Rootless containers with udocker

Jorge Gomes <jorge at lip.pt>

eosc-hub.eu

@EOSC_eu

Dissemination level: Public

EOSC-hub receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 777536.

EOSC-hub

udocker is a tool to run containers in user space

without Docker
without privileges
without system installation

EOSC-hub

udocker empowers users to run applications encapsulated in Docker containers

but can be used to run any container whose payload does not require privileges

udocker supports multiple execution technologies

udocker can run in many Linux systems, new and old:
Ubuntu 14, Ubuntu 16, Ubuntu 18,
CentOS 6, CentOS 7,
Fedora, etc

and is well suited for:
computing farms , grids , GPU computing

EOSC-hub

How does it work

1. Download udocker
2. Using udocker get a container image:
   - Pull containers from dockerhub
   - Load containers saved by Docker
   - Import containers exported by Docker
   - Import an OS filesystem tarball
3. Use udocker to run the container

Commands

- udocker syntax is simple and docker like:

udocker search
udocker pull
udocker create
udocker run
udocker import

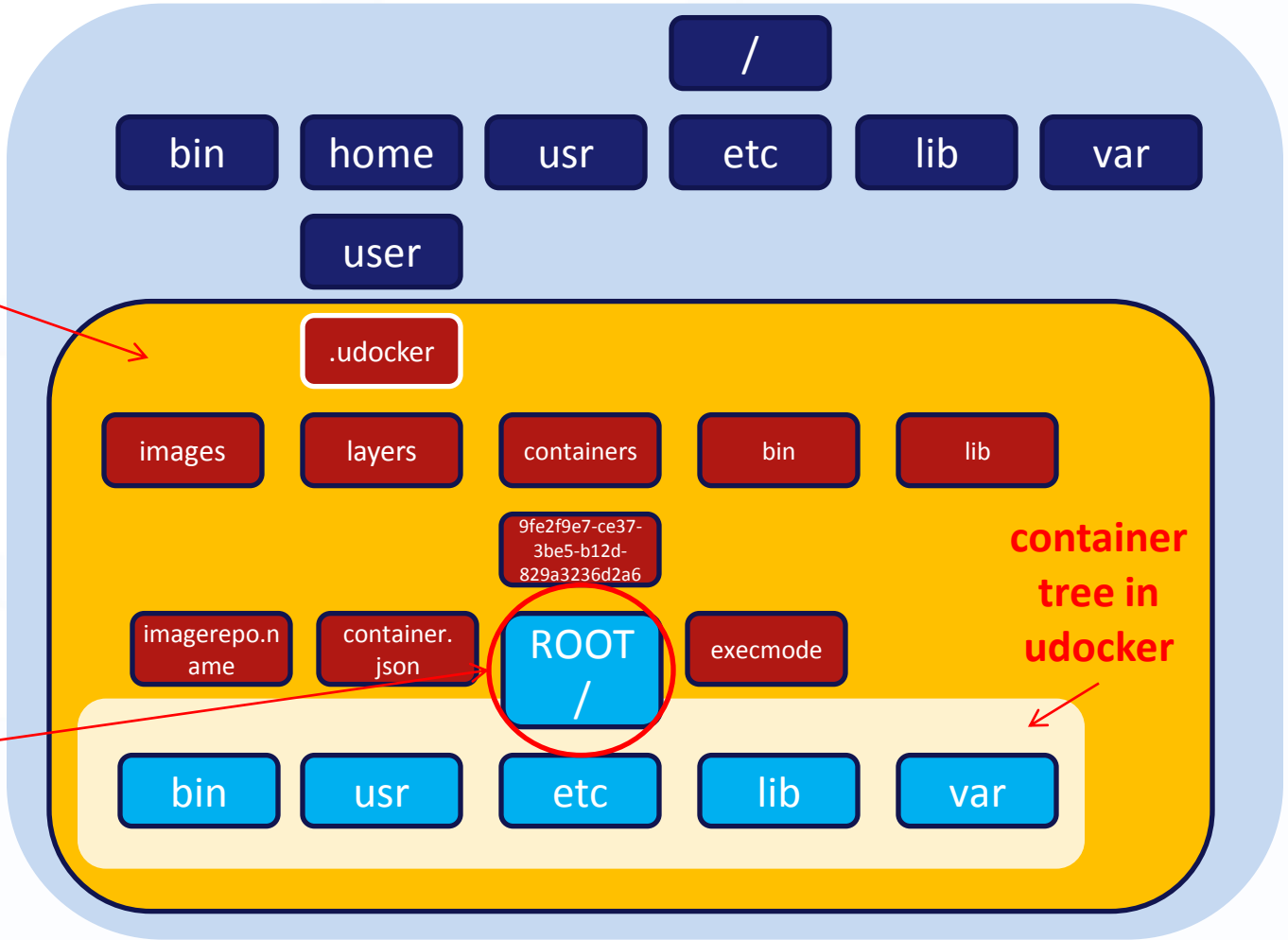
udocker load
udocker images
udocker rmi
udocker ps
udocker rm

Execution

- Execution
- chroot-like

udocker directory tree $HOME/.udocker

chroot to this directory becomes the new root for container processes



EOSC-hub

udocker integrates technologies udocker can execute your containers using several methods

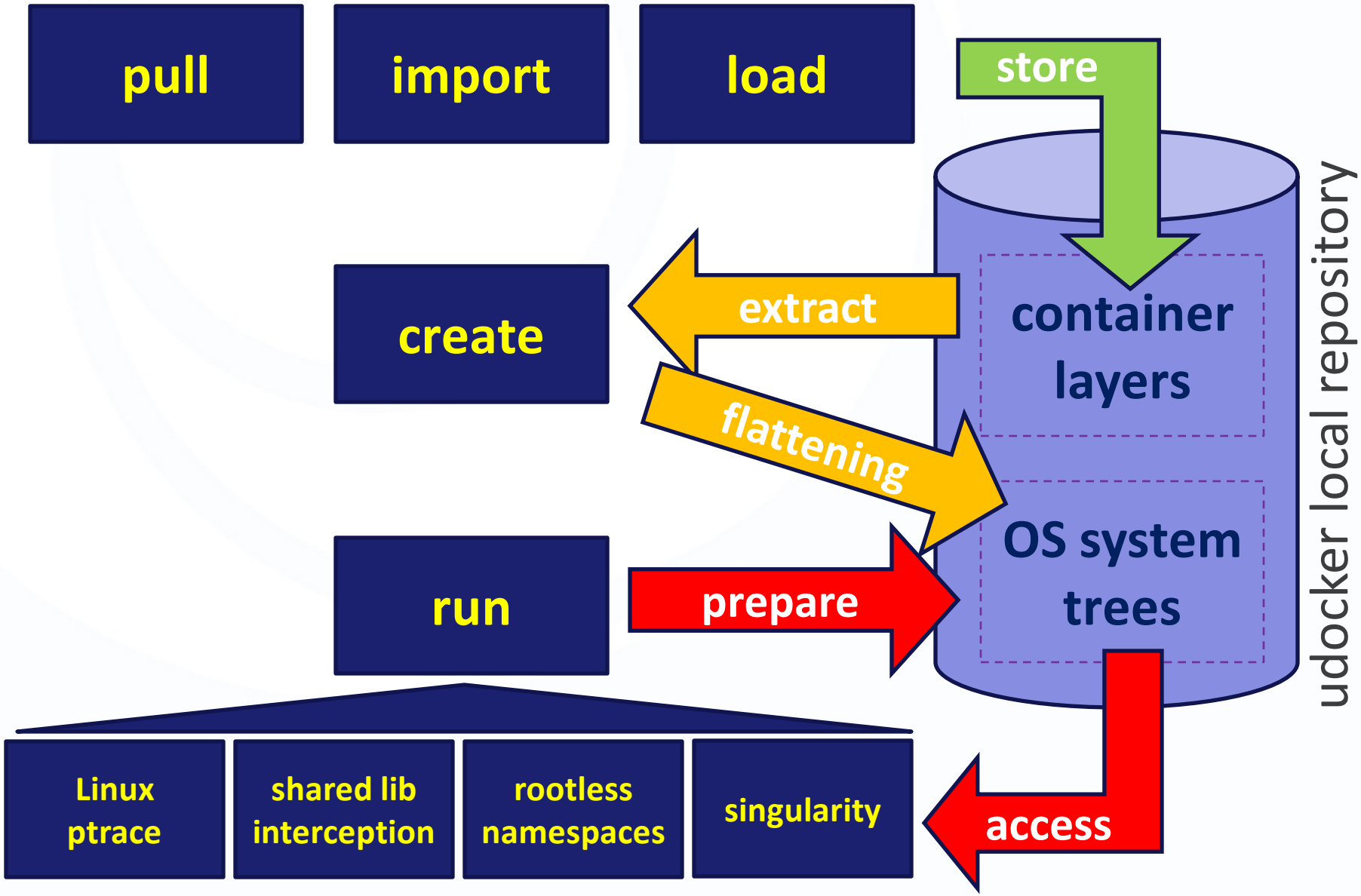
- ptrace
- shared lib interception
- user namespaces
- singularity

Execution methods

- udocker supports several techniques to achieve the equivalent to a chroot without using privileges
- They are selected per container id via execution modes

Mode	Base	Description
P1	PRoot	PTRACE accelerated (with SECCOMP filtering) ← DEFAULT
P2	PRoot	PTRACE non-accelerated (without SECCOMP filtering)
R1	runC	rootless unprivileged using user namespaces
F1	Fakechroot	with loader as argument and LD_LIBRARY_PATH
F2	Fakechroot	with modified loader, loader as argument and LD_LIBRARY_PATH
F3	Fakechroot	modified loader and ELF headers of binaries + libs changed
F4	Fakechroot	modified loader and ELF headers dynamically changed
S1	Singularity	where locally installed using chroot or user namespaces

EOSC-hub


pull
import
load
store
create
extract
container layers
flattening
udocker local repository
run
prepare
OS system trees
Linux ptrace
shared lib interception
rootless namespaces
singularity
access

EXAMPLES

using udocker

EOSC-hub

Downloading udocker

udocker in open source, available from github

https://github.com/indigo-dc/udocker

- https://github.com/indigo-dc/udocker/tree/master
- https://github.com/indigo-dc/udocker/tree/devel

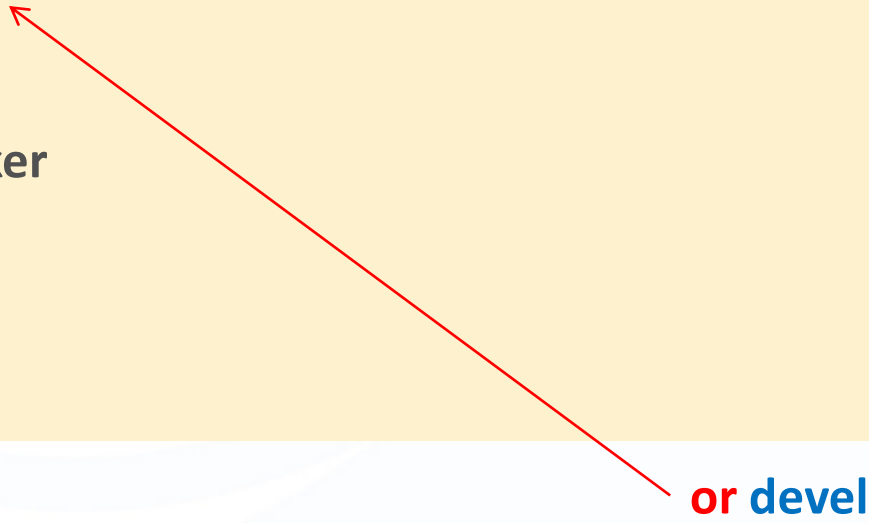
https://github.com/indigo-dc/udocker/tree/master/doc

Install from github

```
$ curl https://raw.githubusercontent.com/indigo-dc/udocker/master/udocker.py > udocker

$ chmod u+rx udocker

$ ./udocker install
```



Does not require compilation or system installation
Tools are delivered statically compiled

EOSC-hub

Pull container from dockerhub

```
$ udocker pull ubuntu:18.04
Downloading layer: sha256:aafe6b5e13de557451e1781fe7276620275625f970015cbd10036ab7d8ae27c0
Downloading layer: sha256:0a2b43a726608d3835aa027bbe181624789130c212eb191baa481f1d788a0676
...
```

Extract it to your home directory

```
$ udocker create --name=ub18 ubuntu:18.04
de13a504-dd22-3e77-8fd5-37e3376f703a
```

Run a command in the container

```
$ udocker -q run ub18 cat /etc/lsb-release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=18.04
DISTRIB_CODENAME=bionic
DISTRIB_DESCRIPTION="Ubuntu 18.04 LTS"
```

EOSC-hub

```
$ udocker -q  run  ub18   /bin/bash
root@host:/#   apt-get   update
root@host:/#   apt-get   install  firefox
```

Interactive shell

Install software

Run as yourself

Use the host environment variables

```
$ udocker -q  run  --user=$USER --hostenv   ub18
user@host:~$   firefox  --no-remote
```

EOSC-hub

```
$ udocker  setup   ub18
execmode: P2
```

The current engine is ptrace

```
$ udocker  setup  --execmode=R1  ub18
```

Select engine rootless namespace

```
$ udocker -q  run  --user=$USER \
  --hostenv  --bindhome  --hostauth  ub18
root@host:~#   firefox  --no-remote
```

Run in the same manner

```
$ udocker  setup  --execmode=P2  ub18
```

Get back to ptrace engine

https://github.com/indigo-dc/udocker

Thank you
for your attention!

Questions?

EOSC-hub

eosc-hub.eu @EOSC_eu