Docker nie je len Docker

a môže byť bezpečný

18-10-2018

Trusted partner for your **Digital Journey**

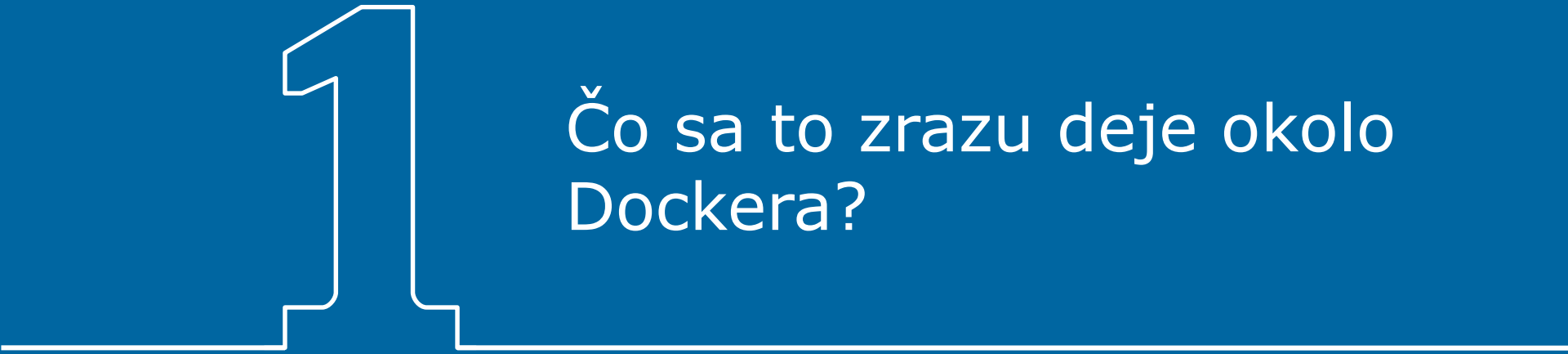
Atos

Program prezentácie

- Čo sa to zrazu deje okolo Dockera?
- Vysvetlenie a živá ukážka ekosystému
- Ako je to s tou bezpečnosťou?

Ako vám môže Atos pomôcť

- Máme tím = od Docker až po ELK a Kafka
- Máme projekty = skúsenosti
- Máme delivery proces = overený kvalitný spôsob dodávky
- Máme globálny produkt Amos Management of OpenShift



Čo sa to zrazu deje okolo Dockera?

Dôvody pandémie menom Docker
hardvér a operačný systém

- Stabilizácia kľúčových komponentov Linux kernel
  - namespaces (od roku 2004)
  - cgroups (od roku 2006)
  - plná podpora kontajnerov v Linux 7 (od roku 2015)

- Dostatočný výkon CPU
  - 2008 – X5260 – 2 jadrá – 1800 eur – 37 bodov SPECInt2006 Rates
  - 2018 – 6126 – 12 jadier – 1800 eur – 770 bodov SPECInt2006 Rates
  - 21 krát nárast výkonu za 10 rokov za rovnakú cenu
  - bežný server má dnes 80 threads, je 50 krát výkonnejší
  - zvýšená réžie Docker a jeho podhubia nie je obmedzením

Dôvody pandémie menom Docker
mikroslužby

- Implementácia Dockera v prevádzke je ťahaná aplikáciami

- Zmena spôsobu tvorby a prevádzky aplikácií: **mikroslužby**
  - umožňujú automatizované škáľovanie

- mikroslužby sa spoliehajú na automatizované rekonfigurácie
  - provisioningu
  - dns
  - lodbalancera
  - sieťových nastavení a prestupov
  - proxy
  - debug/tuning

Dôvody pandémie menom Docker
automatizácia nasadzovania

- Ako to spolu hrá?
  - Docker má API
  - Docker API používa SWARM
  - Portainer je UI na správu Docker a SWARM fariem (jeden z viacerých)
  - Kubernetes je nadstavba Docker na správu
  - Kubernetes má API
  - Kubernetes API používa OpenShift

- Už ste sa stratili?
  - Aj tak sa to všetko používa z nástrojov na nasadzovanie ako Jenkins alebo GitLAB

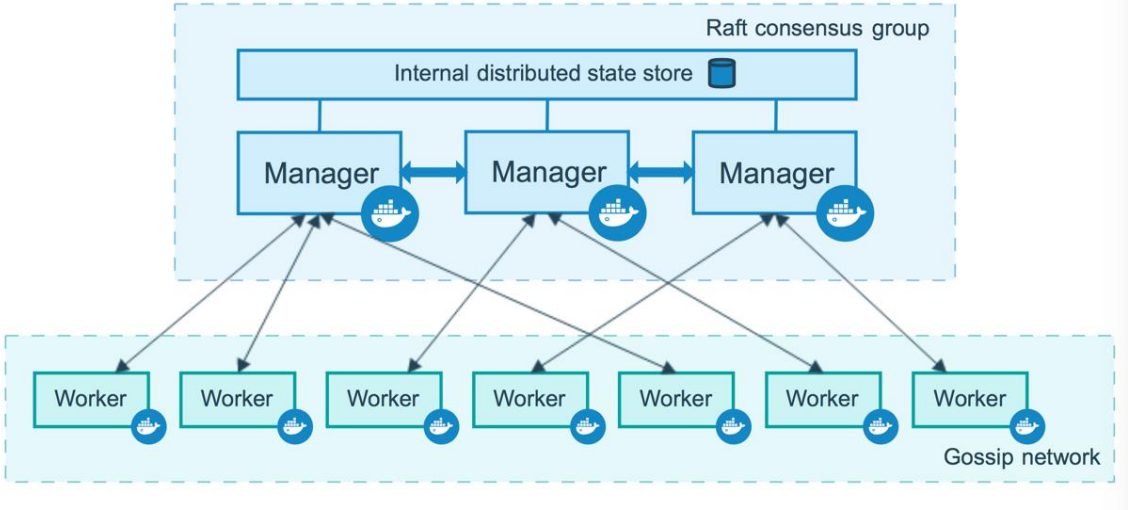
2

Vysvetlenie a živá ukážka ekosystému

Docker Swarm

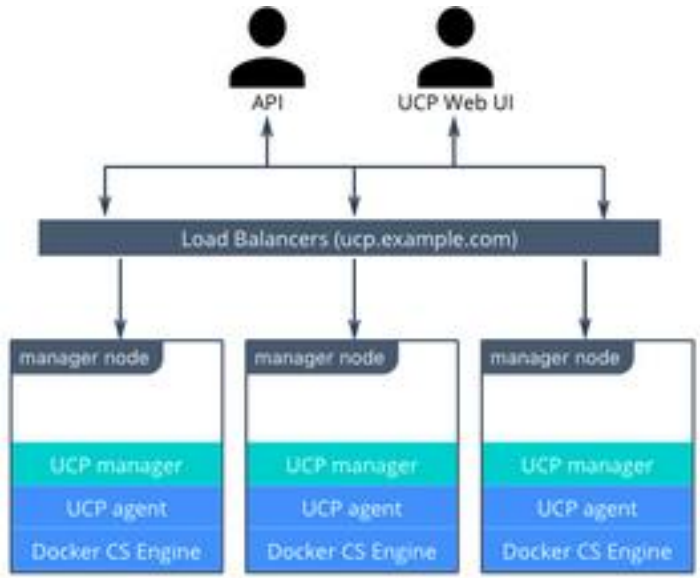
Container as a Service model

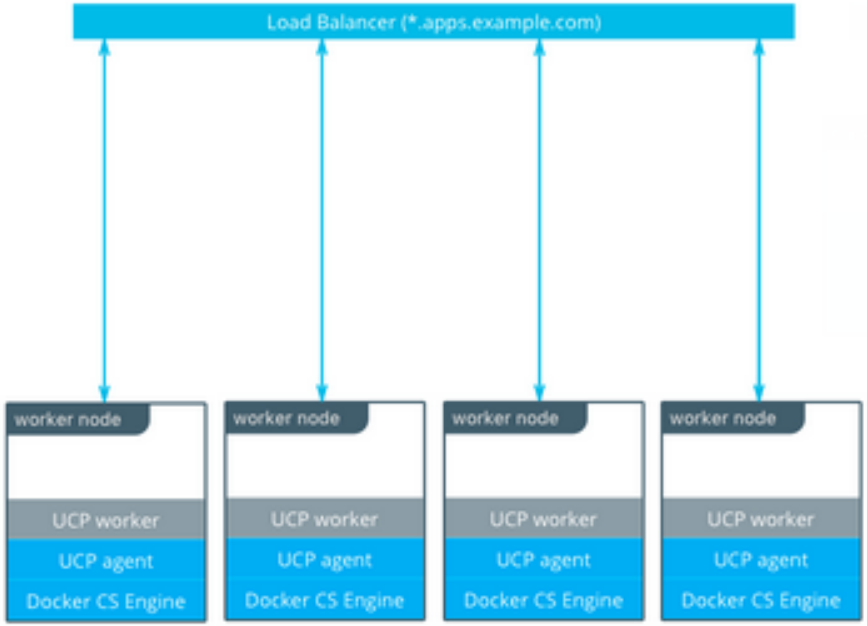
- Decentralized design
- Scaling
- Desired state reconciliation
- Multi-host networking
- Service discovery
- Load balancing
- Secure by default
- Rolling updates
- Cluster management integrated with Docker Engine



Docker Swarm Components

Managers and Workers

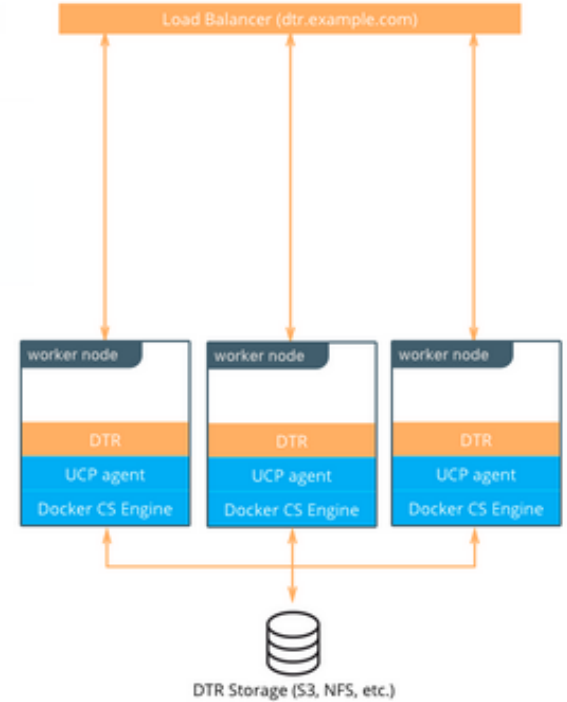




Docker Swarm Components

Docker Trusted Registry

- Image management
  - image repository
- Availability
  - replicas
- Efficiency
  - Image caching
- Built-in access control
  - RBAC, LDAP, AD
- Security scanning
  - CVEs
- Image signing



Live Demo

- Build an image
  - docker build -t httpd:v1 -f Dockerfile_v1 .
- Tag image
  - docker tag httpd:v1 dtr.example.com/admin/httpd:v1
- Push image
  - docker push dtr.example.com/admin/httpd:v1
- Deploy service
  - docker service create --name http --publish 8080:80 --replicas=4 dtr.example.com/admin/httpd:v1
- Update service
  - docker service update --image dtr.example.com/admin/httpd:v2 http
- Rollback service
  - docker service rollback http

Ako je to s tou bezpečnosťou?

V čom je nebezpečenstvo

- Technické chyby
  - v Linux kernel a v samotnom docker procese
  - vo ostatných podporných „aplikáciách“
  - „vyžieranie“ výkonu servera niektorým kontajnerom
- Ľudské chyby
  - v (ne)zabezpečení Linux a kontajnerov
  - sťahovanie images hlava-nehlava
- Principiálne problémy:
  - jasné oddelenie zodpovedností vývoja a prevádzky
  - izolácia prostredí

A čo s tým?

- Technické chyby
  - patchovať – čím väčšia nadstavba, tým jednoduchšie patchovanie
  - nasadiť dobrý nástroj na bezpečnostnú analýzu (Qualys Container Security)
  - nasadiť dobrý nástroj na výkonnostnú analýzu (AppDynamics)

- Ľudské chyby
  - implementovať dobrý proces
  - nasadiť dobrý nástroj na bezpečnostnú analýzu

- Principiálny problém:
  - akceptovať, alebo vyskúšať CloudFoundry
  - nasadiť Docker do virtuálnych serverov nad VMware alebo Hyper-V

Ďakujeme

adela.bobovska@atos.net
peter.wolek@atos.net

Atos