

Bezpieczeństwo czy automatyzacja?

Red Hat Ansible Automation Platform (AAP) czyli złoty środek
między bezpieczeństwem a automatyzacją!

Dariusz Puchalak

21 marca 2023

Spis treści.

- 1 Wprowadzenie do automatyzacji z Ansible.
- 2 Bezpieczeństwo a automatyzacja.
- 3 Nadzór nad automatyzacją.

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, konsultacje

Ansible, Red Hat Ansible Tower, Red Hat Ansible Automation Platform

- Narzędzia do automatyzacji wszystkiego.
- Ansible - techniczna część automatyzacji
- Red Hat Ansible Tower - zarządzanie automatyzacją
- Red Hat Ansible Automation Platform - zarządzanie zarządzaniem automatyzacją 8]

Ansible

- Małe wymagania - Python 3.x (PowerShell - do Windowsów)
- natywny protokół do komunikacji z zarządzanymi systemami (SSH, WINRM, ...)
- bez agentowy
- wielosystemowy
- bardzo prosty w użyciu i zrozumieniu
- potężne możliwości
- automatyzacja praktycznie wszystkiego (Linux/Unix/MainFrame/urz. sieciowe/Cloudy/...)

Ansible

Minimalne elementy Ansible:

- `ansible.cfg` - konfiguracja
- inventory - lista automatyzowanych systemów
- playbook - kod automatyzacji

playbook

Ansible playbook - zdefiniowanie w formacie YAML oczekiwanego stanu systemów wraz z podaniem kroków jakie należy wykonać aby ten stan osiągnąć.

Role.

Role - zebranie razem tego co nam potrzebne aby z mniejszych klocków stworzyć większy klocek, który można następnie wielokrotnie wykorzystać w innych miejscach.

Ansible galaxy - <https://galaxy.ansible.com/> - biblioteka publicznych ról (i nie tylko).

Kolekcje.

Ansible Collection - jeszcze większe „klocki” do budowy automatyzacji.

- plugins
- roles
- modules
- playbooks

<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>

Instalowanie Ansible.

ansible-core + FQCN vs ansible

Zaufane kolekcje.

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

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

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:

Zaufane kolekcje.

```
$ 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:

```
888d961cdadef854e1d51aeb66c85e3dc87a5ca6bd117bb05585ed061b68d78
```

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

Ansible Tower.

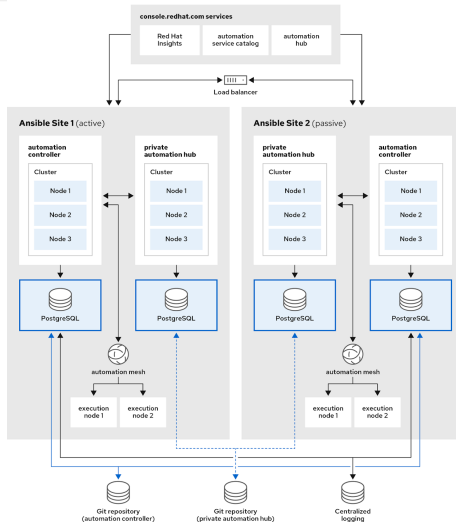
Ansible Tower - narzędzie do zarządzania automatyzacją (część RH AAP):

- kto
- czym
- co
- jak
- rozliczalność

Red Hat Ansible Automation Platform.

- Automation Controller
- Automation Hub
- Execution Node

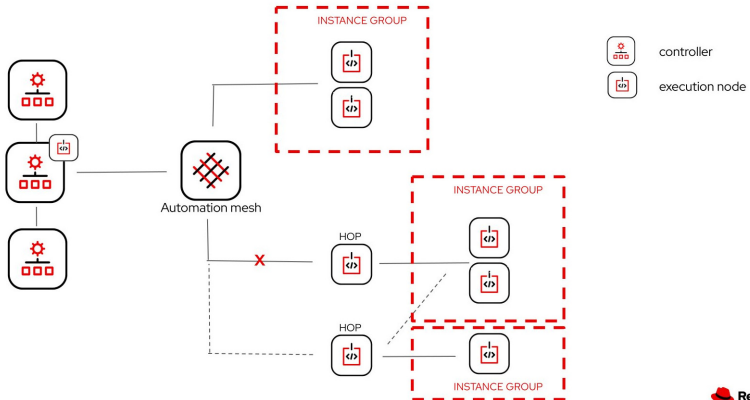
Architektura RH AAP.



Replication of automation controller PostgreSQL via Webhooks

Replication of private automation hub PostgreSQL via Webhooks

Architektura RH AAP.



Obniżyć bezpieczeństwo aby zyskać bezpieczeństwo.

- Automatyzacja „nie lubi się” z interakcją.
- Jeśli odpuścimy „interakcję bezpieczeństwa” zyskujemy lepsze i szybciej wprowadzane zmiany.

ansible-vault

Ansible vault - rozwiązanie pozwalające zaszyfrować prawie wszystko co jest używane przez Ansible:

- zmienne/pliki ze zmiennymi (np. klucze API, dane dostępowe)
- pliki z danymi wrażliwymi (np. klucze prywatne certyfikatów)
- nawet playbooki

Vaults.

- `azure.azcollection.azure_keyvault_secret` - returns the content of secret saved in Azure Key Vault.
- `community.hashi_vault.vault_kv1_get` - Gets a secret from HashiCorp Vault's KV version 1 secret store
- `ansible-doc -t lookup -l | grep -i vault`
- `ansible-doc -l | grep -i vault`

Dynamic inventory.

W Ansible można łączyć wiele różnych inventory:

- statyczne
- dynamiczne (tworzone poprzez uruchomienie skryptu/programu odwołującego się do zew. „bazy prawdy”)

Pluginy. typu inventory.

- amazon.aws.aws_ec2
- azure.azcollection.azure_rm
- google.cloud.gcp_compute
- hetzner.hcloud.hcloud
- community.general.nmap
- community.kubernetes.openshift
- infoblox.nios_modules.nios_inventory
- netbox.netbox.nb_inventory
- ansible-doc -t inventory -l

Ansible Execution Environment

Rozwiązanie do uruchamiania playbooków Ansiblowych wew. kontenera w celu:

- standaryzacji środowiska uruchomieniowego
- „kapsuła czasowa” dot. naszego contentu Ansible do zarządzania naszymi systemami

Automation Controller.

Ansible controller - zarządzania automatyzacją na poziomie menadżerskim („nietechniczna” część automatyzacji):

- izolacja zadań
- model RBAC
- bezpieczne przechowywanie „credentials”
- „system auditor”
- podsystem audytu i logowania (pełna rozliczalność)
- konsola webowa
- RESTfull API
- schedulowanie zadań

Automation Controller - credentials.

- Możliwość zaimportowania do kontrolera danych dostępowych.
- używa wew. ansible-vault
- Użytkownicy Controllera mogą tylko skorzystać z danych dostępowych - nie mogą ich poznać.

Możliwości.

Możliwości jakie daje nam RH AAP:

- automatyczne weryfikowanie polityki bezp. na wszystkich wykrytych systemach
- automatyczne generowanie raportów odnośnie wszystkich posiadanych zasobach do których ma dostęp Ansible
- automatyczne (lub pół automatyczne) uaktualnienia konfiguracji systemów IT do aktualnej polityki bezpieczeństwa
- bardzo łatwe wykorzystywanie „zbudowanych” klocków do automatyzacji przez ludzi „mniej technicznych”

Własna biblioteka zawartości Ansiblowej mogącej składać się z:

- publicznych kolekcji
- certyfikowanych kolekcji
- własnych kolekcji
- zweryfikowanych „trzecich” kolekcji

RH AAP - gdzie zmierza?

Red Hat Ansible Automation Platform - wybrane z release notes.

- RH AAP 2.2:
 - Digitally signed Red Hat Ansible Certified Content Collections on Ansible automation hub.
 - Digitally sign your user-built, community, or third-party Ansible Content Collections on private automation hub.
- RH AAP 2.3:
 - Project signature verification in automation controller.
 - Sign and validate Ansible content via a WebUI.
 - Introducing Ansible validated content.

Pytania?

Dariusz.Puchalak@osec.pl

Dziękuję.

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