

Jak si ochočit Ansible

Tomáš Kukrál

klub tech@SU - Studentská unie ČVUT
SDN labs - ČVUT FEL

7.3.2015



Opakovat **jednoduché úkoly** dokáže i vycvičená **opice**, opici je třeba nejdříve **ochočit** a **vycvičit**.

Výhody

- žádné překlepy a chyby
- rychlejší správa
- opakování
- definované prostředí
- centralizovaná správa

Nevýhody

- lavinové chyby
- SSH přístup
- obtížně dohledatelné
- a skláři nebudou mít co jíst



ANSIBLE

Agenti

- přistupujeme přes SSH, takže není třeba instalovat žádné agenty
- (SSH klíče || hesla) && (root || sudo)

Agenti

- přistupujeme přes SSH, takže není třeba instalovat žádné agenty
- (SSH klíče || hesla) && (root || sudo)

Moduly

- apt, authorized_key, copy, synchronize, cron, docker, gem, pip, group, hostname, stat, sysctl, user, shell, git, template, *win_**
- 200 připravených modulů

Agenti

- přistupujeme přes SSH, takže není třeba instalovat žádné agenty
- (SSH klíče || hesla) && (root || sudo)

Moduly

- apt, authorized_key, copy, synchronize, cron, docker, gem, pip, group, hostname, stat, sysctl, user, shell, git, template, *win_**
- 200 připravených modulů

Akce

- spuštění příkazu na více strojích
- žádné další nástroje

Inventář

- seznam adres
- stroje, skupiny, proměnné
- dynamický inventář (JSON)

Inventář

- seznam adres
- stroje, skupiny, proměnné
- dynamický inventář (JSON)

Playbook

- skupina akcí/stavů
- využívají moduly
- YAML formát

Inventář

- seznam adres
- stroje, skupiny, proměnné
- dynamický inventář (JSON)

Playbook

- skupina akcí/stavů
- využívají moduly
- YAML formát

Role

- spojují dohromady playbooky a jejich nastavení
- přiřadíme inventáři role

Odpověď od všech strojů

```
ansible all -m ping
```

Příklady - příkazy

Odpověď od všech strojů

```
ansible all -m ping
```

Informace o strojích

```
ansible all -m setup
```

Příklady - příkazy

Odpověď od všech strojů

```
ansible all -m ping
```

Informace o strojích

```
ansible all -m setup
```

Spustit

```
ansible all -m shell -a "uptime"  
ansible all -m command -a "uptime"  
ansible all -a "uptime"
```

Příklady - příkazy

Odpověď od všech strojů

```
ansible all -m ping
```

Informace o strojích

```
ansible all -m setup
```

Spustit

```
ansible all -m shell -a "uptime"  
ansible all -m command -a "uptime"  
ansible all -a "uptime"
```

Zjistit eth0 MAC adresu

```
ansible all -m shell -a "ip a show eth0 | grep ether"
```

Instalujeme vim

```
ansible all -m apt -a "name=vim state=present"
```

```
name: install vim
```

```
apt: name=vim state=present
```

Instalujeme vim

```
ansible all -m apt -a "name=vim state=present"
```

```
name: install vim
```

```
apt: name=vim state=present
```

Instalujeme hromadně

```
name: install handy packages
```

```
apt: name={{item}} state=present
```

```
with_items:
```

- htop
- tmux
- nmap
- iptraf
- toilet

NTP server

```
apt: name=ntp state=present
copy: src=ntp.conf dest=/etc/ntp.conf owner=root mode=0644
service: name=ntp state=restarted enabled=yes
```

NTP server

```
apt: name=ntp state=present
copy: src=ntp.conf dest=/etc/ntp.conf owner=root mode=0644
service: name=ntp state=restarted enabled=yes
```

Nehashovat known_hosts

```
lineinfile: dest=/etc/ssh/ssh_config \
  regexp='^\s*HashKnownHosts' \
  line='HashKnownHosts no'
```

Příklady - nastavení

NTP server

```
apt: name=ntp state=present
copy: src=ntp.conf dest=/etc/ntp.conf owner=root mode=0644
service: name=ntp state=restarted enabled=yes
```

Nehashovat known_hosts

```
lineinfile: dest=/etc/ssh/ssh_config \
  regexp='^\s*HashKnownHosts' \
  line='HashKnownHosts no'
```

Nastavení hesla uživatele root

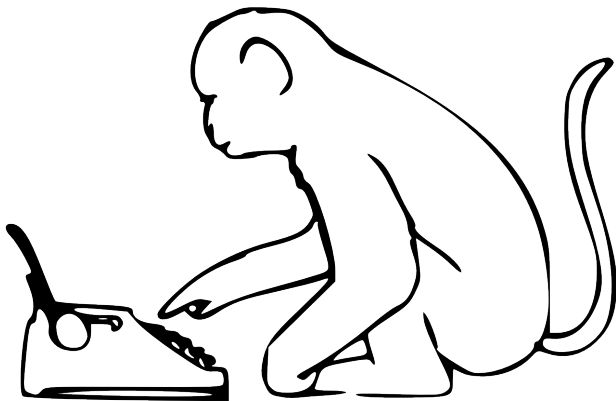
```
user: name=root groups=root state=present \
  password="nejaky hash hesla"
```

Best practises

- Neděláme výjimky
- Na servery nesaháme
- Dokumentujeme a komentujeme
- Tagujeme
- Verzujeme
- Píšeme KISS

Dejte si pozor

- Sdružování akcí a spuštění skriptu
- Jiné prostředí (PATH ...)
- Bezstavové spuštění (notify)
- Příliš specifická pravidla
- Změníme si heslo roota nebo smažeme klíč
- Omezení počtu SSH spojení



Děkuji za pozornost
jděte na workshop - **dnes 15:00**

http://docs.ansible.com/playbooks_best_practices.html