Touring the container developer tooling landscape

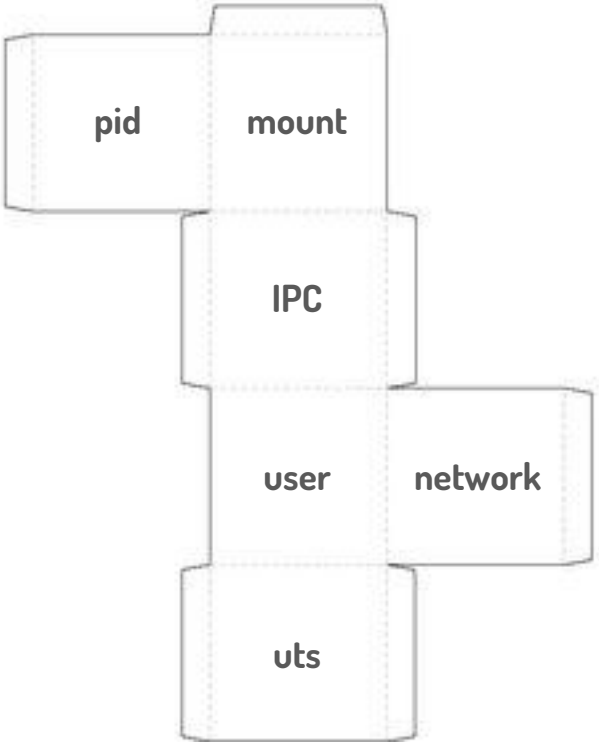
...

February 4, 2023

2013: “hello wowlrd”

aws

Containers have (mostly)* always been about Linux

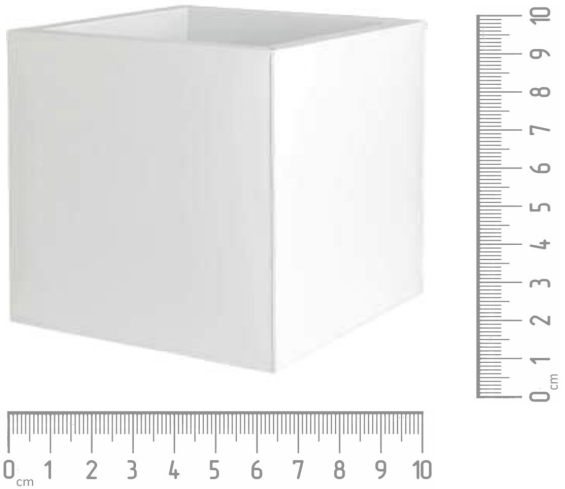


(Process Isolation)

NAMESPACES

CGROUPS

(Resource Limits)



*apologies to my friends at Microsoft

Cgroups and namespaces and...

Don't forget:

- SELinux or AppArmor
- Seccomp profiles
- Image construction (based on Linux userspace filesystem, usually)
- Linux capabilities

Where are developers developing?

Significant use distills down to three OS platforms:

Worst case, potentially 80+% of developers are not using Linux at work

Problem: I want to develop Linux containers on non-Linux OSs
Solution: Linux in a VM!

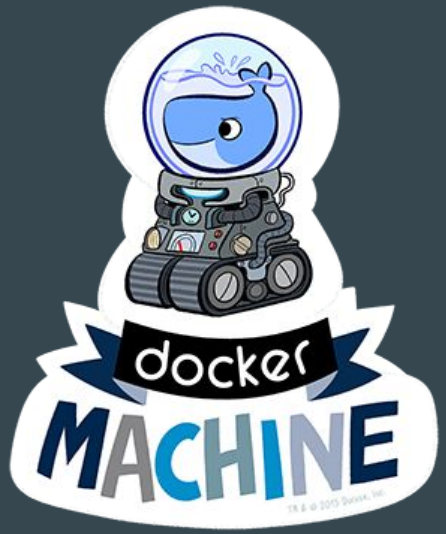
aws

New solutions bring new problems

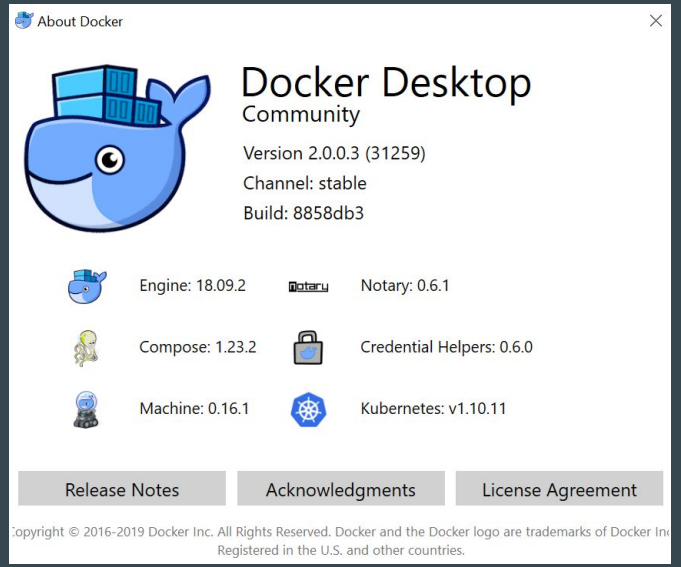
Including but not limited to:

- Management of another OS image (CVEs, updates, configuration)
- VM Boundary issues: file sharing, network pass-through
- Workflow inhibitors: in VM vs. on host tools, commands, etc.

2014
Docker machine is born



2016-17
Docker Desktop

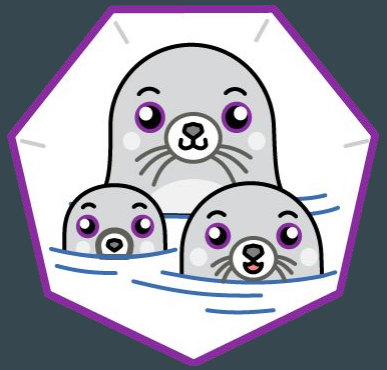


aws

Benefits

- Feels seamless to the developer; container lifecycle commands are run “locally”
- File and network pass-through magic; no configuration
- Bundling of related/relevant tools (e.g. Kubernetes)

Meanwhile...



aws

Podman Desktop

- New release: v0.11.0, Jan 2023
- Windows, macOS, and Linux support
- Kubernetes, plugins, new DNS/network service
- Built around existing podman, buildah, skopeo tools & containers/* libraries
- Provides foundation of rootless+unprivileged, daemon-less container runtime (podman+crun)
- Via podman+libpod get both command line compat and Docker API

aws

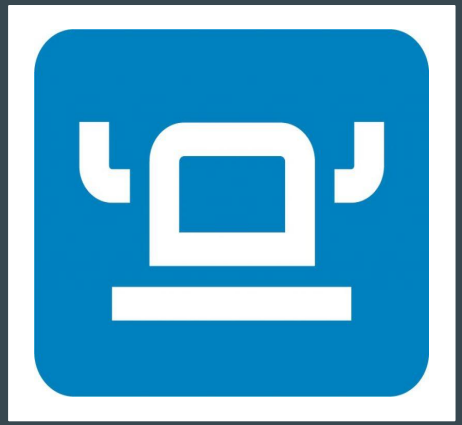
Lima

nerdctl

Lima + containerd projects

- Nerdctl provides a Docker-compatible command line with compose support
- Lima uses qemu for virtualization and handles file sharing and networking pass-through via associated projects, all for macOS only today
- Exposes experimental features (lazy-load snapshotters, image encryption)
- Enables rootless, unprivileged mode by default

aws



Rancher Desktop & colima

- Both built on the Lima foundation for macOS support
- Both offer Docker engine in addition to containerd+nerdctl; colima defaults to Docker engine as the runtime
- Both provide a full Kubernetes local cluster experience
- Rancher Desktop adds Windows and Linux support (not using Lima)

aws

Finch

- Initial project founding: November 2022
- Built on Lima+nerdctl+BuildKit
- Homebrew and Apple signed installer releases
- Supports ARM64 and Intel macOS
- Plans for extension framework (similar to Podman Desktop & Docker Desktop)
- Planning for added Windows and Linux support

aws

Collaborating on Finch

- We're working upstream in containerd, Lima, nerdctl, BuildKit, and the OCI specs (e.g. OCI v1.1 reference types)
- Finch is a **community open-source project**; working on a public roadmap as we speak
- Would love collaboration around:
  - Added OS support
  - Extension system design/implementation

https://github.com/runfinch/finch

#finch on CNCF Slack

aws

Thank You!

Phil Estes, AWS

Principal Engineer, Core Container Tech

OCI Technical Oversight Board (TOB),
CNCF containerd maintainer

aws