Kontajnery a Docker pre každého

4/21/17

Michal Juranyi

Obsah

- Úvod
- Virtualizácia a izolácia
  - Rozdelenie, porovnanie
  - Bezpečnosť, poriadok
- Docker
  - Teoreticky
  - Prakticky
  - Ako ho využívame my

Úvod – bežné starosti zo života (linuxáka)

- Potrebujem Windows (na školské zadanie)
  - kontajner mi nepomôže :(
- Mám starý systém, potrebujem nové knižnice
- Mám nový systém, potrebujem staré knižnice
- Potrebujem súčasne rôzne verzie programov
- Chcem si udržať čistý systém

Izolácia (dátová)

- Oddelenie časti dát od zvyšku systému
  - iba závislosti (knižnice, moduly, interpret)
  - celé prostredie
- Jednoducho odstrániteľné (`rm -r`)
- Jednoducho replikovateľné
- Súčasne nainštalované rôzne verzie SW
- Netreba byť root (niekedy)

Izolácia (dátová) - virtualenv

- Python, Ruby, Perl…
- Každý projekt môže mať svoj virtualenv
  - projekty môžu mať vzájomne sa vylučujúce závislosti
- Beh programu nie je oddelený

Izolácia (dátová) - chroot

- Natívna podpora Linux/UNIX
- Oddeľuje sa celá štruktúra FS (/bin,/usr,...)
- Beh programu je oddelený iba dostupnou časťou FS (čiastočná bezpečnosť)
- Ostatné zdroje nie sú oddelené
- Nie veľmi komfortné používanie
- Nepovažuje sa za dostatočne bezpečné

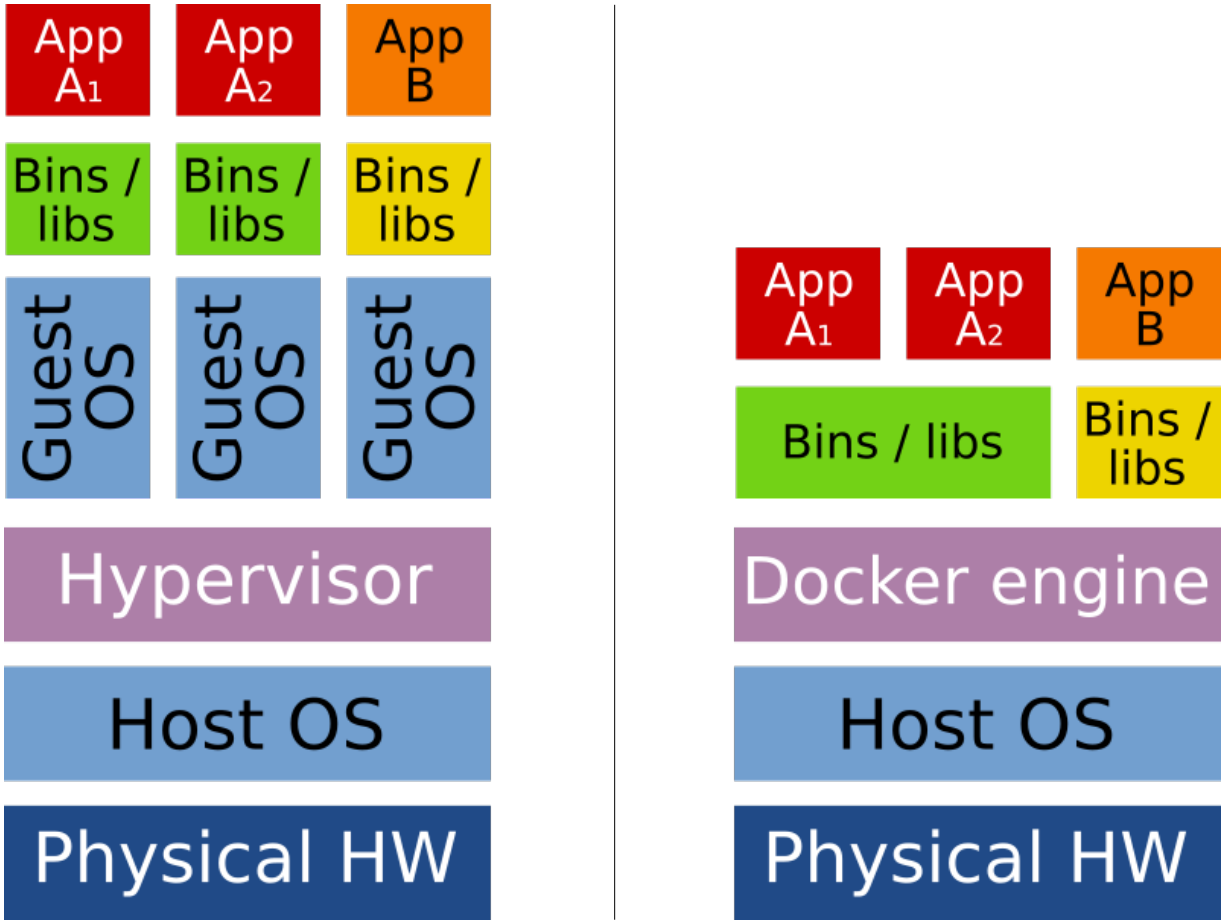
Izolácia (celková) – jails

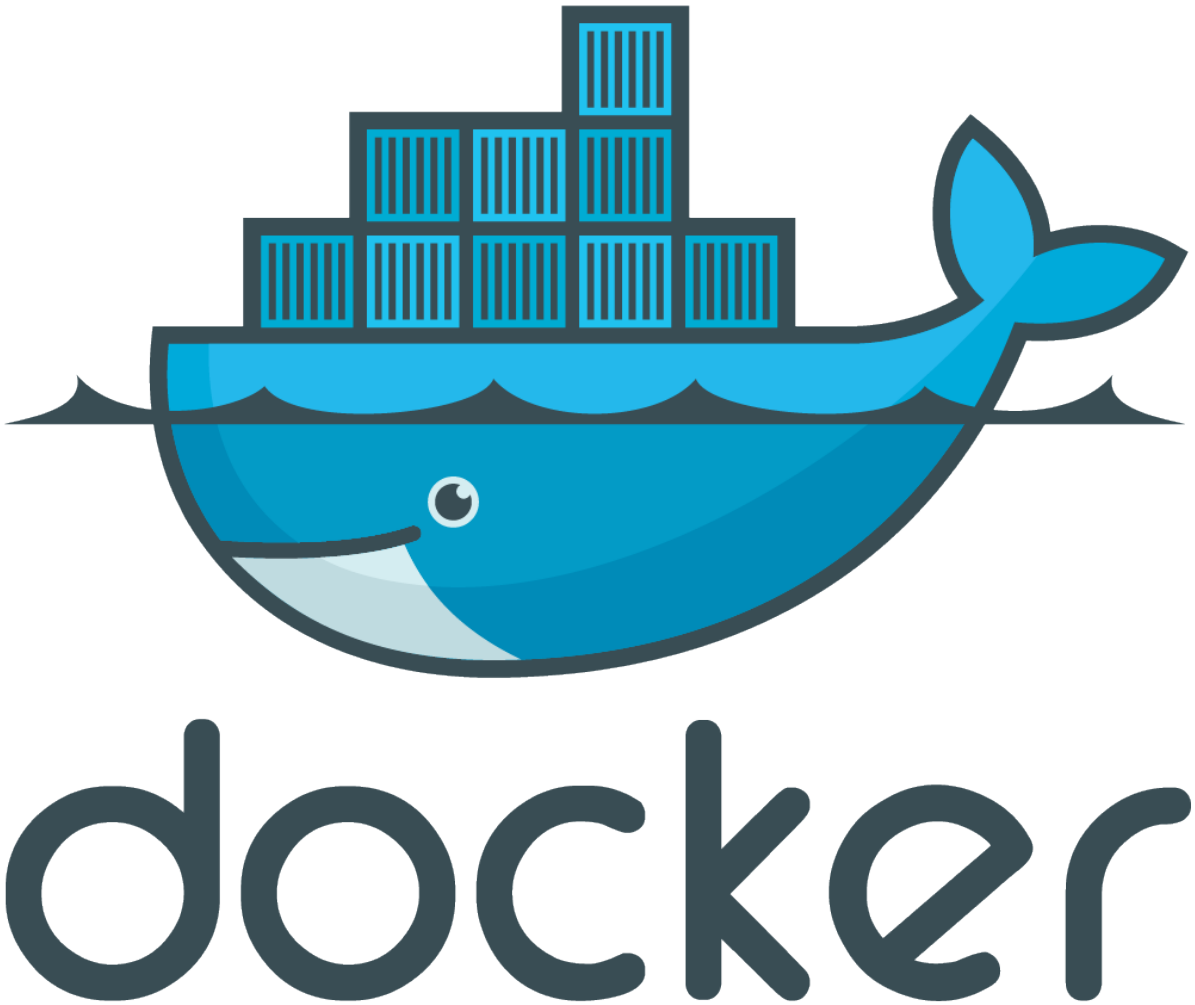
- „Chroot na steroidoch“
- Pridáva virtualizáciu používateľov a sieťového subsystému
- Dá sa považovať za základ OS-level virtualizácie
- FreeBSD – od 4.X (rok 2000)

Virtualizácia

Full- / Para-virtualizácia	OS-level virtualizácia
Virtualizujeme HW	Oddeľujeme systémové zdroje
Spustíme ľubovoľný OS	“Spustíme” len rovnaký OS (zdieľame jadro)
Veľká réžia (výpočtová aj dátová)	Zanedbateľná réžia
KVM, VirtualBox, QEMU	OpenVZ, LXC, (Docker)

Virtualizácia




docker

Docker

- Nepriniesol novú technológiu, iba prístup
  - spopularizoval kontajnery
- Automatizuje a zjednodušuje správu kontajnerov
- Mení spôsob používania kontajnerov (full-server -> single-service)
- „Multiplatformový“, natívne hlavne Linux

Docker - multiplatformovosť

- Linux
  - natívna podpora, LXC
- FreeBSD
  - experimentálne od 11-CURRENT
  - ZFS, jails, Linux compatibility layer

Docker - multiplatformovosť

- macOS
  - boot2docker
- Windows
  - VirtualBox – boot2docker
  - Hyper-V Containers – od Windows 10 a Windows Server 2016, neúplná funkcionalita

Docker - Dockerfile

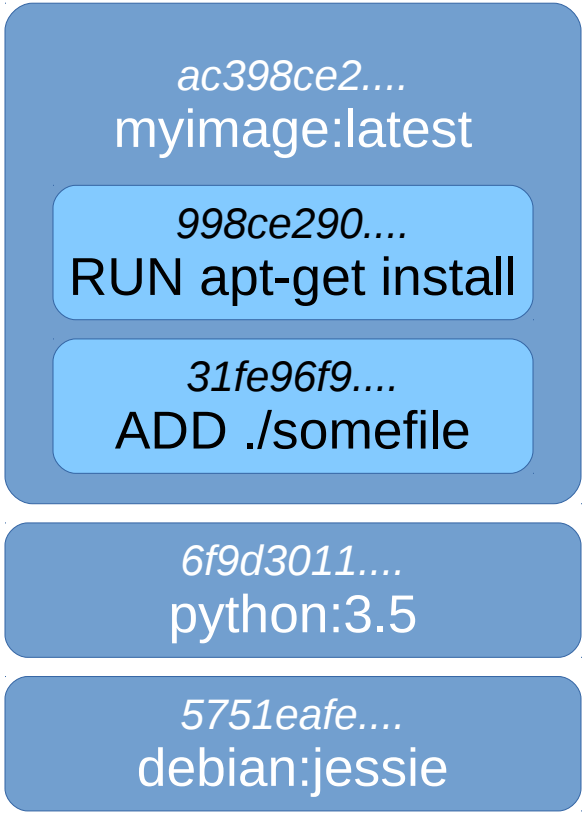
- Definícia („konfigurák“) Docker obrazu
- Jediný súbor potrebný pre vytvorenie obrazu
- Docker hello-world:

```
FROM scratch
COPY hello /
CMD ["/hello"]
```

Docker - Image

- Read-only filesystem
- Vrstvené (snapshoty) – AUFS, Btrfs, ZFS
  - znovupoužiteľnosť – inštrukcia FROM
  - cachovanie
- Zdieľanie
  - s kolegami, komunitou...
- Deployment
  - lokálna príprava produkčného prostredia

Docker - Image



Docker - Registry

- Úložisko pre docker obrazy
- Oficialne verejné: hub.docker.com
  - novinka: store.docker.com
- Možnosť prevádzkovať aj privátny register
  - Docker image „registry“ (oficiálny)
  - GitLab
  - Pulp

Docker - Container

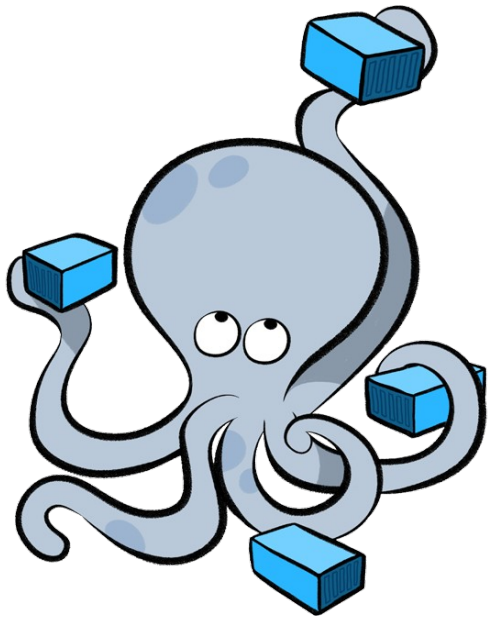
- Read-write vrstva nad obrazom
- Run-time
- Ephemeral *(angl. prchavý)*
  - dôležité dáta ukladáme externe - *volumes*
- Zdieľajú spoločný image
  - nové inštancie „zadarmo“

Docker - Architektúra

- Docker Client
  - REST klient
  - Komunikuje s Docker Engine-om
  - Základný CLI klient
- Docker Engine
  - Docker server/daemon, REST server
- Docker Machine
  - spravuje „Dockerizované“ vzdialené stroje

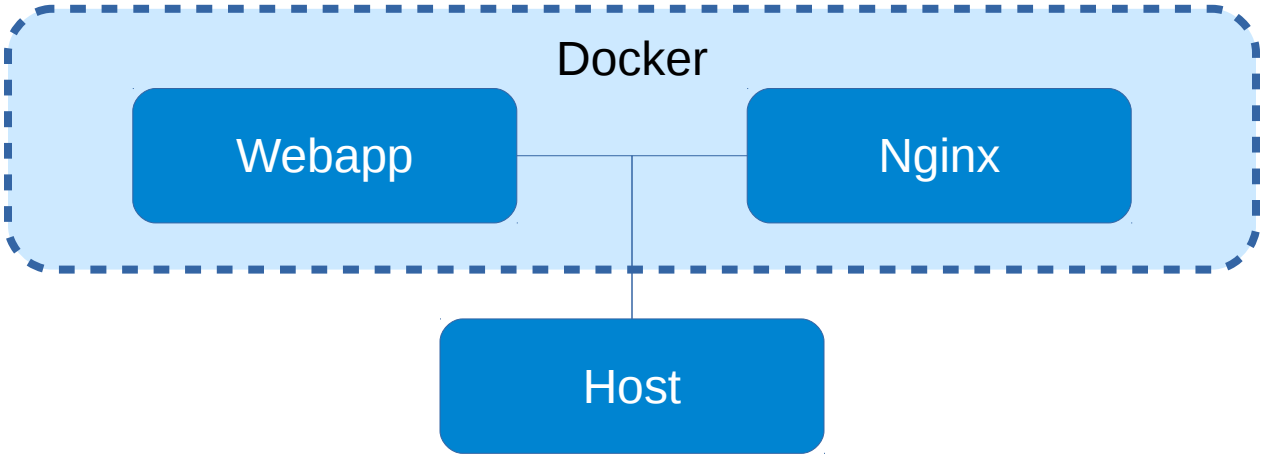
Docker - Compose

- Docker orchestrátor
- Ďalší REST klient
- Zjednodušuje/automatizuje prácu s kontajnermi
- Pomáha konfigurovať a spravovať viackontajnerové prostredia
  - viacvrstvové aplikácie



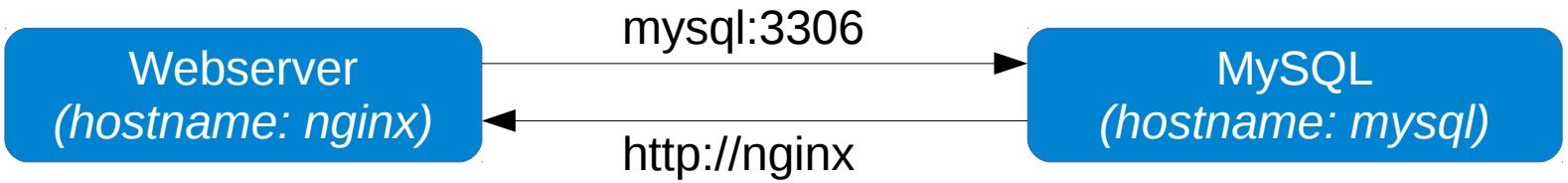
Docker - Networking

- Oddelené virtuálne siete
- Explicitne definované „verejné“ porty
- Porty zdieľané s hostom musia byť takisto explicitne definované



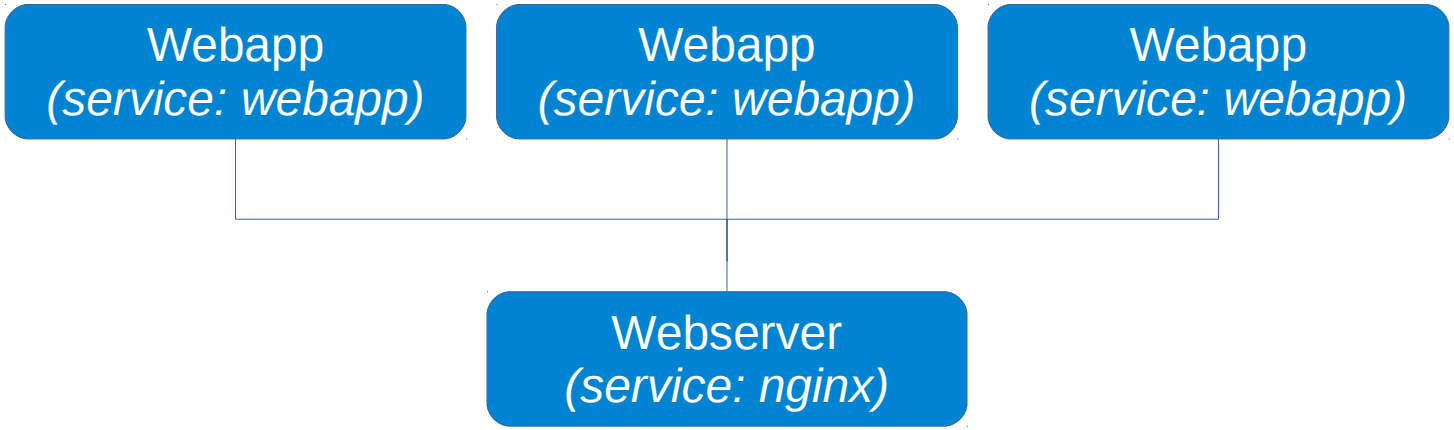
Docker - DNS

- Vlastný DNS mechanizmus
- Kontajnery sú dostupné pod svojim menom, resp. menom služby (Compose)



Docker – Load balancing

- Vlastný loadbalancing na princípe DNS
  - RFC 3484 – longest common prefix selection
- Round-robin mechanizmus
- Umožňuje jednoduché škálovanie

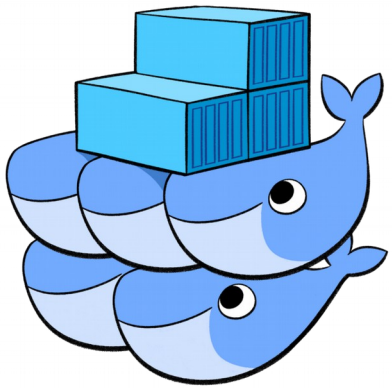


Docker – One process container

- Minimalizácia počtu možných vektorov útoku
- Rýchlo replikovateľné prostredie
- „Reštart“ má minimálny dopad na iné služby
  - navyše je rýchly (reštart jediného procesu)
- „Treat containers like cattle not pets“
  - keď nefunguje, neliečim - zabijem

Docker – Swarm

- Nástroj pre nasadzovanie, správu a škálovanie Docker kontajnerov
- Od v1.12 súčasťou Docker Engine
- Umožňuje produkčné nasadenie a škálovanie kontajnerov vytvorených s Docker Compose



Docker – Ako ho používame my

- Testovanie – testovacie prostredie
- Build proces
- „Stabilizovanie“ legacy skriptov
- Klastrové nasadenie projektov – Kubernetes
- Replikácia produkčného prostredia pri vývoji
- Zdieľanie s kolegami pri vývoji

Praktická ukážka