How to start a Docker container as non-root user

Montreal Hack&Tell 2, Nov 16, 2016

Quan Nguyen
<mr.quan.nguyen@gmail.com>
https://github.com/2uanta/udocker

```
[root@localhost ~]# docker run -it --rm kaggle/python
Unable to find image 'kaggle/python:latest' locally
latest: Pulling from kaggle/python
c289280e4ecc: Pull complete
307524089b33: Pull complete
c88a5495ae41: Pull complete
1b7d075bc4bb: Pull complete
5b58f3d008b4: Pull complete
1e062780939a: Pull complete
31a095b4c846: Pull complete
04dcdc8a4368: Pull complete
5c778e1a313e: Pull complete
77f24c74ee5a: Pull complete
a1ed74ef5cb6: Pull complete
b9721ccdf423: Pull complete
de49a7941796: Pull complete
4463f4d9d01b: Pull complete
```

container

(cont'd)

```
Digest:
sha256:f9c47a738efbccb0e81e4dd7db0ce45d0c62524924e15acae4e5e298ba3
71e39
Status: Downloaded newer image for kaggle/python:latest
```

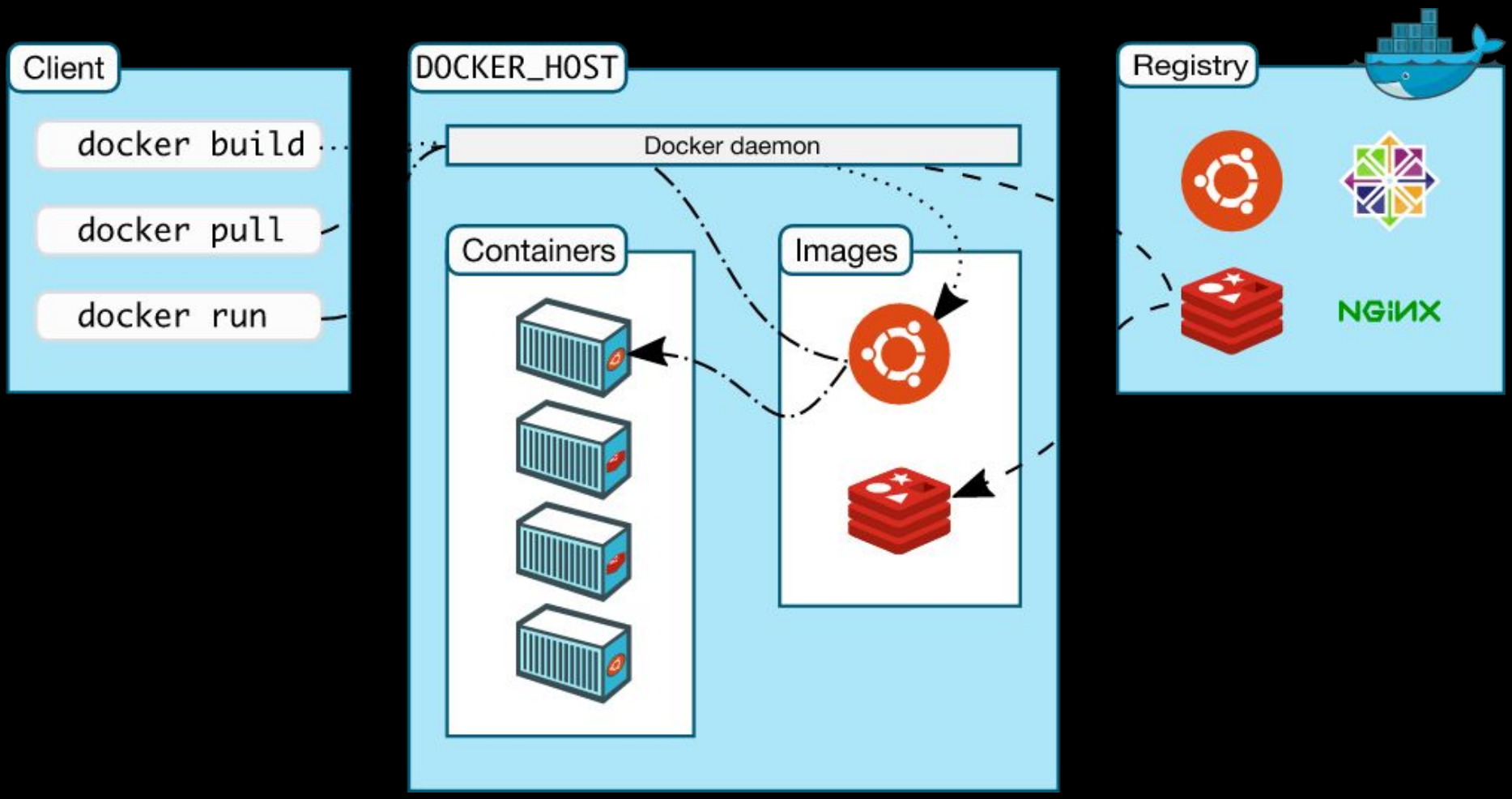

```
root@369bb4621447:/# python
Python 3.5.2 |Anaconda 4.2.0 (64-bit)| (default, Jul  2 2016,
17:53:06)
[GCC 4.4.7 20120313 (Red Hat 4.4.7-1)] on linux
Type "help", "copyright", "credits" or "license" for more
information.
>>> import numpy as np
>>> import matplotlib.pyplot as plt
...
>>> plt.show()

root@369bb4621447:/# exit
[root@lm-2r02-n77 ~]#
```


R00T
ACCESS

```
[root@lm-2r02-n77 ~]# sudo su mysql
```


```
bash-4.1$ docker run -it --rm kaggle/python
Post http:///var/run/docker.sock/v1.19/containers/create: dial
unix /var/run/docker.sock: permission denied. Are you trying to
connect to a TLS-enabled daemon without TLS?
```

```
bash-4.1$ udocker run -it --rm kaggle/python
I have no name!@d1fd1ea99365:/var/lib/mysql$ python
Python 3.5.2 |Anaconda 4.2.0 (64-bit)| (default, Jul  2 2016,
17:53:06)
[GCC 4.4.7 20120313 (Red Hat 4.4.7-1)] on linux
Type "help", "copyright", "credits" or "license" for more
information.
>>>
```



https://docs.docker.com/engine/understanding-docker/

https://docs.docker.com/engine/security/security/#/docker-daemon-attack-surface

Docker daemon attack surface

Running containers (and applications) with Docker implies running the Docker daemon. This daemon currently requires `root` privileges, and you should therefore be aware of some important details.

First of all, only trusted users should be allowed to control your Docker daemon. This is a direct consequence of some powerful Docker features.

udocker

- force uid so that the container will run under this user privilege
- map /etc/sudoers to /dev/null to disable sudo su
- automatically map user home directory and present it as a volume to the container
- force work dir to be user's home dir

udocker

- force interactive container, i.e. `-d` is not allowed and `-i` forced
- user can specify `-t` if a console session is desired
- force `--rm` option to remove the container on exit
- many other options are disabled

The “udocker” wrapper must run as suid and owned by root.

Alternatives: customize sudo command (less flexible)

History

The setuid bit was invented by Dennis Ritchie[8] and included in su.[8] His employer, then Bell Telephone Laboratories, applied for a patent in 1972; the patent was granted in 1979 as patent number US 4135240 "Protection of data file contents". The patent was later placed in the public domain.[9]