**LAB 11**

Ansible Vault

Zawartość dokumentu:

[**Wstęp**](#_vehizxwv9xfe) **1**

[**Plan ćwiczenia**](#_6m59hr95si7n) **1**

## Wstęp

W tym ćwiczeniu zapoznamy się narzędziem Ansible-Vault, pozwalającym na bezpieczne przechowywanie poufnych treści w zaszyfrowanej formie razem z innymi plikami. Pozwala to przykładowo na umieszczenie ich w dostępnym repozytorium. Jednocześnie vault jest natywny dla Ansible i nie przeszkadza w jego wykonaniu.

## Plan ćwiczenia

1. Włączamy nasz ulubiony terminal (Windows: Putty; Ubuntu: Terminal; macOS: Mac Terminal)
2. Logujemy się do serwera zarządzającego mgmt.muszynski.pro
   * ssh ansible.sysopspolska.pl -l <id\_uzytkownika>
3. Znajdujemy się w katalogu domowym  
   nasz\_uzytkownik@mgmt-server:/home/nasz\_uzytkownik$
4. Przechodzimy do katalogu szkolenie
   * cd akademiaansible
5. Ładujemy środowisko (można dodać do np do .bashrc)
   * source environment.sh  
     Oczekiwany rezultat:
   * **(venv)** nasz\_uzytkownik@mgmt-server:~/akademiaansible$
6. Przeanalizuj pliki i role
   * zauważ że w pliku playbooks/init\_mgmt.yml ‘includowany’ jest między innymi plik *vars/szkolenie\_vault.yml*
   * spróbuj poznac jego zawartość (*playbooks/vars/szkolenie\_vault.yml*)
7. Zapoznaj się z <http://docs.ansible.com/ansible/playbooks_vault.html>
8. Jak można zauważyć w includowanym pliku *szkolenie\_vault.yml* znajdują się treści poufne, które mogą być odczytane jedynie przy użyciu komendy ansible-vault, lub po całkowitym odszyfrowaniu pliku.
9. Wykonajmy (celem poznania zawartości pliku)
   * (venv)$ ansible-vault view playbooks/vars/szkolenie\_vault.yml

Dobra praktyka:  
W szablonach używajmy ‘jawnej’ zmiennej w formie odszyfrowanej. Zmienną tą przypiszmy do kolejnej ‘zmiennej tajnej’ ukrytej w zaszyfrowanym pliku valut.  
  
Na przykład, w pliku *szkolenie.yml* umieszczany zmienną   
nasze\_haslo: “{{ nasze\_haslo\_vault }}”   
a następnie w pliku *szkolenie\_vault.yml* definiujemy   
nasze\_haslo\_vault: ‘tojesthaslo’  
  
Plik *szkolenie\_vault.yml* będzie zaszyfrowany i nieczytelny bez posiadania hasła, jednocześnie, dzięki takiemu zabiegowi, zmienna *nasze\_haslo* będzie możliwa do odszukania w katalogu przy pomocy zwykłych narzędzi (np. grep -R -e nasze\_haslo playbooks/).  
  
edycja pliku vault:

(venv)$ ansible-vault edit playbooks/vars/szkolenie\_vault.yml

Przeglądanie różnic w zaszyfrowanych plikach za pomocą ‘git driver’

Zapoznaj sie z plikiem   
~/akademiaansible/.gitattributes

git config --global diff.ansible-vault.textconv "ansible-vault view"

<https://stackoverflow.com/questions/29937195/how-to-diff-ansible-vault-changes>