

Container Tooling by Red Hat

Franta Lachman

Tomas Tomecek

Docker done right

~~Docker done right~~

(You make your own opinion :)

Who's Franta and Tomas?

The tools

- podman
- buildah
- skopeo
- udica
- toolbox
- ~~CRI-O~~

The tools

- podman
- buildah
- skopeo
- udica
- toolbox
- ~~CRI-O~~
- Demos: <https://github.com/containers/Demos.git>

The background tools

- crun
- bubblewrap
- fuse-overlayfs
- conmon
- containers/{storage,image}



podman


```

tt at hops ~/g/7/speaks podman --help
manage pods and images
Usage:
  podman [flags]
  podman [command]

Available Commands:
  attach      Attach to a running container
  build       Build an image using instructions from Containerfiles
  commit      Create new image based on the changed container
  container   Manage Containers
  cp          Copy files/folders between a container and the local filesystem
  create      Create but do not start a container
  diff        Inspect changes on container's file systems
  events      Show podman events
  exec        Run a process in a running container
  export      Export container's filesystem contents as a tar archive
  generate    Generate structured data
  healthcheck Manage Healthcheck
  help        Help about any command
  history     Show history of a specified image
  image       Manage images
  images      List images in local storage
  import      Import a tarball to create a filesystem image
  info        Display podman system information
  init        Initialize one or more containers
  inspect     Display the configuration of a container or image
  kill        Kill one or more running containers with a specific signal
  load        Load an image from container archive
  login       Login to a container registry
  logout      Logout of a container registry
  logs        Fetch the logs of a container
  mount       Mount a working container's root filesystem
  network     Manage Networks
  pause       Pause all the processes in one or more containers
  play        Play a pod
  pod         Manage pods
  port        List port mappings or a specific mapping for the container
  ps          List containers
  pull        Pull an image from a registry
  push        Push an image to a specified destination
  restart     Restart one or more containers
  rm          Remove one or more containers
  rmi         Removes one or more images from local storage
  run         Run a command in a new container
  save        Save image to an archive
  search      Search registry for image
  start       Start one or more containers
  stats       Display a live stream of container resource usage statistics
  stop        Stop one or more containers
  system      Manage podman
  tag         Add an additional name to a local image
  top         Display the running processes of a container
  umount      Unmounts working container's root filesystem
  unpause     Unpause the processes in one or more containers
  unshare     Run a command in a modified user namespace
  untag       Remove a name from a local image
  varlink     Run varlink interface
  version     Display the Podman Version Information
  volume      Manage volumes
  wait        Block on one or more containers

Flags:
  --cgroup-manager string    Cgroup manager is not supported in rootless mode
  --cni-config-dir string    Path of the configuration directory for CNI networks
  --config string            Path of a libpod config file detailing container ser
  --config-dir string        Path of the configuration directory for CNI networks
  --common string            Path of the common binary
  --cpu-profile string        Path for the cpu profiling results
  --events-backend string    Events backend to use ('file'|'journald'|'none')
  --help                     Help for podman
  --hooks-dir strings        Set the OCI hooks directory path (may be set multipl
  --log-level string          Log messages above specified level ("debug"|"info"|"
  --namespace string          Set the libpod namespace, used to create separate vi
  --network string            Set the network namespace, used to create separate vi
  --storage string            Set the storage namespace, used to create separate vi
  --tmp-dir string            Set the temporary directory, used to create separate vi
  --verbose                   Verbose output
  --version                   Display the Podman Version Information
  --volume string             Manage volumes
  --wait                      Block on one or more containers

```

podman (T)

- github.com/containers/libpod
- "The manager of pods"
- The same CLI as docker command

Rootless containers (T)

- Credits:

- <https://www.slideshare.net/AkihiroSuda/rootless-containers>

Rootless containers (T)

- Credits:
 - <https://www.slideshare.net/AkihiroSuda/rootless-containers>
- Running a container as an unprivileged user

Rootless containers (T)

- Credits:
 - <https://www.slideshare.net/AkihiroSuda/rootless-containers>
- Running a container as an unprivileged user
- Very tricky to be done on the system level
 - User namespaces (UID mapping), Filesystem, Networking

Rootless containers (T)

- Credits:
 - <https://www.slideshare.net/AkihiroSuda/rootless-containers>
- Running a container as an unprivileged user
- Very tricky to be done on the system level
 - User namespaces (UID mapping), Filesystem, Networking
- Demo `github.com/containers/Demos/security`

Let's talk security

- Credits:
 - <https://devconfcz2020a.sched.com/event/YOo2/the-state-of-container-security>

Let's talk security

- Credits:
 - <https://devconfcz2020a.sched.com/event/YOo2/the-state-of-container-security>
- Security is not very popular.
- Security hates user experience (setenforce 0).

Let's talk security

- Credits:
 - <https://devconfcz2020a.sched.com/event/YOo2/the-state-of-container-security>
- Security is not very popular.
- Security hates user experience (setenforce 0).
- `podman run --privileged` vs. `podman run --cap-drop`

Let's talk security

- Credits:
 - <https://devconfcz2020a.sched.com/event/YOo2/the-state-of-container-security>
- Security is not very popular.
- Security hates user experience (setenforce 0).
- `podman run --privileged` vs. `podman run --cap-drop`
- SELinux blocked most of docker's CVEs
 - breakouts of containers (filesystem based)

Oci-seccomp-bpf-hook

- <https://github.com/containers/oci-seccomp-bpf-hook>
- Generate a seccomp profile based on live container behaviour.

Oci-seccomp-bpf-hook

- <https://github.com/containers/oci-seccomp-bpf-hook>
- Generate a seccomp profile based on live container behaviour.
- Also, what is seccomp?

Oci-seccomp-bpf-hook

- <https://github.com/containers/oci-seccomp-bpf-hook>
- Generate a seccomp profile based on live container behaviour.
- Also, what is seccomp?
- No demo, the tool is not packaged, yet.

udica

- [Credits](#)
- Examines container configuration
- Generate SELinux policy
- Demo: `Demos/security/SELinuxUdica`



Features in podman and not in docker (F)

- [upstream table](#)
- UX enhancements
- not-merged proposals for `docker`
- pod manipulation

Features in podman and not in docker I/VII

- podman container checkpoint
- podman container restore

Checkpoints one or more running containers. The container name or ID can be used.

Usage:

```
podman container checkpoint [flags] CONTAINER [CONTAINER...]
```

Examples:

```
podman container checkpoint --keep ctrID
podman container checkpoint --all
podman container checkpoint --leave-running --latest
```


Features in podman and not in docker II/VII

- podman container cleanup
- podman container exists
- podman container runlabel
- podman healthcheck run

Examples:

```
podman container cleanup --latest  
podman container cleanup ctrID1 ctrID2 ctrID3  
podman container cleanup --all
```

```
podman container exists containerID  
podman container exists myctr || podman run --name myctr [etc...]
```

Features in podman and not in docker III/VII

- podman image exists
- podman image sign | podman image trust
- podman image tree

```
$ podman image tree --whatrequires e7d92cdc71fe
```

Image Layers

```
└─ ID: 5216338b40a7 Size: 5.857MB Top Layer of: [docker.io/library/alpine:latest]
   └─ ID: c07692cd6afc Size: 61.23MB
      └─ ID: 680cc73971b8 Size:      0B
         └─ ID: 79328d443872 Size:      0B
      └─ ID: b876d8a9551e Size: 61.23MB
         └─ ID: a2cdfa446b03 Size:      0B
            └─ ID: 003c10d311c8 Size:      0B
      └─ ID: 92a673328d5d Size: 61.23MB Top Layer of: [localhost/hello:latest]
         └─ ID: 33a5ba140a3f Size:      0B
            └─ ID: 45b17e59ed3b Size:      0B
```

Features in podman and not in docker IV/VII

- podman mount
- podman umount

(Un)mount a working container's root filesystem.

Features in podman and not in docker V/VII

- podman varlink

Run varlink interface

Description:

Run varlink interface. Podman varlink listens on the specified unix domain socket for

Tools speaking varlink protocol can remotely manage pods, containers and images.

Usage:

```
podman varlink [flags] [URI]
```

Examples:

```
podman varlink unix:/run/podman/io.podman
```

```
podman varlink --timeout 5000 unix:/run/podman/io.podman
```

Features in podman and not in docker VI/VII

- podman system service

Run API service

Description:

Run an API service

Enable a listening service for API access to Podman commands.

Features in podman and not in docker VII/VII

- `podman play`
- `podman play kube`
- `podman generate`
- `podman generate kube`
- `podman pod *`

podman → k8s (T)

- podman can create definitions based on live containers
- `podman generate kube`
- `podman generate systemd`

podman → k8s (T)

- podman can create definitions based on live containers
- `podman generate kube`
- `podman generate systemd`
- Demo!

skopeo (T)

- move container images around
- registry, dockerd, containers/storage, a file
- transports

```
skopeo inspect docker://docker.io/usercont/packit
{
  "Name": "docker.io/usercont/packit",
  "Digest": "sha256:4918b3a8511b7ca91...",
  "RepoTags": [
    "latest",
    "prod"
  ],
  "Created": "2020-02-19T15:24:13.408449229Z",
```



buildah (F)

- shell-based container builder tool
- no container runtime daemon needed
- simple, efficient



buildah: benefits

- no need for build/install requirements in the final image
- read/write volumes during the build
- rootless usage
 - buildah images available at quay.io/repository/buildah/stable
- `buildah build-using-dockerfile`

toolbox (F)

Toolbox is a tool that offers a familiar package based environment for developing and debugging software that runs fully unprivileged using Podman.

```
[user@hostname ~]$ toolbox create  
Created container: fedora-toolbox-30  
Enter with: toolbox enter
```

```
[user@hostname ~]$ toolbox enter
```







```
●[user@toolbox ~]$
```



You've seen these demos

- intro (F)
- rootless containers (T)
- building images (F)
 - basic
 - speeding up builds
- security (T)
 - basic
 - udica
- ~~from podman to k8s~~

The end

-  github.com/TomasTomecek/speaks
-  github.com/lachmanfrantisek
-  gitlab.com/lachmanfrantisek
-  github.com/containers
-  [@TomasTomec](https://twitter.com/TomasTomec)
-  blog.tomecek.net