

Ansible – przydatne narzędzia (mniej znane).

Dariusz Puchalak

20 czerwca 2023

- ▶ 25+ lat Linux/Unix Sysadmin
- ▶ 15+ lat trener
- ▶ 9+ lat w OSEC
- ▶ 9+ lat z Ansiblem

<http://www.OSEC.pl>

- ▶ Od 2009 na rynku
- ▶ doświadczona kadra (ACNI, RHCA)Używane przede wszystkim do porównań.
- ▶ specjalizacja open-source
- ▶ subskrypcje, szkolenia, konsultacje

Ścieżka edukacyjna Ansible.

- ▶ Lista aktualnych kursów, egzaminów:
<https://osec.pl/red-hat-ansible-automation/>
- ▶ RH294 - RHCE - Podstawowy kurs Ansible
- ▶ DO417 - Ansible dla inżynierów Windows (alternatywa dla RH294)
- ▶ DO457 - Ansible dla inżynierów sieciowych (alternatywa dla RH294)
- ▶ RH358 - „Dawne RH300 @RHEL7”, czyli usługi Linuksowe ręcznie i Ansiblem
- ▶ DO374 - „Dawne Advanced Ansible”, czyli zaawansowane elementy Ansible (kontynuacja RH294)
- ▶ DO467 - „Dawny Tower”, czyli jak używać Ansible Automation Platform

Spis treści.

Wbudowana dokumentacja.

Narzędzie które warto znać.

Best Practices.

Pytania?

ansible-doc -t become

- ▶ `ansible.builtin.su`
- ▶ `ansible.builtin.sudo`
- ▶ `ansible.builtin.runas`
- ▶ `containers.podman.podman_unshare`

ansible-doc -t cache

- ▶ `community.general.memcached`
- ▶ `community.general.redis`
- ▶ `community.mongodb.mongodb`

ansible-doc -t callback

- ▶ `ansible.builtin.oneline`
- ▶ `ansible.posix.timer`
- ▶ `community.general.jabber`
- ▶ `community.general.selective`
- ▶ `community.general.syslog_json`
- ▶ demo - `OSEC_Forum_2023/Watermaker/`

ansible-doc -t callback

- ▶ `ansible.posix.profile_roles`
- ▶ `ansible.posix.profile_tasks`
- ▶ `ansible.posix.cgroup_perf_recap`

ansible-doc -t connection

- ▶ `ansible.builtin.local`
- ▶ `ansible.builtin.ssh`
- ▶ `community.docker.docker`
- ▶ `community.docker.docker_api`
- ▶ `kubernetes.core.kubectl`
- ▶ `community.okd.oc`

ansible-doc -t inventory

- ▶ `amazon.aws.aws_ec2`
- ▶ `ansible.builtin.script`
- ▶ `azure.azcollection.azure_rm`
- ▶ `community.general.nmap`
- ▶ `community.vmware.vmware_host_inventory`
- ▶ `community.okd.openshift`
- ▶ `kubernetes.core.k8s`
- ▶ `microsoft.ad ldap`
- ▶ `ovirt.ovirt.ovirt`

ansible-doc -t lookup

- ▶ DEMA na kolejnej prezentacji o godz. 13:30

ansible-doc -t module

- ▶ Znane i lubiane.

ansible-doc -t strategy

► `ansible.builtin.free`

- ▶ DEMA na kolejnej prezentacji o godz. 13:30

ansible-doc -t keyword

- ▶ DEMO - ansible-doc -t keyword -l
- ▶ DEMO - throttle.yml

ansible-config

- ▶ ANSIBLE_RETRY_FILES_ENABLED
- ▶ DEMO - serial.yml

- ▶ Interaktywna zabawa „ad-hoc” Ansible

ansible-pull

- ▶ pobiera sobie playbooka z gita i uruchamia lokalnie
- ▶ --only-if-changed - tylko gdy playbook został uaktualniony

- ▶ Część RH AAP
- ▶ można używać standalone (bez RH AAP)
- ▶ daje TUI do pracy z Ansiblem (uruchamianie)
- ▶ daje nam dodatkową „interaktywność” w przeglądaniu co wyników działania playbooksa
- ▶ dodaje kolejną warstwę abstrakcji w postaci kontenera do uruchamiania playbooków (overkill)?

ansible-navigator - execution environment

- ▶ Kontenery do uruchamiania Ansible nie są przerostem formy nad treścią, bo można z nich nie korzystać (`--execution-environment false`)
- ▶ Kontenery do uruchamiania Ansible są genialne bo:
 - ▶ skończy się przy uruchamianiu playbook'ów „Dziwne, u mnie działa?”
 - ▶ można zrobić kapsułę czasowa na konkretną wersję Ansible, Pythona, bibliotek Pythonowych, innego oprogramowania - do utrzymania ciągłości automatyzacji systemów które „wypadną ze wsparcia” nowszych wersji

- ▶ Rozwiązanie do modyfikacji i tworzenia własnych kontenerów dla ansible-navigатора.

- ▶ Wskazywanie niedociągnięć naszego kody Ansiblowego
- ▶ DEMO - znęcanie się nad
Watermaker/request_redhat_pdfs.yml
- ▶ # noqa: rule

- ▶ Wspiera proces testowania naszych playbooków/ról/kolekcji.

- ▶ Pozwala uruchamiać akcje (jak playbook, moduł), wygenerować zdarzenie, czy ustawić zmienną w reakcji na określone zdarzenia/zdarzenia.
- ▶ Zdarzeniem może być min.:
 - ▶ url_check
 - ▶ watchdog
 - ▶ webhook
 - ▶ inne jak alertmanager, azure_service_bus, kafka
- ▶ Zmiana modelu PUSH na model event-driven

ansible-aisnippet

- ▶ Pozwala wygenerować kod Anisbleowy z wykorzystaniem OpenAI
- ▶ DEMO - `ansible-aisnippet generate -f test.yml -p`

Najlepsze praktyki.

- ▶ Prostota (na ile się da).
- ▶ Ponownie wykorzystuj te same zmienne.
- ▶ Przewiduj, że będziesz rozbudowywał kod i go zmieniał.
- ▶ Zastosuj filozofię Uniksa
https://en.wikipedia.org/wiki/Unix_philosophy
- ▶ `https://redhat-cop.github.io/automation-good-practices/`

- ▶ Używać. :)
- ▶ Rola powinna robić tylko jedną rzecz (z punktu widzenia funkcjonalności)
- ▶ Jeśli rola jest zrobiona pod różne technologie - to podzielić taski na mniejsze pliki i włączać przez `import_tasks/include_tasks`
- ▶ Uwaga na nazwy zmiennych (i ich konflikt z innym kodem przy użyciu `--extra-vars`)
 - ▶ nazwy zmiennych poprzedzać nazwą roli
 - ▶ nazwy wew. poprzedzać dodatkowo dwoma podkreślnikami `__`

- ▶ Testować z `check_mode`
- ▶ Rola uruchomiona po raz drugi nie powinna nic zmieniać (ani raportować zmian).
- ▶ Różnice między dystrybucjami/systemami chować w zmiennych (przykład - `vars_inclusions.yml`)
- ▶ Warto używać zależności ról i/lub `include_role/import_role`
- ▶ Kolekcje powinny zbierać content na poziomie strukturalnym.
- ▶ Używać tagów - bardzo przydatne przy testowaniu, czy wprowadzaniu niewielkich zmian.

Quotes

- ▶ W większości przypadków Ansible zdejmie znaki cytatu przy użyciu.
- ▶ Jeśli chcemy ich użyć należy zastosować filtr `| quote`
- ▶ Ale nie zawsze są automatycznie zdejmowane `8]` - patrz przykład `Folded_Block_Scalar_test.yml`

Python potrafi skorzystać z proxy http/https

```
environment:
```

```
  https_proxy: http://localhost:5001
```

- ▶ OpenSSH potrafi forwardować porty:
 - ▶ RemoteForward 127.0.0.1:5001 127.0.0.1:5001
- ▶ DEMO: environment.yml

Przykłady

- ▶ ssh-config-files.yml
- ▶ Zigbee2MQTT.yml
- ▶ urlsplit.yml
- ▶ combine_demo/combine.yml
- ▶ looping_over_packages.yml

Pytania?

Dariusz.Puchalak@osec.pl

Przykłady

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

Dziękuję.

Ansible – przydatne (a mniej
znane) narzędzia

OSEC
FORUM 2023

