cesnet

ROLE ORCHESTRACE PŘI SPRÁVĚ SYSTÉMŮ

Pavel Valach

CESNET

7. února 2023

Seminář o bezpečnosti sítí a služeb 2023, Praha

Představení

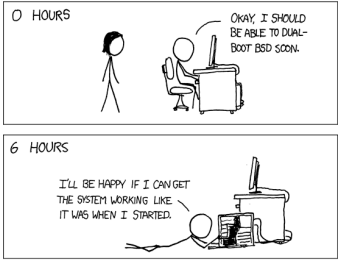
Pavel Valach
člen bezpečnostního týmu CESNET-CERTS
součástí oddělení Security Operation Centre (713 / `rwx--x-wx`)

O čem bude tato prezentace?

- Co Vám orchestrace může přinést
- Čemu se vyhnout

Chci Vás přesvědčit, že byste měli orchestrovat.

Běžná správa serveru



Obrázek: útržek z https://xkcd.com/349/

cesnet

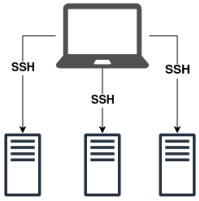
Běžná správa serveru

- Manuální práce, omyly
- Ne vždy předvídatelné změny v konfiguraci
- Sledování změn – `etckeeper`?

cesnet

Běžná správa serveru

- Manuální práce, omyly
- Ne vždy předvídatelné změny v konfiguraci
- Sledování změn – `etckeeper`?
- **„Jedním serverem to nikdy neskončí“**
- Vzniká malá flotila – co teď?
- Ruční instalace? Kopírování konfigurace?
-  Klonování stroje?



P. Valach,
Role orchestrace při správě systémů,
CESNET

cesnet

Když už tedy dokumentujeme

- Je dokumentace *aktuální?*
- Nejsou v ní chyby?

cesnet

Když už tedy dokumentujeme

- Je dokumentace *aktuální?*
- Nejsou v ní chyby?

- ... máte aspoň ty zálohy?
- Změna distribuce?
  - Příliš náročné?


ORCHESTRATE
ALL THE THINGS

Základní přínosy orchestrace

Konfigurační proces, který je:

- Opakovatelně použitelný

Základní přínosy orchestrace

Konfigurační proces, který je:

- Opakovatelně použitelný
- Striktně definovaný a *dokumentovaný*

Základní přínosy orchestrace

Konfigurační proces, který je:

- Opakovatelně použitelný
- Striktně definovaný a *dokumentovaný*
- Dělitelný

Základní přínosy orchestrace

Konfigurační proces, který je:

- Opakovatelně použitelný
- Striktně definovaný a *dokumentovaný*
- Dělitelný
- Škálovatelný
- Testovatelný a *replikovatelný*

Orchestrace může být **stavební kámen**

Výhoda oproti skriptům

A jakou výhodu mi to přinese oproti mým skriptům?

Výhoda oproti skriptům

A jakou výhodu mi to přinese oproti mým skriptům?

- Rozdílná nastavení pro různé skupiny (podle OS, testing/produkce apod.)
- Sjednocení stylu nastavení
- Zabudované mechanismy pro řešení problémů
- *atd., atd.*

Orchestrační nástroje **jsou určeny na správu systémů!**

cesnet

Další výhody orchestrace

- Rychlý sběr informací → **lepší informovanost**
  - Distribuce, verze kernelu, nainstalované balíčky
  - Ukládání do historie

cesnet

Další výhody orchestrace

- Rychlý sběr informací → **lepší informovanost**
  - Distribuce, verze kernelu, nainstalované balíčky
  - Ukládání do historie
- Tvorba auditní stopy → **víte, co se dělo**
  - Možnost přeposílání do centrálního systému

cesnet

Další výhody orchestrace

- Rychlý sběr informací → **lepší informovanost**
  - Distribuce, verze kernelu, nainstalované balíčky
  - Ukládání do historie
- Tvorba auditní stopy → **víte, co se dělo**
  - Možnost přeposílání do centrálního systému
- Rychlé testování → **rychlejší vývoj**

cesnet

Další výhody orchestrace

- Rychlý sběr informací → **lepší informovanost**
  - Distribuce, verze kernelu, nainstalované balíčky
  - Ukládání do historie
- Tvorba auditní stopy → **víte, co se dělo**
  - Možnost přeposílání do centrálního systému
- Rychlé testování → **rychlejší vývoj**
- Minimalizace lidského faktoru → **méně chyb**
  - Nebo naopak jedna obří?

Kde všude se orchestrace používá

- Servery, kontejnery, VMs
- Data, microservices
- Sítě
- *a další...*

Orchestraci nemíchat s ruční správou!

Příklady běžně používaných nástrojů

- Ansible - push-based (stanice konfiguruje servery)
- Puppet - pull-based (agent stahuje od masteru)
- Terraform - infrastructure-as-a-code
- Salt, Chef atd.

Konkrétní nástroj je na Vás!
Vybírejte podle svých potřeb.

cesnet

Praktické principy

Stažení systému a instalace

- Stažení a nastavení systému
- Sestavení obrazu stroje – např. `packer.io`
- Cloudové obrazy VM s podporou `cloud-init`
  - Nastavení síťování, uživatelů, SSH klíčů, repozitářů...
  - Umí např. Ubuntu či RHEL
  - Podpora většiny cloudových platforem

cesnet

Udržování aktuálnosti

- Automatické bezpečnostní aktualizace – `unattended-upgrades`
- Těžko lze použít u kontejnerů
- Dokumentace použitých verzí, rychlý přehled

Bezpečné připojení

- ~~Jménem a heslem~~
- SSH klíči

cesnet

Bezpečné připojení

- ~~Jménem a heslem~~
- SSH klíči
- SSH klíči s OTP

cesnet

Bezpečné připojení

- ~~Jménem a heslem~~
- SSH klíči
- SSH klíči s OTP
- SSH klíč s tajným klíčem na FIDO/U2F klíči

cesnet

Bezpečné připojení

- ~~Jménem a heslem~~
- SSH klíči
- SSH klíči s OTP
- SSH klíč s tajným klíčem na FIDO/U2F klíči
- Certifikáty (i časově omezené)

cesnet

Bezpečné připojení

- ~~Jménem a heslem~~
- SSH klíči
- SSH klíči s OTP
- SSH klíč s tajným klíčem na FIDO/U2F klíči
- Certifikáty (i časově omezené)
- TLS ověření serveru/klienta (Puppet)

cesnet

Bezpečné připojení

- ~~Jménem a heslem~~
- SSH klíči
- SSH klíči s OTP
- SSH klíč s tajným klíčem na FIDO/U2F klíči
- Certifikáty (i časově omezené)
- TLS ověření serveru/klienta (Puppet)
- One-use login - mechanismy typu Vault SSH / AWS Instance Connect
  - Otázka: Dají se integrovat k Ansible?
  - Odpověď: Ano, ale může to vyžadovat trochu práce.

Hesla a klíče - Vault

```
ansible-vault create group_vars/all/pass.yml
New Vault password:
Confirm New Vault password:
```

... ale kolik hesel si reálně musíte k něčemu pamatovat?

cesnet

Různé způsoby správy hesel

- Držení hesel v nějakém Vaultu

cesnet

Různé způsoby správy hesel

- Držení hesel v nějakém Vaultu
- Na krátký čas lze držet v paměti, zatímco je Ansible přenese na další stroj

Různé způsoby správy hesel

- Držení hesel v nějakém Vaultu
- Na krátký čas lze držet v paměti, zatímco je Ansible přenese na další stroj
- Generování v průběhu
- Hesla lze generovat přímo na daném stroji (`password_lookup`)

cesnet

Různé způsoby správy hesel

- Držení hesel v nějakém Vaultu
- Na krátký čas lze držet v paměti, zatímco je Ansible přenese na další stroj
- Generování v průběhu
- Hesla lze generovat přímo na daném stroji (`password_lookup`)
- Varianta s certifikáty, resp. veřejným a privátním klíčem – asi nejbezpečnější

Samozřejmostí by mělo být správné nastavení přístupových práv.

cesnet

Zálohování

Zálohování

Lze zálohovat buď z centrálního místa (pull model), či tak, že stroj se zálohuje sám v pravidelných intervalech (push model). Popř. kombinovat.
Co lze orchestrovat?

Zálohování

Lze zálohovat buď z centrálního místa (pull model), či tak, že stroj se zálohuje sám v pravidelných intervalech (push model). Popř. kombinovat.
Co lze orchestrovat? (vše)

Zálohování

Lze zálohovat buď z centrálního místa (pull model), či tak, že stroj se zálohuje sám v pravidelných intervalech (push model). Popř. kombinovat.
Co lze orchestrovat? (vše)

- Nastavení přístupů

Zálohování

Lze zálohovat buď z centrálního místa (pull model), či tak, že stroj se zálohuje sám v pravidelných intervalech (push model). Popř. kombinovat.
Co lze orchestrovat? (vše)

- Nastavení přístupů
- Jednotná konfigurace pro zálohu

Zálohování

Lze zálohovat buď z centrálního místa (pull model), či tak, že stroj se zálohuje sám v pravidelných intervalech (push model). Popř. kombinovat.
Co lze orchestrovat? (vše)

- Nastavení přístupů
- Jednotná konfigurace pro zálohu
- Kontrola, zda zálohování skutečně probíhá

Zálohování

Lze zálohovat buď z centrálního místa (pull model), či tak, že stroj se zálohuje sám v pravidelných intervalech (push model). Popř. kombinovat.
Co lze orchestrovat? (vše)

- Nastavení přístupů
- Jednotná konfigurace pro zálohu
- Kontrola, zda zálohování skutečně probíhá
- **Obnova ze zálohy!** (a testy obnovy :-))

cesnet

Disaster recovery

cesnet

„Houstone, máme problém!“

- Služba neběží!
- Utíkají nám zákazníci!

„Houstone, máme problém!“

Namísto victim blamingu a vět:

- Proč jsme na to nebyli připraveni?
- Co teď máme dělat?

„Houstone, máme problém!“

Namísto victim blamingu a vět:

- Proč jsme na to nebyli připraveni?
- Co teď máme dělat?

budete schopni vytáhnout dokumentaci a říct:

- Známe postup, jak systém obnovit,
- Potrvá to 42 hodin a je třeba udělat následující kroky... *výpis kroků*

cesnet

Využití při disaster recovery

- Zjištění aktuálního stavu (pokud je co zjišťovat),
- Rapid re-deployment
- Přenastavení IP adres, DNS záznamů, oprava konfigurace
- Hromadná obnova ze zálohy
- Minimalizace lidského faktoru – **méně chyb**

Využití při disaster recovery

- Zjištění aktuálního stavu (pokud je co zjišťovat),
- Rapid re-deployment
- Přenastavení IP adres, DNS záznamů, oprava konfigurace
- Hromadná obnova ze zálohy
- Minimalizace lidského faktoru – **méně chyb**

Na co si dávat pozor:

cesnet

Využití při disaster recovery

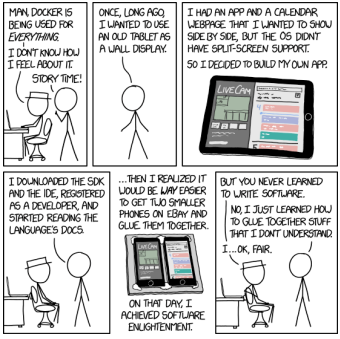
- Zjištění aktuálního stavu (pokud je co zjišťovat),
- Rapid re-deployment
- Přenastavení IP adres, DNS záznamů, oprava konfigurace
- Hromadná obnova ze zálohy
- Minimalizace lidského faktoru – **méně chyb**

Na co si dávat pozor:

- Pravidelné testování, hlavně po změnách v infrastruktuře
- Mít připravený proces pro detekci a řešení selhání

cesnet

Krátce k bezpečnosti kontejnerů



Obrázek: https://xkcd.com/1988/

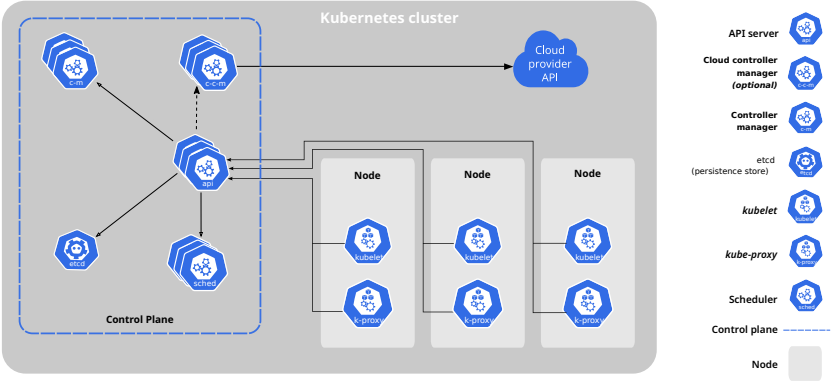
Krátce k bezpečnosti kontejnerů

- Praktické výhody
  - Lepší kontrola závislostí
  - Oddělení prostředí (namespaces)
  - **Automatizované nasazení**

Krátce k bezpečnosti kontejnerů

- Praktické výhody
  - Lepší kontrola závislostí
  - Oddělení prostředí (namespaces)
  - **Automatizované nasazení**
- Opatření pro zvýšení bezpečnosti
  - Omezení kernel capabilities
  - Uzavření do namespaces
  - Běh pod jiným uživatelem než rootem
  - UID/GID remapping

Orchestrace – Kubernetes



P. Valach,
Role orchestrace při správě systémů,
CESNET

Obrázek: https://kubernetes.io/docs/concepts/overview/components/

cesnet

Shrnutí

cesnet

To podstatné

1. Orchestrace umožňuje automatizaci, dokumentaci, kontrolu, a spolupráci
2. Minimalizuje chyby a vnitřní nekonzistence
3. Usnadňuje testování nové konfigurace
4. Umožňuje bezpečnou správu

Děkuji Vám za pozornost.

Dotazy?
Teď, nebo ~~nikdy~~ později na
pavel.valach@cesnet.cz