



# Introduction to Ansible

Martin Vicián • [martin.vician@nic.cz](mailto:martin.vician@nic.cz) • [/ptvician](https://twitter.com/ptvician) • [vician.cz](http://vician.cz)

OpenAlt Praha • 19. července 2018

# Motivace



# Pojmy

## Automatizace



## Orchestrace



# Orchestrace

## Cíl

- Konfigurace, správa a deploying všech serverů najednou
- IaaS (Infrastructure as a service)
- Propojení se službami poskytujícími "zdroje" (Amazon, OpenStack, DigitalOcean, ...)
- *A admini nebudou mít co žrát.*

## Řešení

- Puppet
- Chef
- CFEngine3
- SaltStack (OpenSuse)
- **Ansible** (RedHat)
- ...



# Ansible

- Open source v Pythonu.
- Komunikace probíhá přes SSH spojení: šifrované, "bezpečné", pomalé.
- Nepotřebuje nainstalovaného agenta:
  - *Puppet je výborný, ale stejně potřebujete Ansible, abyste jej jednoduše a najednou nainstalovali.* (Věroš Kaplan)
- Potřebuje Python3 (resp. Python2 pro některé moduly 😞)
- Popisujeme stav stroje - jak má vypadat.
- Idempotentní by design (stejná akce = stejný stav).
- Formáty/jazyky: ini, YaML, Jinja2.



# Instalace a konfigurace

Instalace:

- Ubuntu 18.04: 2.5.1
- pip3: 2.5.5

Cesta konfiguračního souboru (dle priority):

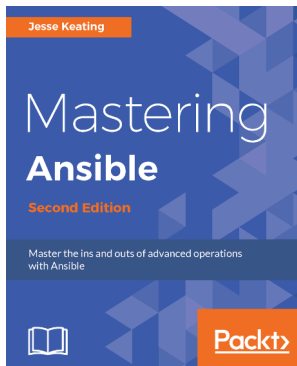
- \$ANSIBLE\_CFG
- ./ansible.cfg
- \$HOME/ansible.cfg
- /etc/ansible/ansible.cfg



# Příprava prostředí

## Zdroj inspirace

Jessee Keating:  
Mastering Ansible -  
Second edition



## Praktické příklady

<https://xmv.cz/ansible>

```
sudo apt install git python3-pip
sudo pip3 install ansible
git clone https://gitlab.labs.nic.cz/\
    mvician/ansible-introduction-examples
cd ansible-introduciton-examples
```

Soubory pro spuštění:

```
./??-run.sh
```

Slajdy: <https://www.vician.cz/pages/slides/>

# Inventory

- konfigurace: `inventory = hosts`
- přepínače: `-i/--inventory INVENTORY_PATH`
- typické cesty:
  - soubor: `hosts`
  - složka: `inventory/*`
- seznam strojů spravovaných Ansiblem
- `ini` formát
- proměnné určující spojení (konvence) - např.:
  - `ansible_connection: local, smart, ssh, paramiko, docker`
  - `ansible_user`
  - `ansible_port`
  - ...
- sdružení strojů do skupin

```
ansible localhost -m ping
```





# Proměnné v inventory

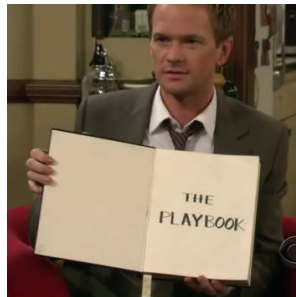
```
muj-pocitac ansible_connection=local
server.example.com ansible_port=9022
turris.example.com ansible_user=root
tajnyserver.tajnadomena.tld ansible_host=1.1.1.1
muj-arch-desktop ansible_python_interpreter=/usr/bin/python2
desktop-doma.example.com ansible_ssh_common_args=' \
-o ProxyCommand="ssh -W %h:%p -q root@turris.example.com"'
```

[https://docs.ansible.com/ansible/latest/intro\\_inventory.html#list-of-behavioral-inventory-parameters](https://docs.ansible.com/ansible/latest/intro_inventory.html#list-of-behavioral-inventory-parameters)



# Playbook

- složka: playbooks (konvence)
- seznam stavů/úkolů
- omezuje se množina serverů z inventory
- lineární procházení úkolů
- standardně se vykonává úkol po úkolu na daných strojích
- yaml - všude stejný počet mezer/tabulátorů



Spuštění:

```
ansible-playbook -i 02-hosts playbooks/02-hello-word.yml
```



# Struktura playbooku

playbooks/03-playbook.yml:

```
- hosts: all
  tasks:
    - debug:
      msg: Hello world!
    - debug:
      msg: And again!
```

Spuštění:

```
ansible-playbook -i 03-hosts playbooks/03-playbook.yml
```

nebo: ./03-run.sh



# Skupiny strojů

## Hosts

```
ginny  
[twins]  
fred  
george  
  
[prefects]  
bill  
charlie  
percy  
ron
```

## Playbook

```
- hosts: twins  
  tasks:  
    - debug:  
      msg: "Weasleys' Wizard Wheezes!!!"  
- hosts: prefects  
  tasks:  
    - debug:  
      msg: Am I also head-boy?
```

```
ansible-playbook -i 04-hosts playbooks/04-playbook-limit.yml
```



# Limit strojů

```
- hosts: all:!percy
  tasks:
    - debug:
      msg: "Where is Percy?"
- hosts: twins
  tasks:
    - debug:
      msg: "Oh, are you a prefect, Percy?"
- hosts: percy
  tasks:
    - debug:
      msg: "Oh, shut up! "
```

```
ansible-playbook -i 05-hosts playbooks/05-playbook-more.yml
```



# Runtime limit

## Playbook

```
- hosts: all
  tasks:
    - debug:
        msg: "I'm Fred or George?"
```

## Hosts

```
fred
george

[all:vars]
ansible_connection=...
```

```
ansible-playbook -i 06-hosts playbooks/06-limit.yml \
  --limit twins
```



# Hierarchy skupin

```
[weasly]
ginny

[twins]
fred
george

[prefects]
bill
charlie
percy
ron

[weasly:children]
twins
prefects
```

## Playbook

```
- hosts: weasly
  tasks:
    - debug:
        msg: "We are ..."
```

## Run

```
ansible-playbooks \
-i 07-hosts \
playbooks/07-groups.yml
```



# Hiearchie skupin - znázornění

```
[all]
+ -- [weasly]
    + -- ginny
    + -- [twins]
        + -- fred
        + -- george
    + -- [prefects]
        + -- percy
        + -- ron
        + -- [finishedschoolbeforefirstbook]
            + -- bill
            + -- charlie

[ungrouped]
+ -- harry
+ -- hermione
```





# Výstupy

```
- hosts: localhost
  tasks:
    - shell: date
      register: currenttime
    - debug:
      msg: "Current time is: {{ currenttime.stdout }}"
```

```
ansible-playbook -i 08-hosts playbooks/08-stdout.yml
```



# Výstupy

```
ok: [localhost] => {
  "msg": {
    "changed": true,
    "cmd": "date",
    "delta": "0:00:00.001941",
    "end": "2018-06-27 12:57:20.775504",
    "failed": false,
    "rc": 0,
    "start": "2018-06-27 12:57:20.773563",
    "stderr": "",
    "stderr_lines": [],
    "stdout": "St čen 27 12:57:20 CEST 2018",
    "stdout_lines": [
      "St čen 27 12:57:20 CEST 2018"
    ]
  }
}
```



# Změny

```
- hosts: localhost
  tasks:
    - debug:
      msg: "No change"
      register: gringotts
    - debug:
      msg: "Was changed"
      when: gringotts | changed
    - debug:
      msg: "Success"
      when: gringotts | success
```

```
ok: [localhost] => {
  "gringotts": {
    "changed": false,
    "failed": false,
    "msg": "No change"
  }
}
```

```
ansible-playbook -i 09-hosts playbooks/09-changed.yml
```



# Návratový kód

```
- hosts: kingscross
  tasks:
    - command: sl
      register: hogwartsexpress
    - debug:
      msg: "Hogwarts Express isn't installed!"
      when: hogwartsexpress.rc == 2
```

```
ansible-playbook -i 10-hosts playbooks/10-return.yml
```



# Návratový kód

[https://docs.ansible.com/ansible/latest/user\\_guide/playbooks\\_error\\_handling.html](https://docs.ansible.com/ansible/latest/user_guide/playbooks_error_handling.html)

```
- hosts: kingscross
  tasks:
    - command: sl
      register: hogwartsexpress
      failed_when: hogwartsexpress.rc == 2
```



# Root? No, thank you!

Přihlašujeme se pomocí SSH klíčů.

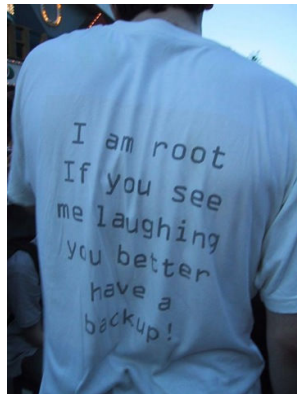
## Hosts

```
localhost ansible_user=lab
```

## Playbook

```
- hosts: localhost  
  tasks:  
    - shell: whoami
```

```
ansible-playbook -i 11-hosts playbooks/11-sudo.yml \  
  --become --ask-become-pass
```



# He-who-must-not-be-named

```
- hosts: ron
  tasks:
    - name: Rat name
      debug:
        msg: "My rat is called Scabbers."
    - name: Mirror of Erised
      debug:
        msg: "I would like to win Quidditch World Cup."
```

```
ansible-playbook -i 12-hosts playbooks/12-names.yml
```



# Inventory

```
./inventory/gryffindor
  johnson
  wood
  [harrysyear]
  weasley
  granger
./inventory/hufflepuff
  diggory
  [harrysyear]
  macmillan
```

```
./inventory/ravenclaw
  lovegood
  [harrysyear]
  patil
./inventory/slytherin
  flint
  [harrysyear]
  malfoy
  crabbe
  goyle
```

```
ansible-playbook -i 13-inventory playbooks/13-inventory.yml
```





# Inventory

Ansible "jen" sloučí všechny soubory v adresáři

```
ansible-playbook -i 13-inventory playbooks/13-inventory.yml \  
-l gryffindor
```

```
- hosts: gryffindor  
  tasks: ...
```

Obojí selže, ale 13-inventory/all funguje:

```
[all:vars]  
ansible_connection=local
```



# Roles

- slučujeme úkoly do logických celků
- sdílíme role (`roles_path = \`  
`roles:shared`)

```
./  
./ansible.cfg  
./hosts  
./playbooks/hello.yml  
./roles/hello/tasks/main.yml  
./roles/myrole/tasks/main.yml  
./shared/users/tasks/main.yml  
./shared/sshd/tasks/main.yml
```

tasks/main.yml:

```
- name: first  
  debug:  
    msg: Hello World!
```

playbooks/hello.yml:

```
- hosts: localhost  
  roles:  
    - hello  
    - users
```

```
ansible-playbook -i 15-hosts playbooks/15-roles.yml
```



# Variables

- V inventory ansible\_port, ...
- group\_vars
- host\_vars
- v rolích
  - vychozí
  - vynucné
- dočasné v úkolech
- v playboocích



```
ansible-playbook -i 16-hosts playbooks/16-variables.yml
```

# Variables - hierarchy

[https://docs.ansible.com/ansible/latest/user\\_guide/playbooks\\_variables.html#variable-precedence-where-should-i-put-a-variable](https://docs.ansible.com/ansible/latest/user_guide/playbooks_variables.html#variable-precedence-where-should-i-put-a-variable)

- Proměnná musí být definovaná!

```
when: variable is not defined
msg: "{{ variable | default('zapomnel jsem definovat') }}"
```

```
ansible-playbook -i 17-hosts playbooks/17-variables.yml
```

- typicky:
  - proměnné do rolí role/myrole/defaults/main.yml
  - změny v host\_vars a group\_vars



# TOP Modules

[https://docs.ansible.com/ansible/latest/modules/modules\\_by\\_category.html](https://docs.ansible.com/ansible/latest/modules/modules_by_category.html)

- ping
- apt, yum, apt\_key, apt\_repo, ...
- pip
- systemd
- sysctl
- user
- git
- copy
- template
- uri



# Files

[https://docs.ansible.com/ansible/latest/modules/copy\\_module.html](https://docs.ansible.com/ansible/latest/modules/copy_module.html)

```
roles/gryffindor/tasks/main.yml  
roles/gryffindor/files/fat-lady-password.txt
```

```
- copy:  
  src: fat-lady-password.txt  
  dest: /etc/gryffindor-door/fat-lady-password.txt  
  owner: percy  
  group: percy  
  mode: 0644
```



# Templates

- [https://docs.ansible.com/ansible/latest/modules/template\\_module.html](https://docs.ansible.com/ansible/latest/modules/template_module.html)
- [https://docs.ansible.com/ansible/latest/user\\_guide/playbooks\\_templating.html](https://docs.ansible.com/ansible/latest/user_guide/playbooks_templating.html)

```
roles/teachers/tasks/main.yml  
roles/teachers/templates/.jinja2
```

```
- copy:  
  src: herbology.jinja2  
  dest: /etc/herbology.txt  
  owner: dumbledore  
  group: dumbledore  
  mode: 0644
```

```
Teacher: {{ teacher }}  
{% for item in ... %}  
- {{ item }}  
{% endfor %}
```

```
ansible-playbook -i 19-hosts playbooks/19-templates.yml
```



# Loops

[https://docs.ansible.com/ansible/latest/user\\_guide/playbooks\\_loops.html](https://docs.ansible.com/ansible/latest/user_guide/playbooks_loops.html)

```
- debug:
  msg: "I'm {{ item }} Weasley."
  with_items: [ Fred, George ]
- debug:
  msg: "I'm {{ item }} Weasley."
  with_items:
    - Fred
    - George
- debug:
  msg: "I'm {{ item }} Weasley."
  with_items: "{{ twins_names }}"
```

```
ansible-playbook -i 20-hosts playbooks/20-loops.yml
```





# Handlers

[https://docs.ansible.com/ansible/latest/user\\_guide/playbooks\\_intro.html#handlers-running-operations-on-change](https://docs.ansible.com/ansible/latest/user_guide/playbooks_intro.html#handlers-running-operations-on-change)

```
roles/gryffindor/tasks/main.yml  
roles/gryffindor/handlers/main.yml
```

```
- copy:  
  dest: /etc/gryffindor-door/fat-lady-password.txt  
  content: "{{ password }}"  
  notify: fatlady reload
```

- notify jen při změně

```
ansible-playbook -i 21-hosts playbooks/21-handlers.yml
```



# Tasks include

```
roles/users/tasks/main.yml
roles/users/tasks/user.yml
```

main.yml:

```
- name: Process each user
  include: user.yml
  with_items: "{{ users }}"
```

user.yml:

```
- user:
  name: "{{ item }}"
```



# Tagy

[https://docs.ansible.com/ansible/latest/user\\_guide/playbooks\\_tags.html](https://docs.ansible.com/ansible/latest/user_guide/playbooks_tags.html)

- tagovat lze:
  - task v roli
  - roli v playbooku

```
- hosts: all
  roles:
    - {role: users, tags: users}
    - {role: sshd, tags: sshd}
```

```
ansible-playbook example.yml --tags "users,sshd"
```



# Konvence

- nepoužívat roli common (není jasné, co dělá)
- závislosti řešit na úrovni playbooku a ne v rolích
- jeden playbook pro jednu činnost
- citlivá data dohromady separátně
- v playbooks žádné tasks
- každá role má README.md
- proměnné jsou v defaults
- playbooky neobsahují duplikátní role
- proměnné obalené mezerami: {{ promenna }}
- proměnné s prefixem názvu role



# Syntaxe

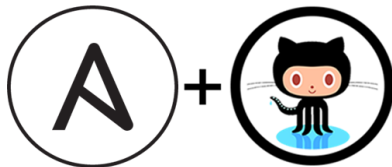
```
- apt: name=sudo state=present  
=>  
- apt:  
  name: sudo  
  state: present
```

state: latest nebo stable zajistí aktualizaci  
(i nežádoucí)



# Git, git, git

- verzování
- merge requesty
- podepisování commitů, tagů, ...
- deploy jenom z master
- CI pro kontrolu konvencí



# Sdílime role!

- ansible-galaxy: <https://galaxy.ansible.com/>  
(spíš inspirace, pozor na bezpečnost)
- git submoduly s tagovanými čísly verzí



ansible.cfg:

```
roles_path = roles:companyroles:galaxy-roles
```

# Vícenasobná hierarchie skupin

```
[weasley]  
ginny
```

```
[twins]  
fred  
george
```

```
[prefects]  
bill  
charlie  
percy  
ron
```

```
[weasley:children]  
twins  
prefects
```

```
[finishedschoolbeforefirstbook]  
bill  
charlie  
lupin
```

```
[hogwartsteacher]  
lupin  
dumbledore
```

```
[werewolf]  
lupin
```

- proměnné dle pohledu skupiny





# SSH Proxy

```
[servers]
```

```
...  
...
```

```
[behind_proxy]  
omina.example.com
```

```
[behind_proxy:vars]  
ansible_ssh_common_args='-o ProxyCommand=\n    "ssh -W %h:%p -q root@nat.example.com"'
```



# Ansible vault

ansible.cfg:

```
vault_password_file = vault.sh
```

```
#!/bin/sh  
DN="$(dirname "$0")"  
gpg2 --batch --use-agent --decrypt "$DN"/pass.gpg \  
2> /dev/null
```

```
ansible-vault [create|edit||view] file
```

- group\_vars/all/secure.yml
- host\_vars/harry/diary.yml



# Become

```
- hosts: localhost
  tasks:
    - name: gitlab projects
      git:
        repo: "ssh://git@gitlab.com/project"
        dest: "/home/{{ ansible_env['USER'] }}/project"
        become: no
```

```
ansible-playbook playbooks/gitproject.yml --become \
  --ask-become-pass
```



# Delegate

```
- include: 'lxchost.yml'  
  delegate_to: '{{ run_on }}'
```

- aplikováno na celé `lxchost.yml`
- `run_on` musí být v `inventory`
- použití: virtualizace, kontejnerizace



# Ansible Tower

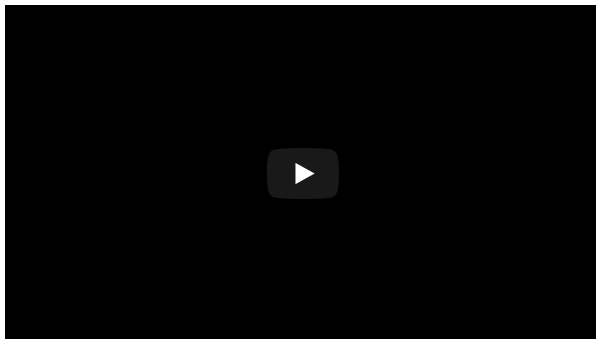
## Pozitiva:

- webové GUI pro ansible
- snadné spouštění na velkém množství severů
- intuitivní přehled stavů

## Negativa:

- ansible na serveru pro automatické spouštění
- ansible-vault

<https://youtu.be/ToXoDdUOzj8>



Otázky?

