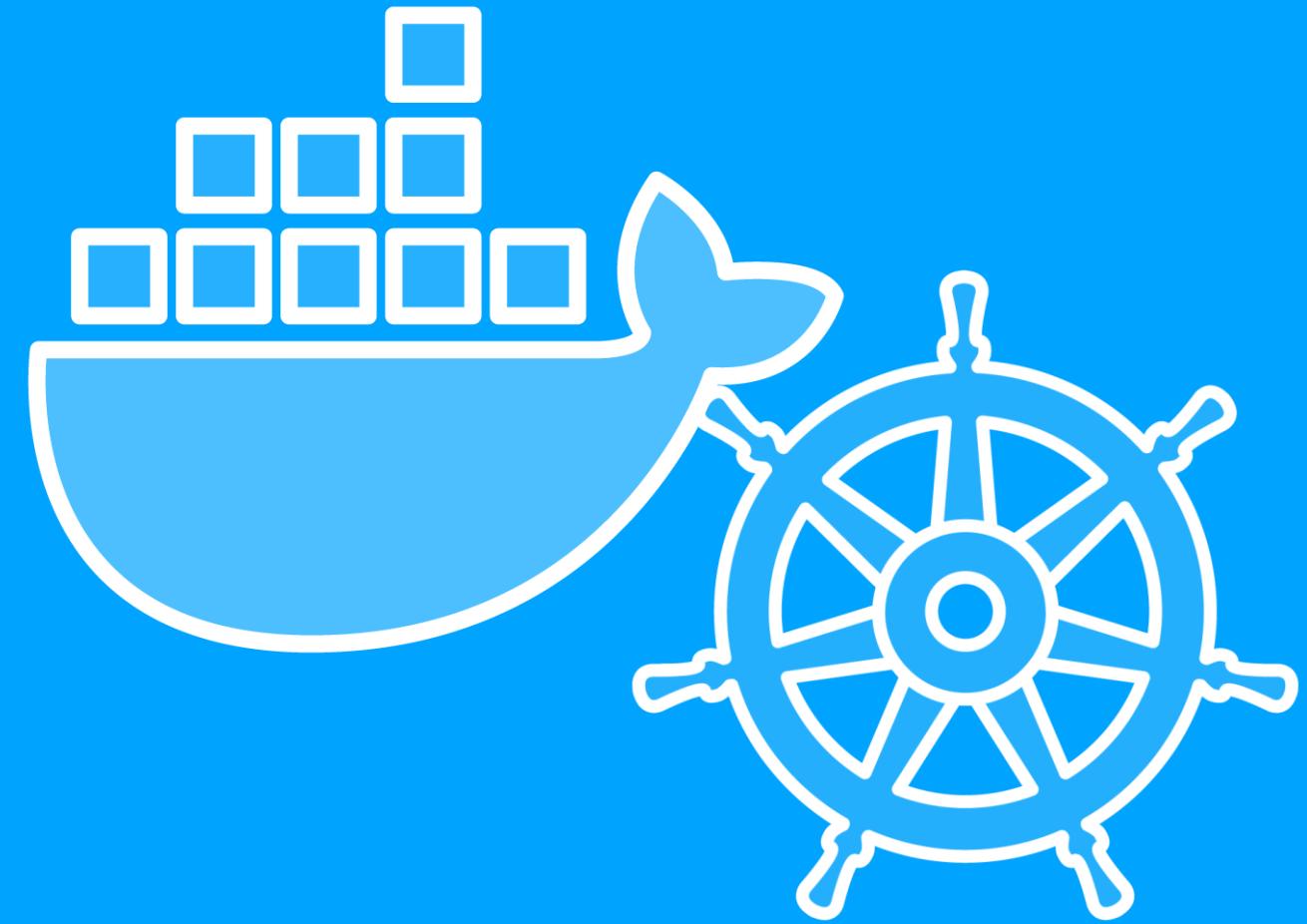


All mean the same
Image
Container image
Docker Image
OCI image



All mean the same
Container
Docker container
OCI container





Docker and Kubernetes

Both use and work with OCI images and
containers...



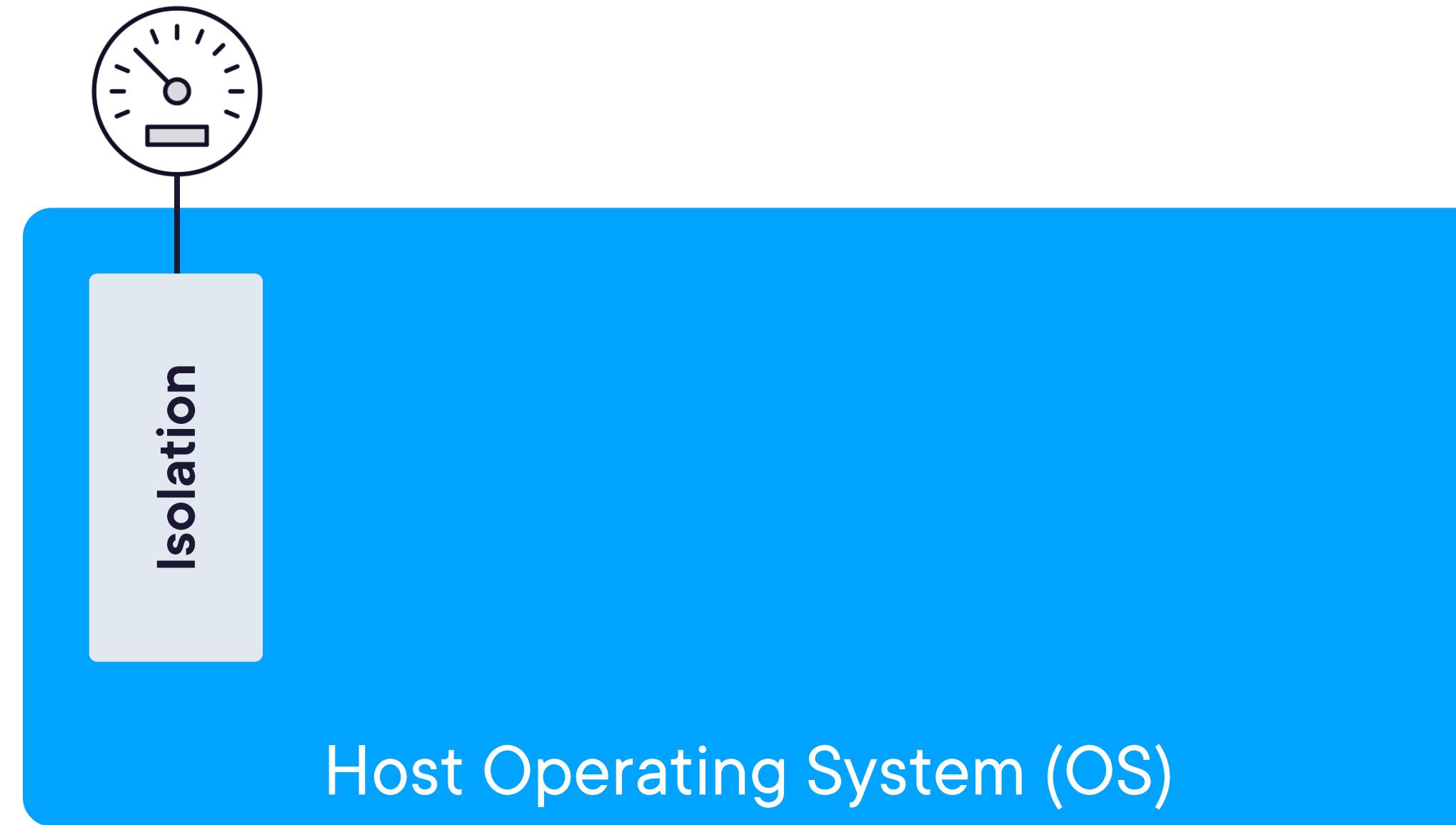
Container

Isolated area of OS with resource limits applied.



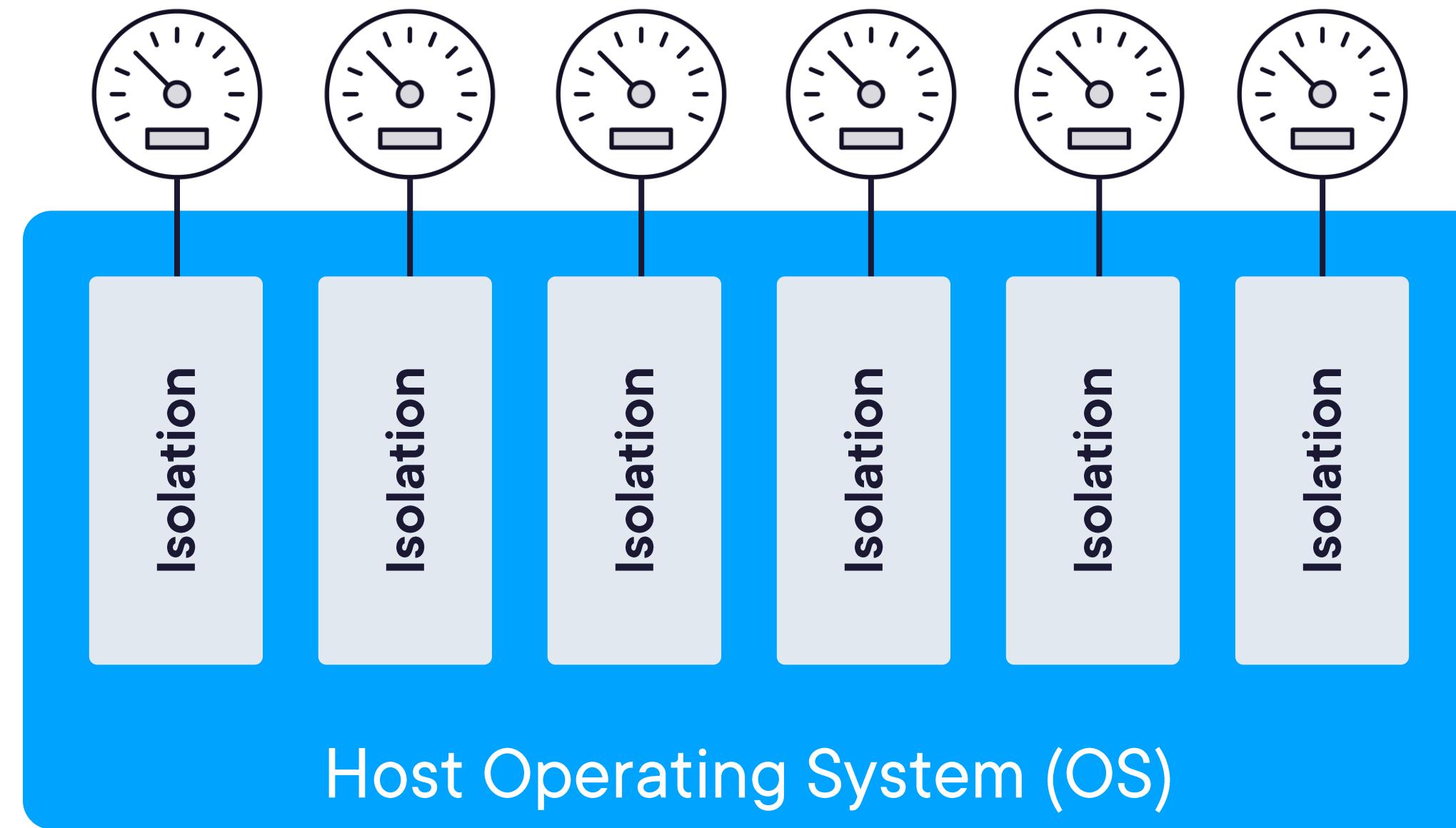
Container

Isolated area of OS with resource limits applied.



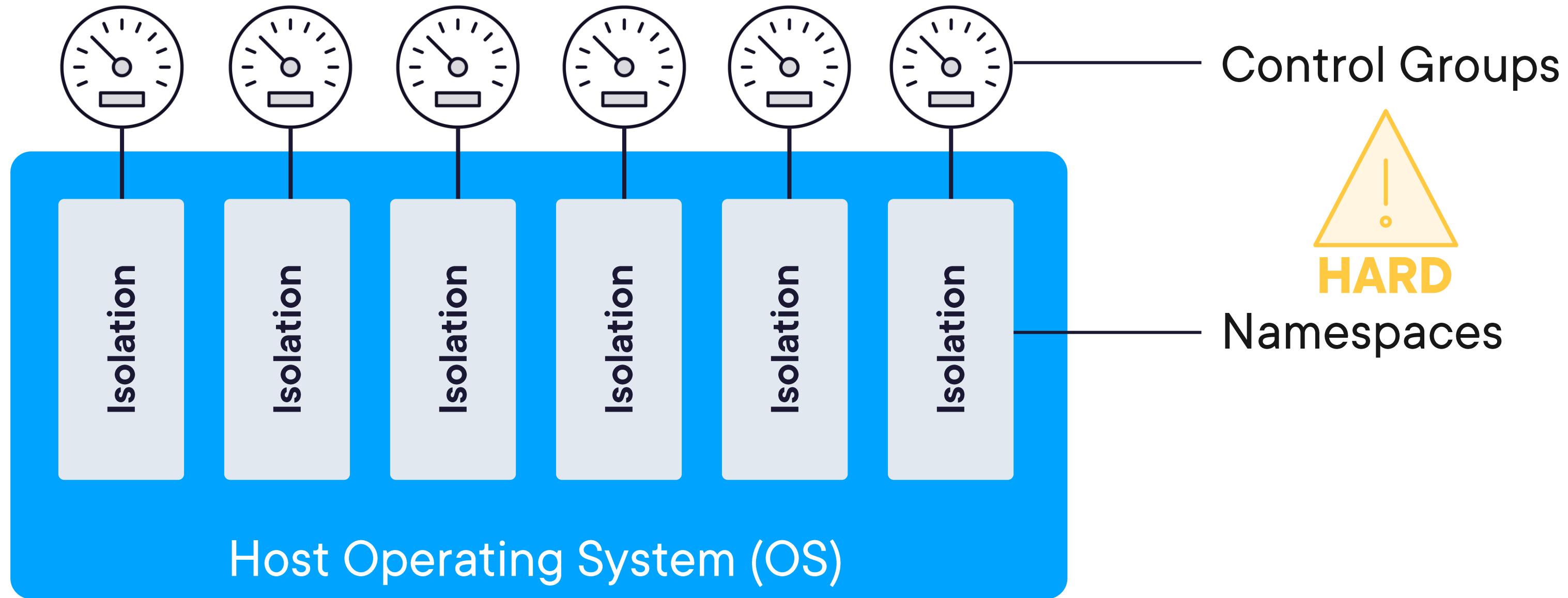
Container

Isolated area of OS with resource limits applied.



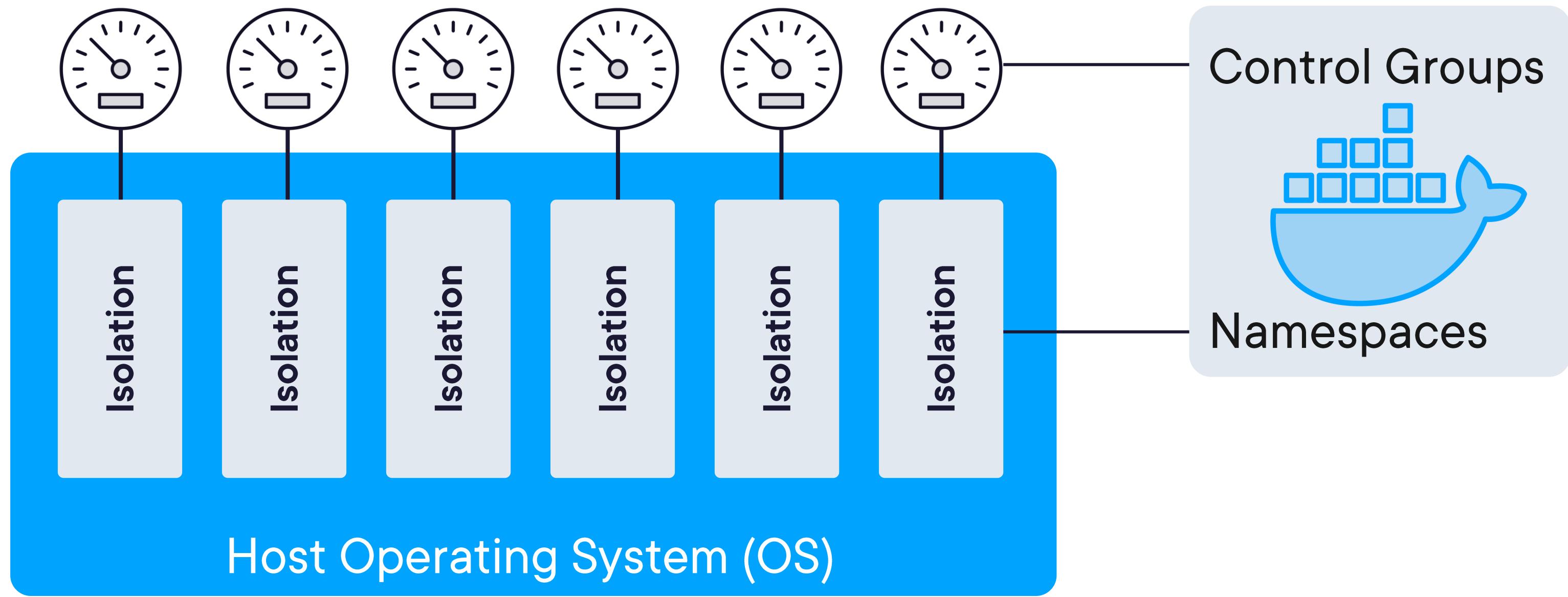
Container

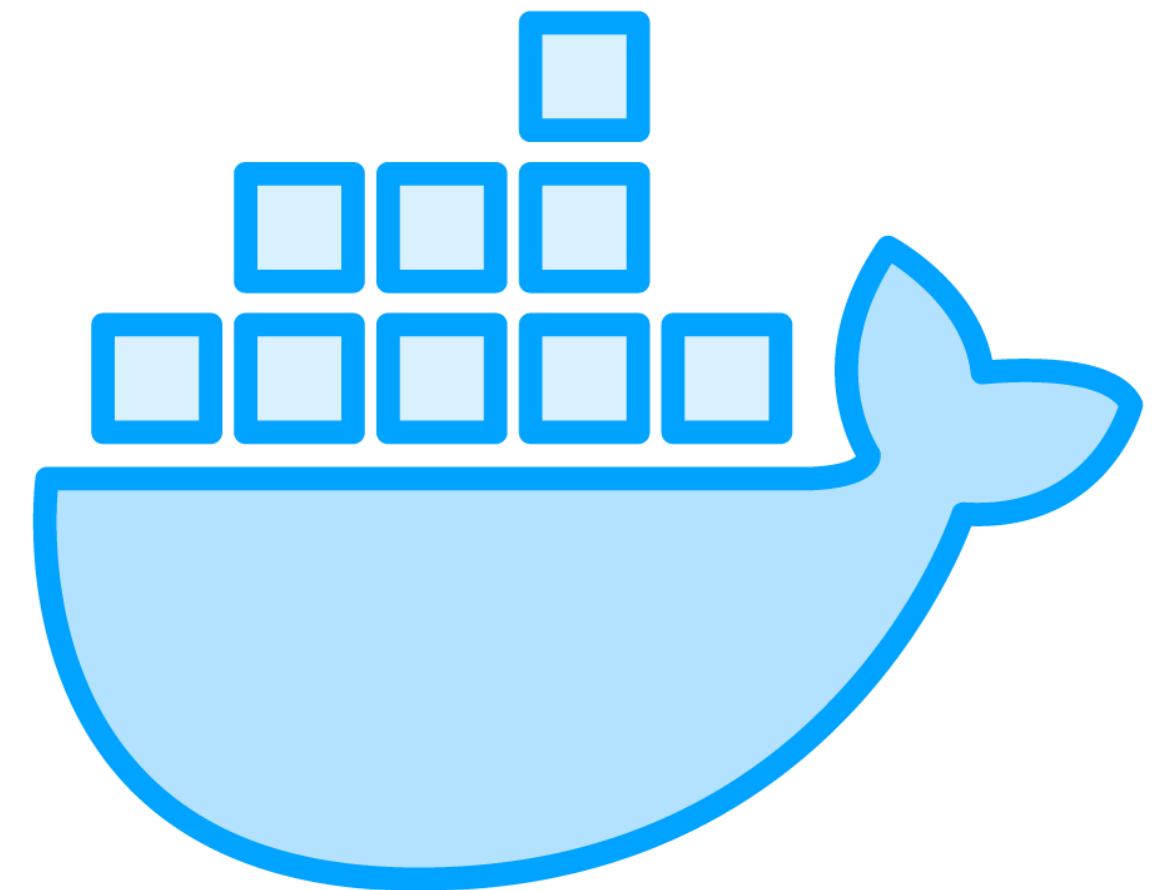
Isolated area of OS with resource limits applied.

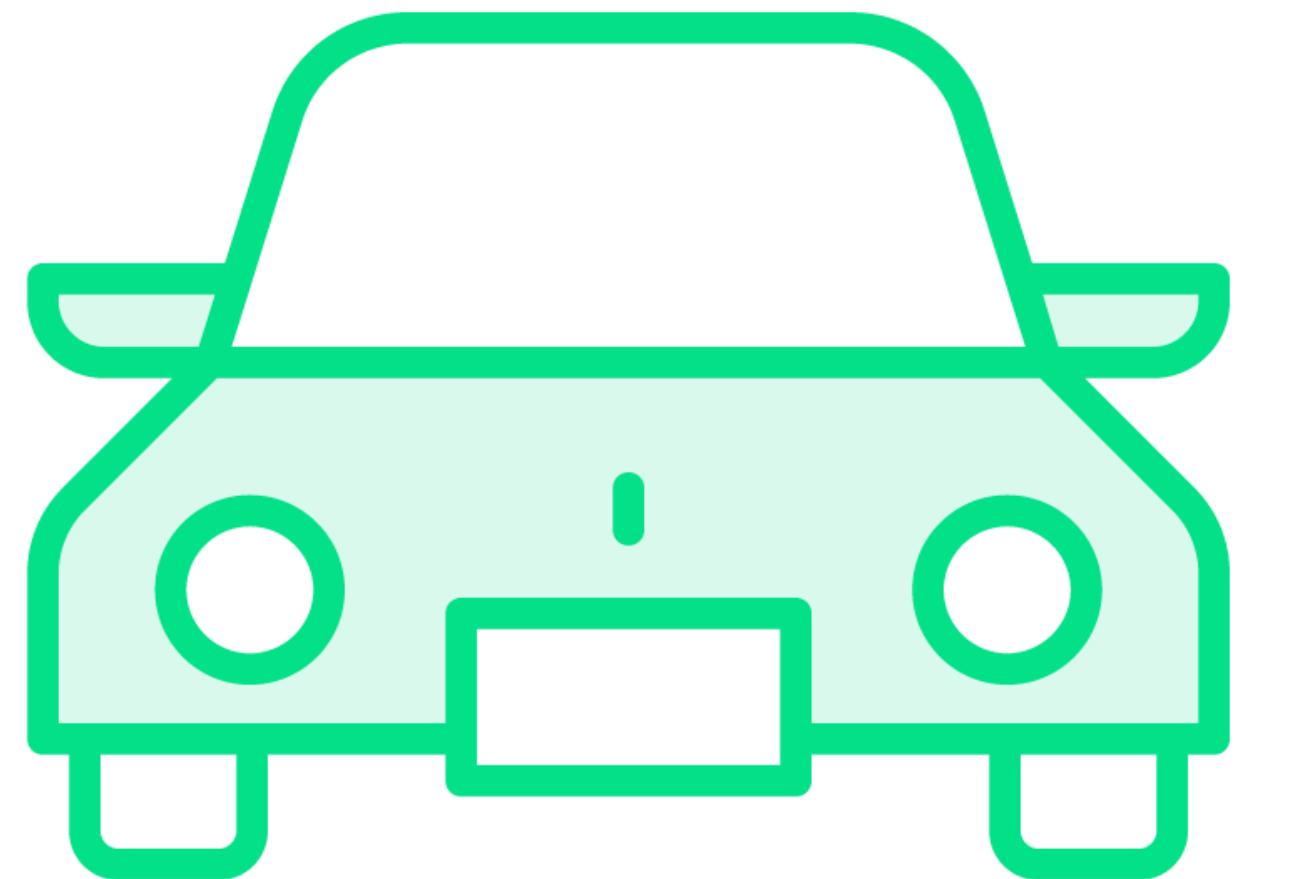


Container

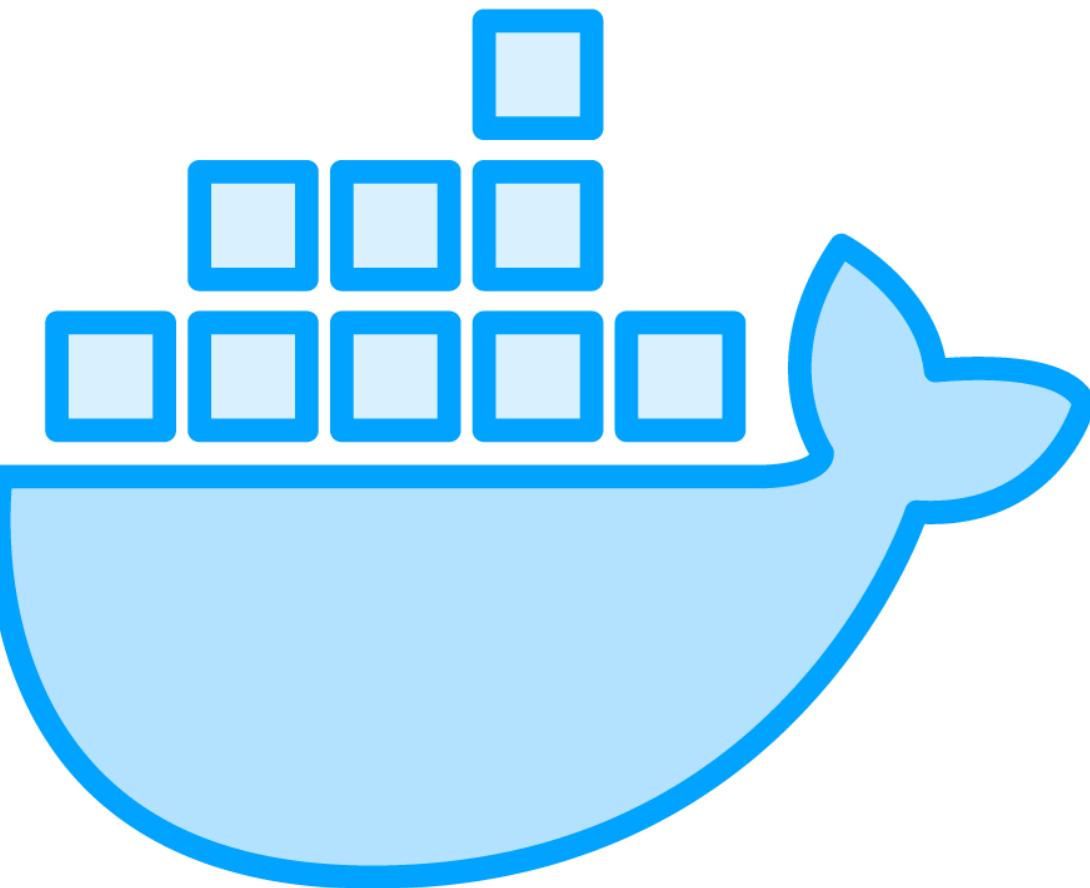
Isolated area of OS with resource limits applied.





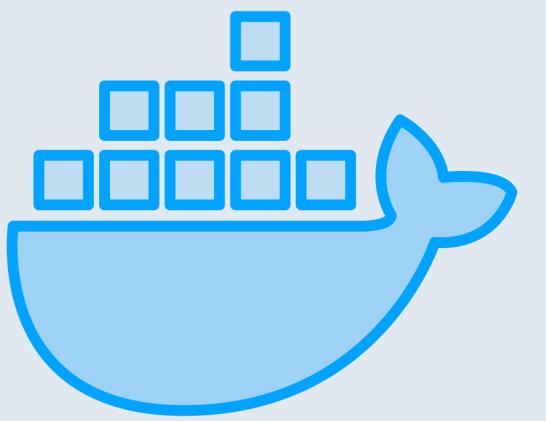


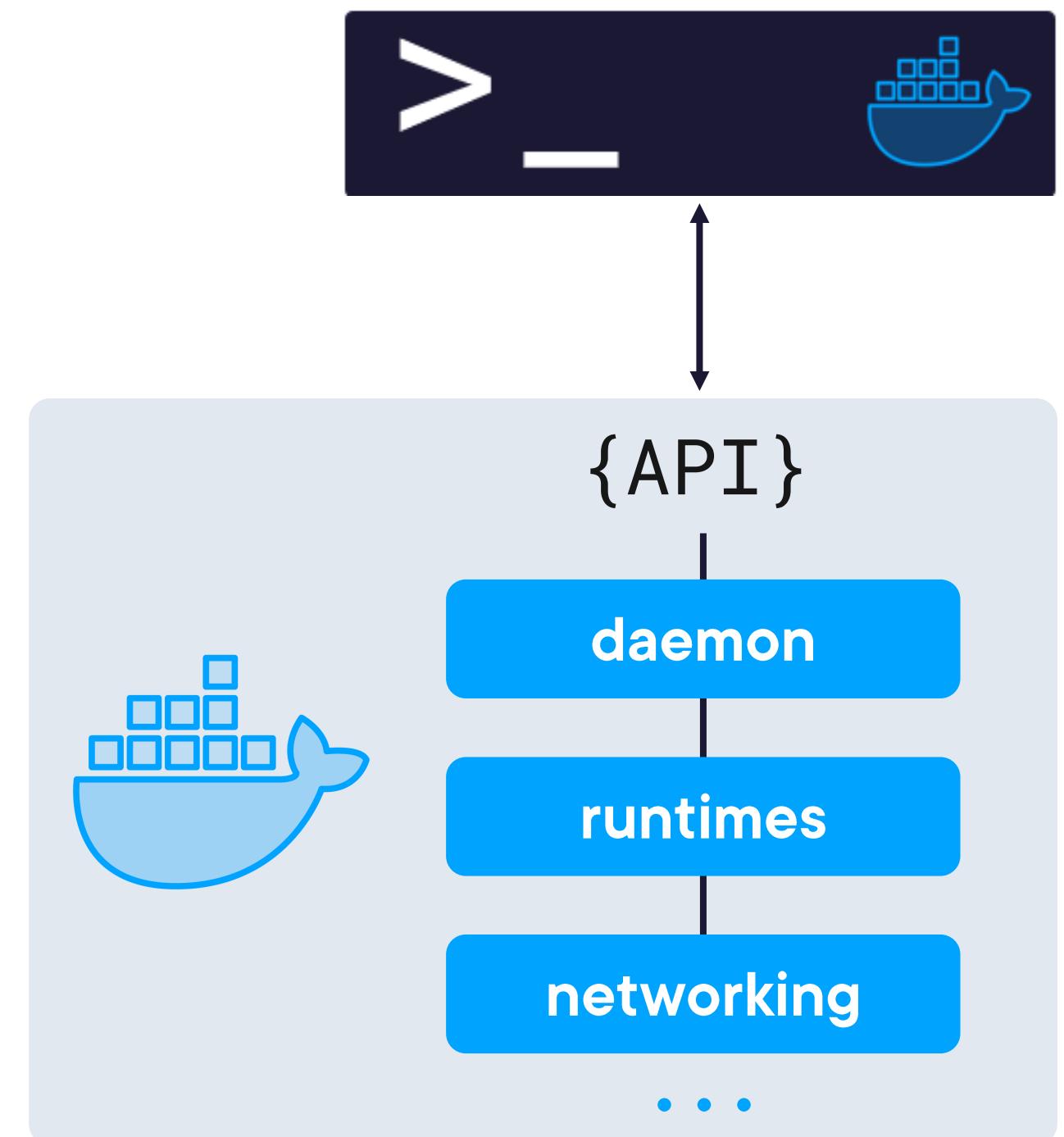
vs

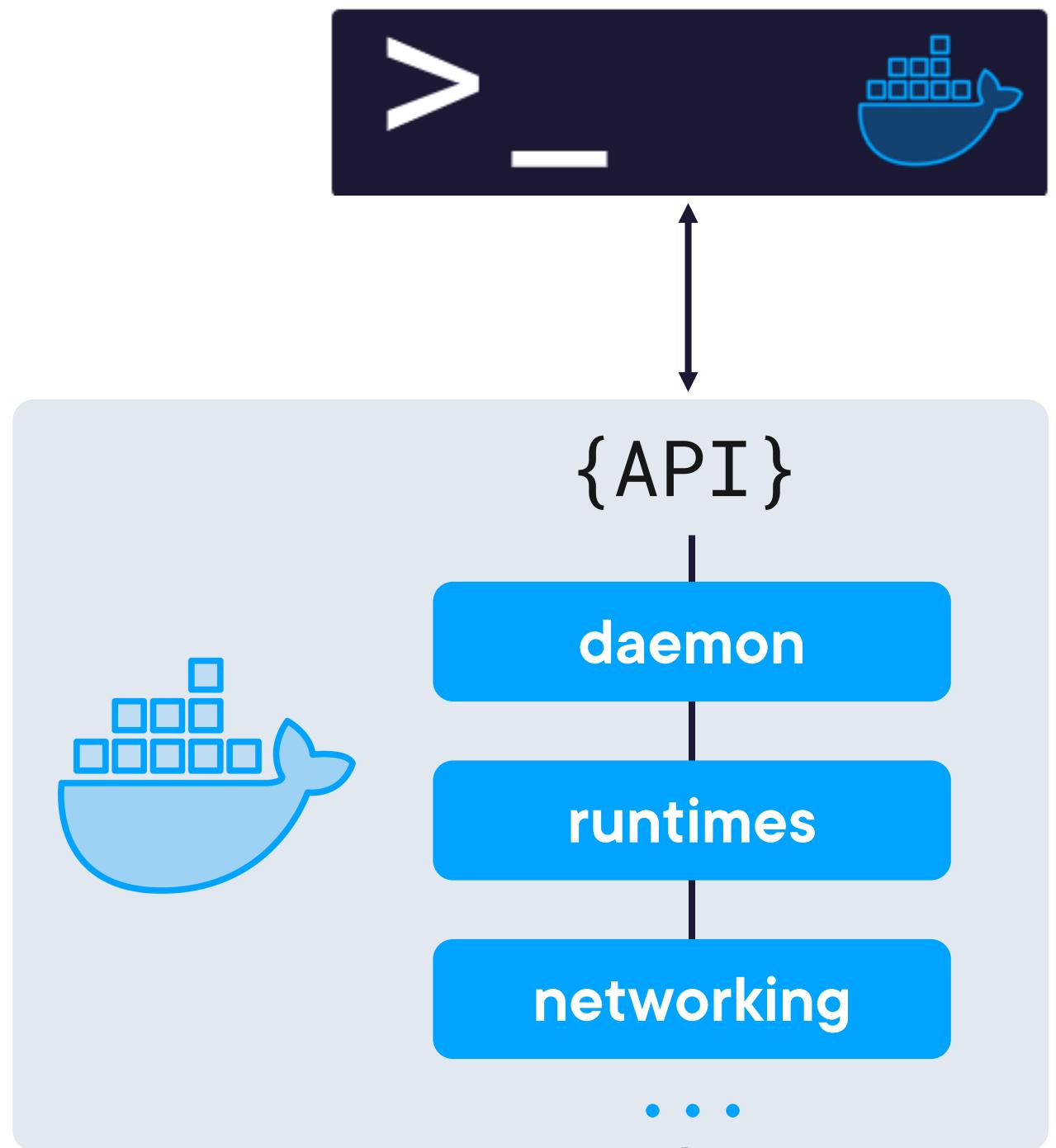




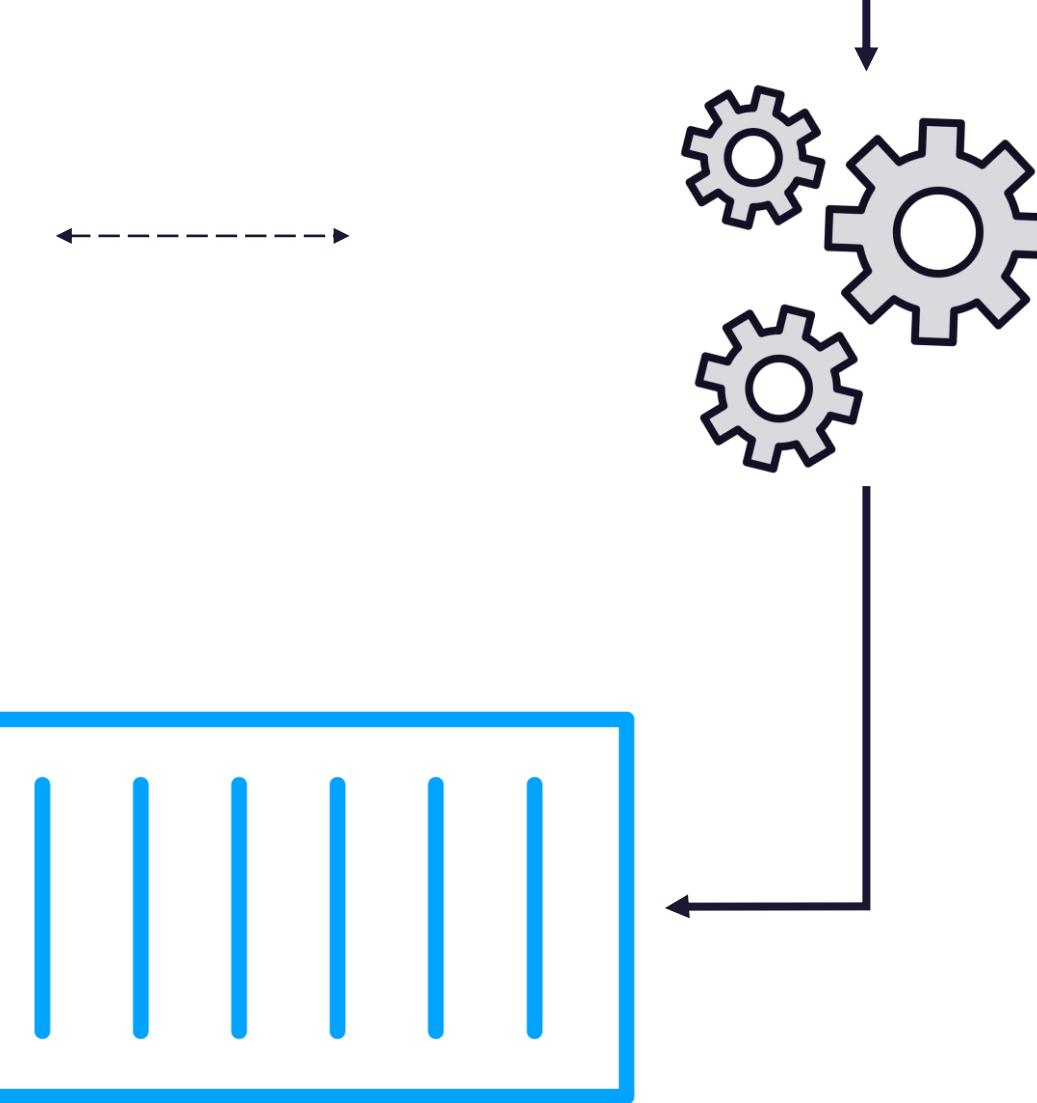
{API}







\$ docker run...
.../api/containers/create



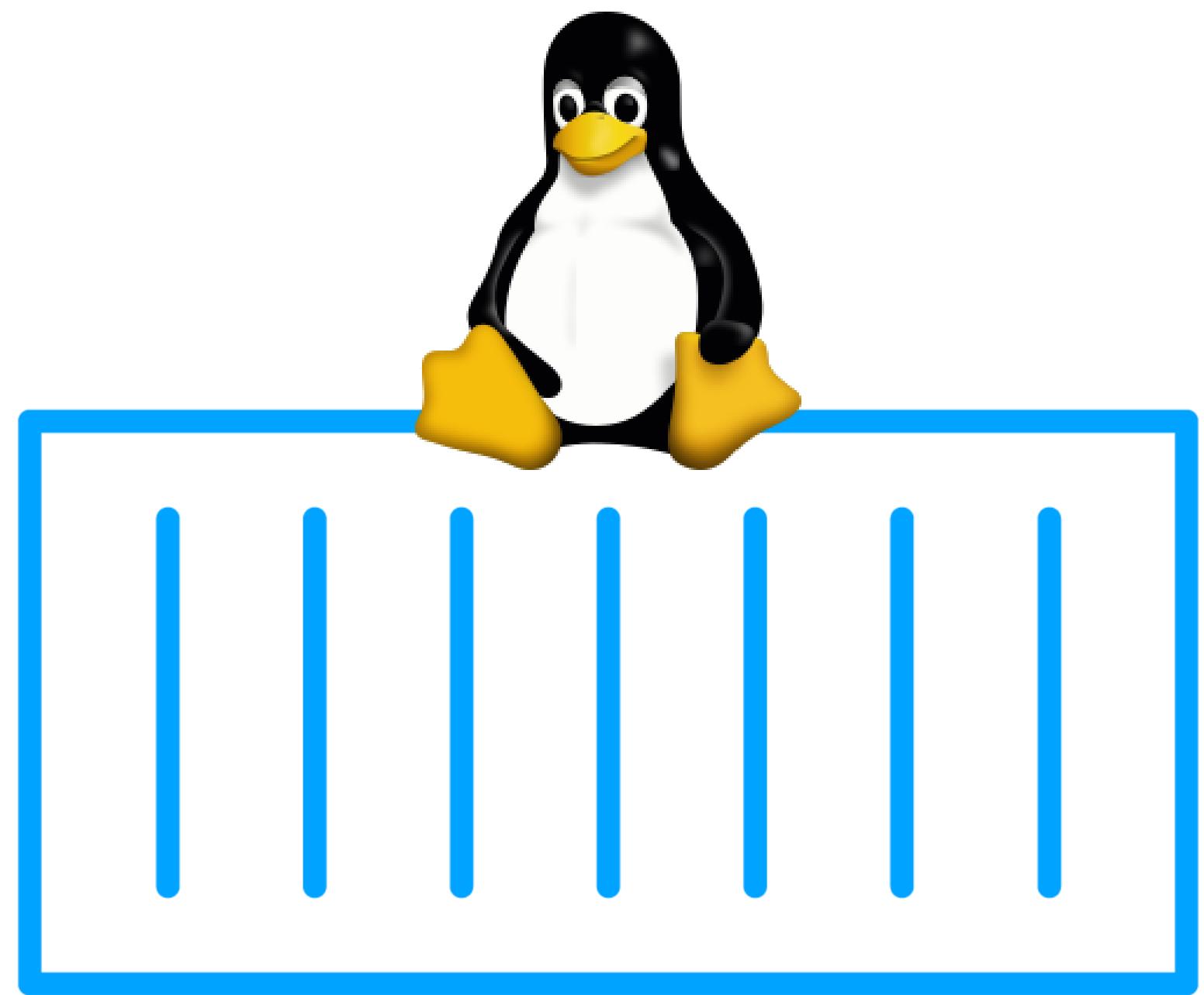
Up Next:

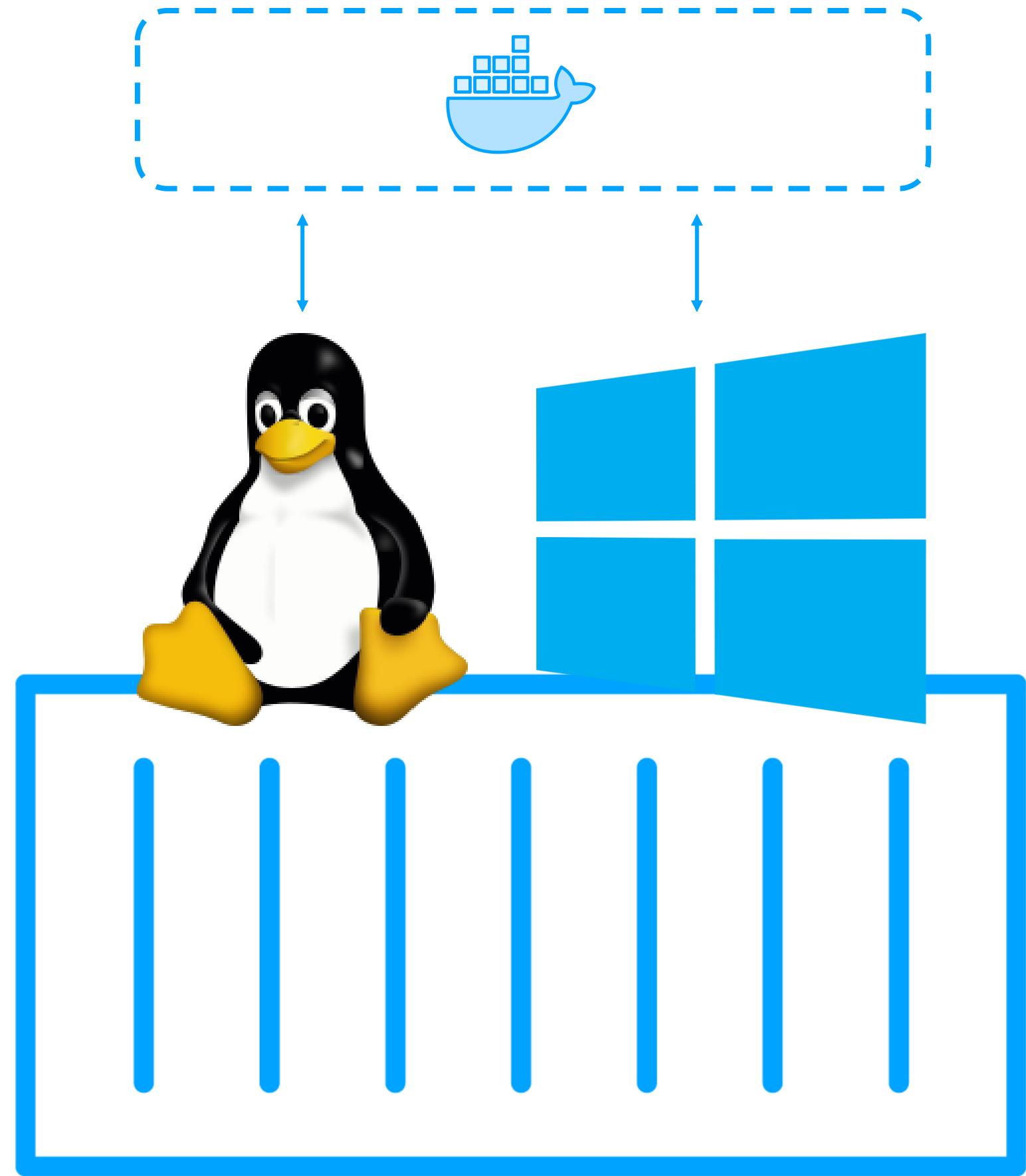
Kernel Internals

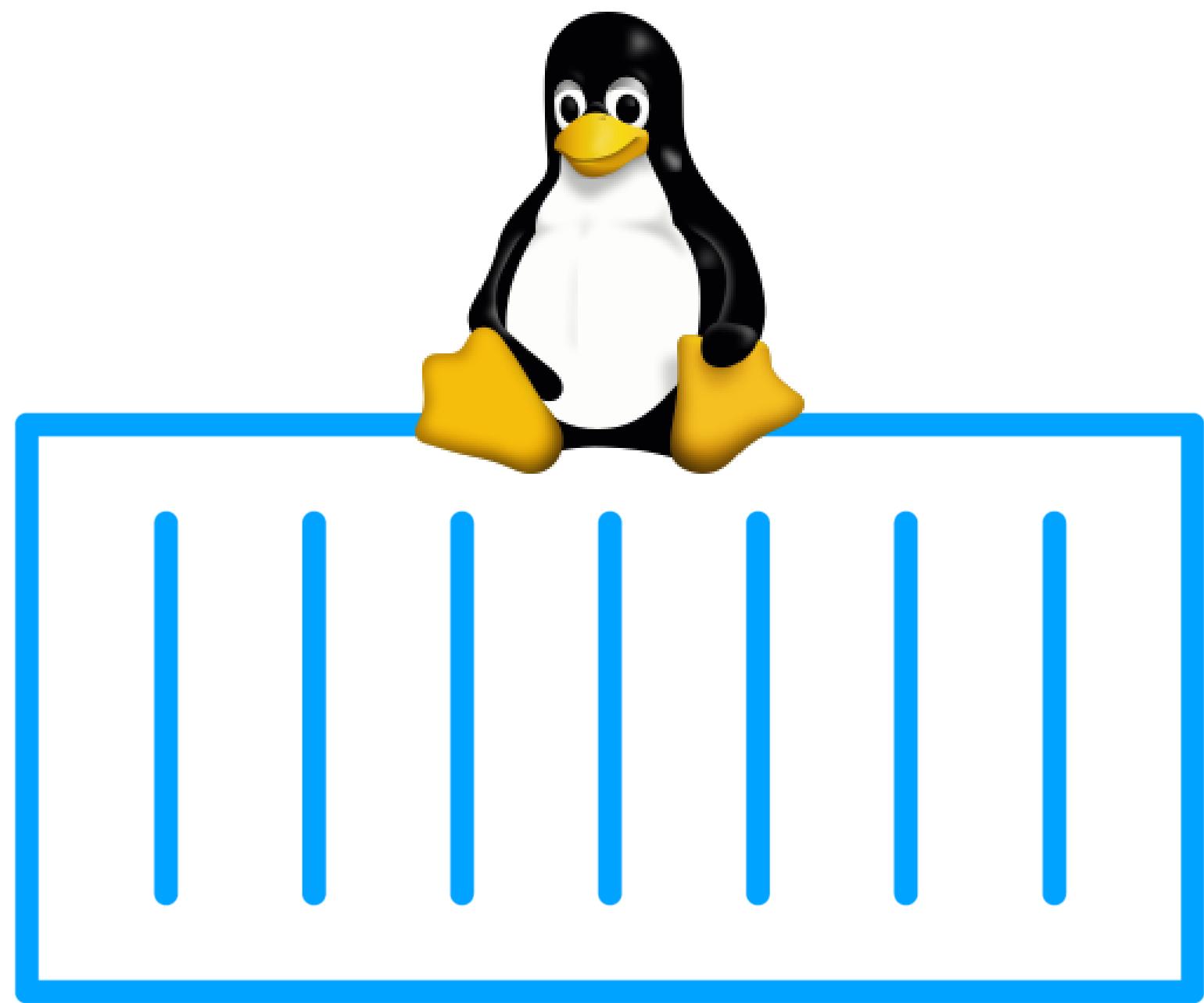


Kernel Internals









Fundamental Container Primitives in Kernel

Namespaces

All about isolation

Control Groups

All about limits



Namespaces
All about isolation

Control Groups
All about limits



Isolation

Isolation

Isolation

Isolation

Isolation

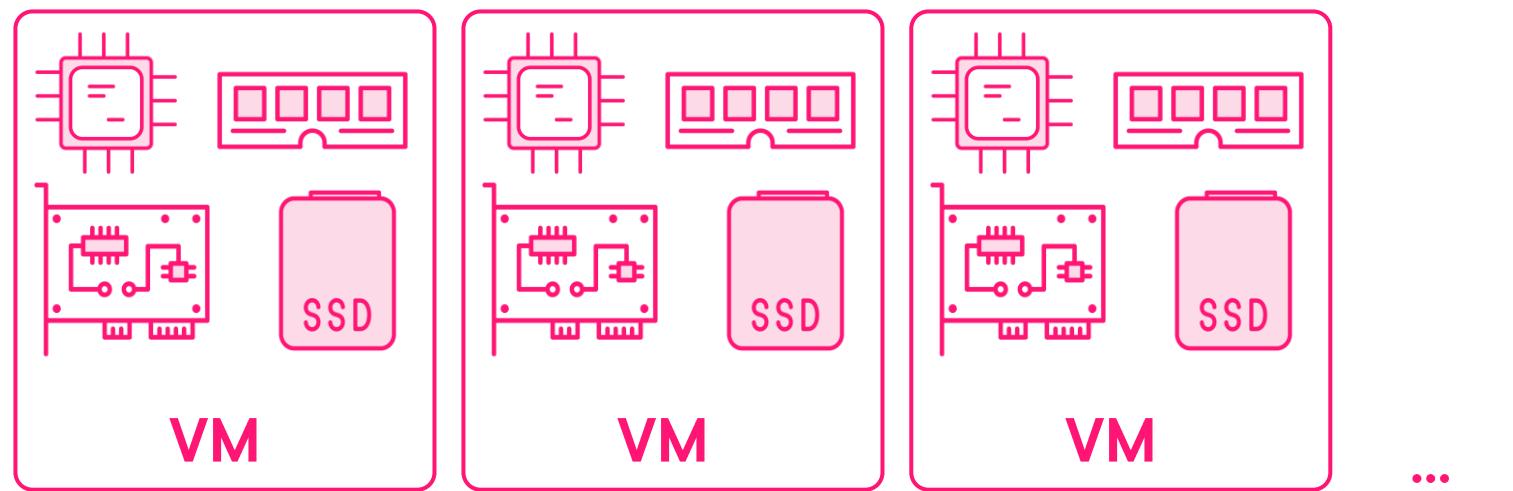
Isolation

Host Operating System (OS)

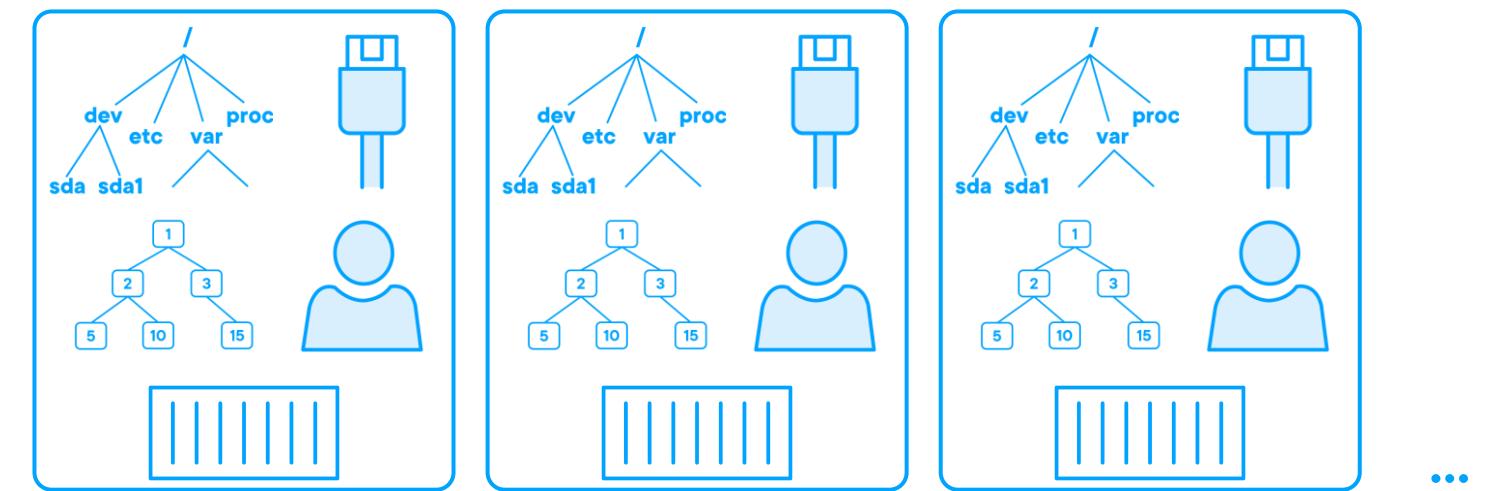
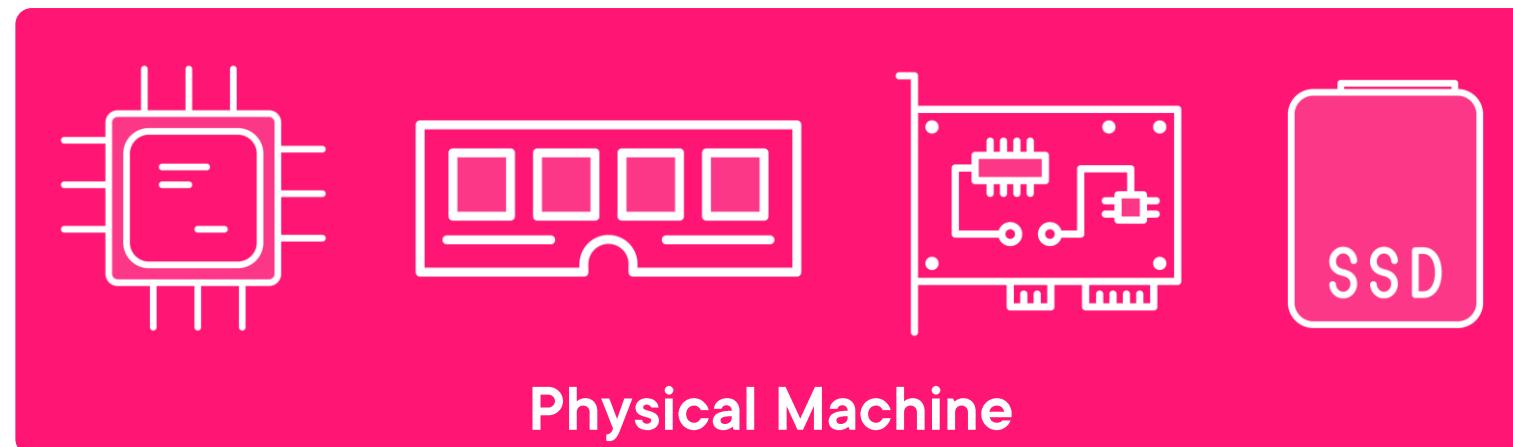
Namespaces
All about isolation

Control Groups
All about limits

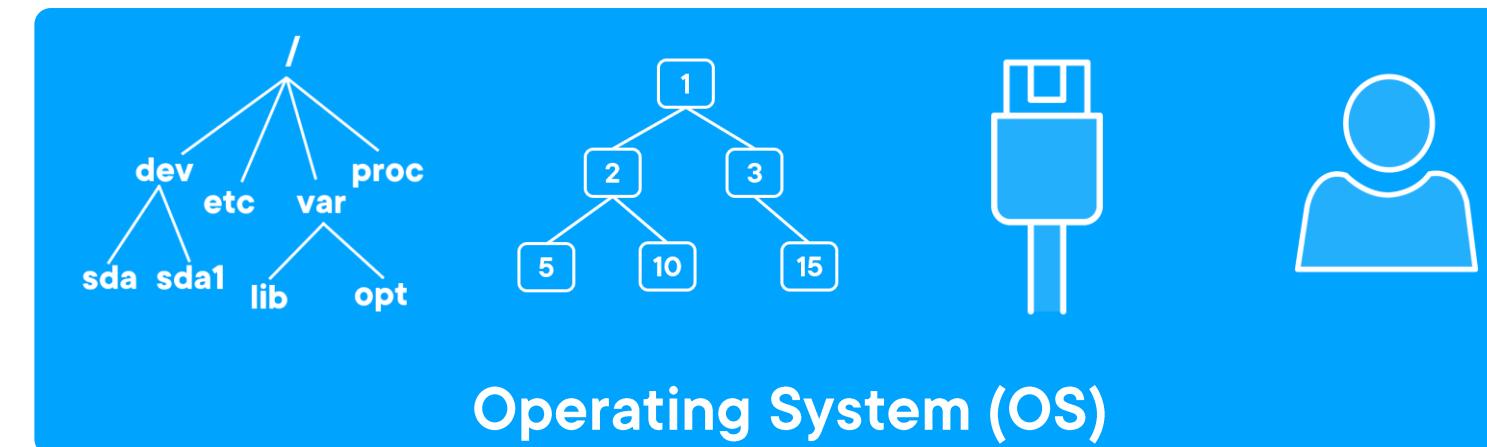




Hypervisor



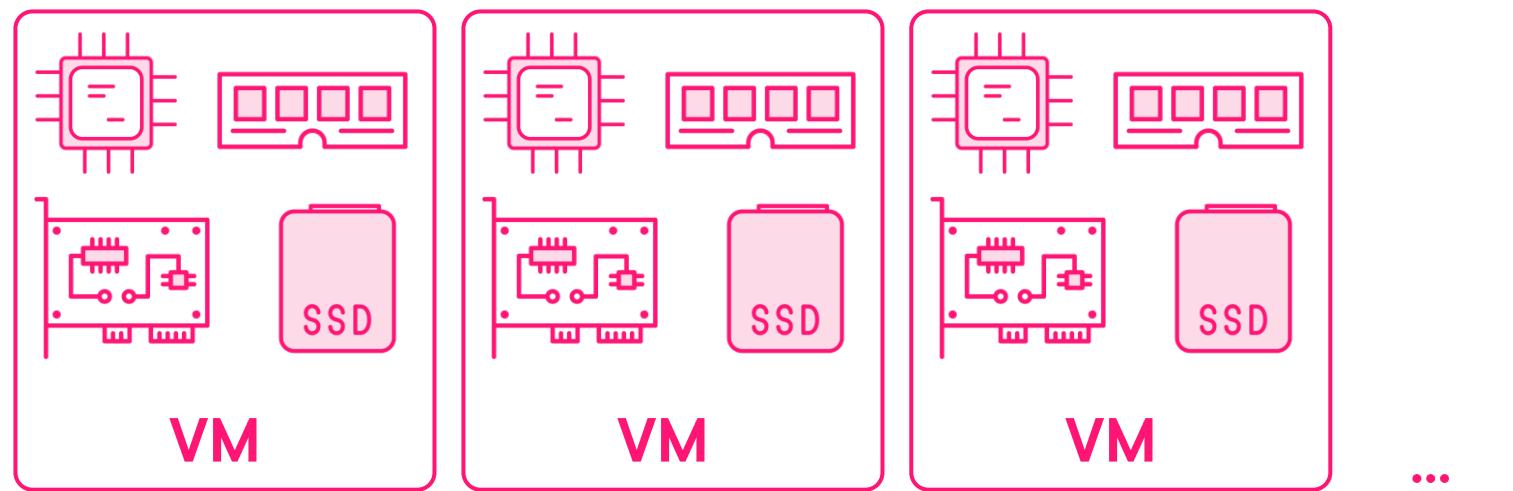
Container Runtime



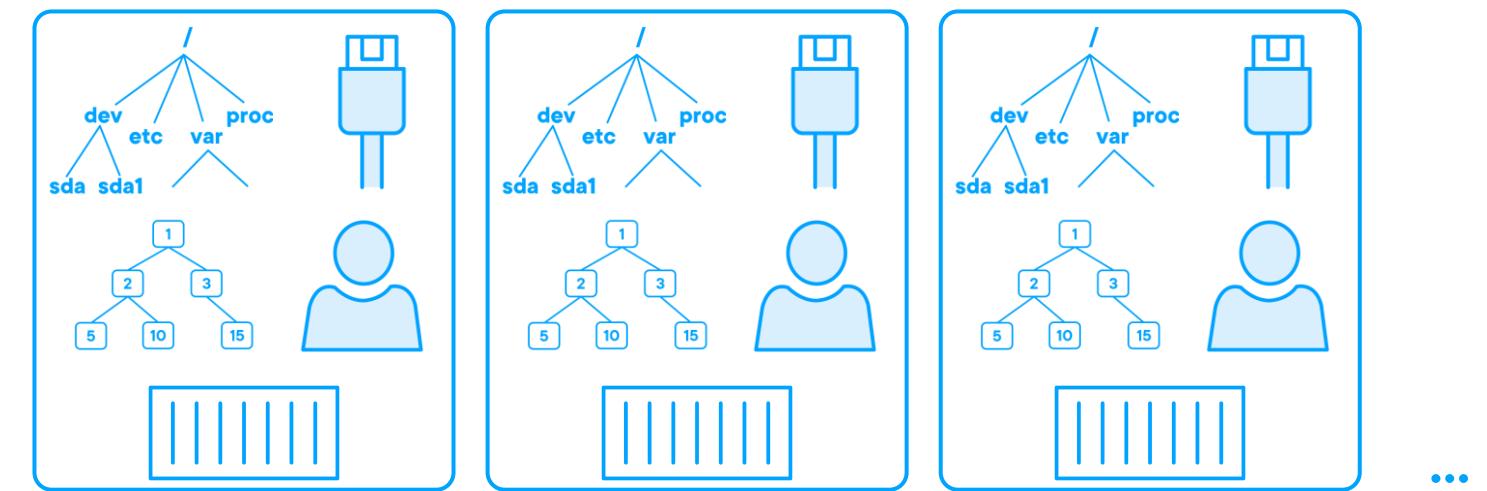
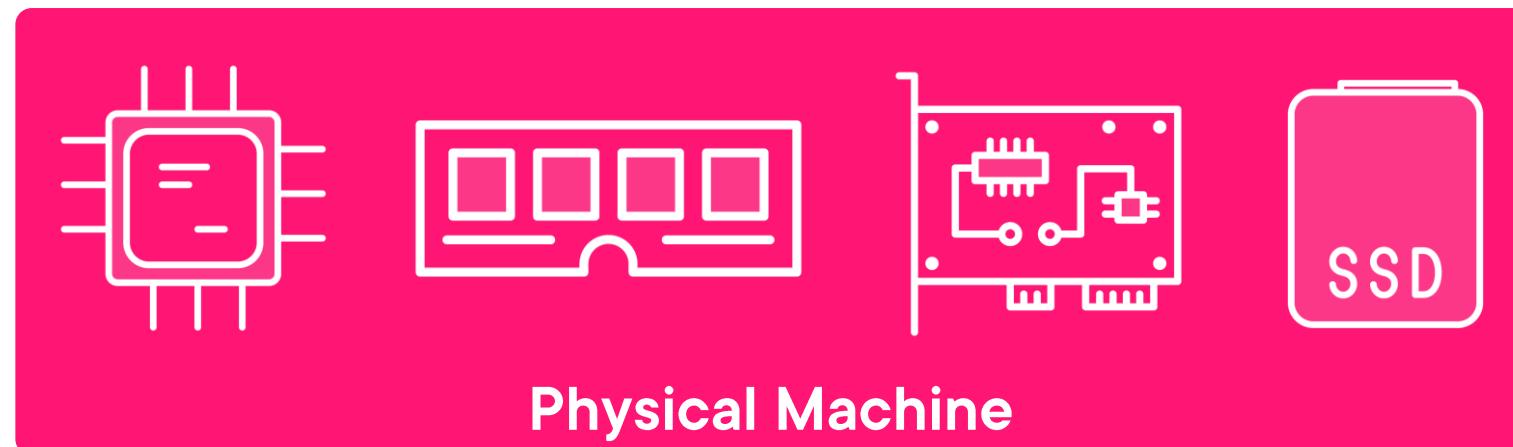
Namespaces
All about isolation

Control Groups
All about limits

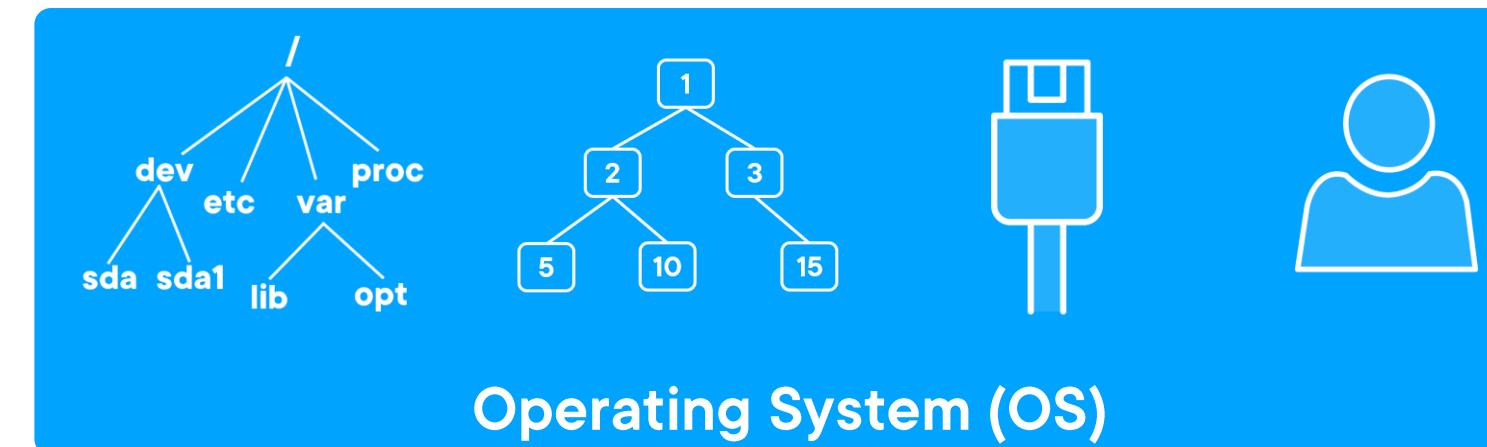




Hypervisor



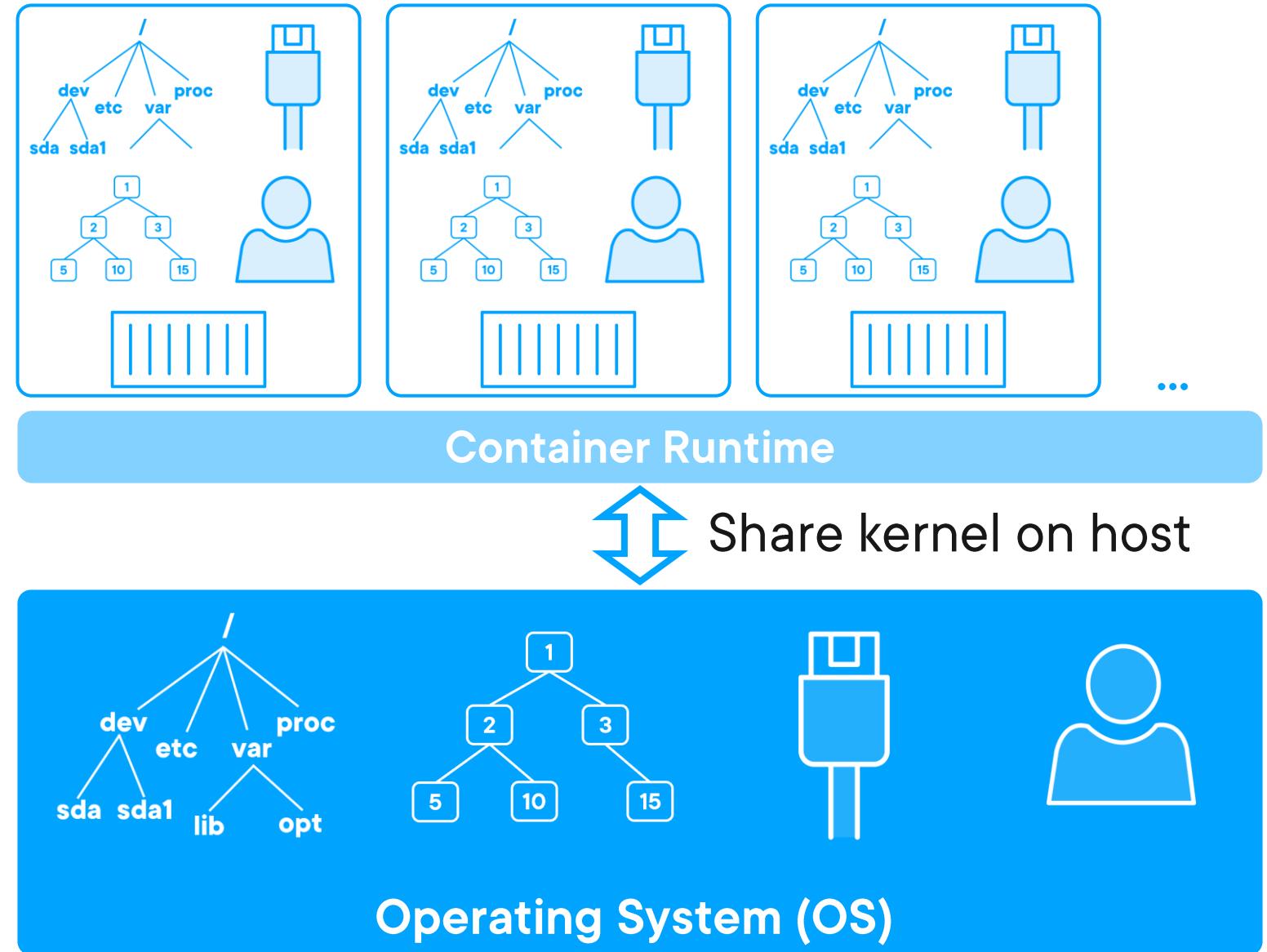
Container Runtime



Namespaces
All about isolation

Control Groups
All about limits





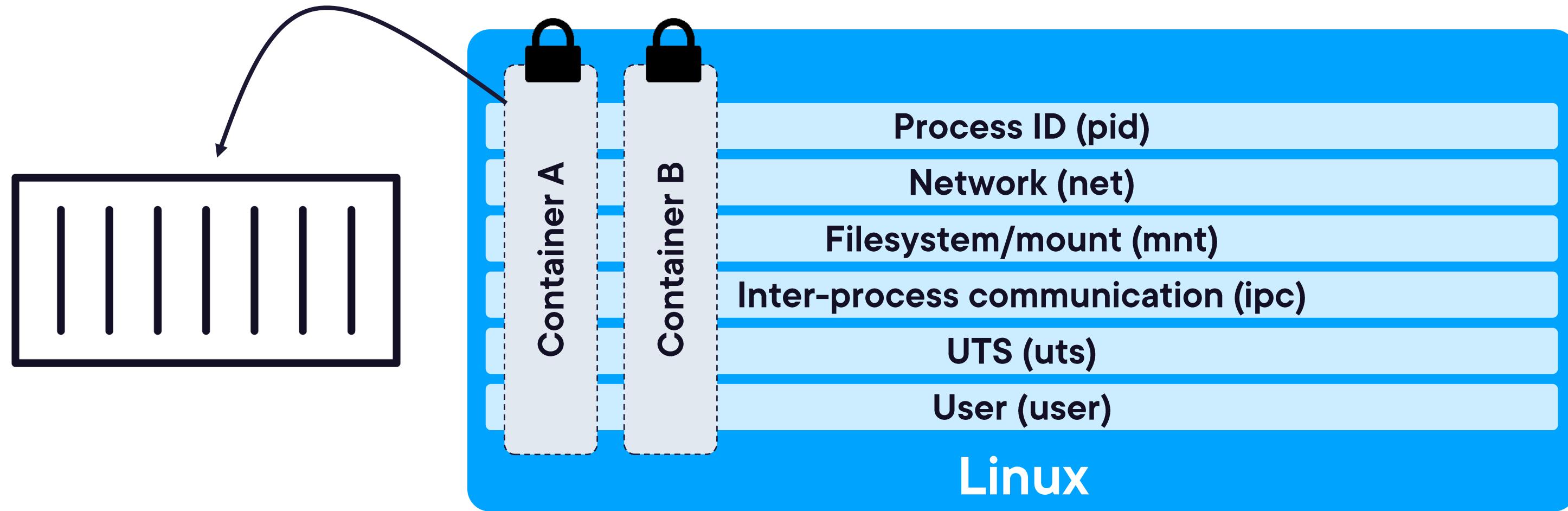
Namespaces

All about isolation

Control Groups

All about limits

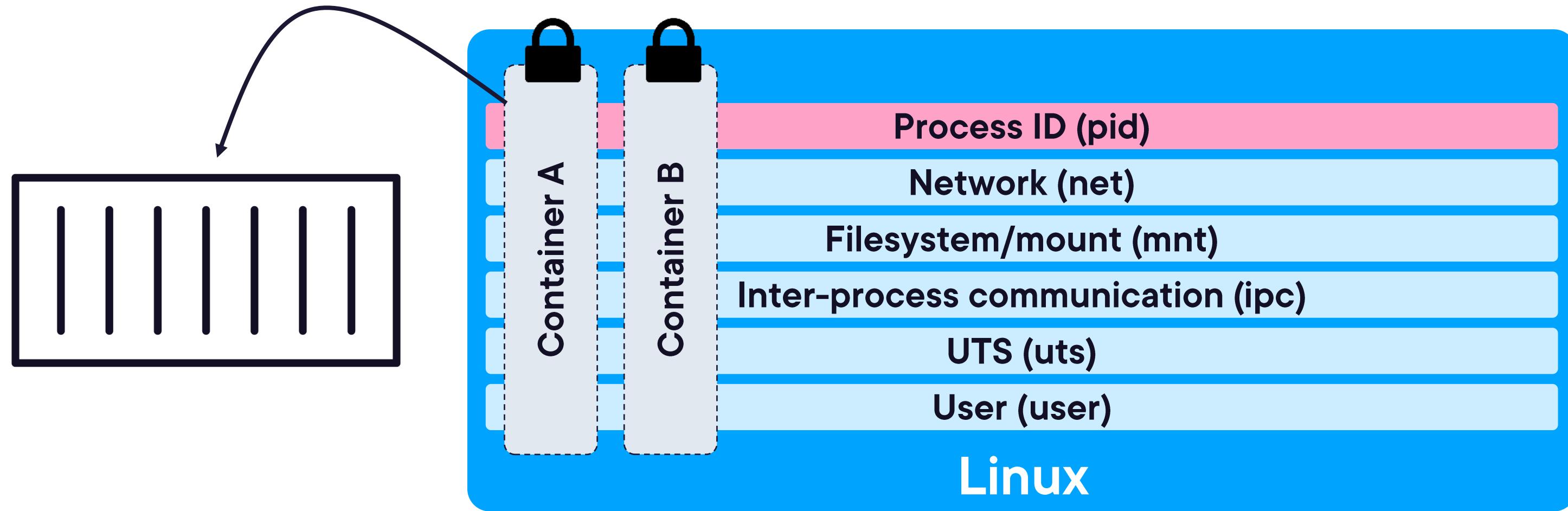




Namespaces
All about isolation

Control Groups
All about limits

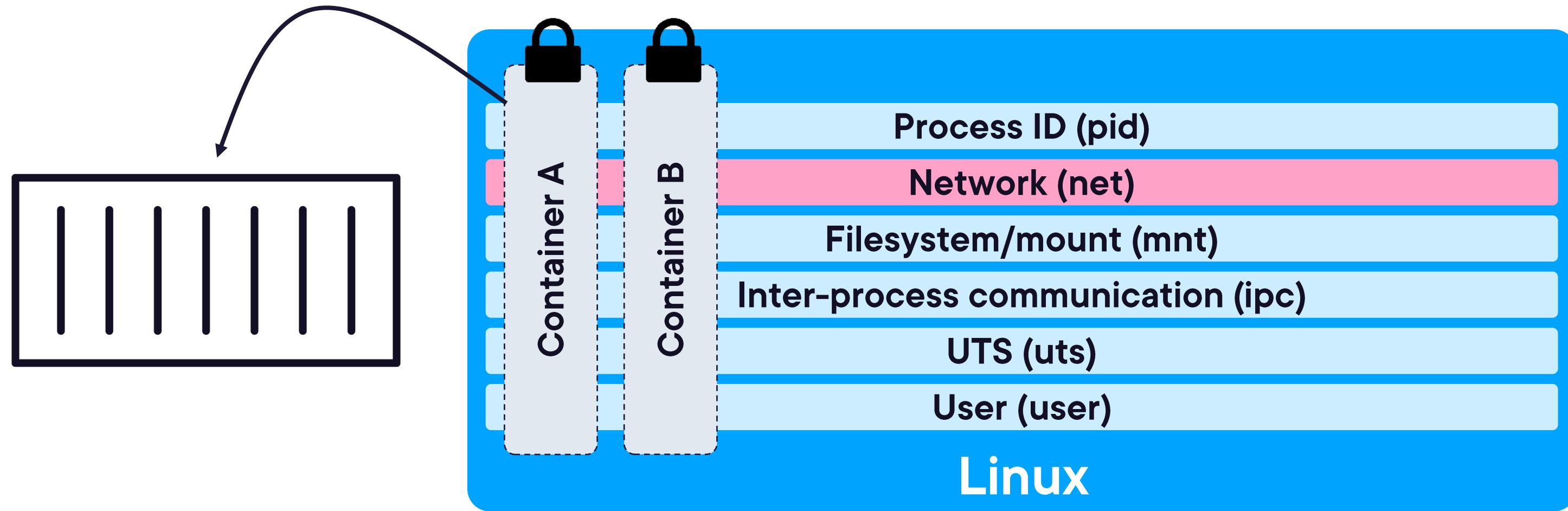




Namespaces
All about isolation

Control Groups
All about limits

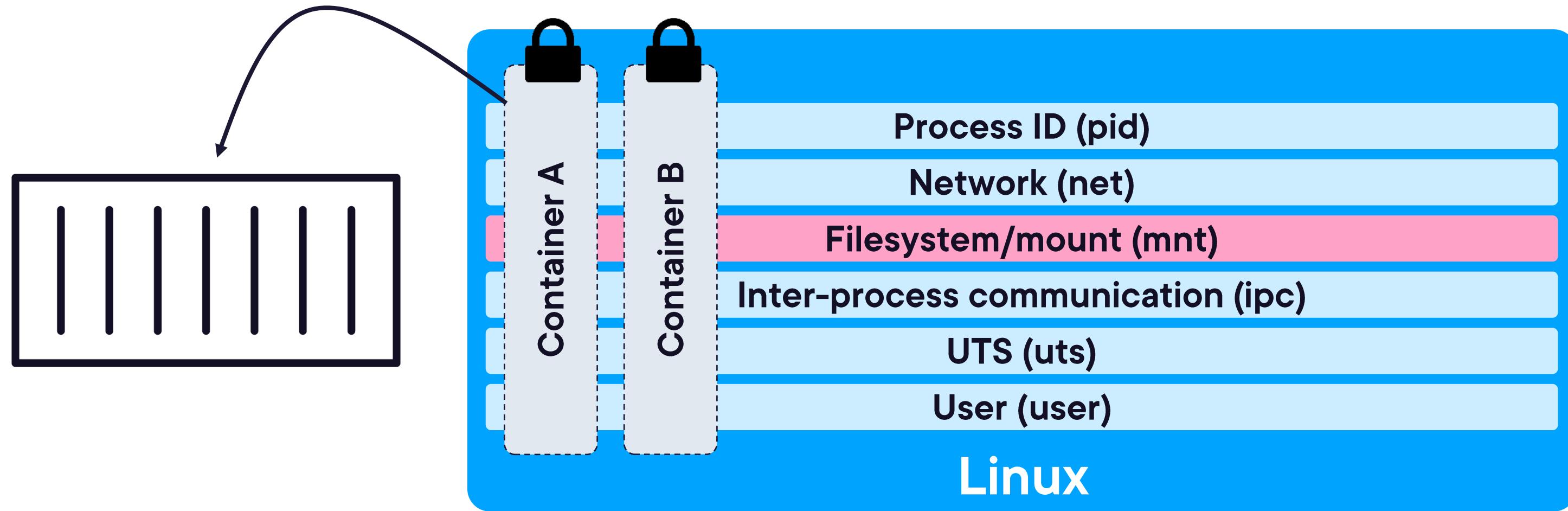




Namespaces
All about isolation

Control Groups
All about limits

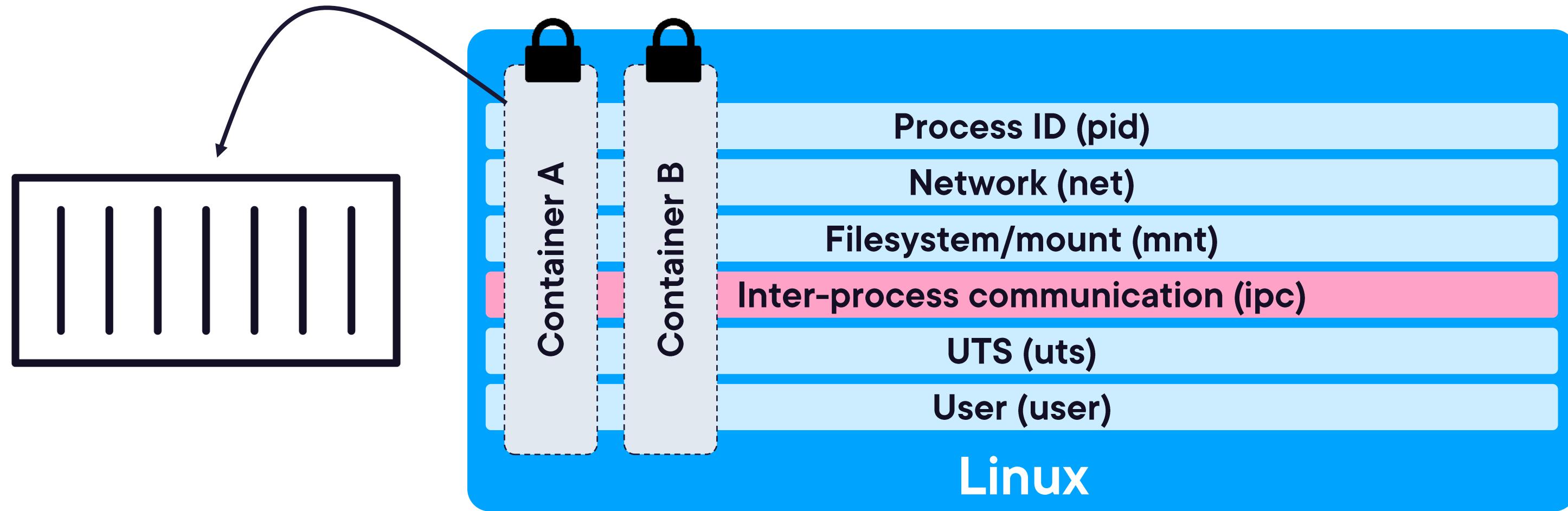




Namespaces
All about isolation

Control Groups
All about limits

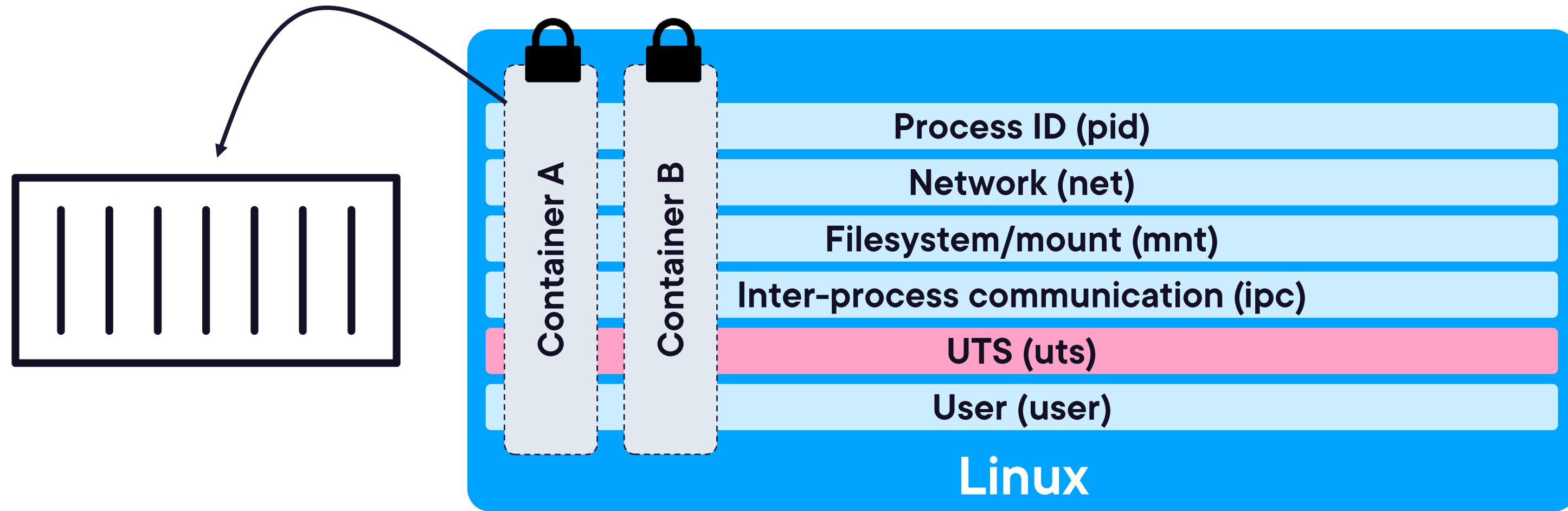




Namespaces
All about isolation

Control Groups
All about limits

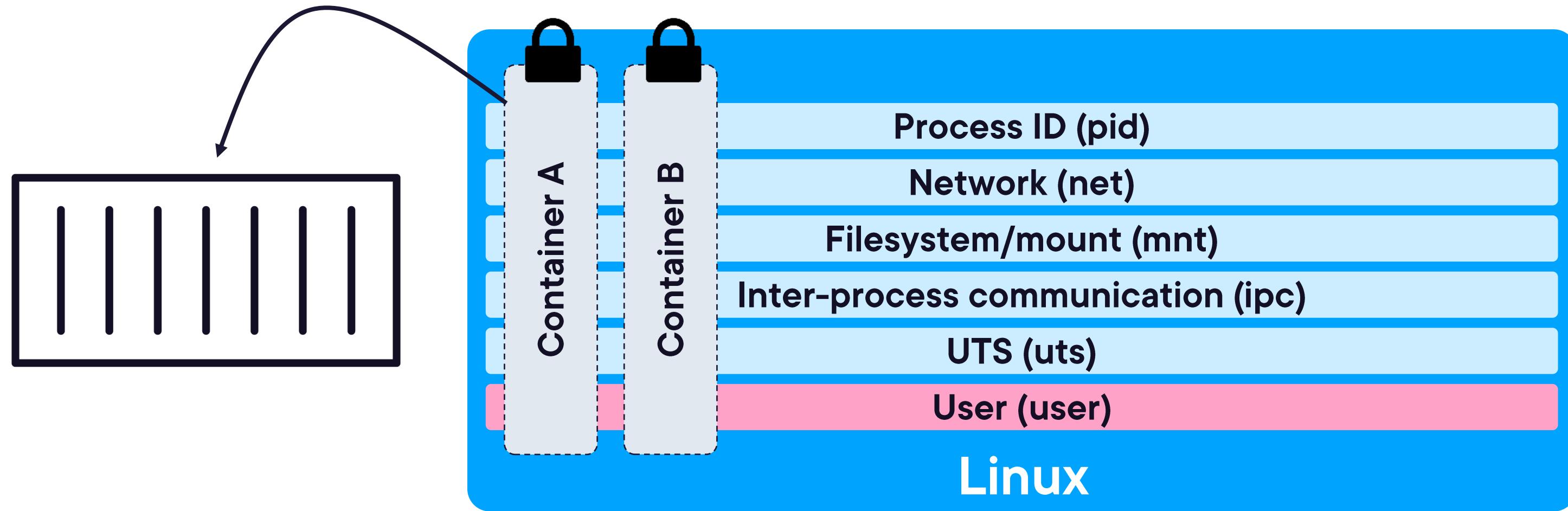




Namespaces
All about isolation

Control Groups
All about limits

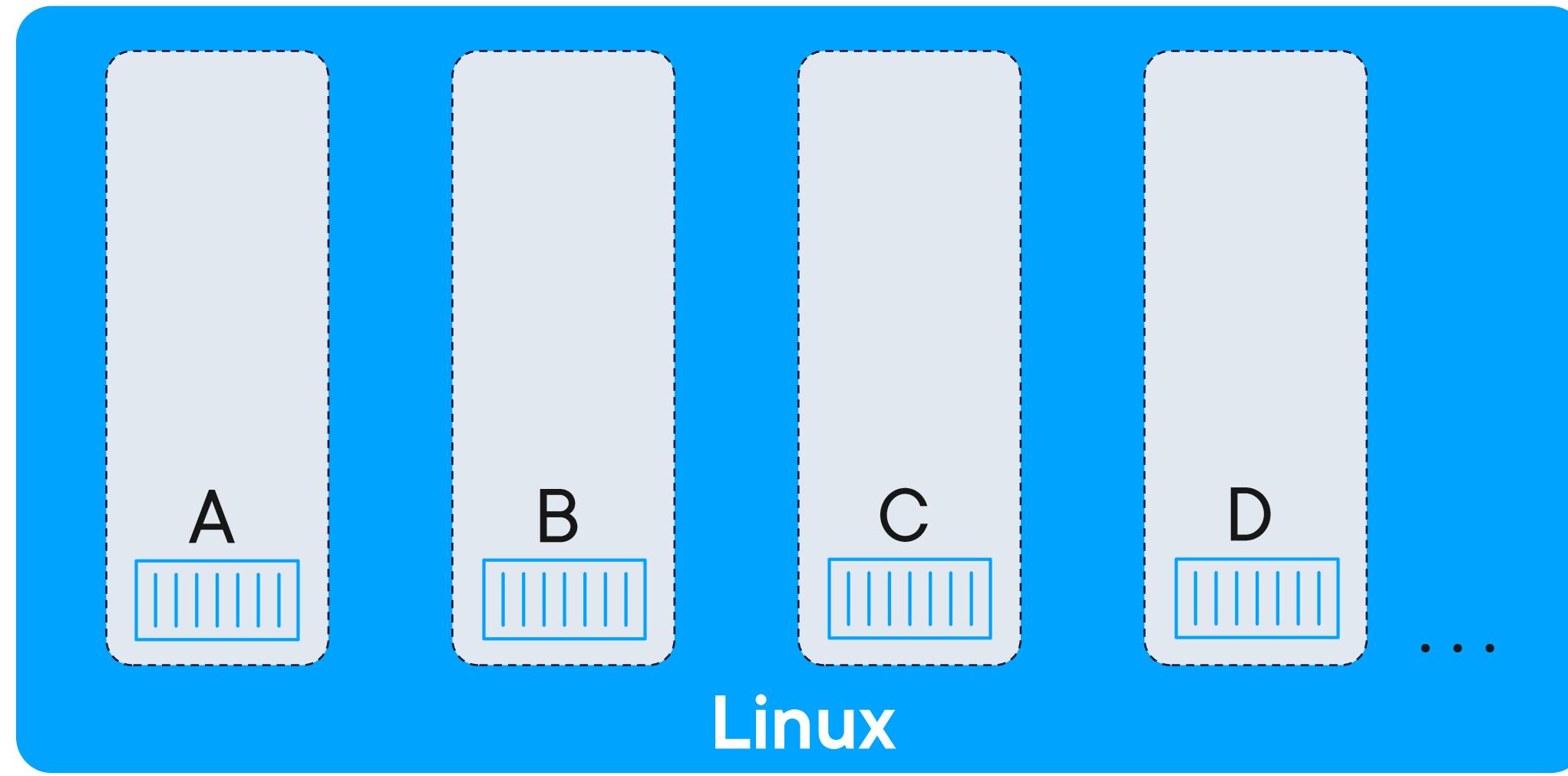




Namespaces
All about isolation

Control Groups
All about limits

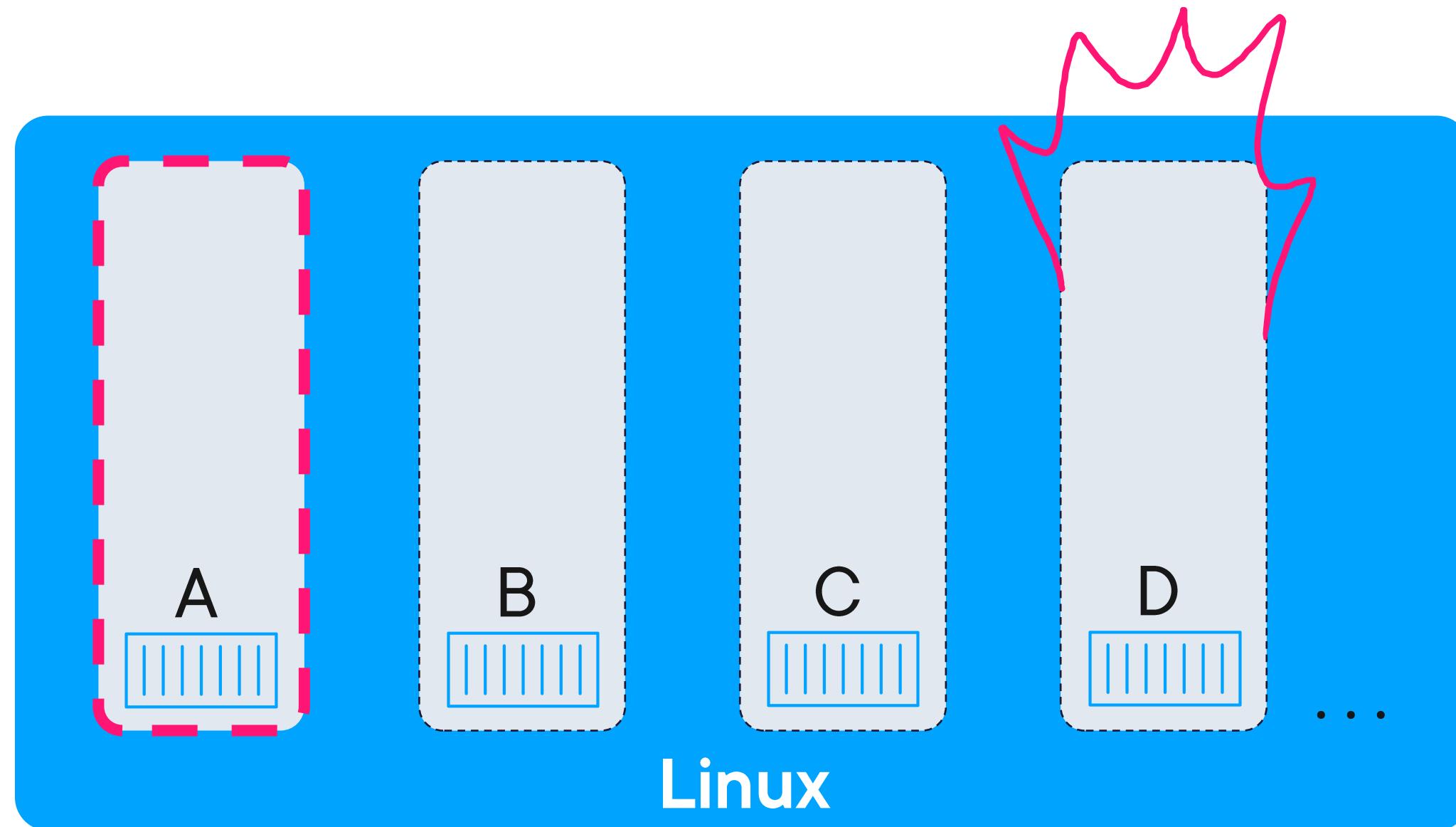




Namespaces
All about isolation

Control Groups
All about limits

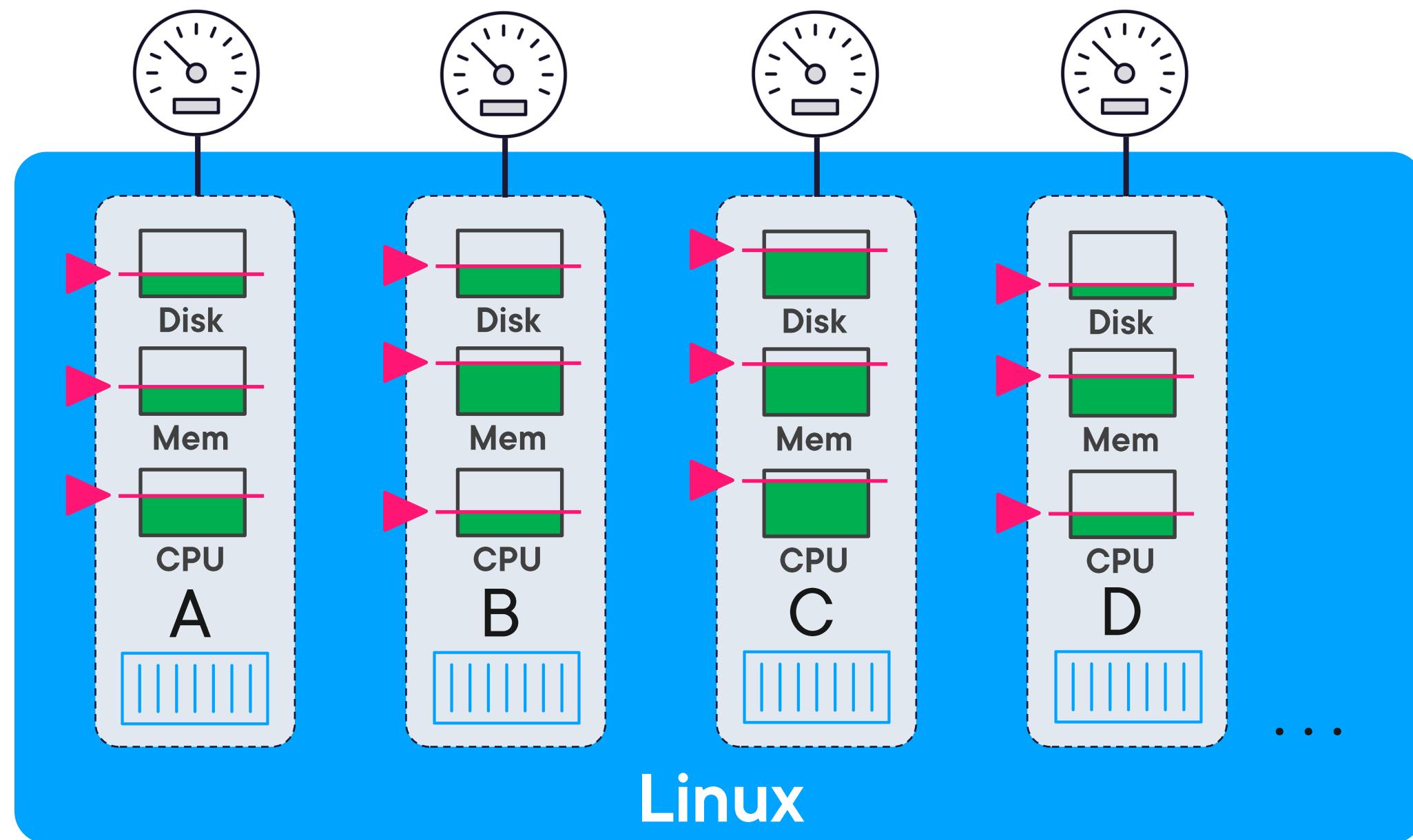




Namespaces
All about isolation

Control Groups
All about limits

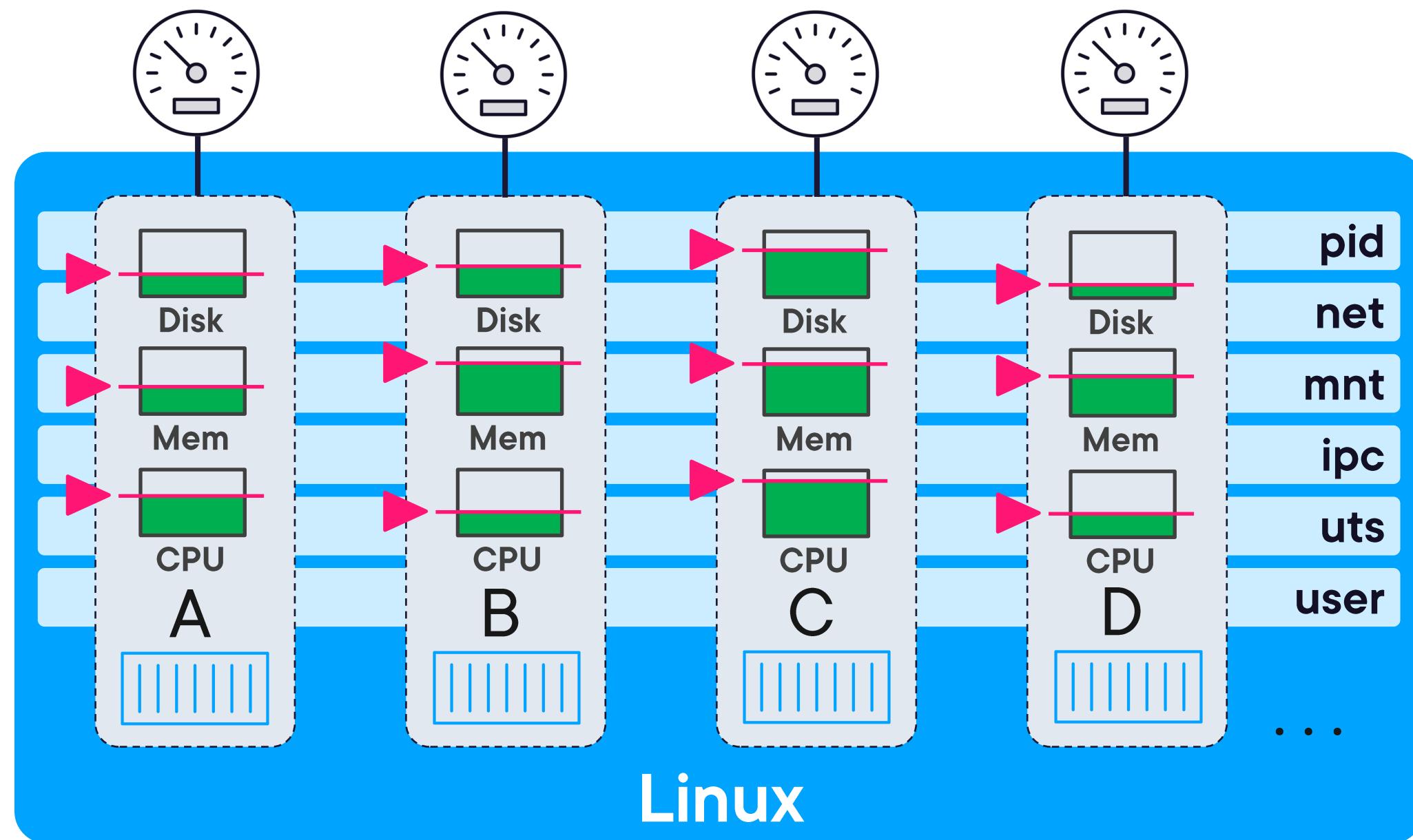




Namespaces
All about isolation

Control Groups
All about limits

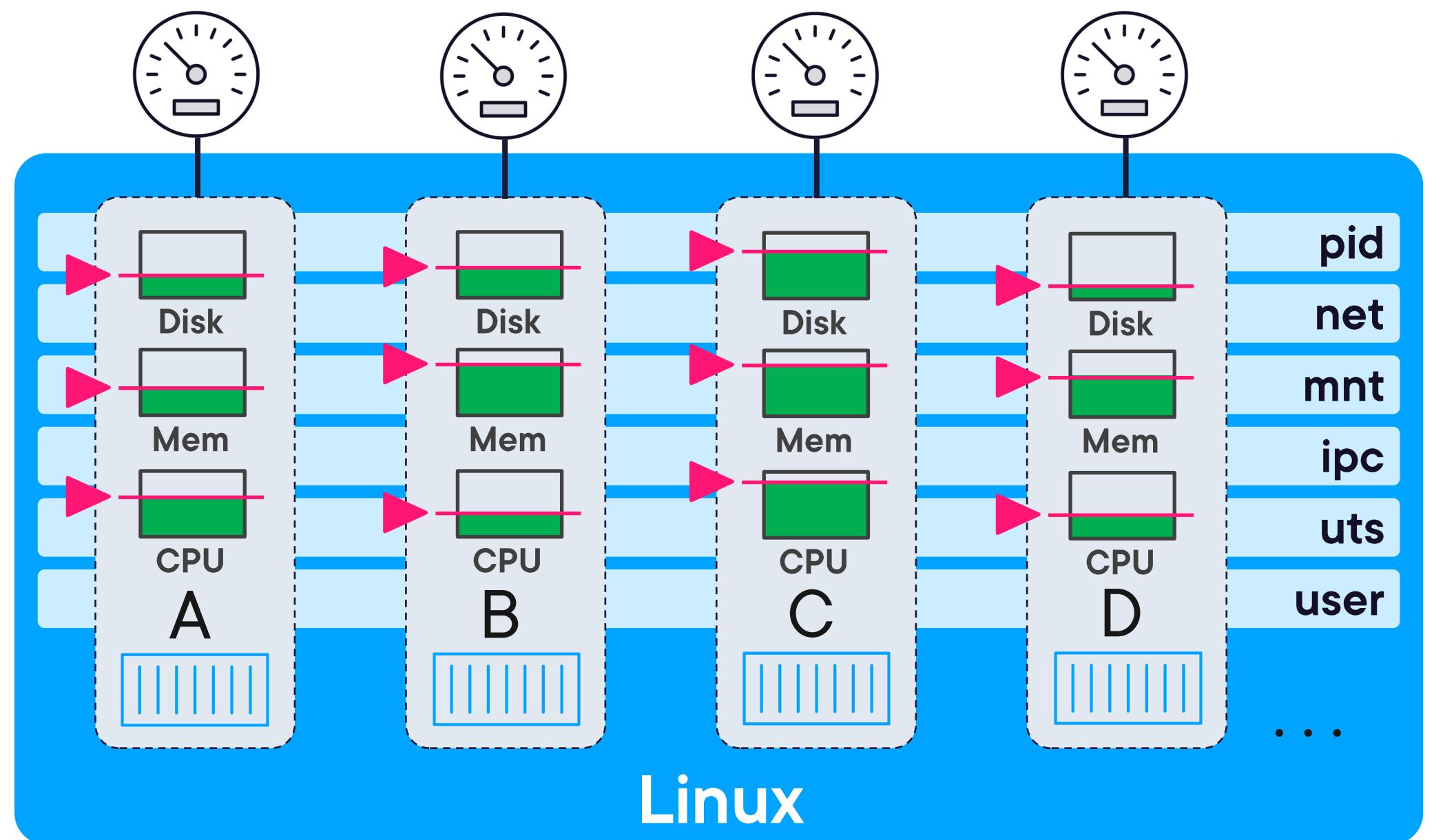




Namespaces
All about isolation

Control Groups
All about limits



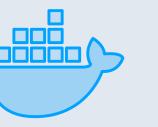


Layered mounts
Copy on Write

Namespaces
All about isolation

Control Groups
All about limits





Docker – The Easy Layer...

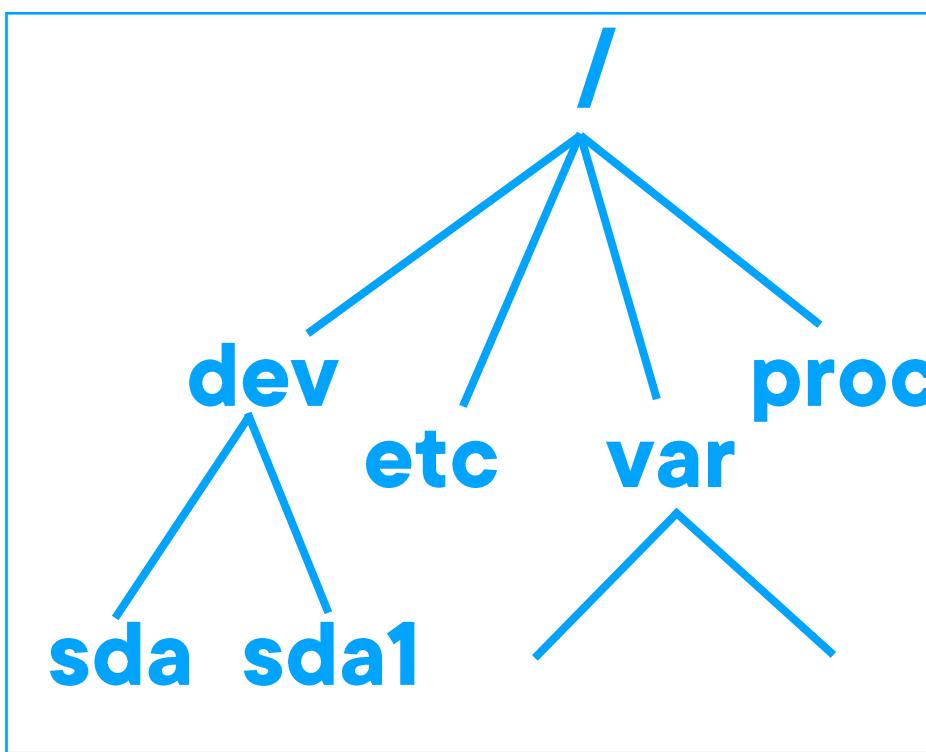
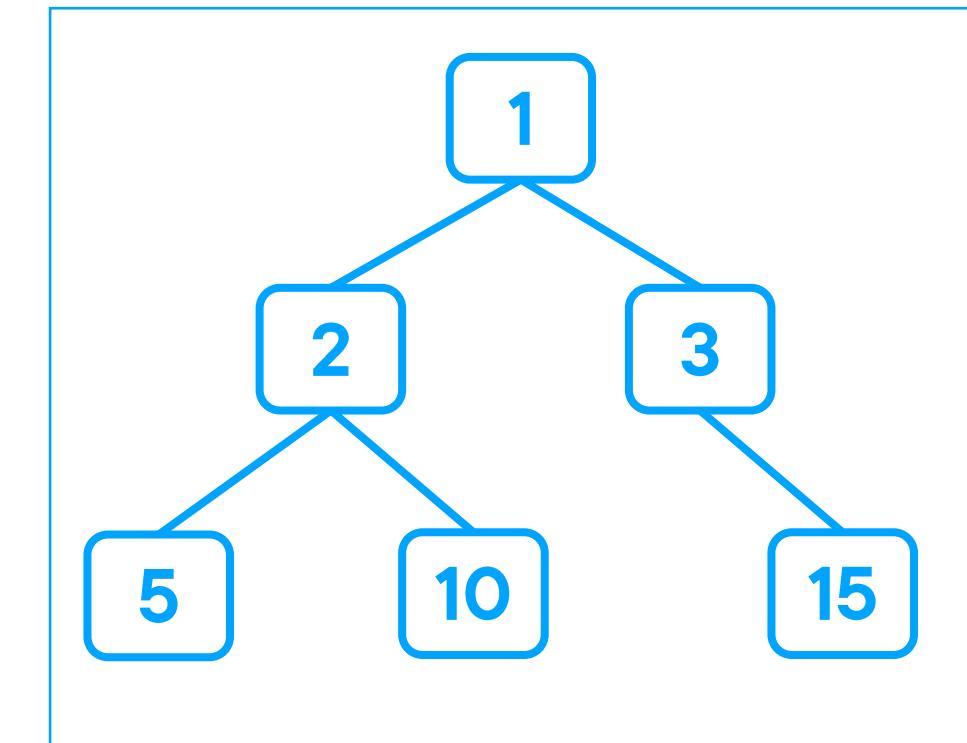
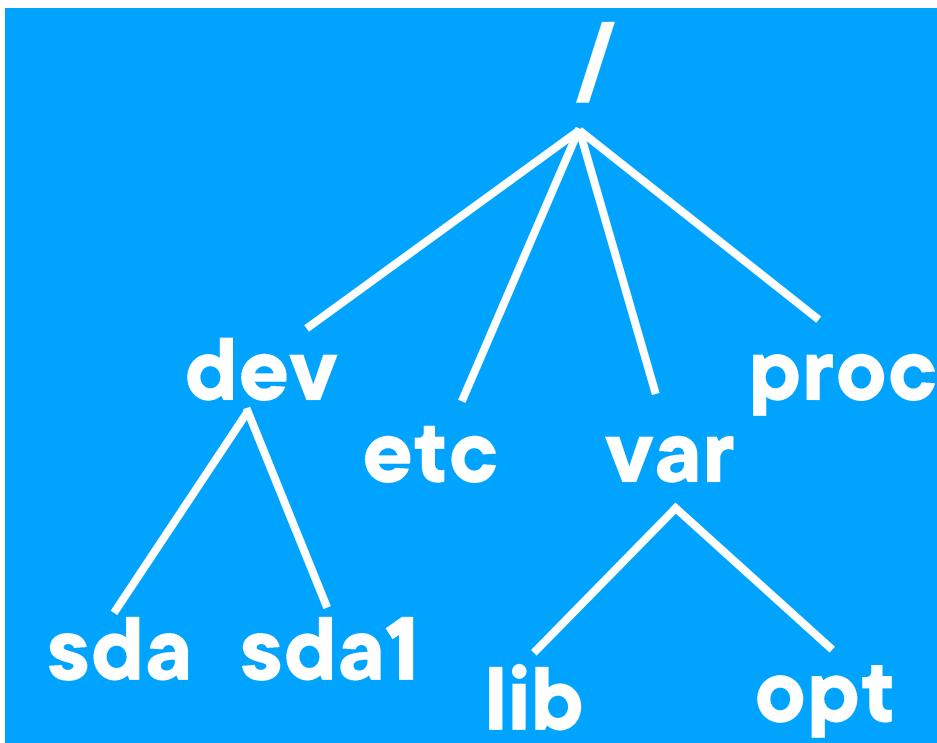
Layered mounts
Copy on Write

Namespaces
All about isolation

Control Groups
All about limits

...

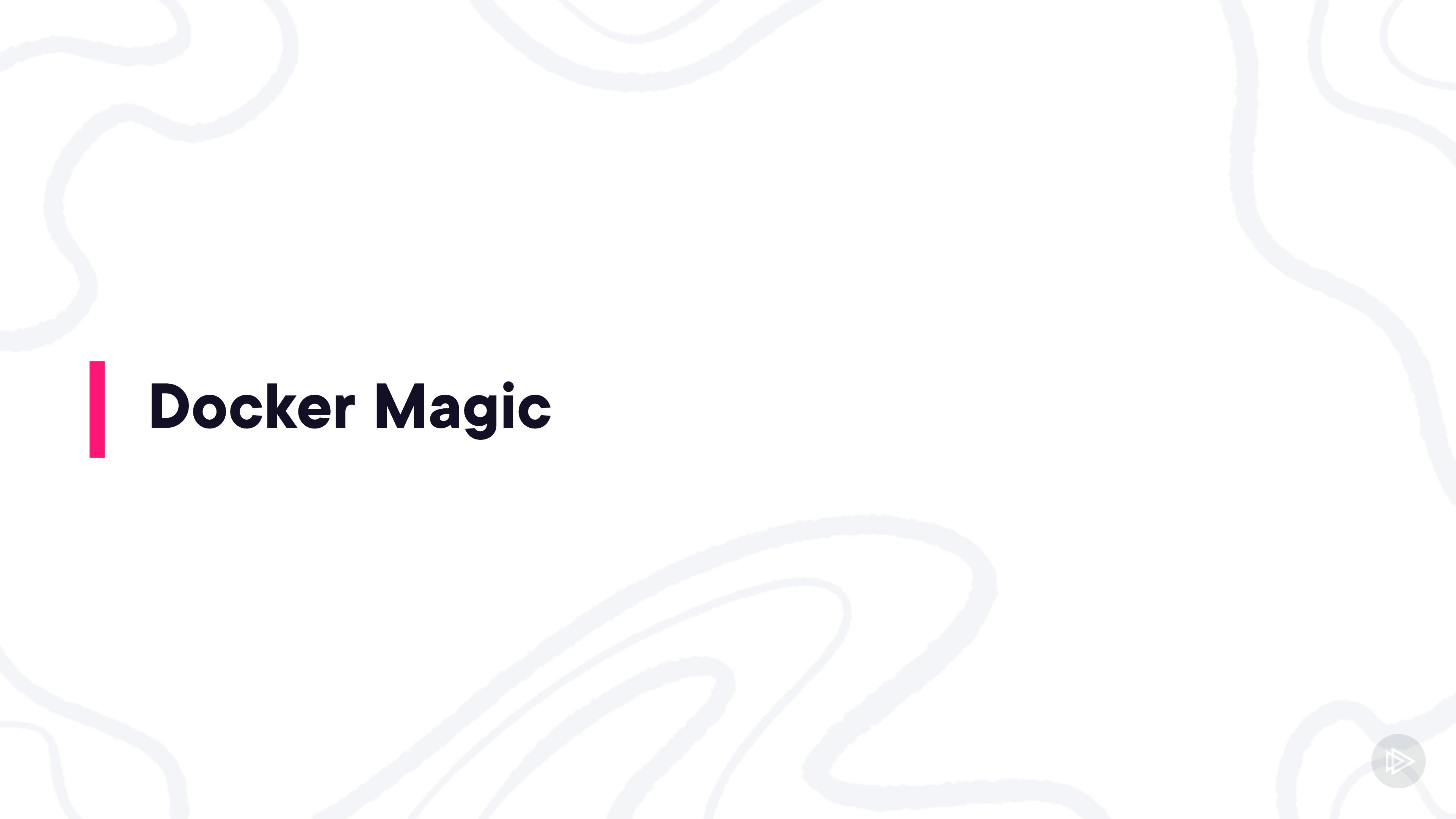




Up Next:

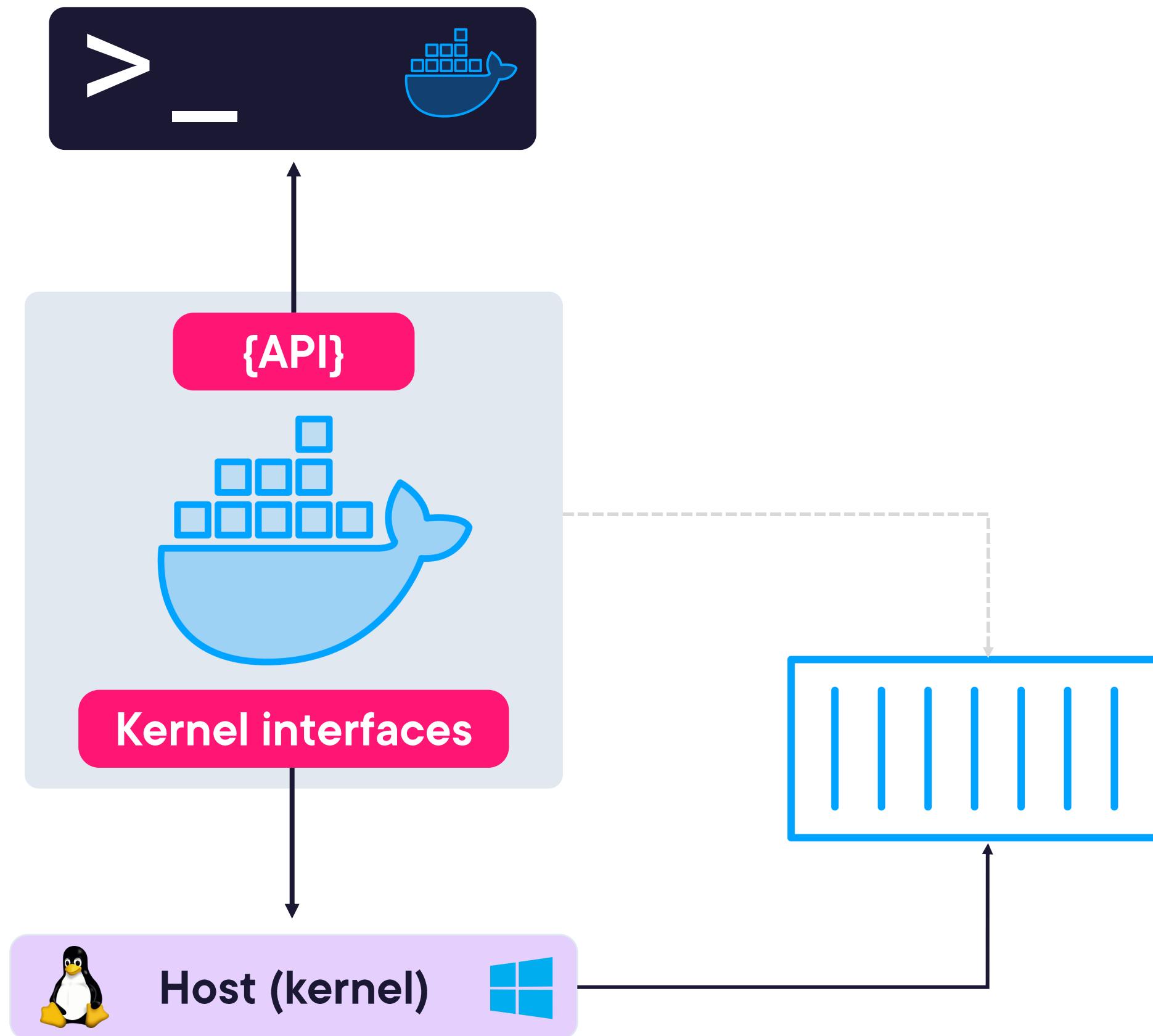
Docker Magic

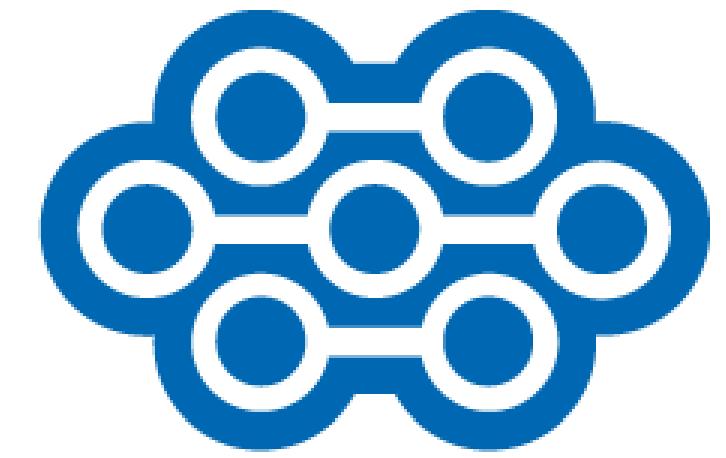




Docker Magic

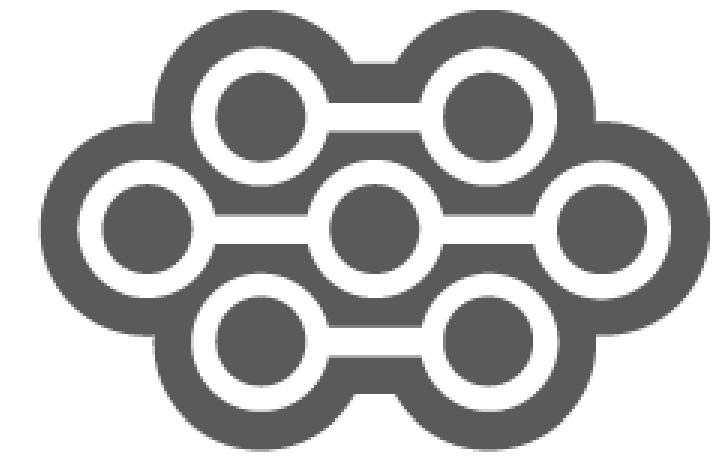






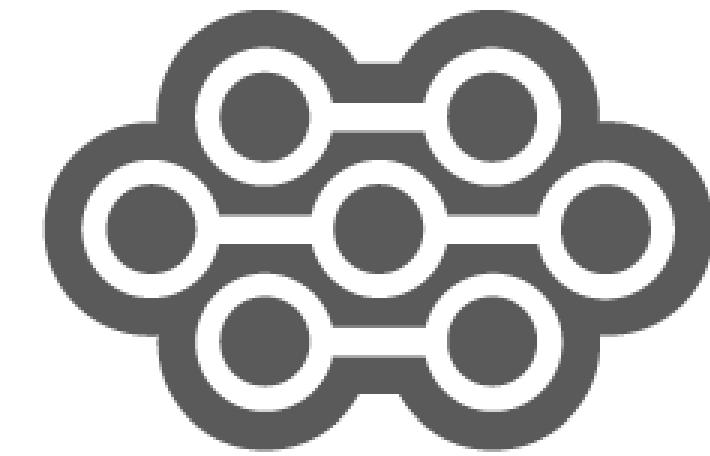
dotCloud



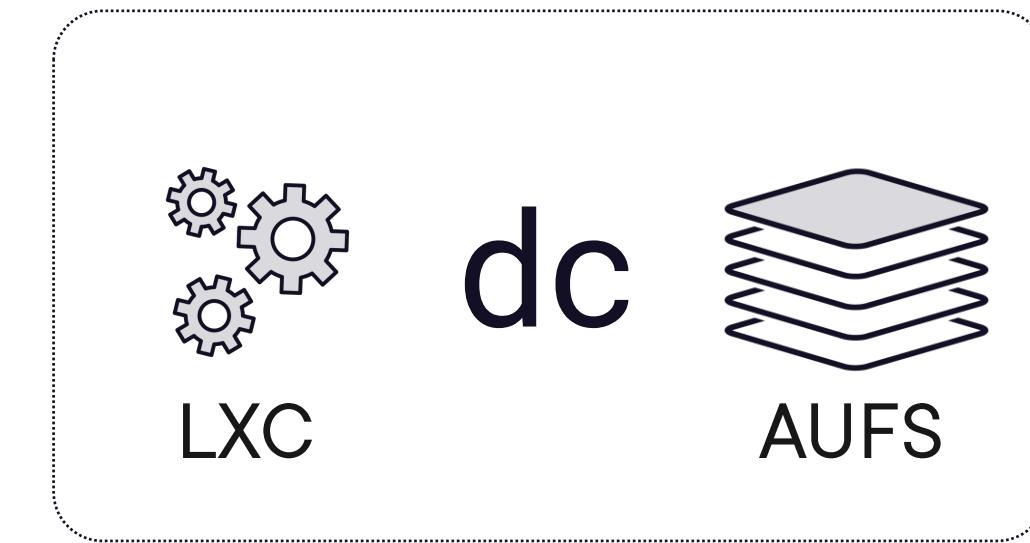


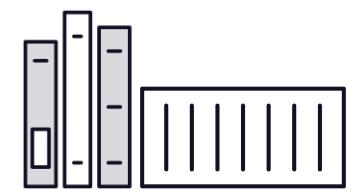
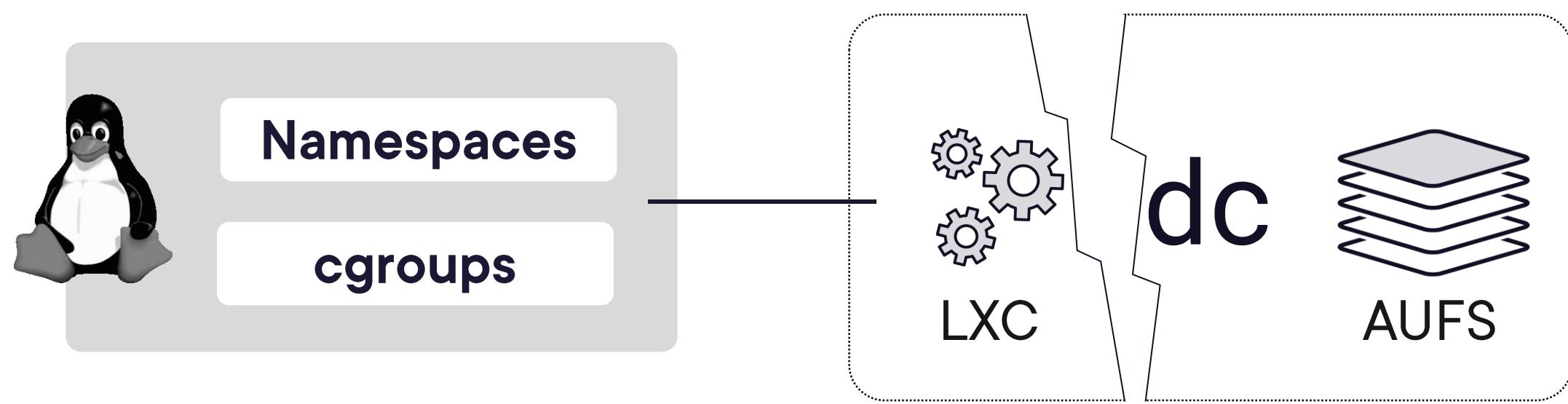
dot**C**loud





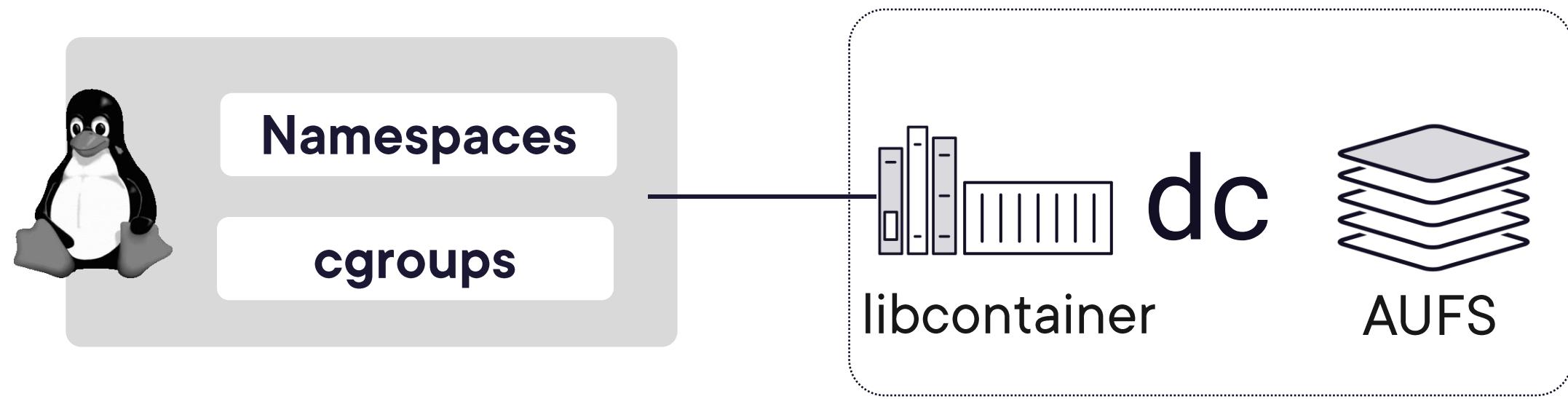
dotCloud

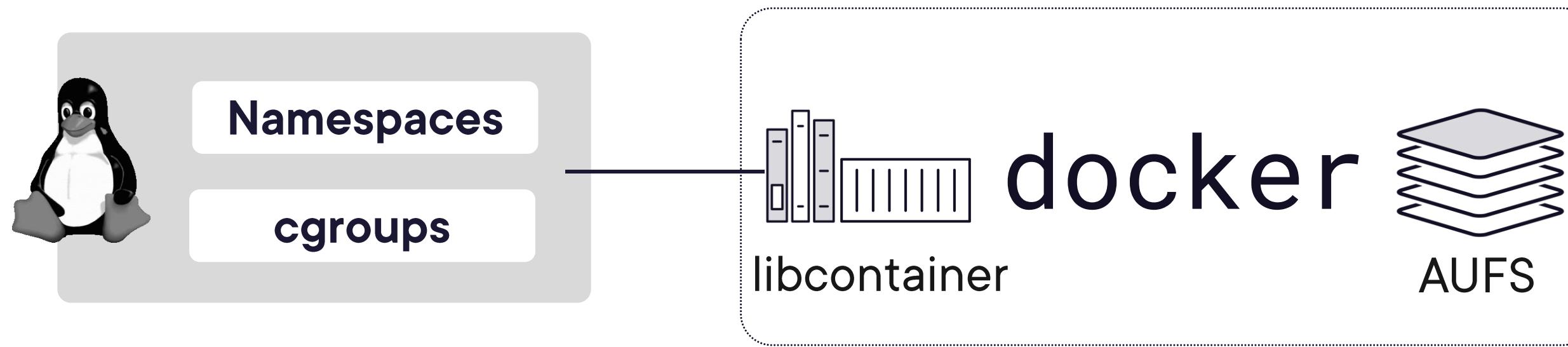


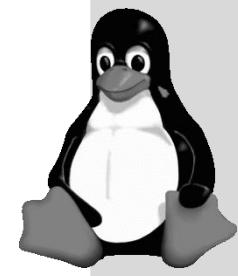


libcontainer

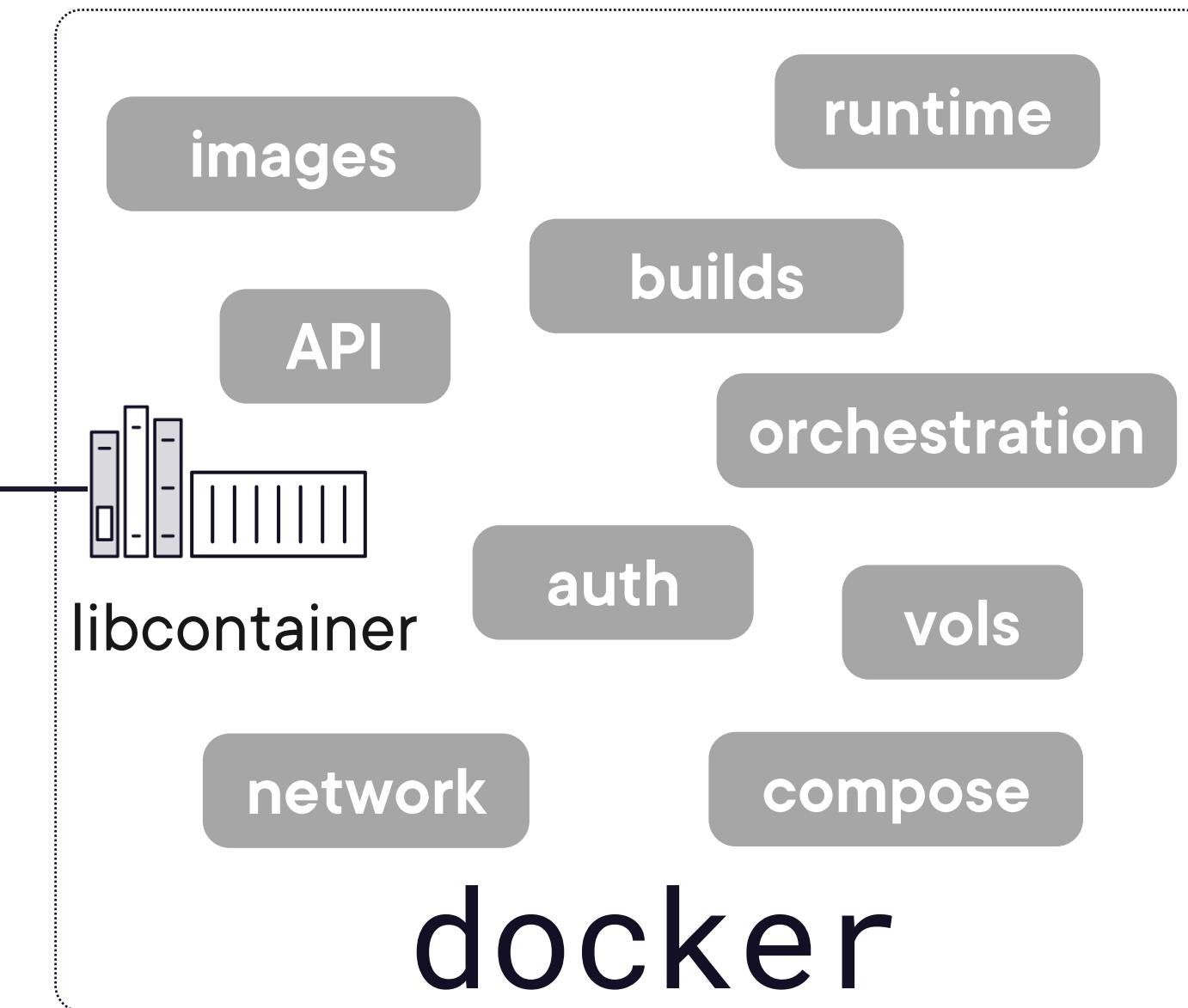






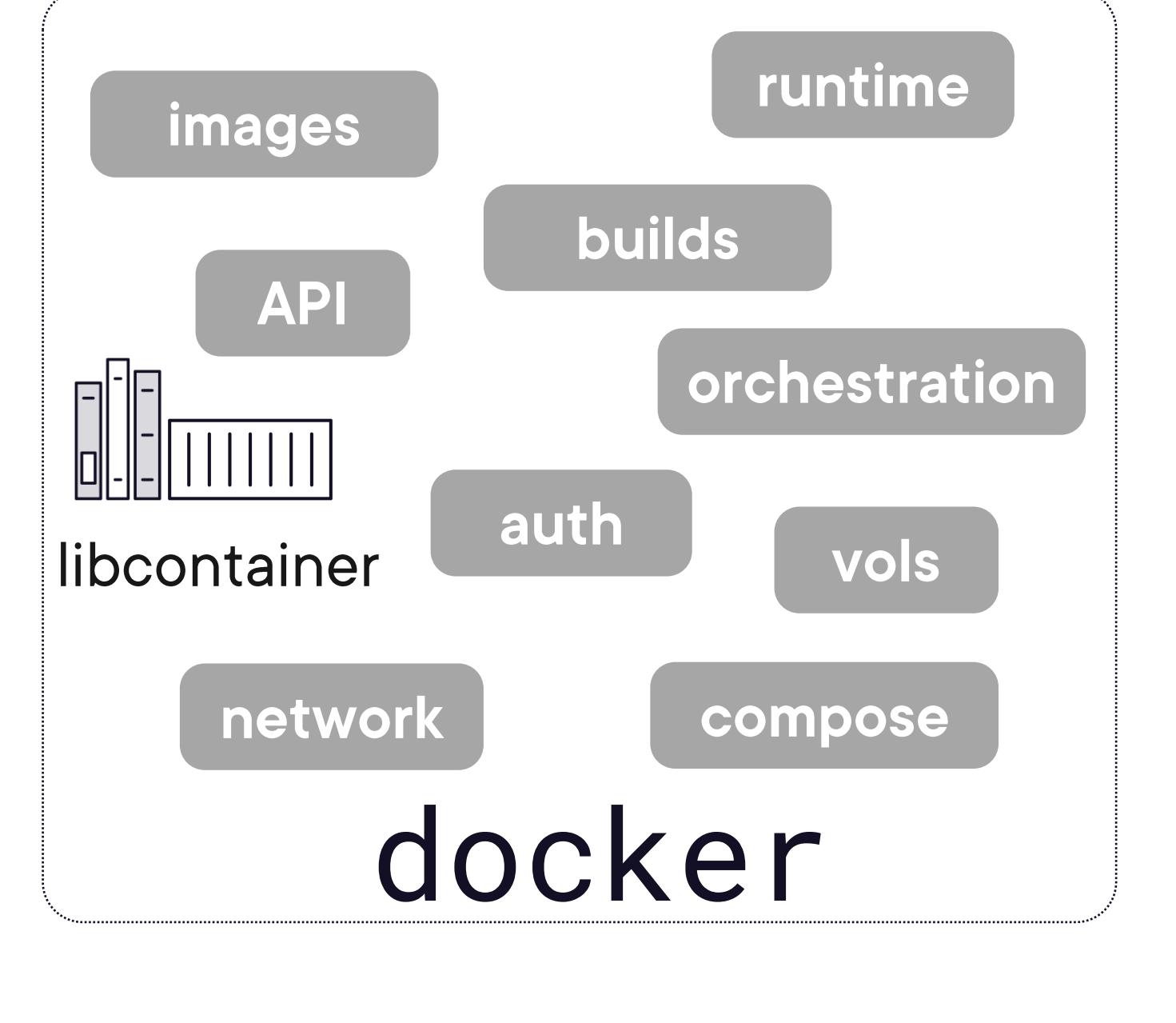


Namespaces
cgroups



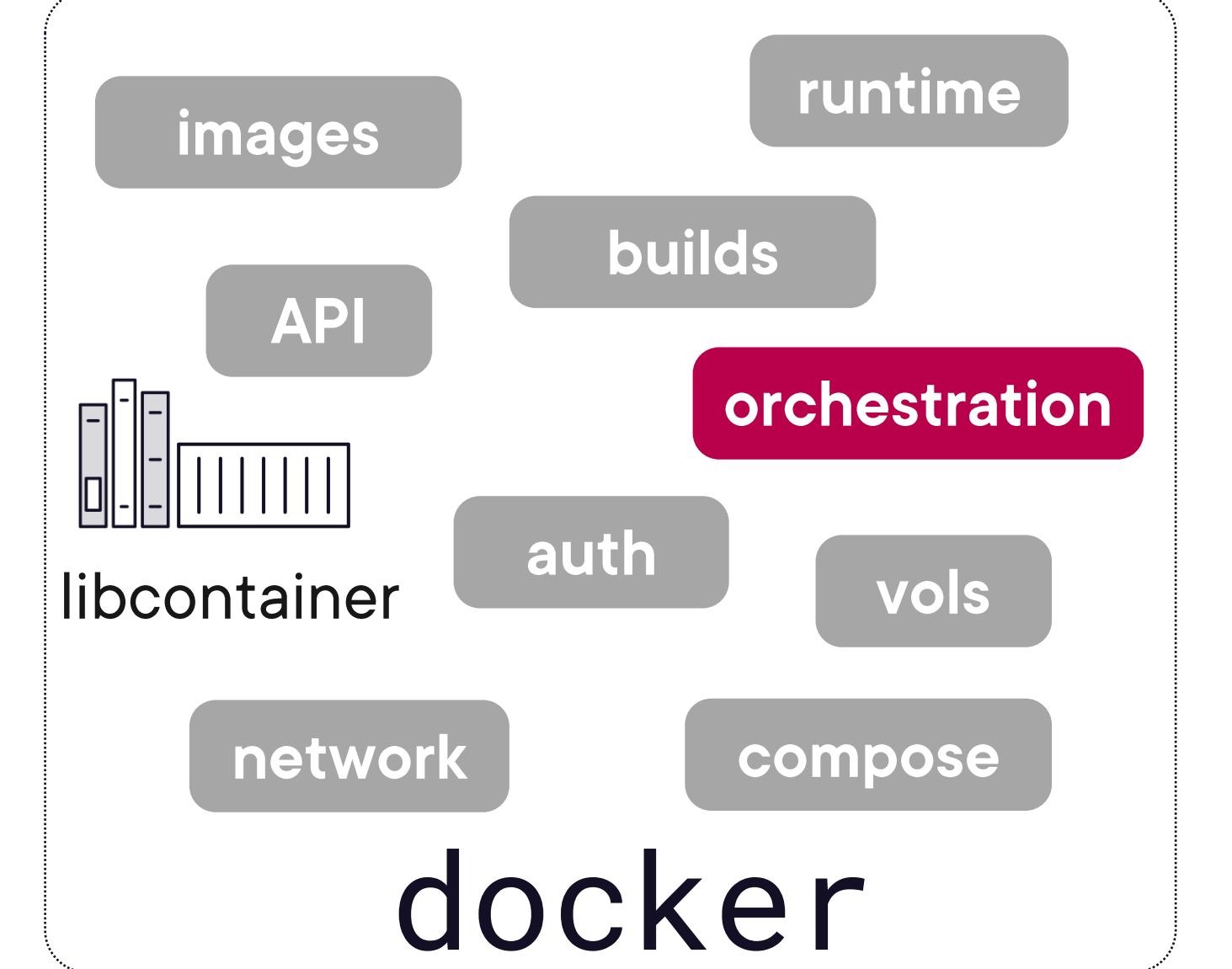


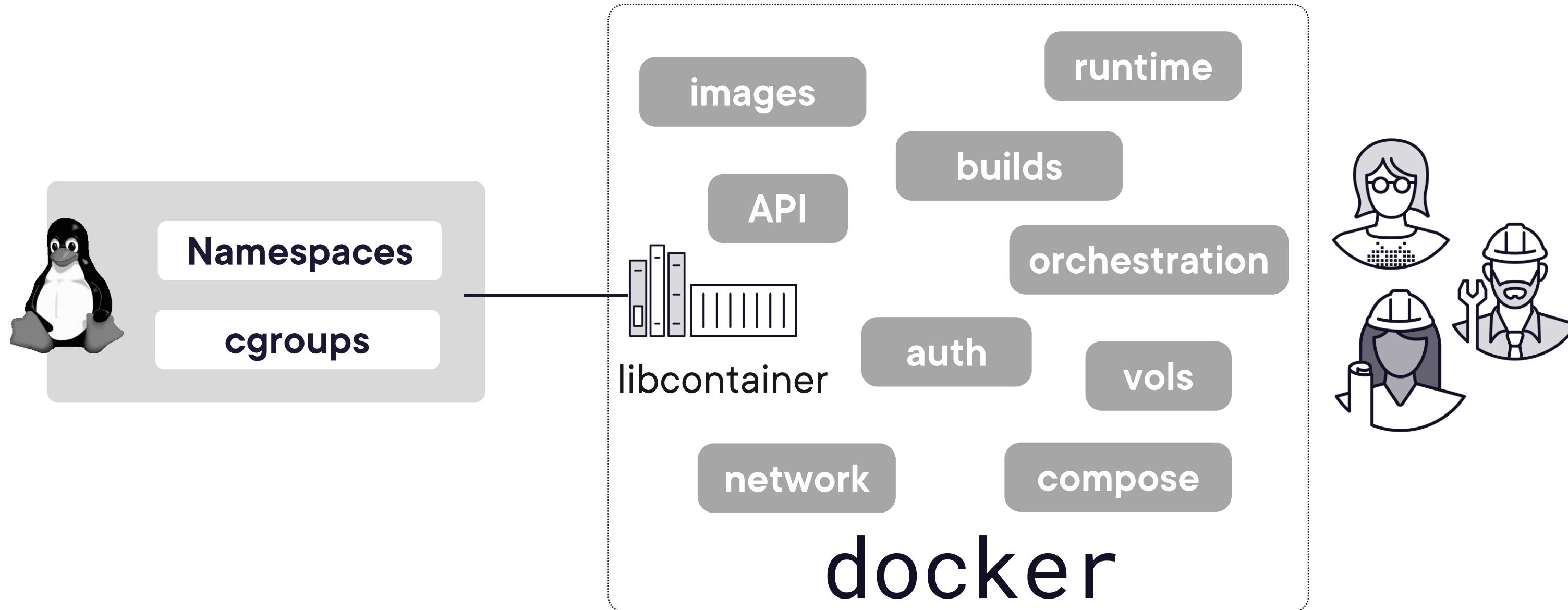
Orchestrator

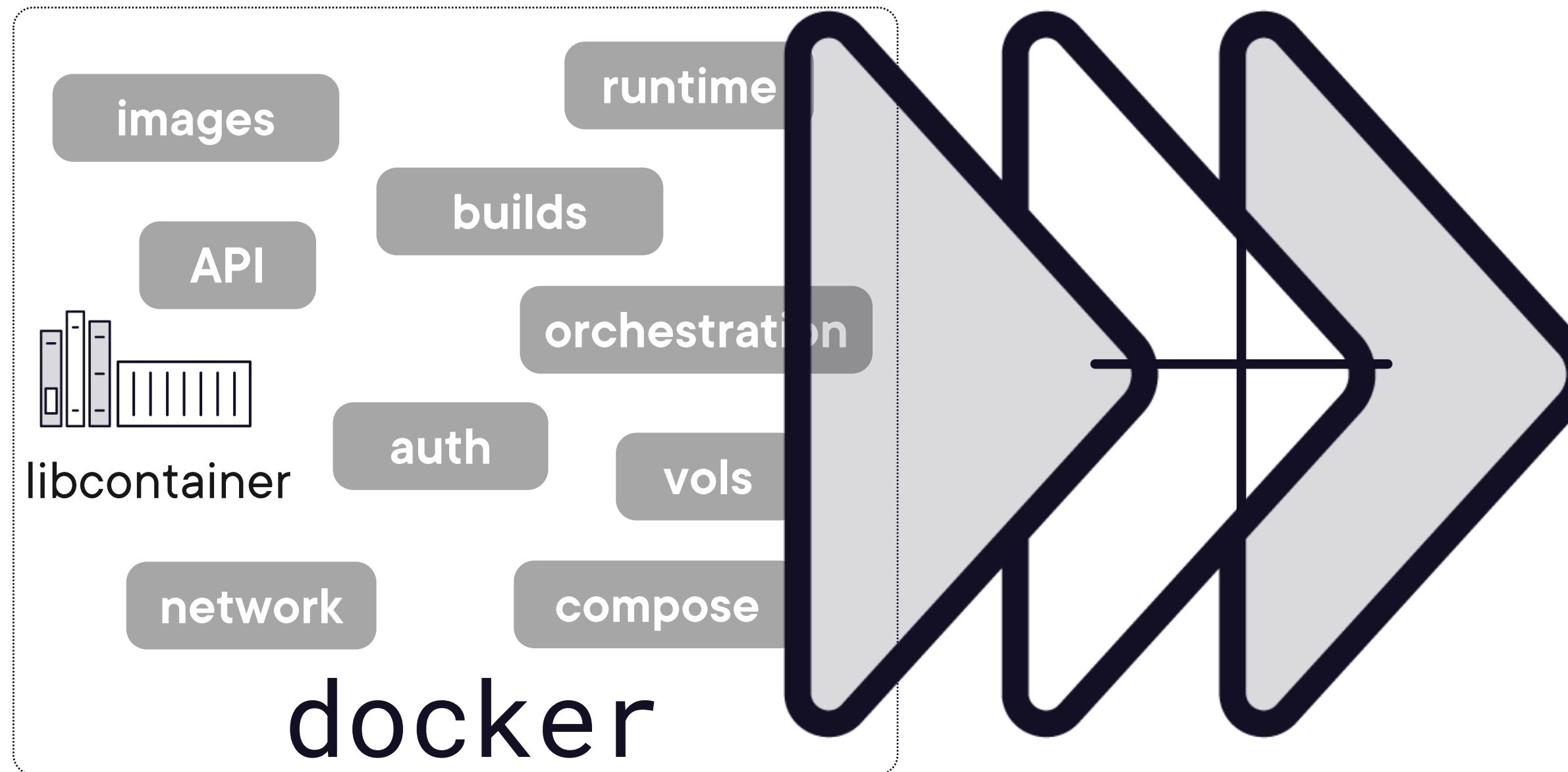




Orchestrator





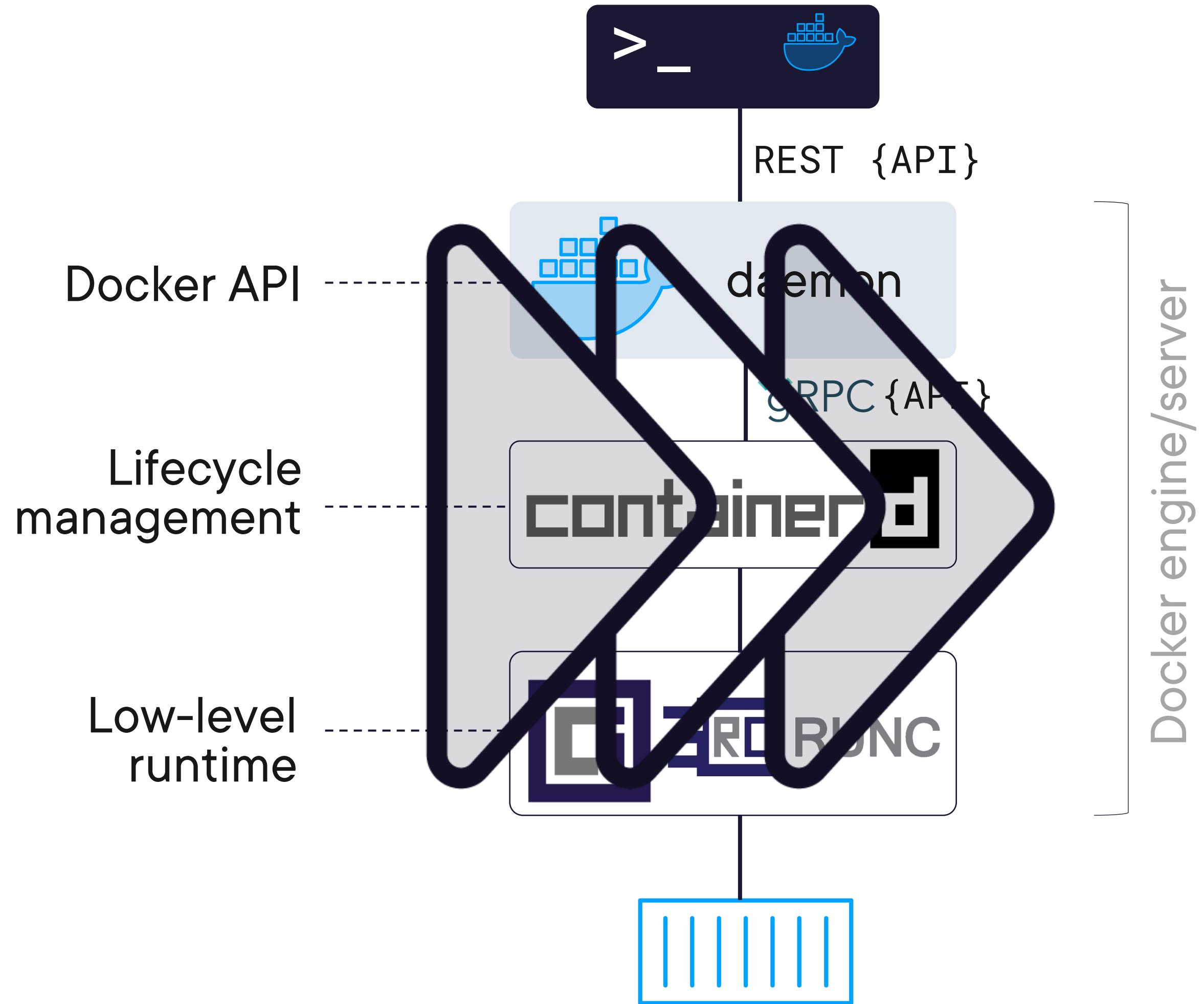


OPEN CONTAINER
INITIATIVE

Image spec

Runtime spec





```
$ docker run
```



{REST} POST /vX.X/containers/create HTTP/1.1

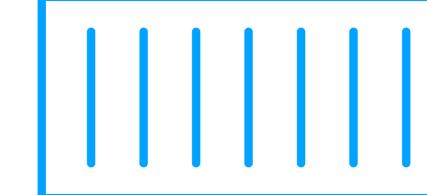


gRPC {API} client.NewContainer(context, ...)



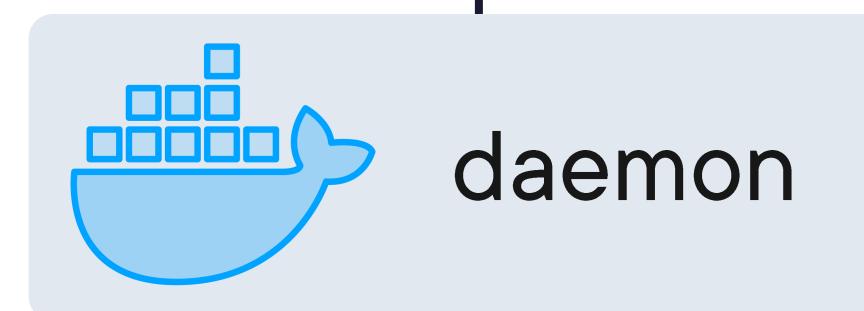
Shim

RUNC



```
$ docker run
```

{REST} POST /vX.X/containers/create HTTP/1.1



daemon

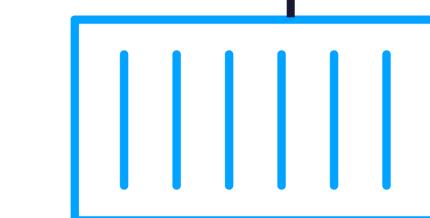
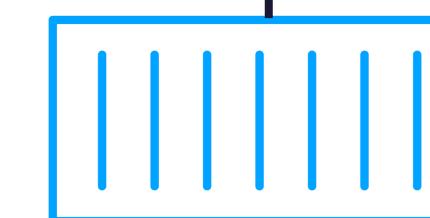
gRPC {API} client.NewContainer(context, ...)

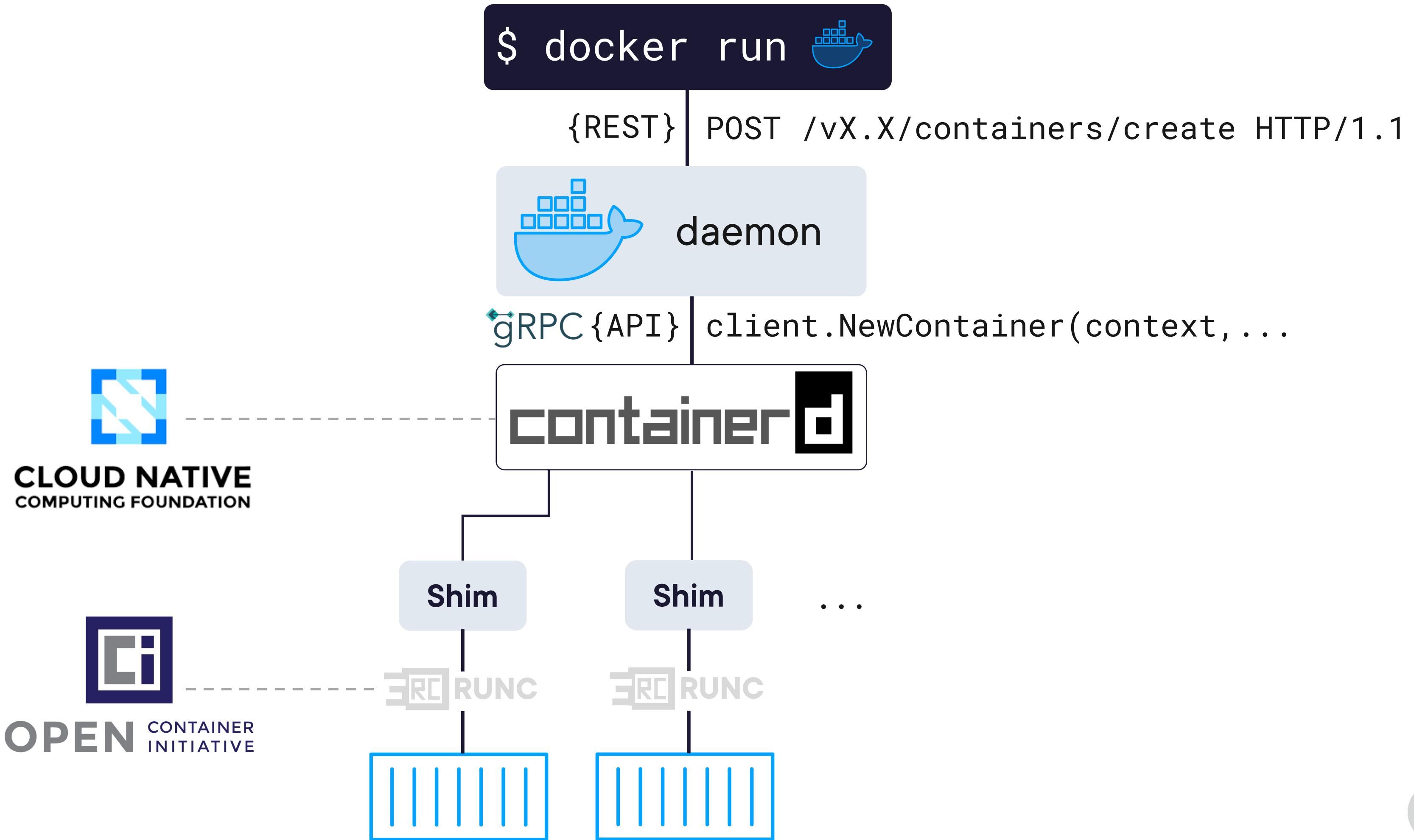


Shim

Shim

...





```
$ docker run
```



Docker API,
Image management...



CLOUD NATIVE
COMPUTING FOUNDATION

containerd

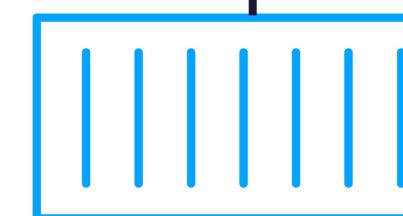
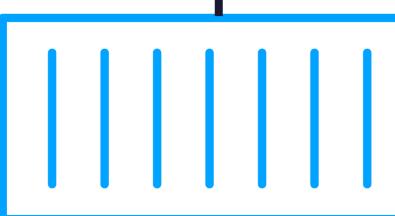
Shim

Shim

...

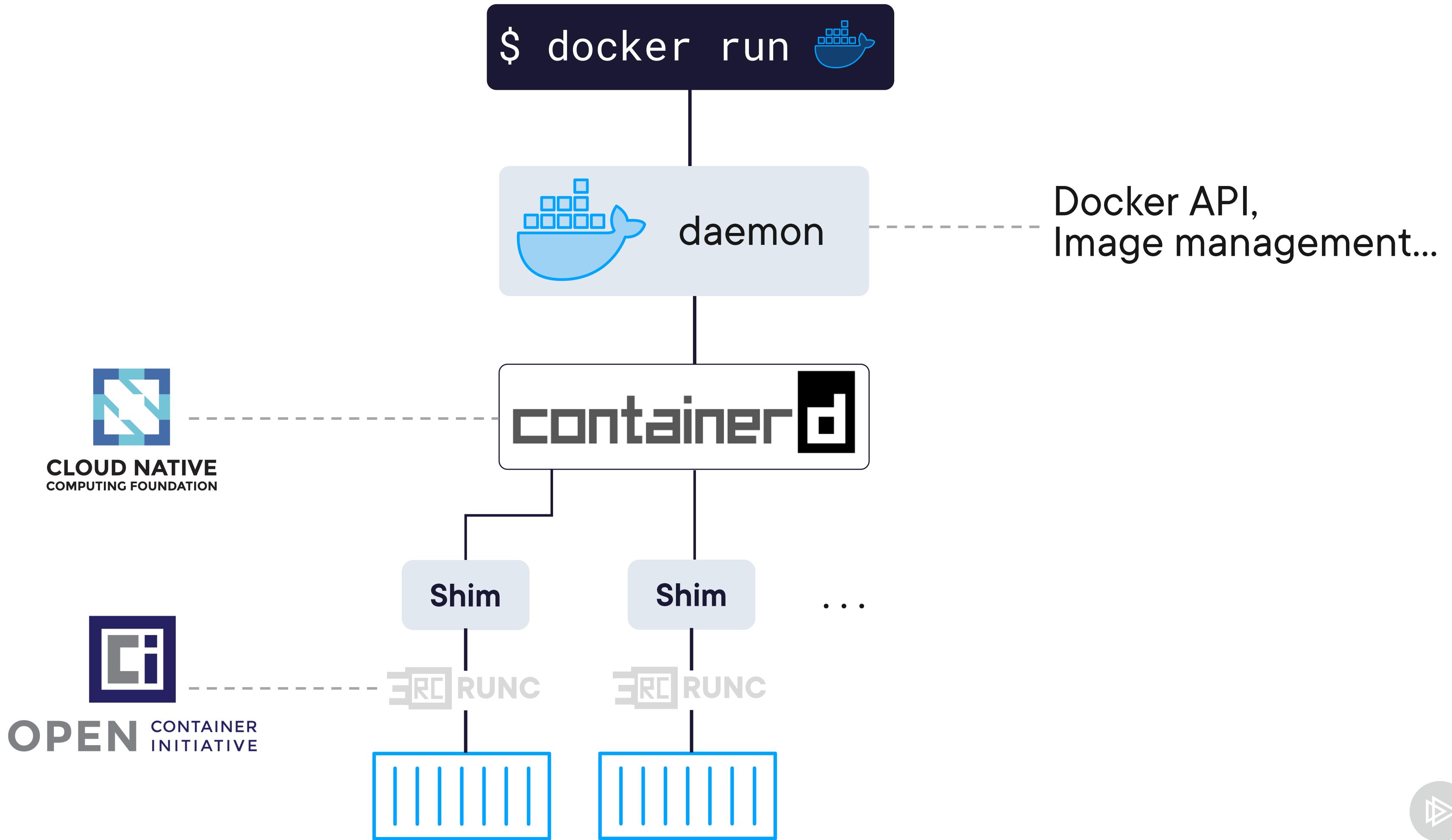
runc

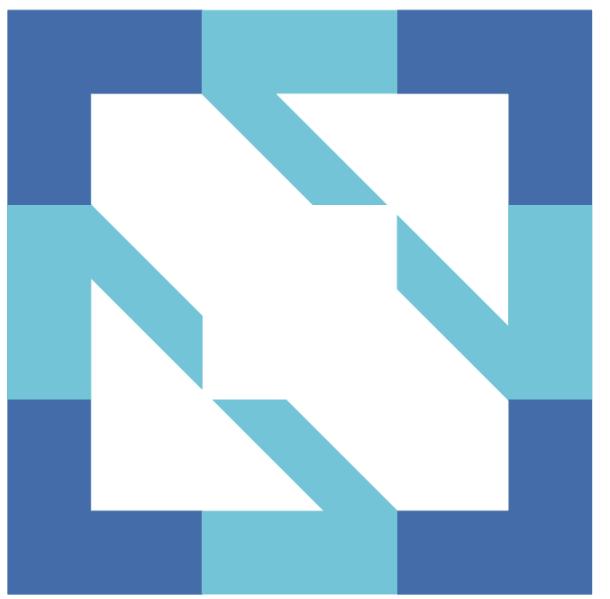
runc



OPEN CONTAINER
INITIATIVE







**CLOUD NATIVE
COMPUTING FOUNDATION**



**OPEN CONTAINER
INITIATIVE**



Up Next:

Containers on Windows



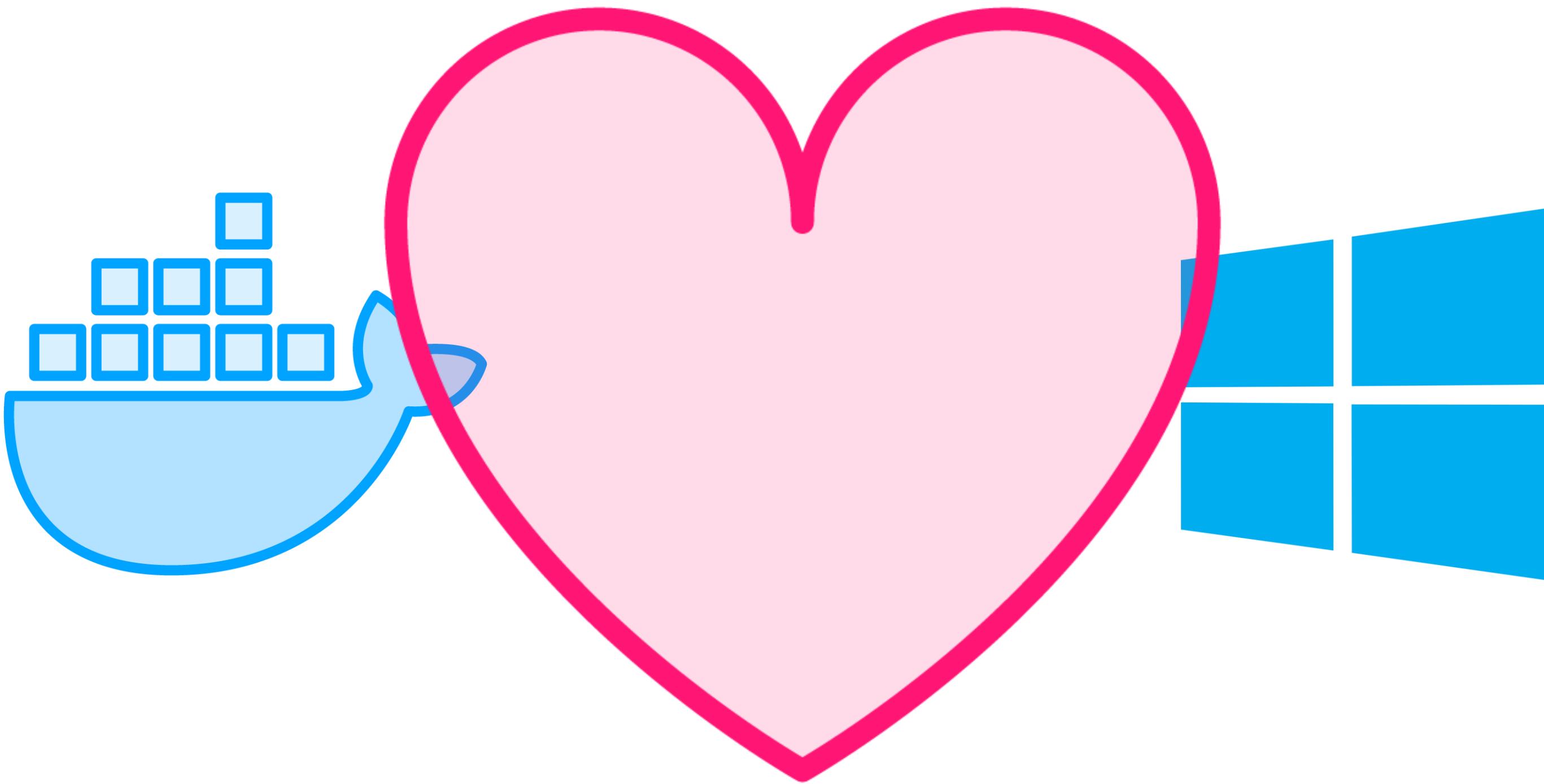
Containers on Windows



Windows Containers

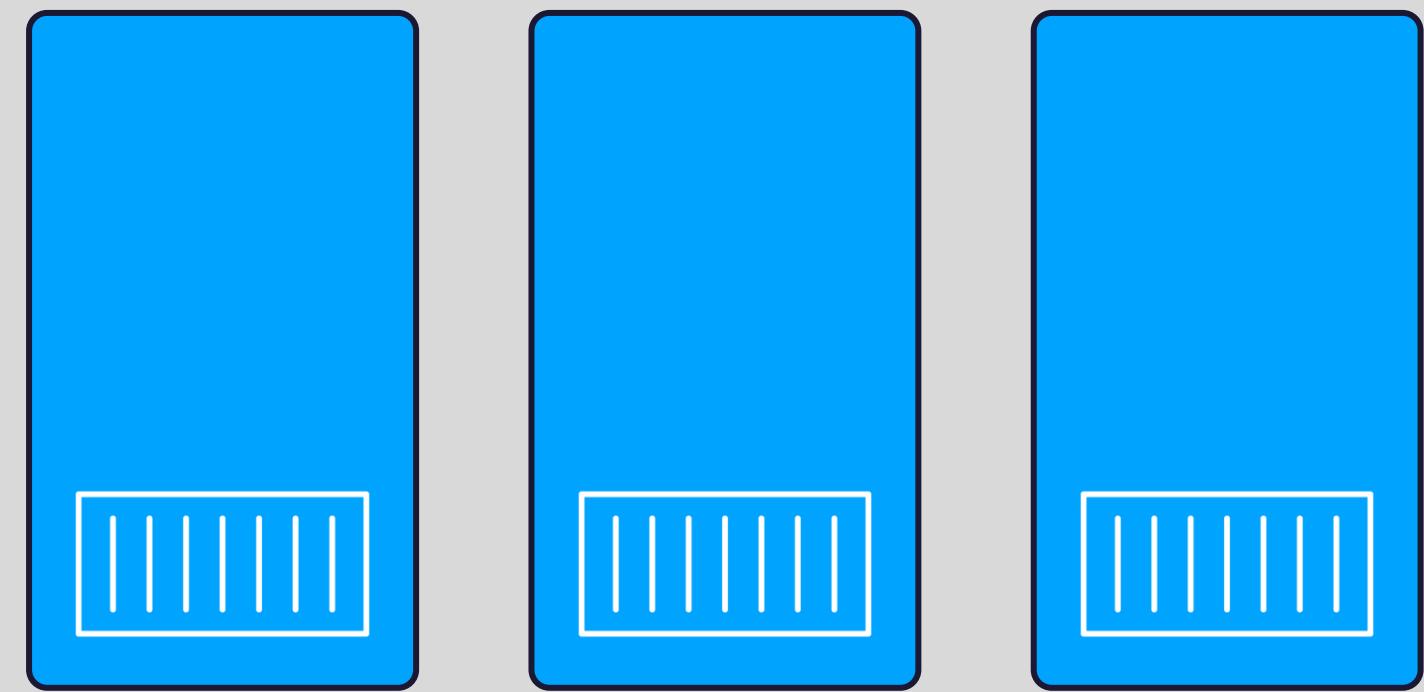
Docker on Windows

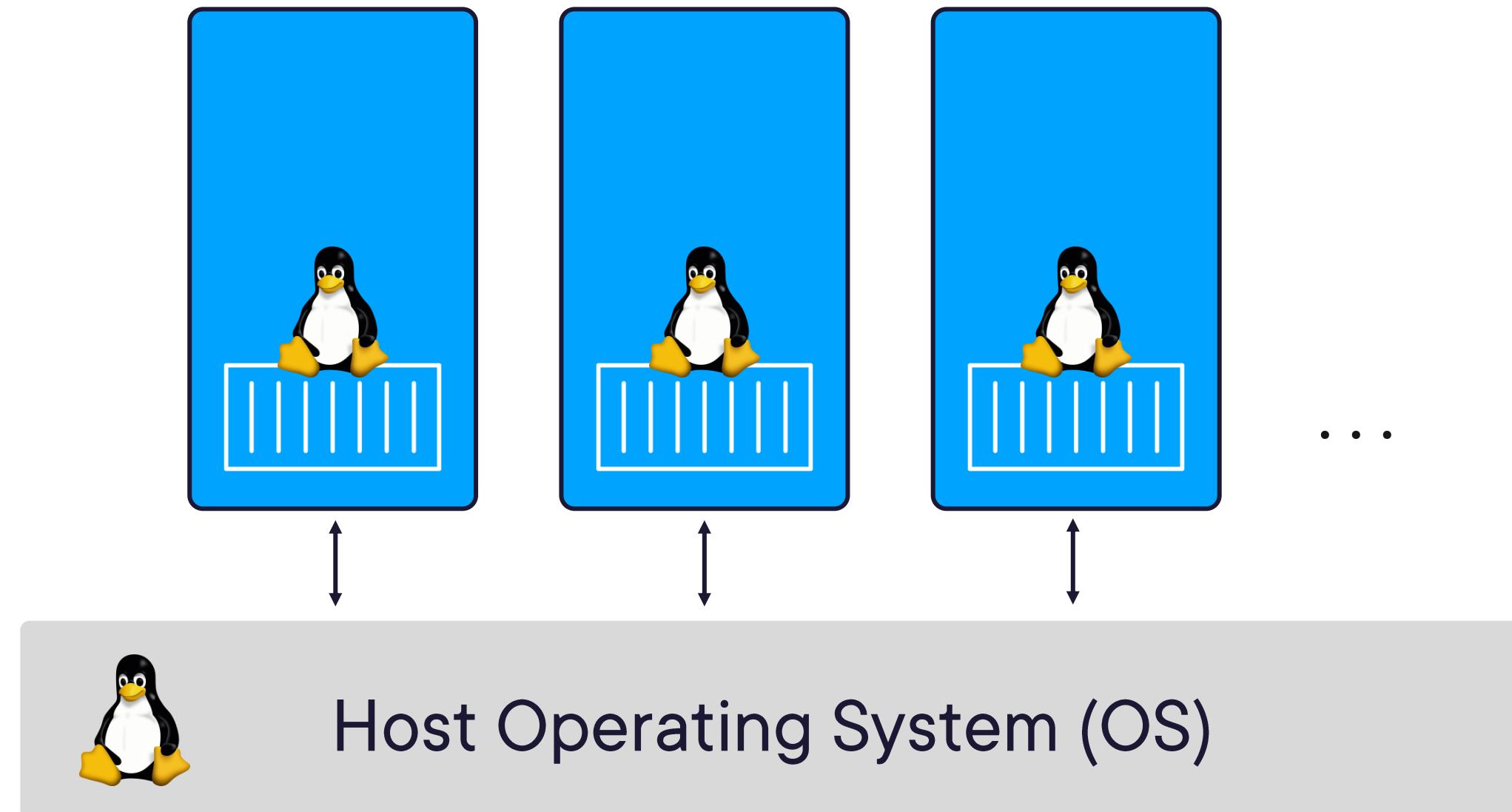


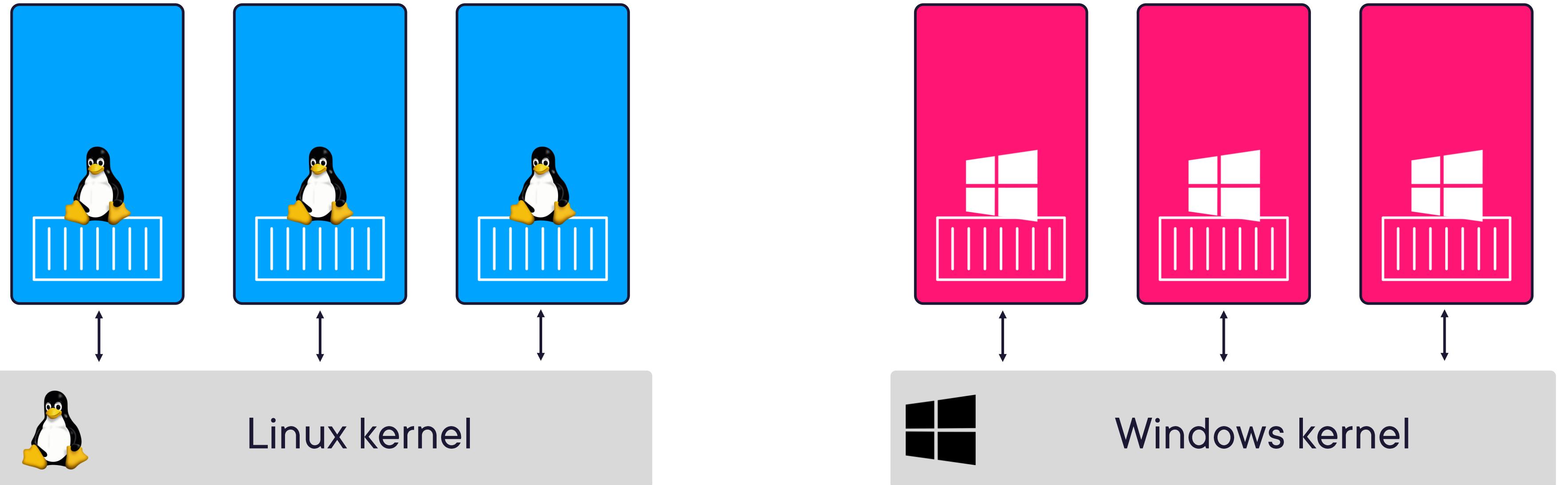


	Docker on macOS	Docker on Linux	Docker on Windows
Linux containers			
Windows containers			









Docker
on
macOS



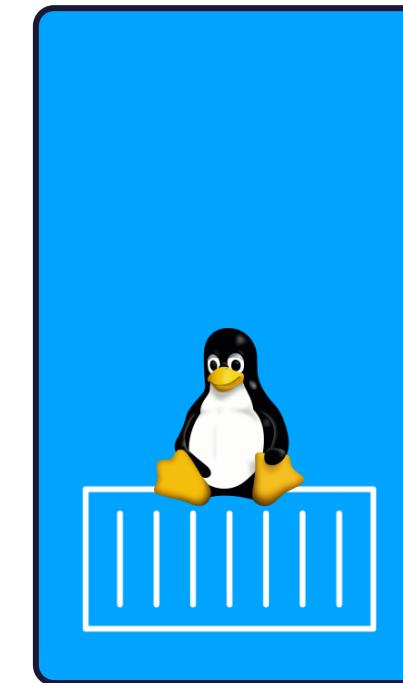
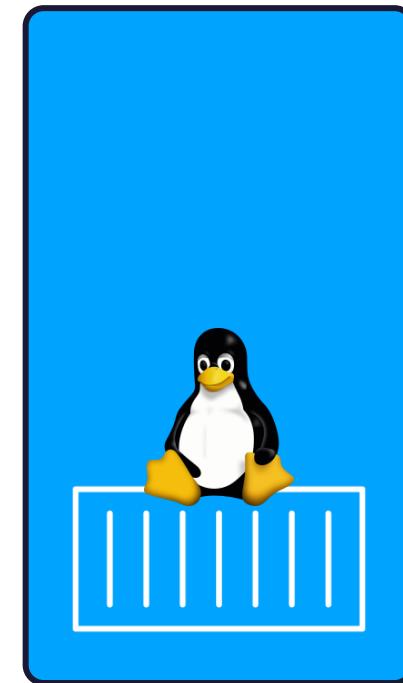
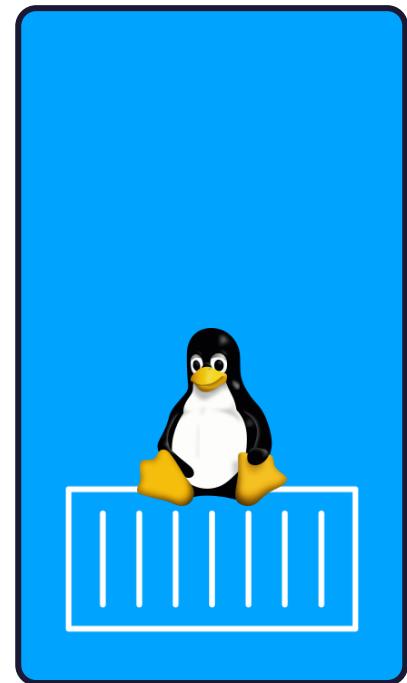
Docker
on
Linux



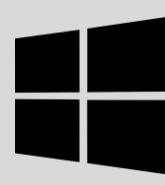
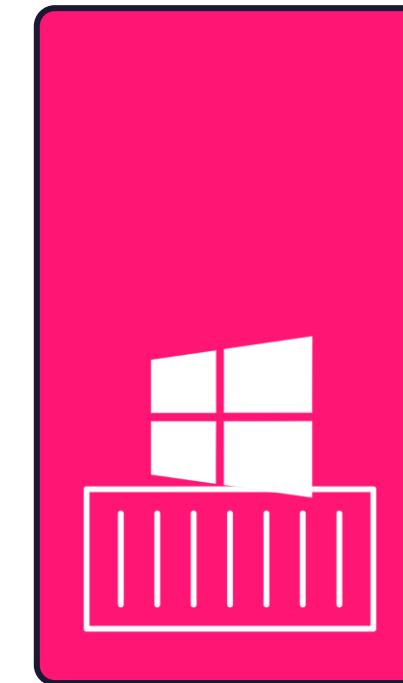
Docker
on
Windows



Docker
on
Windows



Linux kernel

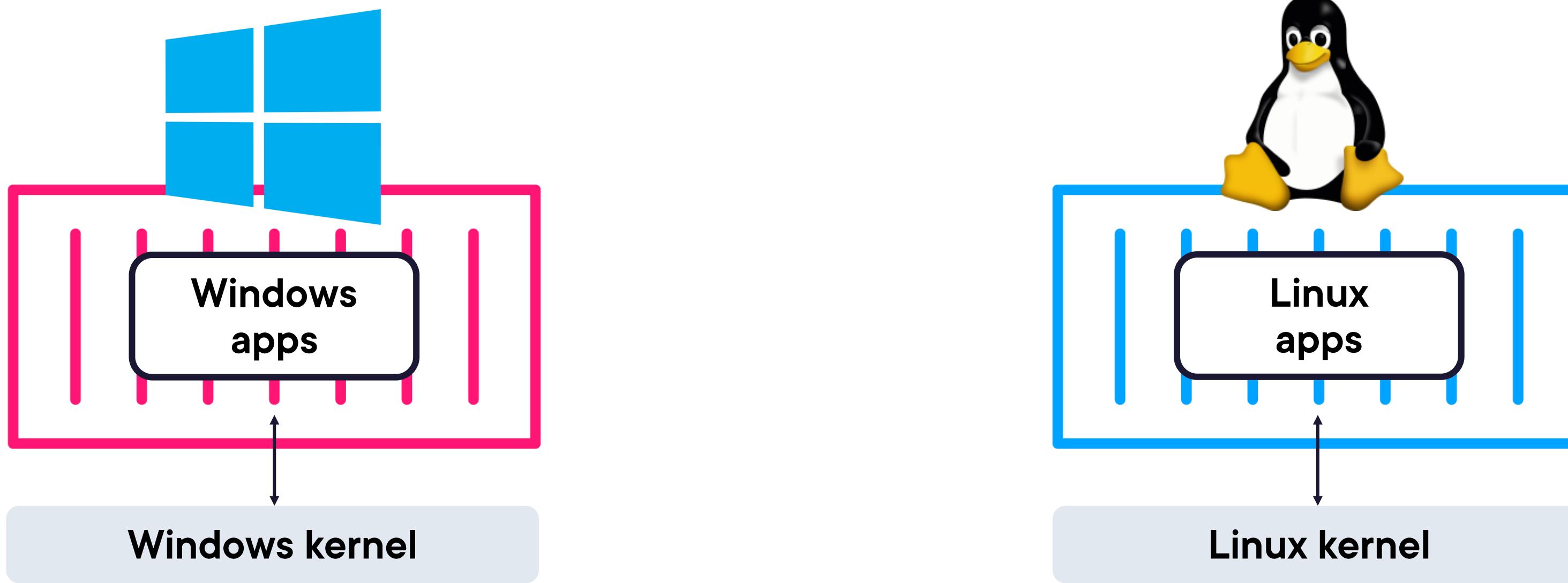


Windows kernel





Docker Desktop on Windows



Up Next:

Recap

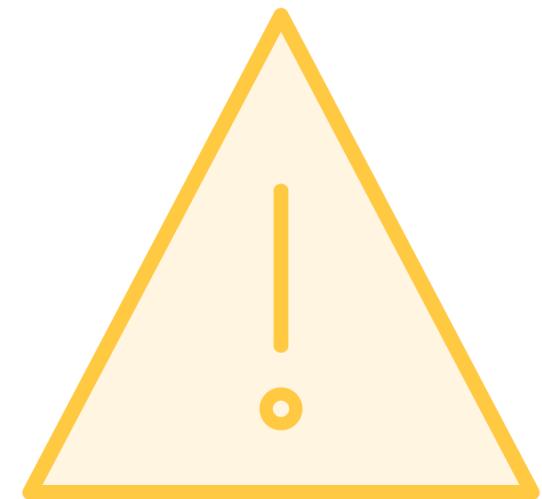
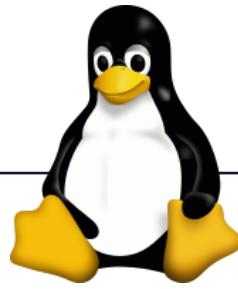


Recap



**Linux has been able to do
containers for a long time,
but it was very hard!**





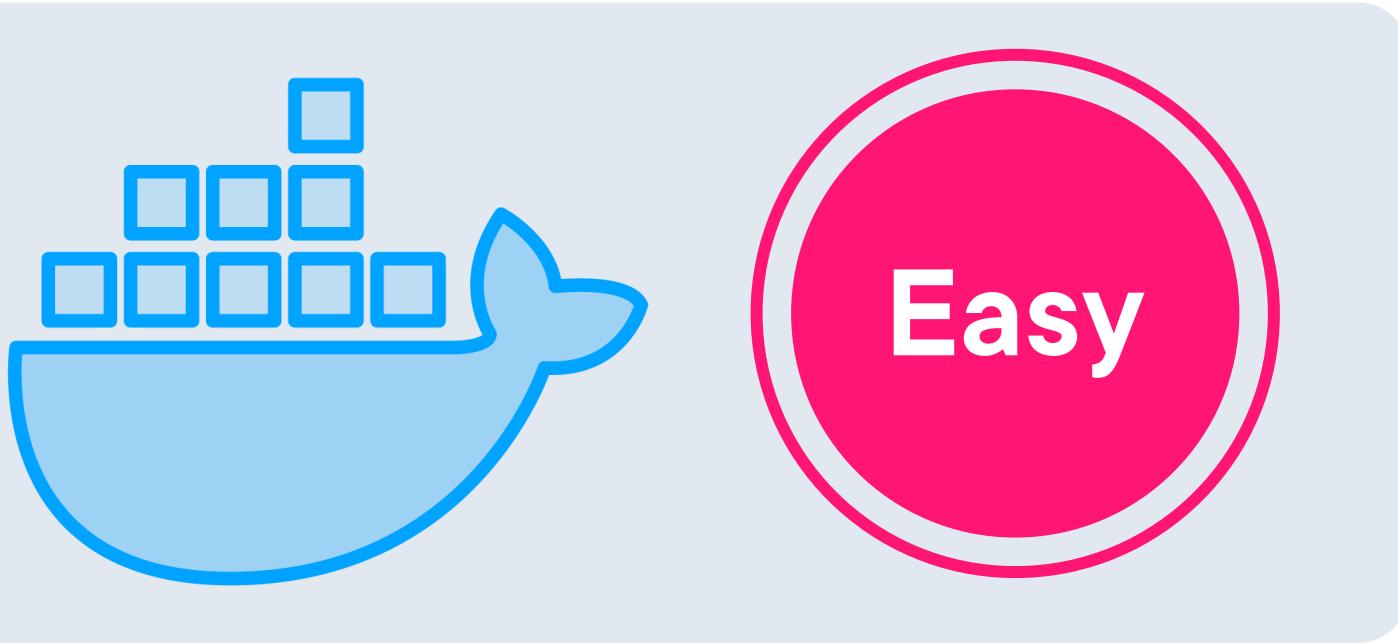
**Layered
mounts**

Namespaces

**Control
Groups**

...





Abstraction



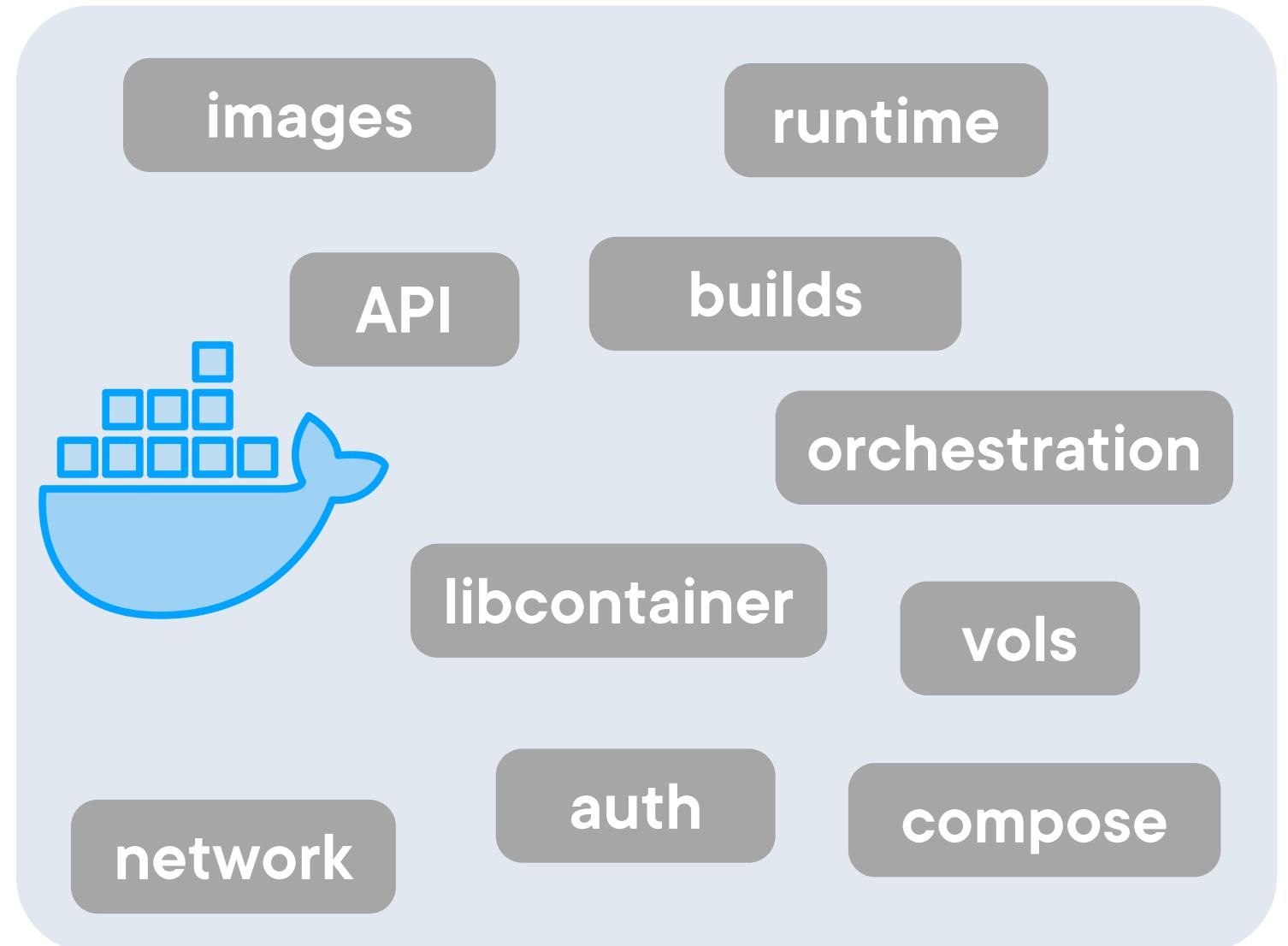
**Layered
mounts**

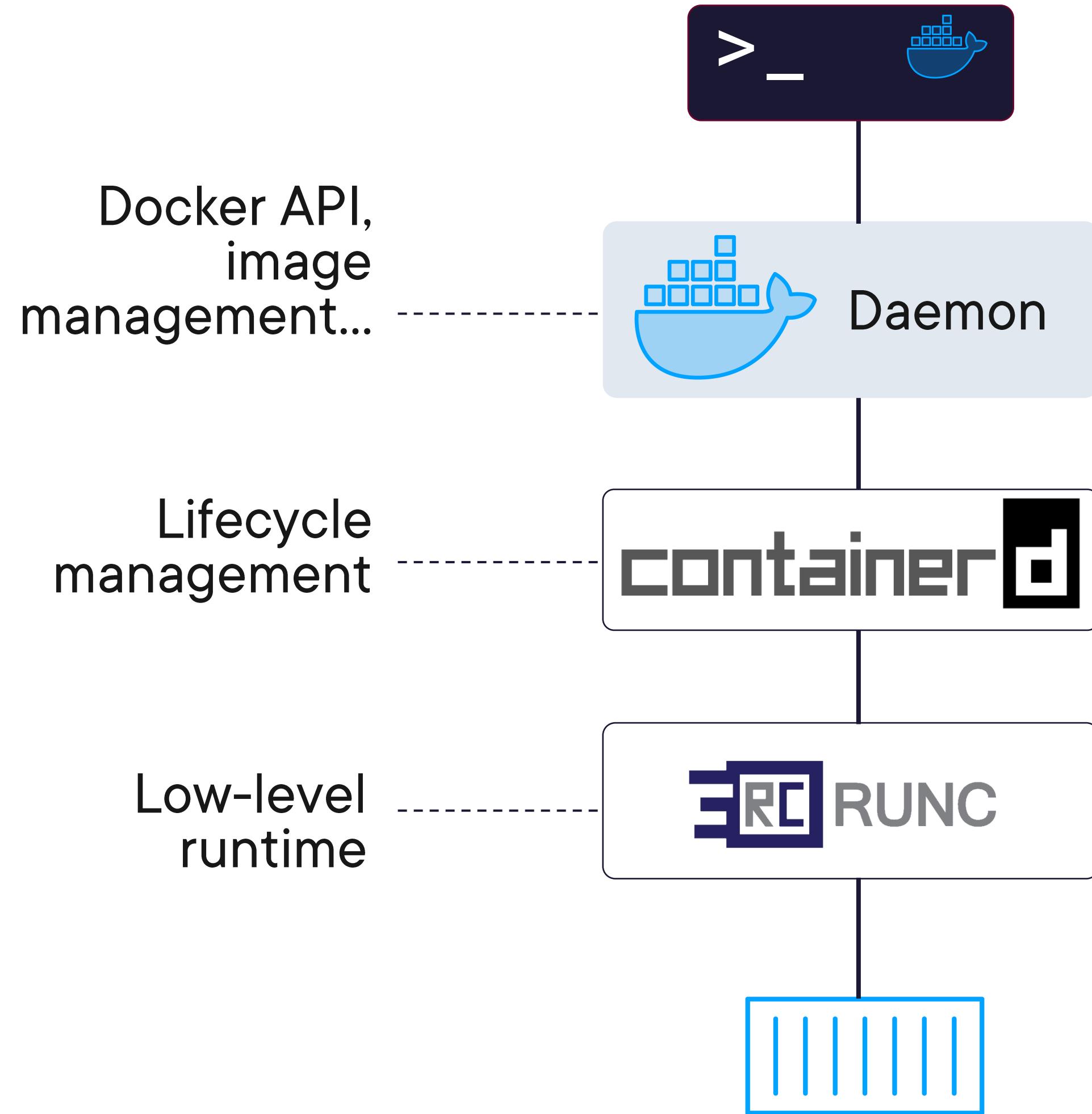
Namespaces

**Control
Groups**

...

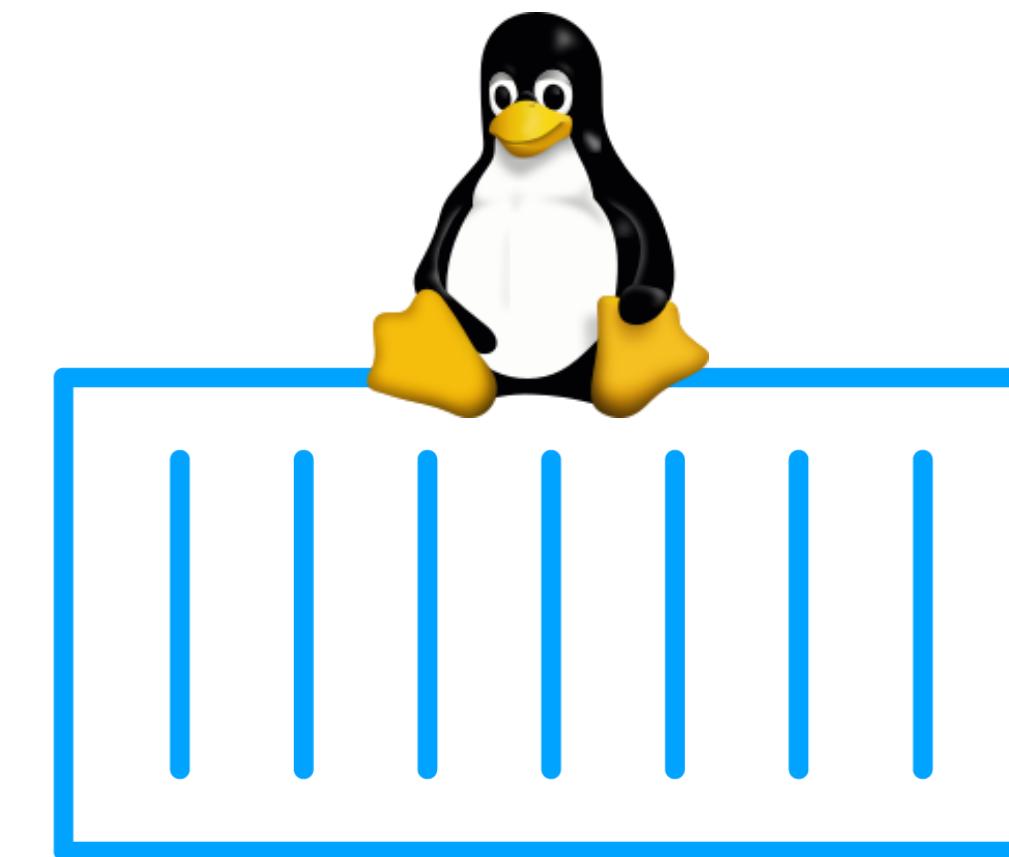
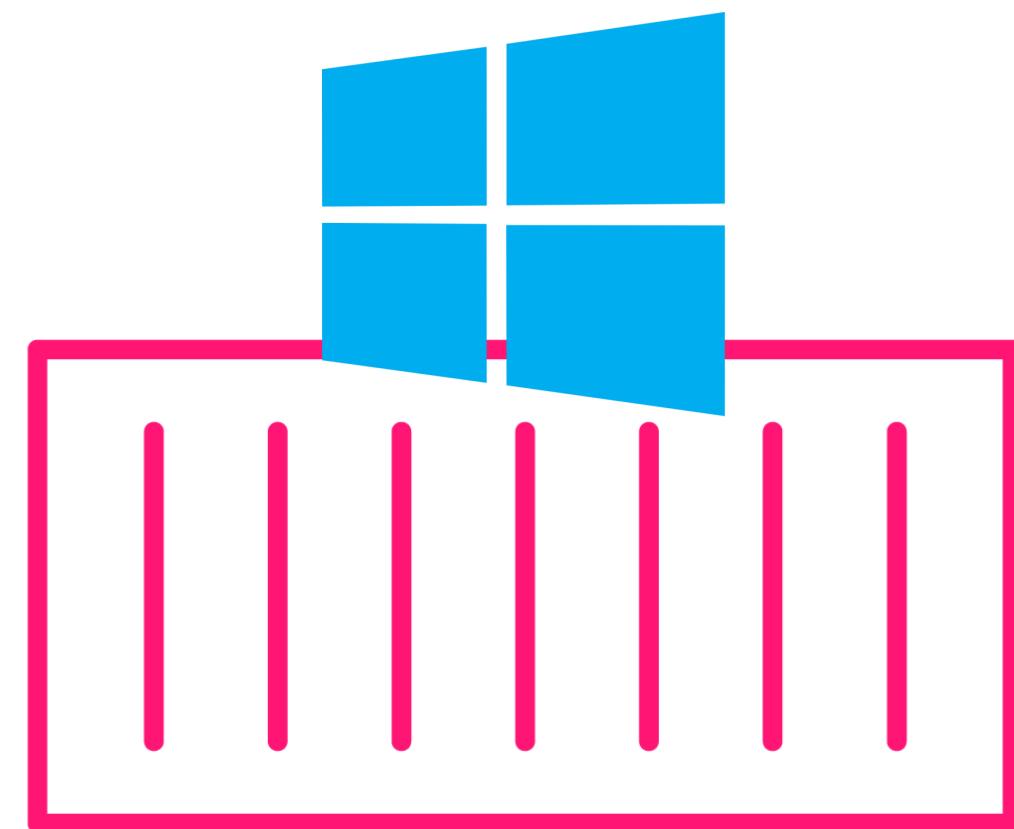








Docker Desktop on Windows



Up Next:

Working with Images

