DevOps 2021:

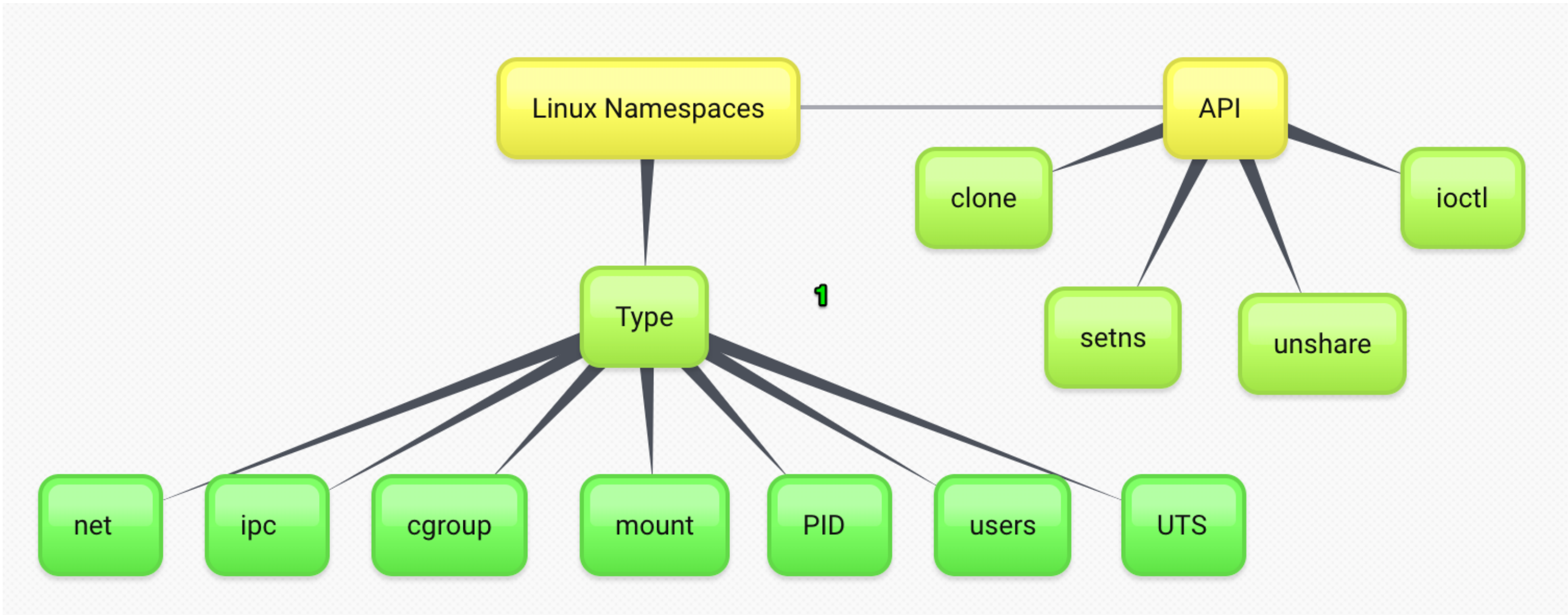
Лекция №11-12 `Контейнеры – определение и принципы.
Виртуальные машины и гипервизоры — определение и принципы.
Docker как система контейнеризации и средства управления.`

Andersen

Что мы узнаем:

* Что такое `Linux Namespace`
* Что такое `Linux Cgroups`
* Linux containers?
* Что такое `классическая виртуализация`?
* Docker – контейнеры и средства управления

Linux namespaces:



Linux namespaces:

1. **MOUNT -** Mounting and unmounting filesystems will not affect the rest of the system, except for filesystems which are explicitly marked as shared.
2. **UTS** (Unique time sharing) **-** Setting hostname or domainname will not affect the rest of the system. Checks for different hostnames of running containers
3. **IPC -** The process will have an independent namespace for POSIX message queues as well as System V message queues, semaphore sets and shared memory segments.
4. **Network -** The process will have independent IPv4 and IPv6 stacks, IP routing tables, firewall rules, the /proc/net and /sys/class/net directory trees, sockets, etc.
5. **PID -** Children will have a distinct set of PID-to-process mappings from their parent.
6. **USER -** The process will have a distinct set of UIDs, GIDs and capabilities.
7. **CGROUP -** The process will have a virtualized view of **/proc/self/cgroup**, and new cgroup mounts will be rooted at the namespace cgroup root.

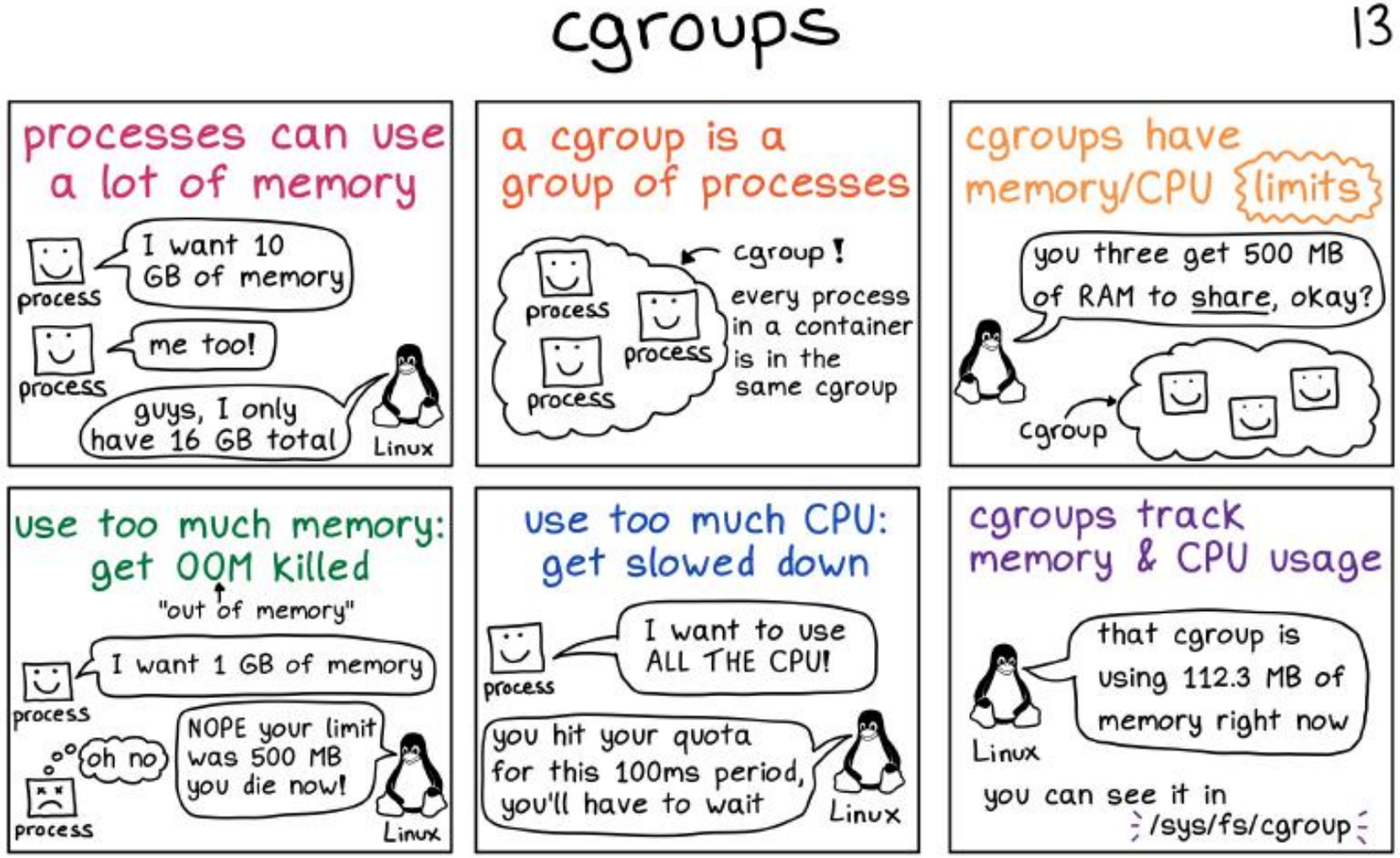
Andersen

Time for a small demo session!

* unshare **UTS** ns + nsenter + mount
* unshare + **PID** ns
* tricks with **USER** ns

Andersen

Linux cgroups:



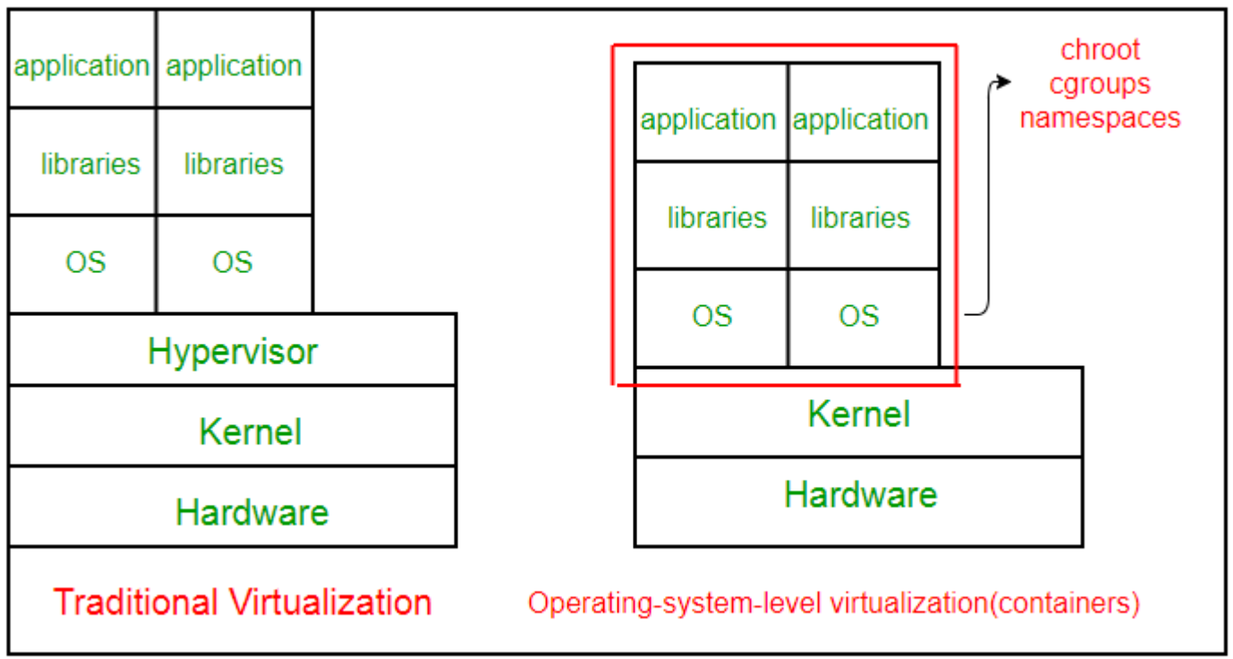
Julia Evans https://jvns.ca

Andersen

Linux cgroups:

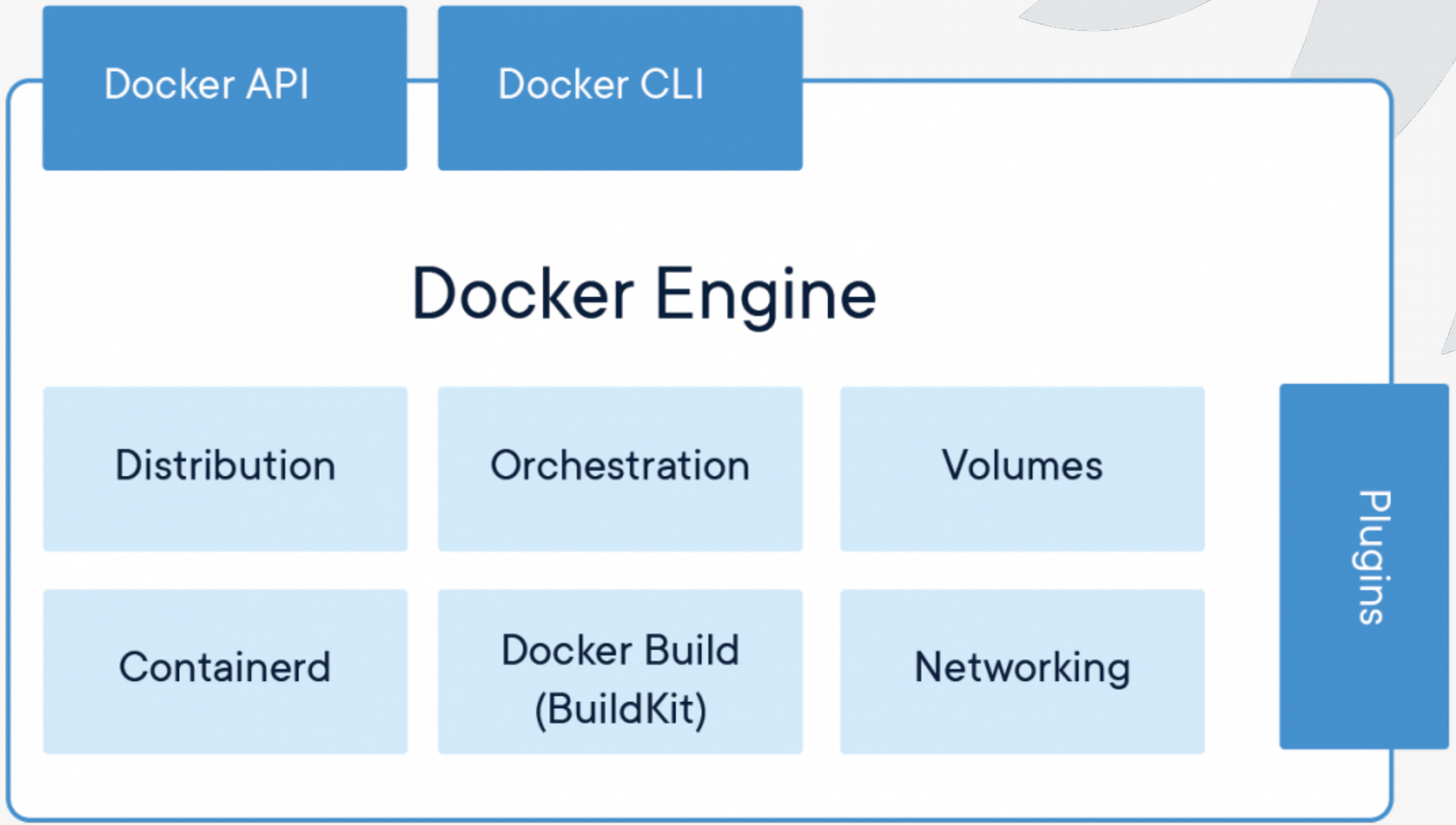
• **blkio** - this subsystem sets limits on input/output access to and from block devices such as physical drives (disk, solid state, USB, etc.)
• **cpu** - this subsystem uses the scheduler to provide cgroup tasks access to the CPU
• **cpuacct** - this subsystem generates automatic reports on CPU resources used by tasks in a cgroup
• cpuset - this subsystem assigns individual CPUs (on a multicore system) and memory nodes to tasks in a cgroup
• devices - this subsystem allows or denies access to devices by tasks in a cgroup
• freezer - this subsystem suspends or resumes tasks in a cgroup
• **memory** - this subsystem sets limits on memory use by tasks in a cgroup, and generates automatic reports on memory resources used by those tasks
• net_cls - this subsystem tags network packets with a class identifier that allows the Linux traffic controller to identify packets originating from a particular cgroup task
• ns — the namespace subsystem

Linux containers:



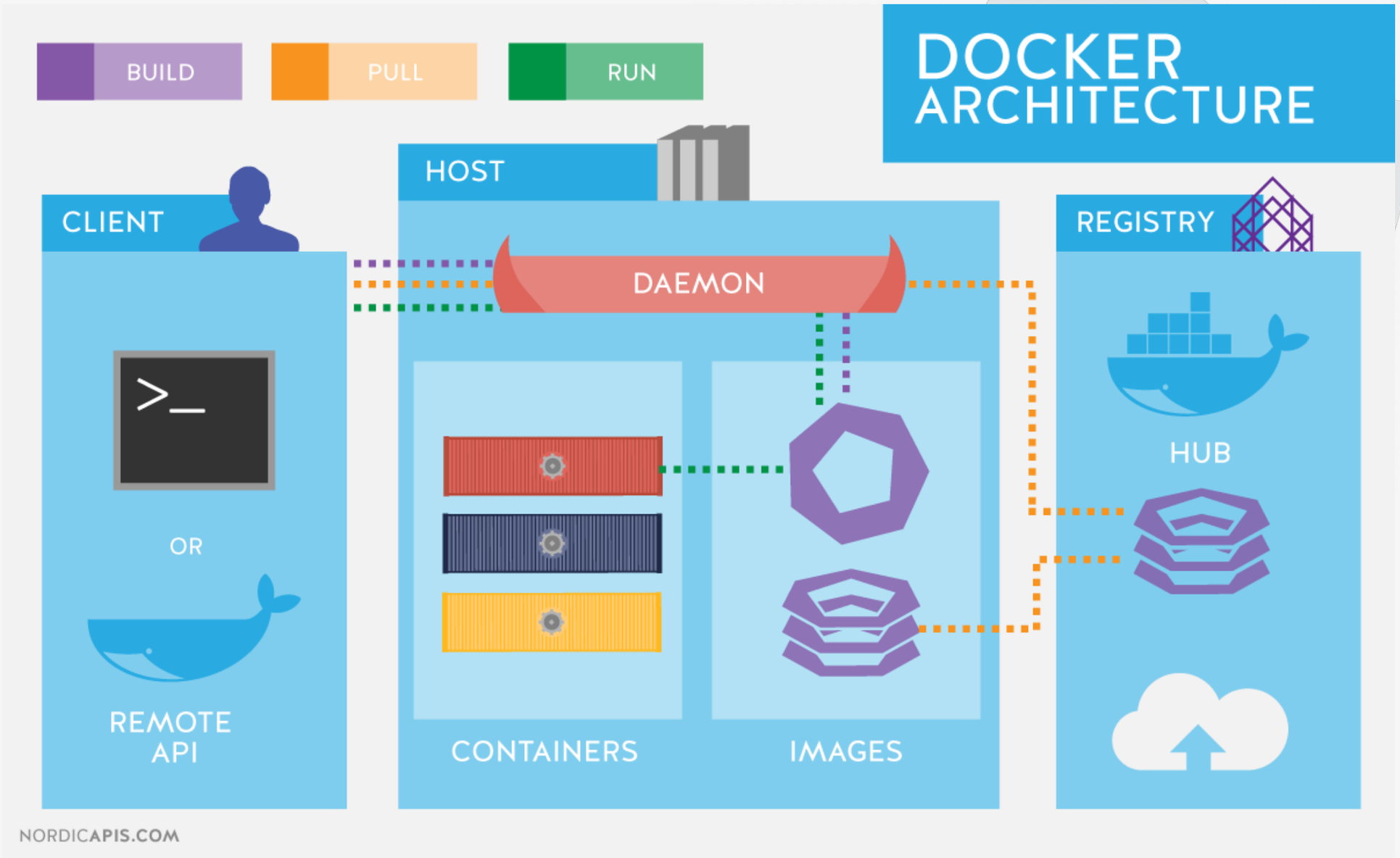
Andersen

Docker:



Andersen

Docker:



www.andersenlab.com

Andersen

Homework:

Build a docker container for your python app!

- this time it needs to listen port 8080, HTTP only
- the lighter in terms of image size it is – the more points you get
- the one who builds the smallest image gets even more points!

Hints:

- use the minimal possible setup
- 100MB is a lot ;-)