

containerd v2.1 β

An industry-standard container runtime

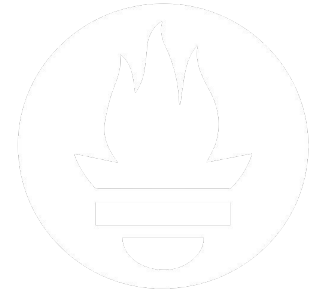
PromCon

North America 2021

- CNCF Graduated since 2019
- Adopted by well-known enterprise Kubernetes services and distributions
- Designed to be pluggable to support cutting-edge features (remote snapshotters, WASM runtimes, ...)

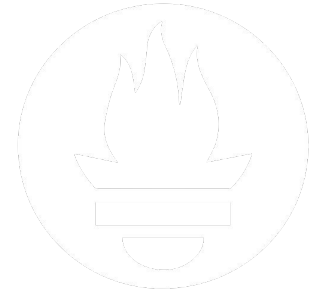
Runtime plugins

- **runc**: the regular runtime for Linux
- **runhcs**: Windows
- **runj**: FreeBSD jail
- **runwasi**: WASM
- **kata**: VM
- **runsc (gvisor)**: ptrace sandbox, etc.



PromCon
North America 2021

Snapshotter plugins



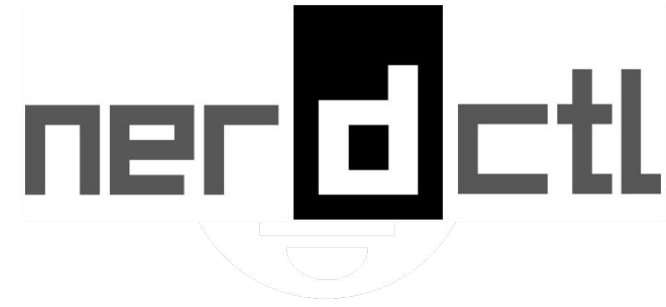
Regular snapshotters: **overlayfs**, **btrfs**, **zfs**, **devmapper**, ...

DockerCon
North America 2021

“Remote” snapshotters support pulling image contents on demand to shorten the container startup time

- **stargz**: Forward compatible with OCI v1 tar.gz images
- **nydus**: Uses an alternate image format
- **overlaybd**: Uses block devices as container images

nerdctl: contaiNERD CTL



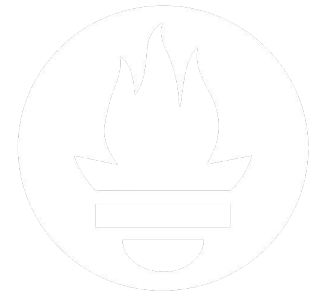
- <https://github.com/containerd/nerdctl>
- Same UI/UX as the docker CLI (including Compose)
- Made for facilitating new experiments in the containerd platform (e.g., stargz, fast rootless with bypass4netns)
- Useful for debugging Kubernetes nodes too

```
$ nerdctl run hello-world  
$ nerdctl compose up
```

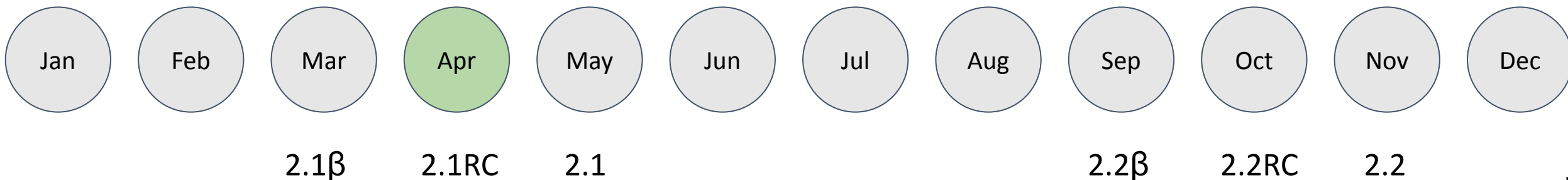
PromCon
North America 2021

containerd v2.1

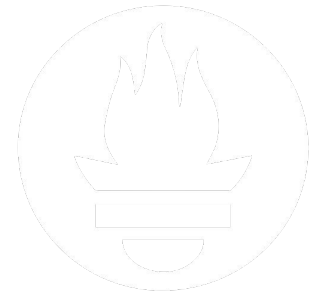
- EROFS (Enhanced Read-Only File System) ([#10705](#))
 - Suitable for images with many layers
- Image volumes ([#10579](#))
 - Allow mounting an image as a Kubernetes volume
 - Useful for distributing AI models, etc.



PromCon
North America 2021

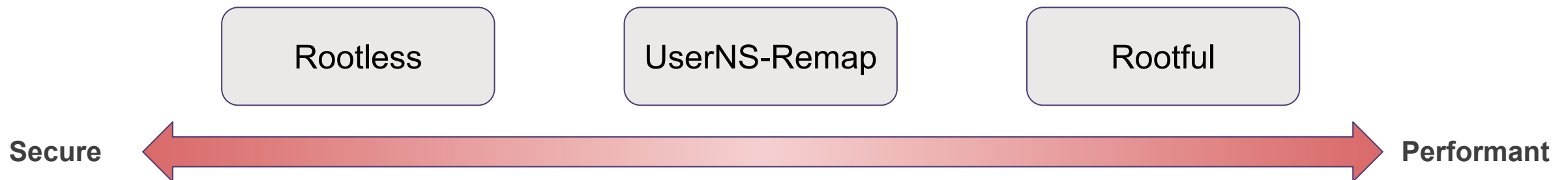


nerdctl v2.1

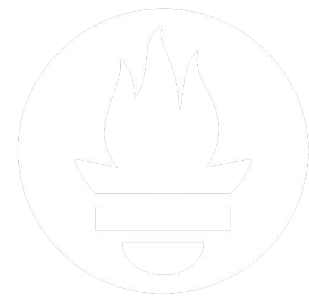


PromCon
North America 2021

- UserNS-remap mode ([#3941](#))
 - Not to be confused with Rootless mode (available since v0.6)
 - **Rootless**: execute everything as a non-root user
 - **UserNS-remap**: execute containers as a non-root, but containerd per se still runs as the root



nerdctl v2.1

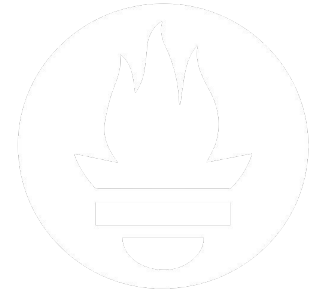


- gomodjail ([#4012](#), experimental)
 - Imposes syscall restrictions on a specific set of Go modules so as to mitigate potential vulnerabilities and supply chain attacks (Not applicable to ones that use unsafe pointers, reflections, etc.)

```
//gomodjail:confined
module github.com/containerd/nerdctl/v2

require (
    github.com/Masterminds/semver/v3 v3.3.1
    ...
    golang.org/x/sys v0.31.0 //gomodjail:unconfined
    ...
)
```

Join the community!



PromCon
North America 2021

- **GitHub:** <https://github.com/containerd>
- **Slack:** <https://slack.cncf.io/>
(Channels: `#containerd` `#containerd-dev`)
- **X (former Twitter):** [@containerd](https://twitter.com/containerd)
- **Bluesky:** [@containerd.dev](https://bsky.app/profile/containerd.dev)

Maintainers' session 17:30-18:00

[containerd: Project Update and Deep Dive](#)

Maksym Pavlenko, NVIDIA

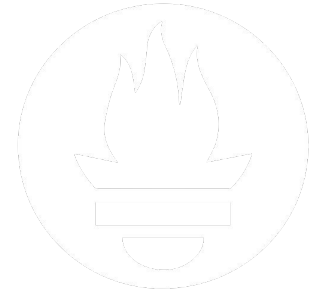
Akihiro Suda, NTT

Laura Brehm, Docker

Samuel Karp, Google

Jiaxiao Zhou, Microsoft

Platinum Suite | Level 3 | Room 3-4



PromCon
North America 2021

