



Know your tools: Ansible

Dariusz Puchalak



Dariusz Puchalak

- 25 lat Linux/Unix Sysadmin
- 15 lat trener
- 8 lat w OSEC
- 8 lat z Ansible

<http://www.osec.pl>

- Od 2009 na rynku
- doświadczona kadra (ACNI, RHCA)
- specjalizacja open-source
- subskrypcje, szkolenia, wdrożenia, konsultacje

Ansible Galaxy

<https://galaxy.ansible.com/> - biblioteka zawartości Ansiblowej

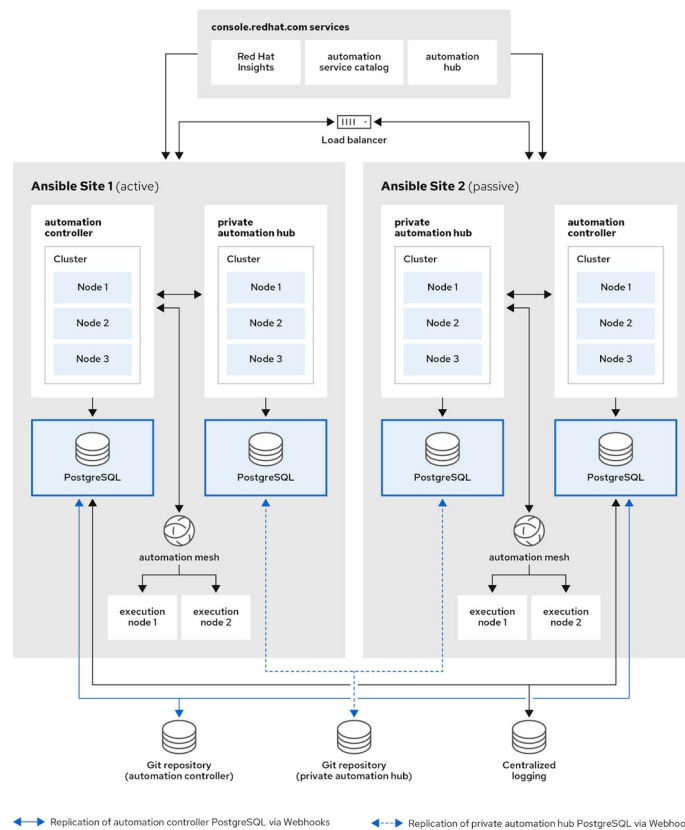
Collections

- <https://docs.debops.org/en/stable-3.0/ansible/role-index.html>
- <https://linux-system-roles.github.io/>
- <https://docs.ansible.com/ansible/latest/collections/index.html>

RH AAP

- Automation Controller
- Automation Hub
- Execution Node

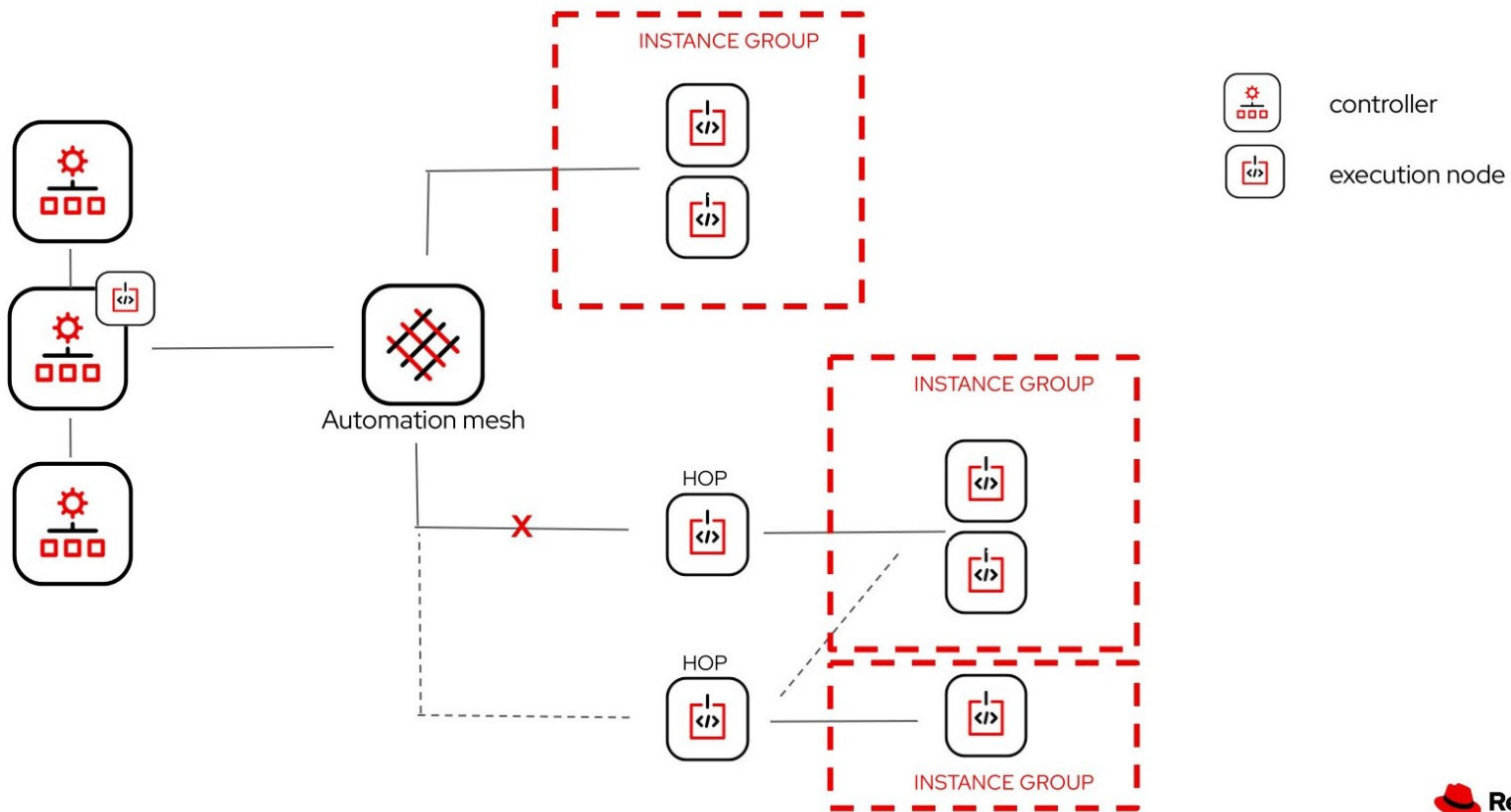
Red Hat Ansible Automation Platform



© 2019 Red Hat, Inc.

RH AAP

- Mesh
- Nodes:
 - Hybrid
 - Control
 - Execution
 - Hop



Wyszukanie roli.

```
$ ansible-galaxy role search ovirt
```

```
Found 59 roles matching your search:
```

Name	Description
----	-----
Akrog.storage	Storage management and consumption
...	
ovirt.cluster-upgrade	Role to upgrade all host in oVirt/RHV cluster.
ovirt.disaster-recovery	Disaster recovery for oVirt engine
ovirt.dpdk-setup	Setup DPDK compatible NIC's to use DPDK via Open vSwitch.
ovirt.dump_db	Role to get oVirt DB dumps

Instalacja roli.

\$ ansible-galaxy role install ovirt.disaster-recovery

Starting galaxy role install process

- downloading role 'disaster-recovery', owned by ovirt
- downloading role from <https://github.com/oVirt/ovirt-ansible-disaster-recovery/archive/1.3.0.tar.gz>
- extracting ovirt.disaster-recovery to
/home/puchalakd/.ansible/roles/ovirt.disaster-recovery
- ovirt.disaster-recovery (1.3.0) was installed successfully

Bezpieczna instalacja roli

- <https://galaxy.ansible.com/docs/using/installing.html>

Instalacja kolekcji.

```
$ ansible-galaxy collection install ovirt.ovirt
```

```
Starting galaxy collection install process
```

```
Process install dependency map
```

```
Starting collection install process
```

```
Downloading https://galaxy.ansible.com/download/ovirt-ovirt-2.4.0.tar.gz to  
/home/puchalakd/.ansible/tmp/ansible-local-288982prh914v/tmpno3g3g50/ovirt-ovirt-  
2.4.0-icdyc3_w
```

```
Installing 'ovirt.ovirt:2.4.0' to  
'/home/puchalakd/.ansible/collections/ansible_collections/ovirt/ovirt'
```

```
ovirt.ovirt:2.4.0 was installed successfully
```

Bezpieczna instalacja kolekcji.

- https://docs.ansible.com/ansible/latest/user_guide/collections_using.html

Kolekcje/role – dobre praktyki.

Jesteśmy coraz częściej odbiorcami ról/kolekcji Ansible dlatego powinniśmy pamiętać o weryfikacji kodu który używamy.

- `$ ansible-galaxy install -r requirements.yml`
 - version: ...
- `$ ansible-galaxy collection install -r requirements.yml`
 - version: ...
 - signatures:
- `$ ansible-galaxy collection verify -r requirements.yml`

Downloading <https://galaxy.ansible.com/download/ovirt-ovirt-2.4.0.tar.gz> to
/home/puchalakd/.ansible/tmp/ansible-local-293493b9ymf8k/tmpoxyoucsu/ovirt-ovirt-2.4.0-mr4t9e8o

Verifying 'ovirt.ovirt:2.4.0'.

Installed collection found at '/home/puchalakd/.ansible/collections/ansible_collections/ovirt/ovirt'

MANIFEST.json hash: 888d961cdadef854e1d51aeb66c85e3dc87a5ca6bd117bb05585ed061b68d785

Successfully verified that checksums for 'ovirt.ovirt:2.4.0' match the remote collection.



Ansible-doc i pluginy

Różne pluginy

DEMO


```

---
- hosts: windows
  gather_facts: yes

  tasks:
  - debug:
      msg: "Reboot following {{ inventory_hostname }} Windows systems."
      when: ansible_reboot_pending

- hosts: windows
  gather_facts: yes
  serial:
    - 1
    - 3
    - 5%
  max_fail_percentage: 10

  vars_prompt:
  - name: temp
    prompt: Press Enter to reboot selected Windows systems!!!
    default: 'Enter'
    private: no

  tasks:

```

```

- name: Only when reboot needed
  block:
  - name: Schedule downtime in nagios
    nagios:
      action: downtime
      minutes: 10
      service: host
      host: '{{ inventory_hostname }}'
      comment: "Reboot scheduled"
      delegate_to: "{{ check_mk_server }}"

  - win_reboot:

  - name: wait for host/hosts to start up
    wait_for_connection:
      timeout: 600

  - name: start Windows time service
    win_service:
      name: W32Time
      start_mode: auto
      state: started

  - name: Delete downtime from nagios
    nagios:
      action: delete_downtime
      service: host
      host: '{{ inventory_hostname }}'
  ## comment is essential
      comment: "Reboot scheduled"
      delegate_to: "{{ check_mk_server }}"
      tags: test

  when: ansible_reboot_pending

```

Rolling upgrades

- https://docs.ansible.com/ansible/latest/user_guide/guide_rolling_upgrade.html

serial vs throttle

DEMO

serial.yml, throttle.yml



Filtry i testy

ansible.builtin.get_url:

„If `dest` is a directory, the file will always be downloaded (regardless of the `force` and `checksum` option), but replaced only if the contents changed.”

```
- name: Download isos
  get_url:
    url: "{{ item }}"
    dest: /var/lib/libvirt/images/{{ item | basename }}
    tmp_dest: /var/lib/libvirt/images/
  loop:
    - https://cdimage.debian.org/debian-cd/current/amd64/iso-dvd/debian-10.9.0-amd64-DVD-1.iso
    - https://dotsrc.dl.osdn.net/osdn/clonezilla/74519/clonezilla-live-2.7.1-22-amd64.iso
    - https://dl.fedoraproject.org/pub/fedora/linux/releases/33/Workstation/x86_64/iso/Fedora-Workstation-Live-x86_64-33-1.2.iso
    - http://ftp.icm.edu.pl/pub/Linux/distributions/centos/8.3.2011/isos/x86_64/CentOS-8.3.2011-x86_64-dvd1.iso
    - http://download.opensuse.org/distribution/leap/15.2/iso/openSUSE-Leap-15.2-DVD-x86_64.iso
```

```
# SSH access for admins
SSH/ACCEPT:$LOG      any:{{ admin_ips | join(",") }}  fw
# SSH access for monitoring
SSH/ACCEPT:$LOG      any:{{ check_mk_servers | join(",") }}  fw
# Proxy for apt-get/yum to access repositories
ACCEPT:debug  fw      any:{{ proxy_repo | urlsplit('hostname') }}      tcp      {{ proxy_repo | urlsplit('port') }}
# Syslog remote
ACCEPT:debug  fw      any:{{ rsyslog_server }}      tcp      514
# system mails
ACCEPT:debug  fw      any:{{ mail_relay }}      tcp      25
# NTP
ACCEPT:debug  fw      any:{{ ntp_servers | join(",") }}  udp      ntp
```

1,1

All



```
- name: Create remote users for share Umowy
win_user:
  account_disabled: no
  account_locked: no
  name: "{{item.name}}"
  fullname: "{{item.fullname if item.fullname is defined else ''}}"
  description: "{{item.description if item.description is defined else ''}}"
  groups: "{{item.groups | join(',') }}"
  password: "{{item.password if item.password is defined else default_password}}"
  groups_action: add
  password_expired: no # Don't require user to change password on first login
  password_never_expires: yes
  state: present
  update_password: on_create # If it exists do not update password
  user_cannot_change_password: yes
with_items: "{{ users }}"
tags: [users, config, windows]
-- INSERT --
```

Filtry i testy

- https://docs.ansible.com/ansible/latest/user_guide/playbooks_filters.html
- https://docs.ansible.com/ansible/latest/user_guide/playbooks_filters_ipaddr.html
- https://docs.ansible.com/ansible/latest/user_guide/playbooks_tests.html



DEMO

gather_email_logs.yml, request_redhat_pdfs.yml

A decorative header at the top of the slide featuring a light gray background with a network of thin gray lines. Various white icons are placed along these lines, including an envelope, a camera, a cloud, a musical note, a gear, a smartphone, a thumbs up, and a star.

DEMO

async.yml

Vaults

- `ansible-vault`
- `ansible-doc -l | grep vault`
- `ansible-doc -t lookup -l | grep -i vault`
- `no_log: true`
- https://docs.ansible.com/ansible/latest/reference_appendices/faq.html#how-do-i-keep-secret-data-in-my-playbook
- https://docs.ansible.com/ansible/latest/user_guide/vault.html

Dynamiczne dodanie nowego hosta do playbooka.

```
- name: playbook
  gather_facts: no
  hosts: localhost
  # become: true

  vars_prompt:
  - name: target
    prompt: "Put servername"
    private: no

  tasks:
  - add_host:
    hostname: "{{ target }}"
    group: test
    ansible_host: "{{ target }}"
    ansible_port: 22

- name: playbook
  gather_facts: yes
  hosts: test

  tasks:
  - debug:
    msg: "Hostname: {{ ansible_hostname }}"

~
~
~
```

1,1 All



Pytania?
Dariusz.Puchalak@osec.pl



Dziękuję.

Przykłady: <https://dariusz.puchalak.net./Ansible/>