NTT

Rootless build with BuildKit

Akihiro Suda (@_AkihiroSuda_)
NTT Software Innovation Center

What is BuildKit?

- **Next-generation `docker build` with focus on performance and security**
  - Accurate dependency analysis
  - Concurrent execution of independent instructions
  - Support injecting secret files...

- **Integrated to Docker since v18.06 (`export DOCKER_BUILDKIT=1`)**

- **Non-Docker standalone BuildKit is also available**
  - Works with Podman and CRI-O as well :P

Rootless mode

- **Rootless mode allows building images as a non-root user**
  - Dockerfile `RUN` instructions are executed as a “fake root” in UserNS (So `apt-get`/`yum` works!)
- **Produces Docker image / OCI image / raw tarball**
  - Compatible with Rootless Docker / Rootless Podman / … whatever
- **Even works inside a container**
  - Good for distributed CI/CD on Kubernetes
  - Works with default `securityContext` configuration
    (but seccomp and AppArmor needs to be disabled for nesting containers)

Rootless BuildKit vs kaniko

- https://github.com/GoogleContainerTools/kaniko

- **Kaniko runs as the root but “unprivileged”**
  - No need to disable seccomp and AppArmor because kaniko doesn’t nest containers on the kaniko container itself

- **Kaniko might be able to mitigate some vuln that Rootless BuildKit cannot mitigate - and vice versa**
  - Rootless BuildKit might be weak against kernel vulns
  - Kaniko might be weak against runc vulns