INDONESIA
OpenInfra Days

02.11.2019 | Surabaya, Indonesia

Buildah, Podman and Skopeo for Better and Secure Container Management

buildah podman

skopeo

Bachril Qirom - Cloud Engineering
bachril@btech.co.id

Biznet GioCloud Biznet Mellanox TECHNOLOGIES BANK BRI OSF OpenStack Foundation

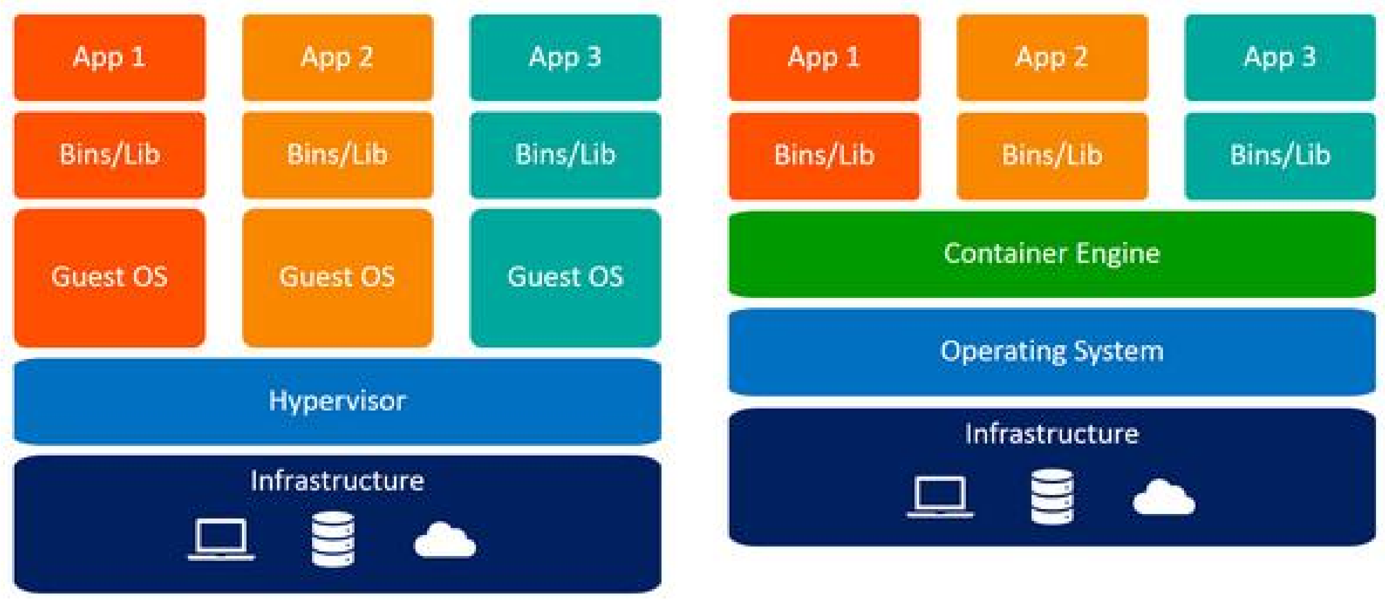
Introduction

- Name : Bachril Qirom
- Education : Now Students at Telkom University
- Experience : Work at BTECH
- Certification : NolSatu and COA

What is Container?

“*a lightweight, stand-alone, executable package of a piece of software that includes everything needed to run it: code, runtime, system tools, system libraries, settings.*“; Docker

VM VS Container



Virtual Machines

Containers

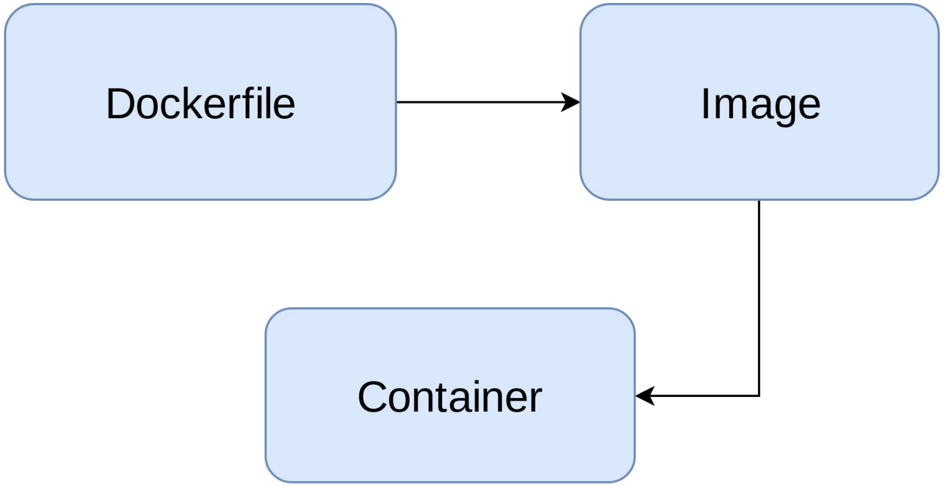
Why Container?

✓ No Booting

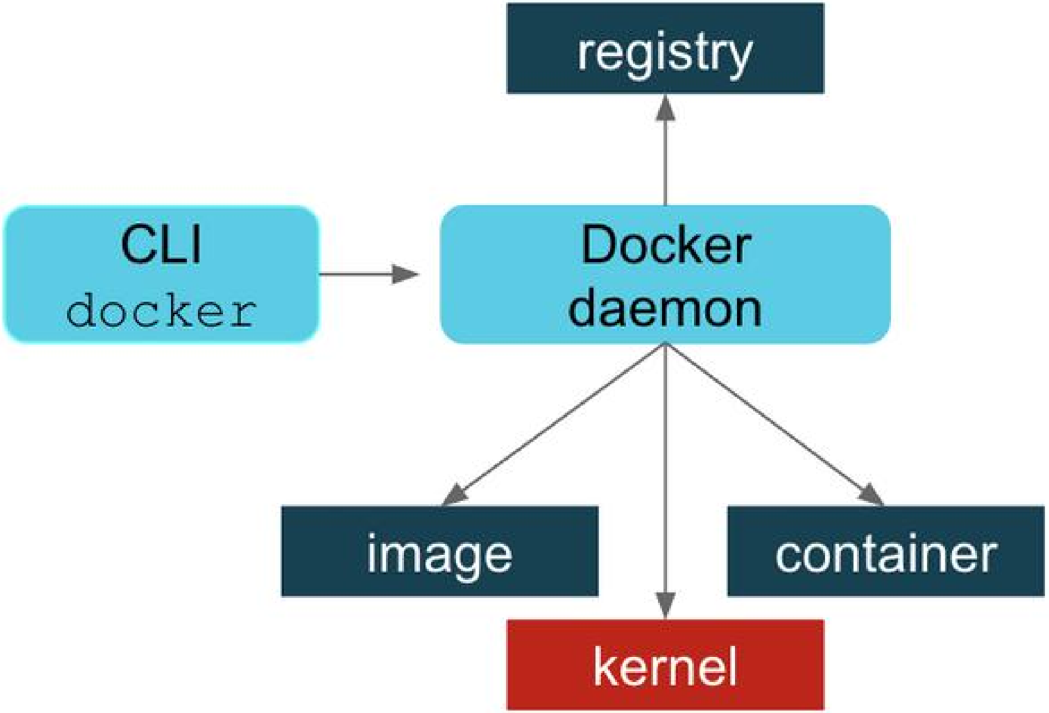
✓ lightweight

✓ Easy To deploy

Reproduce Container in Docker Ways



Docker



Buildah , Podman and Skopeo

Why?

- ✓ Daemon-less
- ✓ Rootless
- ✓ Complete

Why Podman More Secure?

- Docker uses a client/server
- Podman uses a traditional fork/exec model

```
sudo cat /proc/self/loginuid

sudo docker run --privilege -v /:/host fedora touch /host/etc/shadow

sudo podman run --privileged -v /:/host fedora touch /host/etc/shadow
```

Buildah

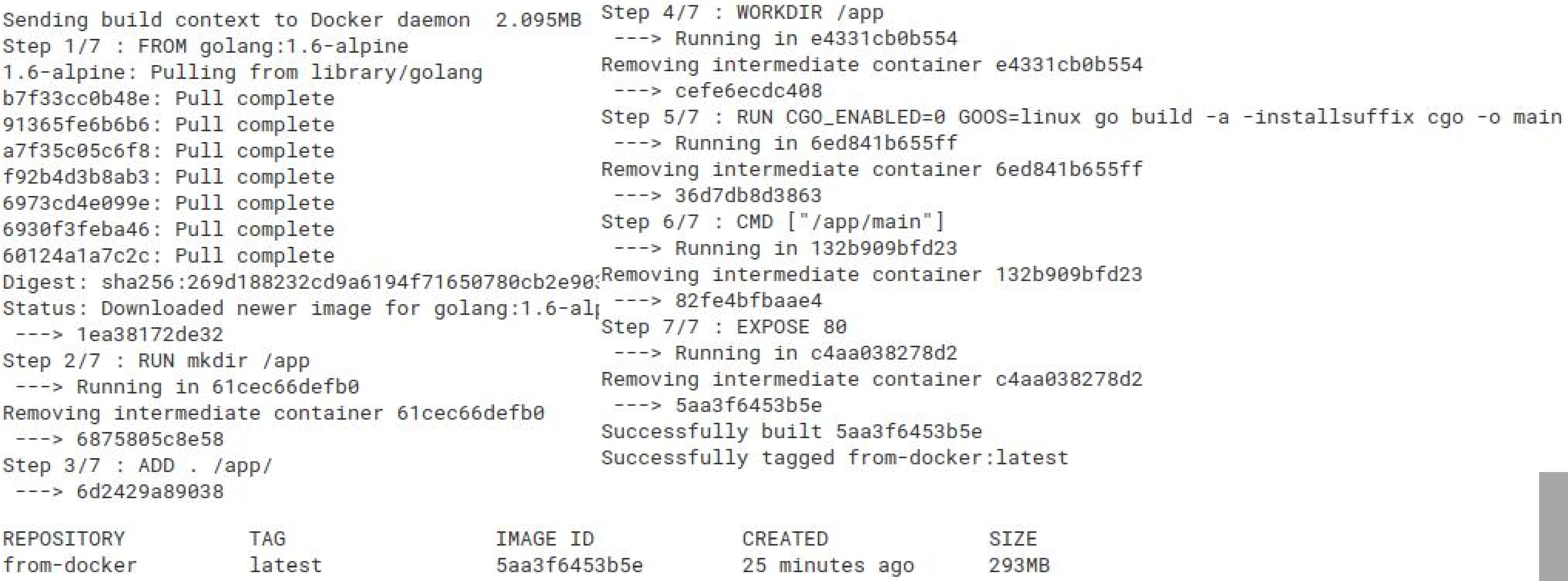
Buildah specializes in building OCI images. We can building images with and without Dockerfiles while not requiring any root privileges. Buildah’s ultimate goal is to provide a lower-level coreutils interface to build images

Type fo Build Image

Buildah	Docker
Multiple layer	Multiple Layer
One Layer	

buildah

Multilayer

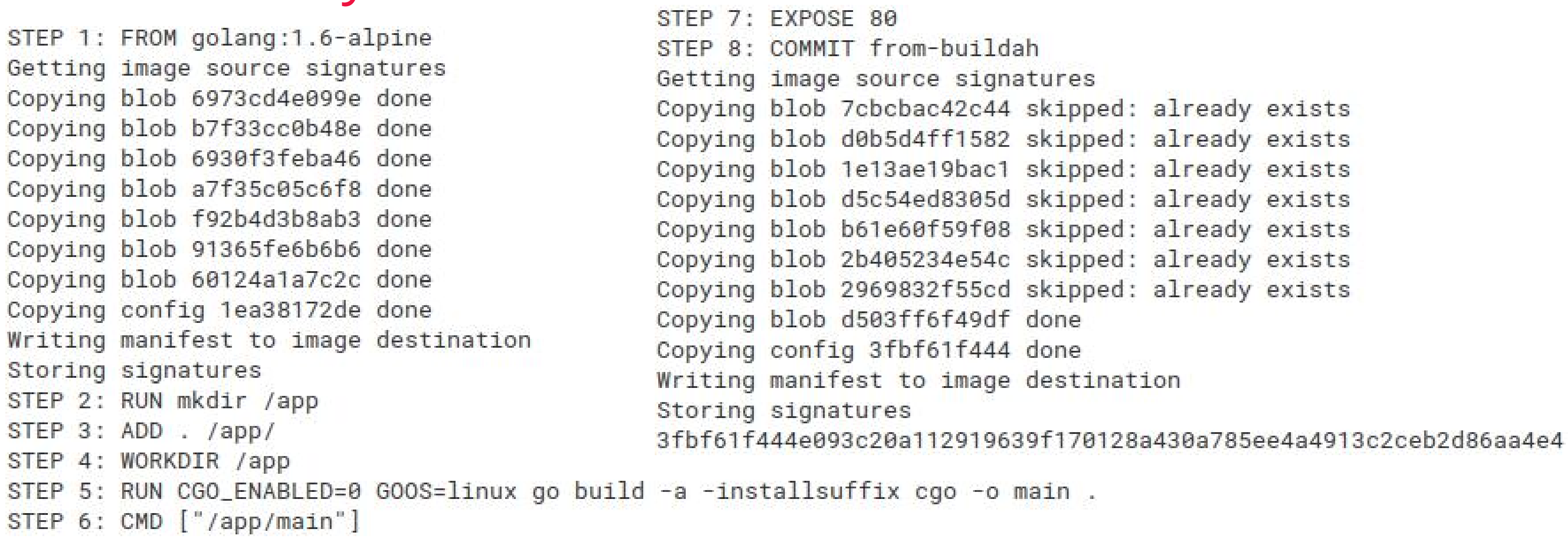


```
Sending build context to Docker daemon  2.095MB
Step 1/7 : FROM golang:1.6-alpine
1.6-alpine: Pulling from library/golang
b7f33cc0b48e: Pull complete
91365fe6b6b6: Pull complete
a7f35c05c6f8: Pull complete
f92b4d3b8ab3: Pull complete
6973cd4e099e: Pull complete
6930f3feba46: Pull complete
60124a1a7c2c: Pull complete
Digest: sha256:269d188232cd9a6194f71650780cb2e90
Status: Downloaded newer image for golang:1.6-al
 ---> 1ea38172de32
Step 2/7 : RUN mkdir /app
 ---> Running in 61cec66defb0
Removing intermediate container 61cec66defb0
 ---> 6875805c8e58
Step 3/7 : ADD . /app/
 ---> 6d2429a89038
```

```
Step 4/7 : WORKDIR /app
 ---> Running in e4331cb0b554
Removing intermediate container e4331cb0b554
 ---> cefe6ecdc408
Step 5/7 : RUN CGO_ENABLED=0 GOOS=linux go build -a -installsuffix cgo -o main
 ---> Running in 6ed841b655ff
Removing intermediate container 6ed841b655ff
 ---> 36d7db8d3863
Step 6/7 : CMD ["/app/main"]
 ---> Running in 132b909bfd23
Removing intermediate container 132b909bfd23
 ---> 82fe4bfbaae4
Step 7/7 : EXPOSE 80
 ---> Running in c4aa038278d2
Removing intermediate container c4aa038278d2
 ---> 5aa3f6453b5e
Successfully built 5aa3f6453b5e
Successfully tagged from-docker:latest
```

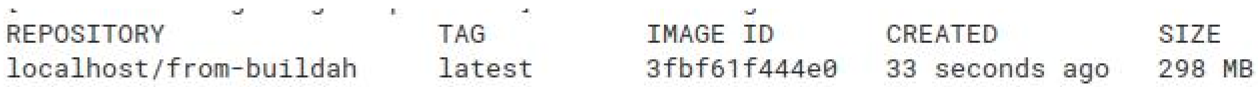
```
REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE
from-docker         latest              5aa3f6453b5e        25 minutes ago      293MB
```

One layer



```
STEP 1: FROM golang:1.6-alpine
Getting image source signatures
Copying blob 6973cd4e099e done
Copying blob b7f33cc0b48e done
Copying blob 6930f3feba46 done
Copying blob a7f35c05c6f8 done
Copying blob f92b4d3b8ab3 done
Copying blob 91365fe6b6b6 done
Copying blob 60124a1a7c2c done
Copying config 1ea38172de done
Writing manifest to image destination
Storing signatures
STEP 2: RUN mkdir /app
STEP 3: ADD . /app/
STEP 4: WORKDIR /app
STEP 5: RUN CGO_ENABLED=0 GOOS=linux go build -a -installsuffix cgo -o main .
STEP 6: CMD ["/app/main"]
```

```
STEP 7: EXPOSE 80
STEP 8: COMMIT from-buildah
Getting image source signatures
Copying blob 7cbcbac42c44 skipped: already exists
Copying blob d0b5d4ff1582 skipped: already exists
Copying blob 1e13ae19bac1 skipped: already exists
Copying blob d5c54ed8305d skipped: already exists
Copying blob b61e60f59f08 skipped: already exists
Copying blob 2b405234e54c skipped: already exists
Copying blob 2969832f55cd skipped: already exists
Copying blob d503ff6f49df done
Copying config 3fbf61f444 done
Writing manifest to image destination
Storing signatures
3fbf61f444e093c20a112919639f170128a430a785ee4a4913c2ceb2d86aa4e4
```



```
REPOSITORY               TAG         IMAGE ID       CREATED          SIZE
localhost/from-buildah   latest      3fbf61f444e0   33 seconds ago   298 MB
```

Dockerfile VS ScriptBASH

```
FROM golang:1.6-alpine

RUN mkdir /app

ADD .

WORKDIR /app

RUN CGO_ENABLED=0 GOOS=linux go
build -a -installsuffix cgo -o main .

CMD ["/app/main"]

EXPOSE 80
```

```
ctr=$(buildah from golang:1.6-alpine)

buildah run $ctr mkdir /app

buildah add  $ctr . /app/

buildah config --workingdir /app/ $ctr

buildah config -e CGO_ENABLED=0 $ctr

buildah config -e GOOS=linux $ctr

buildah run $ctr go build -a -installsuffix cgo -o
main .

buildah config --cmd /app/main $ctr

buildah commit $ctr from-buildah
```

Build From Scratch

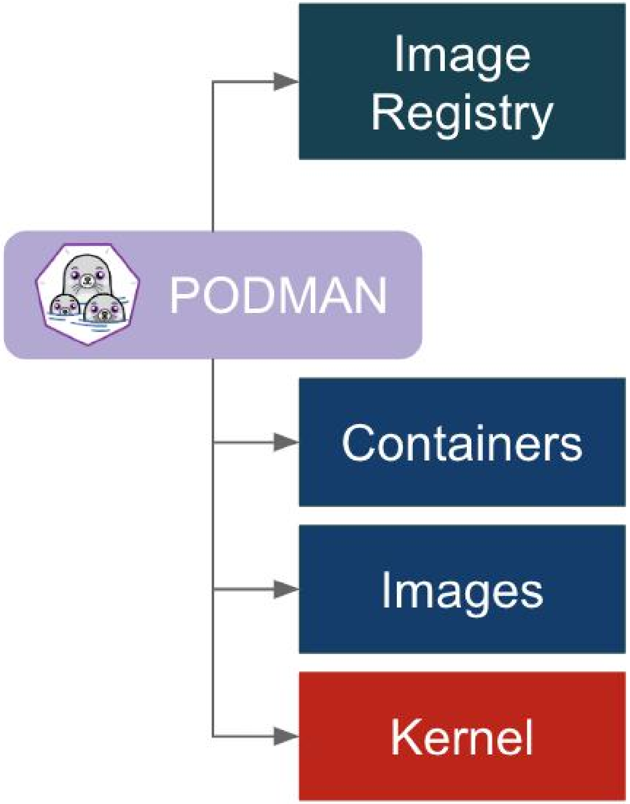
```
newcontainer=$(buildah from scratch)

scratchmnt=$(buildah mount ${newcontainer})

yum install --installroot ${scratchmnt} bash
coreutils --releasever 7 --
setopt=tsflags=nodocs --
setopt=override_install_langs=en_US.utf8 -y

if [ -d "${scratchmnt}" ]; then

  rm -rf "${scratchmnt}"/var/cache/yum

fi
```

```
buildah config --label name=el7-minimal
${newcontainer}

buildah config --cmd /bin/bash
${newcontainer}


buildah unmount ${newcontainer}

buildah commit ${newcontainer} el7-minimal
```

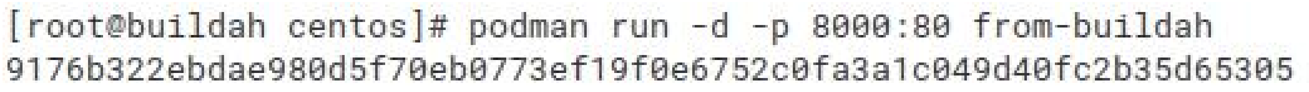
Podman

Pod Manager tool(Podman) is a daemonless container engine for developing, managing, and running OCI Containers on your Linux System.

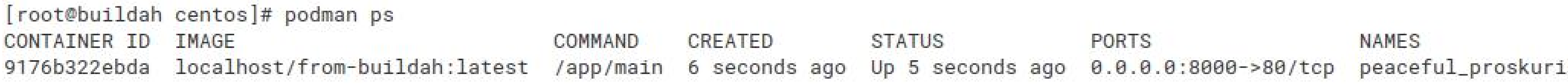
Podman



Run Image

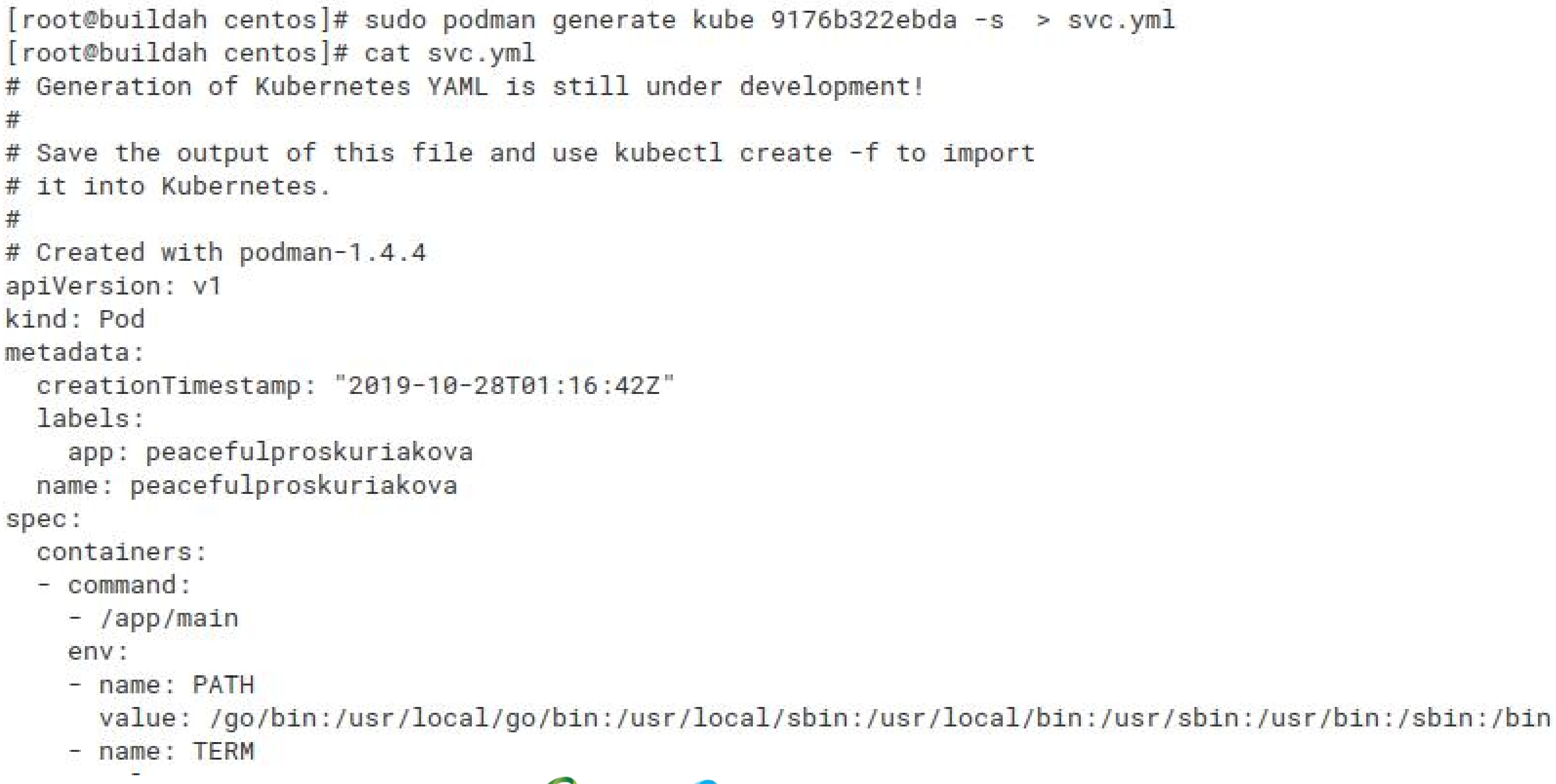


```
[root@buildah centos]# podman run -d -p 8000:80 from-buildah
9176b322ebdae980d5f70eb0773ef19f0e6752c0fa3a1c049d40fc2b35d65305
```



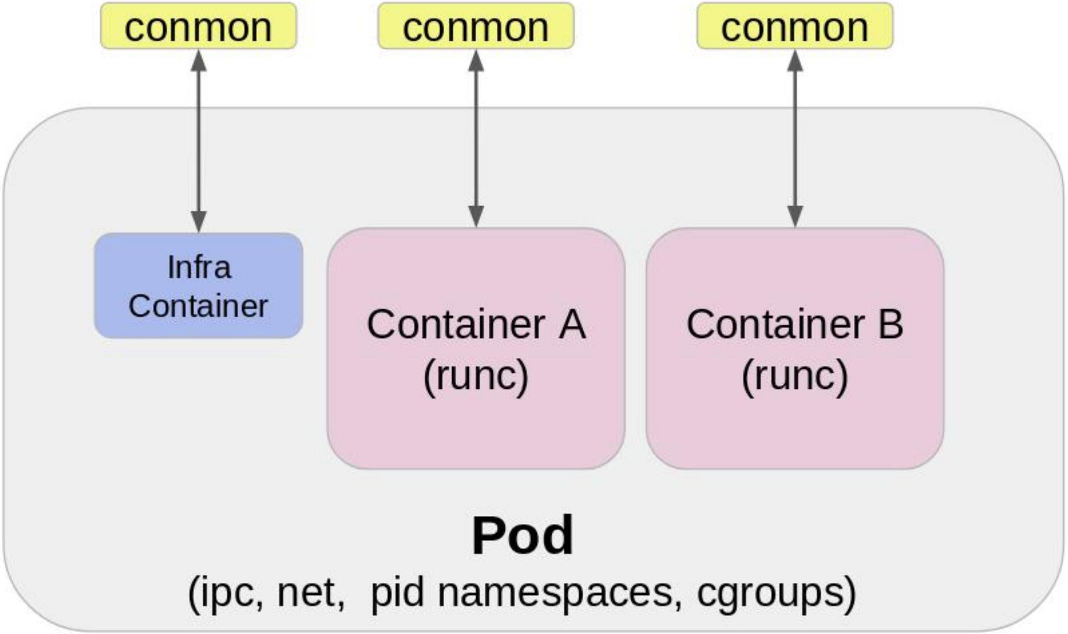
```
[root@buildah centos]# podman ps
CONTAINER ID  IMAGE                         COMMAND    CREATED        STATUS            PORTS                 NAMES
9176b322ebda  localhost/from-buildah:latest /app/main  6 seconds ago  Up 5 seconds ago  0.0.0.0:8000->80/tcp  peaceful_proskuri
```

Generate kubernetes yaml



```
[root@buildah centos]# sudo podman generate kube 9176b322ebda -s  > svc.yml
[root@buildah centos]# cat svc.yml
# Generation of Kubernetes YAML is still under development!
#
# Save the output of this file and use kubectl create -f to import
# it into Kubernetes.
#
# Created with podman-1.4.4
apiVersion: v1
kind: Pod
metadata:
  creationTimestamp: "2019-10-28T01:16:42Z"
  labels:
    app: peacefulproskuriakova
  name: peacefulproskuriakova
spec:
  containers:
  - command:
    - /app/main
    env:
    - name: PATH
      value: /go/bin:/usr/local/go/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
    - name: TERM
```

Podman Pod


conmon
conmon
conmon
Infra Container
Container A (runc)
Container B (runc)
Pod
(ipc, net, pid namespaces, cgroups)

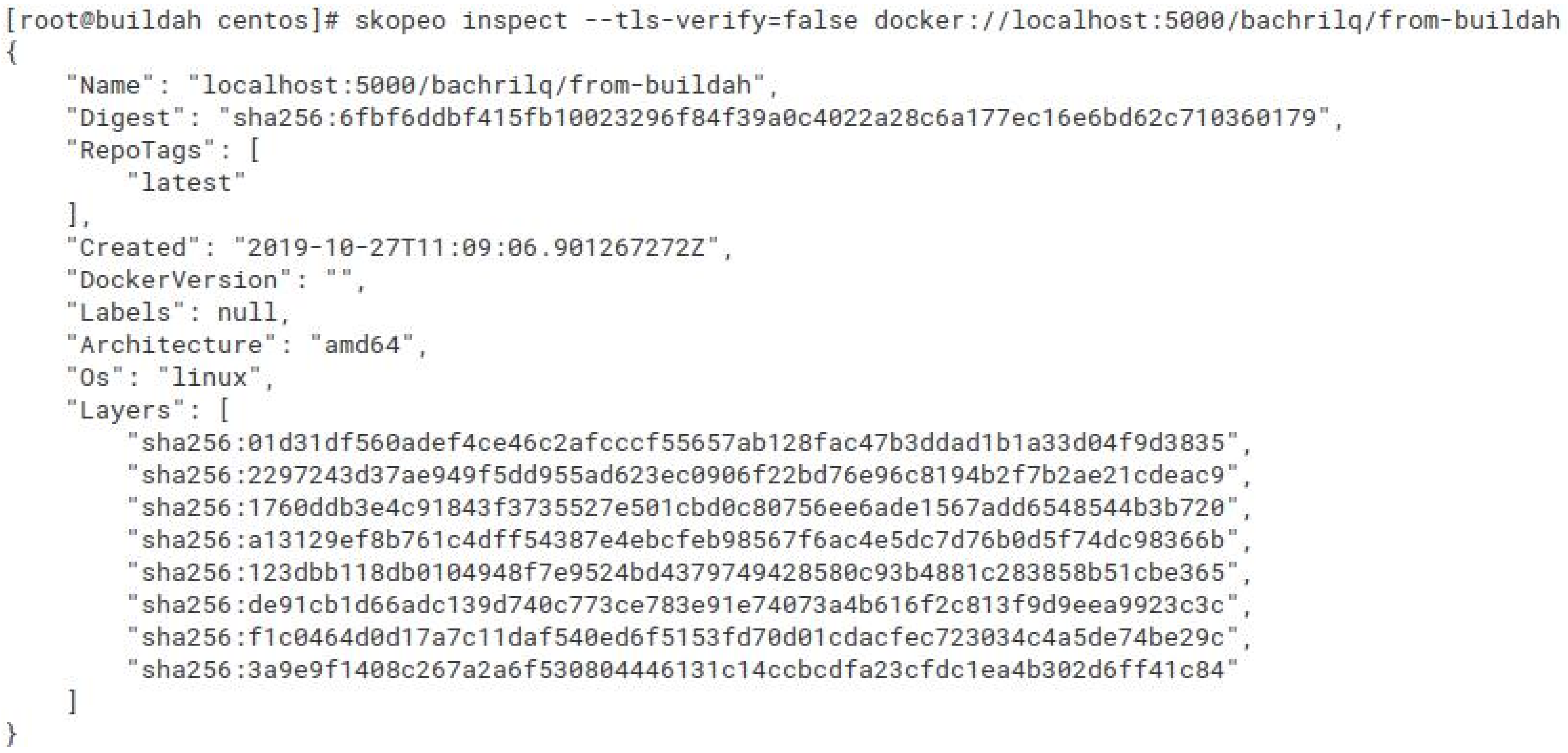
Skopeo

Skopeo is a command line utility that performs various operations on container images and image repositories

skopeo

INDONESIA
OpenInfra Days

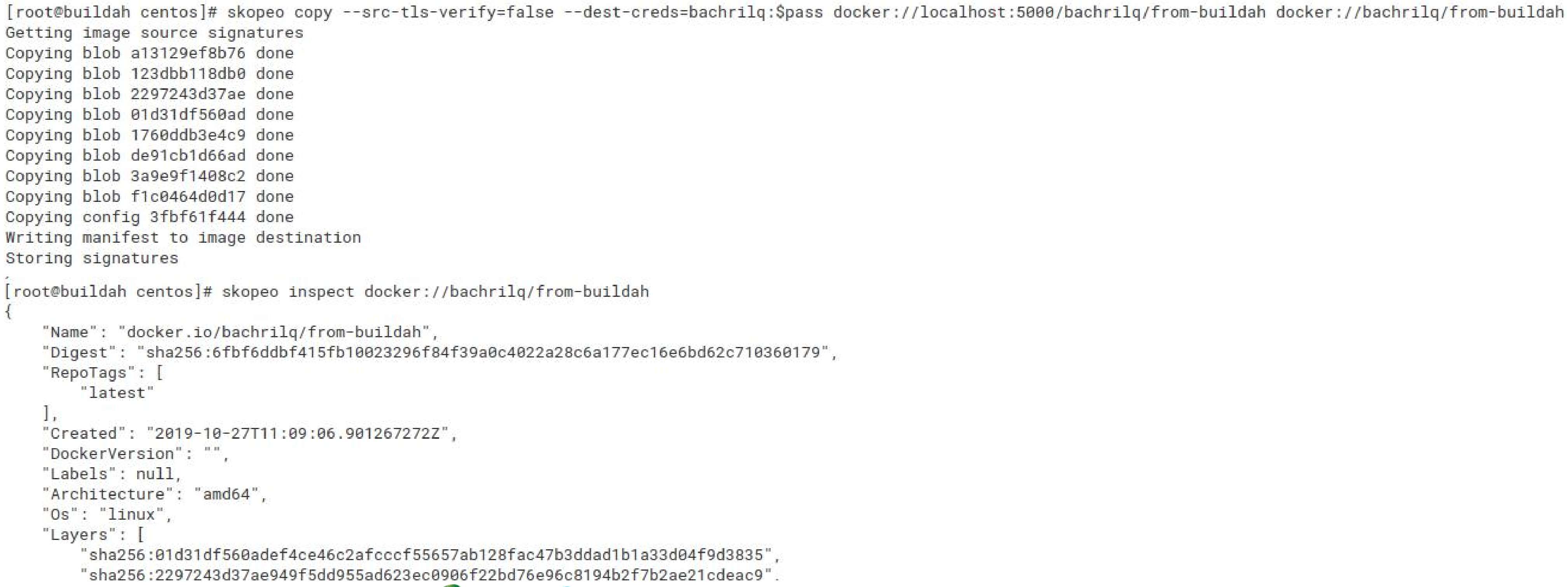
Inspect Image



```
[root@buildah centos]# skopeo inspect --tls-verify=false docker://localhost:5000/bachrilq/from-buildah
{
    "Name": "localhost:5000/bachrilq/from-buildah",
    "Digest": "sha256:6fbf6ddbf415fb10023296f84f39a0c4022a28c6a177ec16e6bd62c710360179",
    "RepoTags": [
        "latest"
    ],
    "Created": "2019-10-27T11:09:06.901267272Z",
    "DockerVersion": "",
    "Labels": null,
    "Architecture": "amd64",
    "Os": "linux",
    "Layers": [
        "sha256:01d31df560adef4ce46c2afcccf55657ab128fac47b3ddad1b1a33d04f9d3835",
        "sha256:2297243d37ae949f5dd955ad623ec0906f22bd76e96c8194b2f7b2ae21cdeac9",
        "sha256:1760ddb3e4c91843f3735527e501cbd0c80756ee6ade1567add6548544b3b720",
        "sha256:a13129ef8b761c4dff54387e4ebcfeb98567f6ac4e5dc7d76b0d5f74dc98366b",
        "sha256:123dbb118db0104948f7e9524bd4379749428580c93b4881c283858b51cbe365",
        "sha256:de91cb1d66adc139d740c773ce783e91e74073a4b616f2c813f9d9eea9923c3c",
        "sha256:f1c0464d0d17a7c11daf540ed6f5153fd70d01cdacfec723034c4a5de74be29c",
        "sha256:3a9e9f1408c267a2a6f530804446131c14ccbcdfa23cfdc1ea4b302d6ff41c84"
    ]
}
```

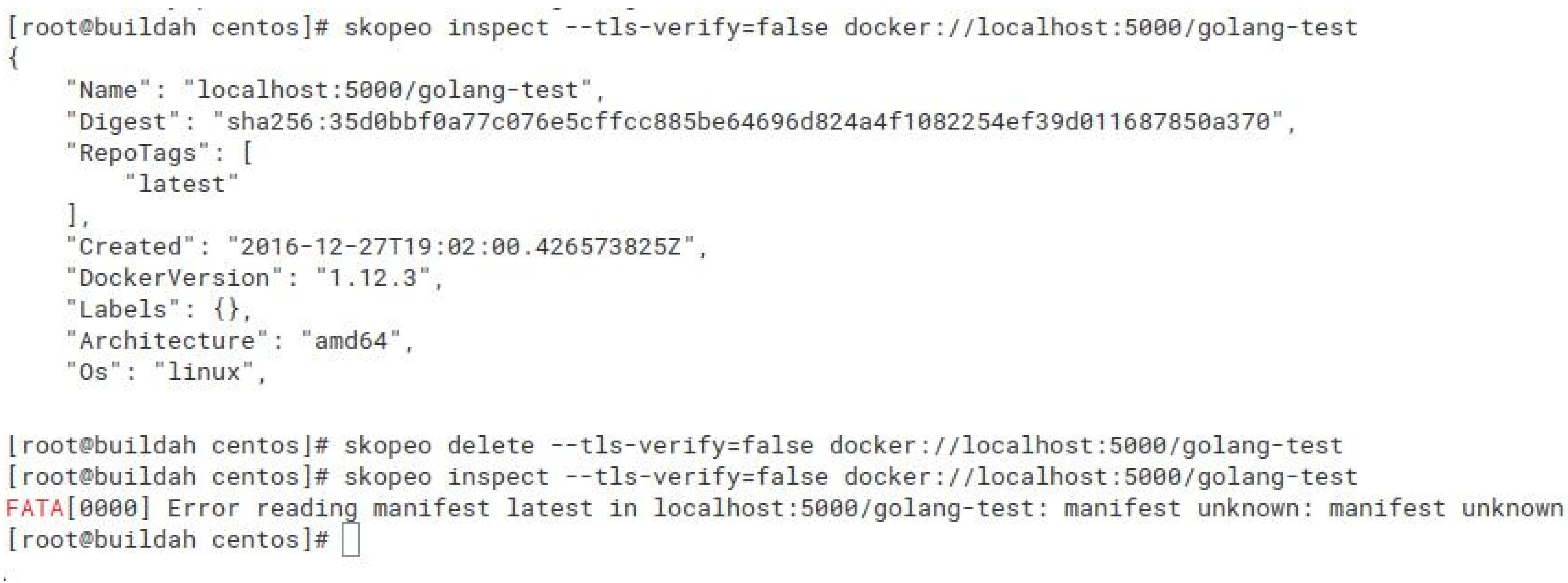
skopeo

Copy Image



```
[root@buildah centos]# skopeo copy --src-tls-verify=false --dest-creds=bachrilq:$pass docker://localhost:5000/bachrilq/from-buildah docker://bachrilq/from-buildah
Getting image source signatures
Copying blob a13129ef8b76 done
Copying blob 123dbb118db0 done
Copying blob 2297243d37ae done
Copying blob 01d31df560ad done
Copying blob 1760ddb3e4c9 done
Copying blob de91cb1d66ad done
Copying blob 3a9e9f1408c2 done
Copying blob f1c0464d0d17 done
Copying config 3fbf61f444 done
Writing manifest to image destination
Storing signatures

[root@buildah centos]# skopeo inspect docker://bachrilq/from-buildah
{
    "Name": "docker.io/bachrilq/from-buildah",
    "Digest": "sha256:6fbf6ddbf415fb10023296f84f39a0c4022a28c6a177ec16e6bd62c710360179",
    "RepoTags": [
        "latest"
    ],
    "Created": "2019-10-27T11:09:06.901267272Z",
    "DockerVersion": "",
    "Labels": null,
    "Architecture": "amd64",
    "Os": "linux",
    "Layers": [
        "sha256:01d31df560adef4ce46c2afcccf55657ab128fac47b3ddad1b1a33d04f9d3835",
        "sha256:2297243d37ae949f5dd955ad623ec0906f22bd76e96c8194b2f7b2ae21cdeac9".
```

Delete Image



```
[root@buildah centos]# skopeo inspect --tls-verify=false docker://localhost:5000/golang-test
{
    "Name": "localhost:5000/golang-test",
    "Digest": "sha256:35d0bbf0a77c076e5cffcc885be64696d824a4f1082254ef39d011687850a370",
    "RepoTags": [
        "latest"
    ],
    "Created": "2016-12-27T19:02:00.426573825Z",
    "DockerVersion": "1.12.3",
    "Labels": {},
    "Architecture": "amd64",
    "Os": "linux",

[root@buildah centos]# skopeo delete --tls-verify=false docker://localhost:5000/golang-test
[root@buildah centos]# skopeo inspect --tls-verify=false docker://localhost:5000/golang-test
FATA[0000] Error reading manifest latest in localhost:5000/golang-test: manifest unknown: manifest unknown
[root@buildah centos]# 
```

Thank you!