Docker day by ING Services Polska | Katowice | 2015-12-16

CONTAINERS & DOCKER SECURITY CONSIDERATIONS

MESOSPHERE

LINUX CONTAINERS

The why and the what

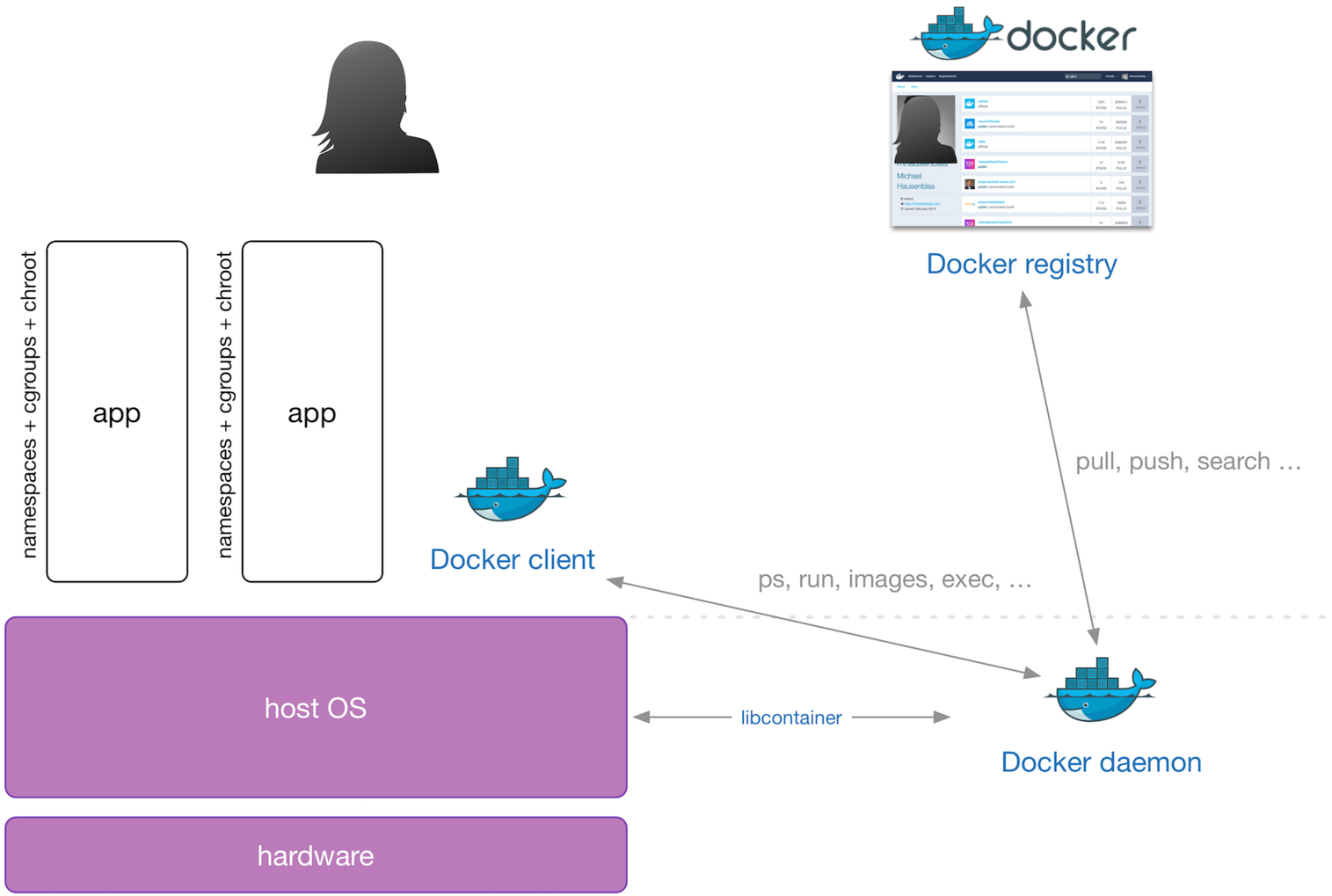
- Containers vs VMs
- app-level dependency management
- lightweight (startup time, footprint, average runtime)
- security considerations
- pets vs cattle (and flock of birds)

LINUX CONTAINERS

- namespaces
  - Isolate PIDs between processes
  - Isolate network resources (stacks, devices, etc.)
  - Isolate hostname/NIS (UTS)
  - Isolate filesystem mount (chroot)
  - Isolate inter process communication (IPC)
  - Isolate users/groups
- cgroups

  https://sysadmincasts.com/episodes/14-introduction-to-linux-control-groups-cgroups

DOCKER



DOCKER

Registries

- Docker Hub

  https://hub.docker.com/

- Google Cloud

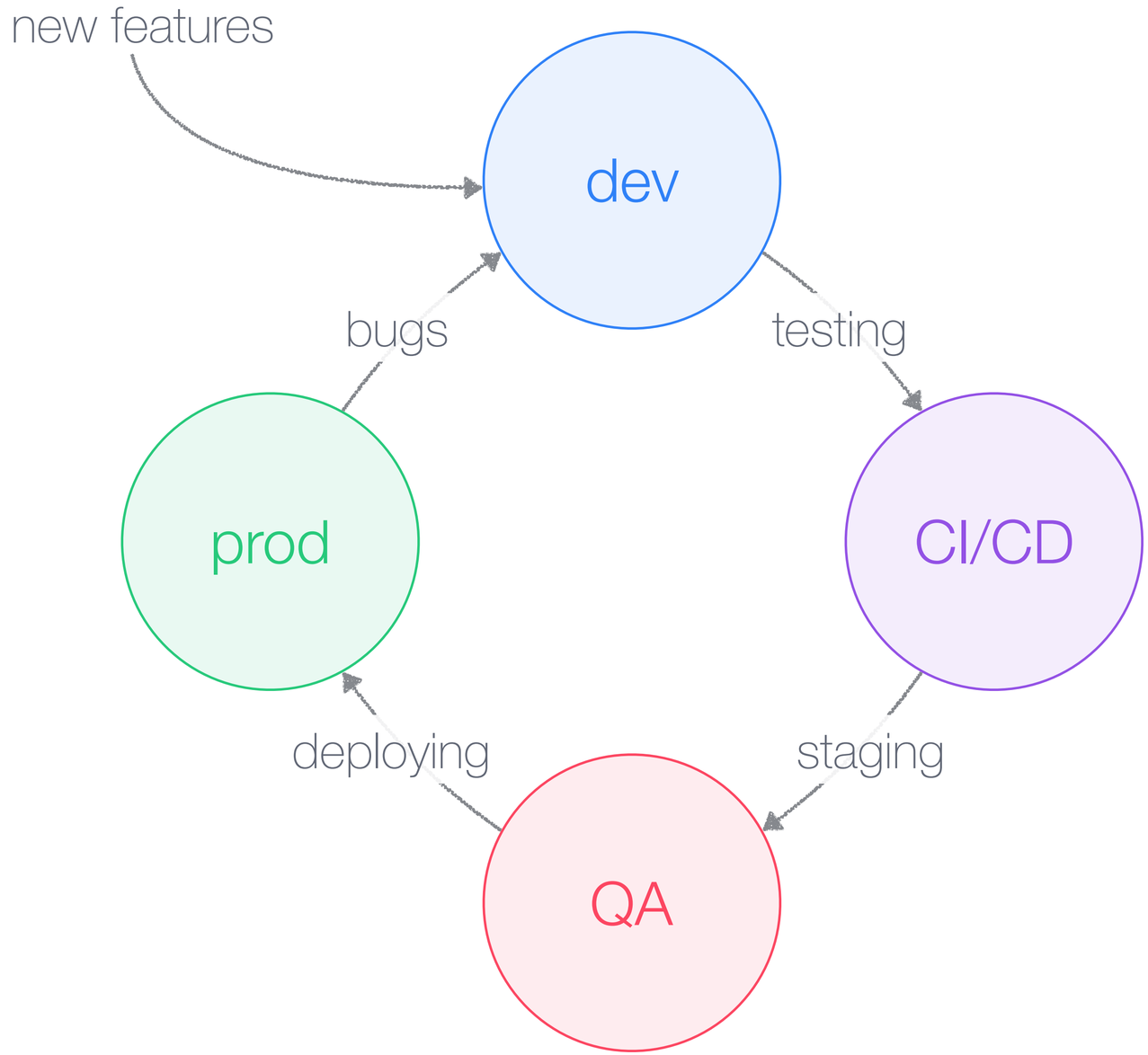
  https://cloud.google.com/tools/container-registry/

- AWS

  https://aws.amazon.com/ecr/

- Run your own

  https://docs.docker.com/registry/deploying/



ARE CONTAINERS SECURE?

ISSUES AND HOW TO ADDRES S THEM

- Basically, nothing has changed, but …
- be aware of new attack vectors
- Think end-to-end, full lifecycle (, ICC, etc.)

ISSUES AND HOW TO ADDRESS THEM

- containers share same kernel
  - kernel exploits
  - DoS
- namespaces (user NS: UID 0 recently introduced)
  - avoid breakouts through least privilege
- networking (lock down ICC, for example)

ISSUES AND HOW TO ADDRESS THEM

Images

- avoid poisoned images
  - use Notary
  - sign images
- set user

```
RUN groupadd -r user_grp && useradd -r -g user_grp user
USER user
```

- define resource constraints (DoS prevention)
- others (limit capabilities, remove setuid/setgid)

ISSUES AND HOW TO ADDRESS THEM

Please, don't bake credentials into images …

rather do:

```
$ docker run -d -e API_TOKEN=SECRET somedatabase
```

```
$ docker run -d -v $(pwd):/fsecret:/fsecret:ro somedatabase
```

ISSUES AND HOW TO ADDRESS THEM

Even better …

Use a key-value in-memory store:

- Square's KeyWhiz
- HashiCorp's Vault
- Crypt

… or native solutions such as Kubernetes Secrets for credentials.

FURTHER RESOURCES

https://github.com/docker/docker-bench-security

http://containerjournal.com/2015/10/22/docker-docker-docker-security-docker/

https://www.youtube.com/watch?v=JvjdfQC8jxM

https://opensource.com/business/14/7/docker-security-selinux

https://mesosphere.github.io/marathon/docs/ssl-basic-access-authentication.html

https://docs.docker.com/engine/articles/security/

https://github.com/brndnmtthws/vault-dcos

https://github.com/docker/notary

http://kubernetes.io/v1.1/docs/design/security.html