



Ansible by Red Hat - święty graal automatyzacji?

Dariusz Puchalak



Dariusz Puchalak

- 20+ lat Linux/Unix Sysadmin
- 9+ lat trener
- 2+ lat w OSEC

<http://www.OSEC.pl>

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



Ansible

Małe wymagania.

- Python 2.x (ale niedługo 3.x)
- SSH
- Brak agentów.

Komunikacja - SSH

- Tak samo jak administrator (od strony sieciowej nic się nie zmienia!)
- Natywny bardzo mocny mechanizm (OpenSSH)
- Bezagentowy.

Uwierzytelnianie == OpenSSH

- password,
- hostbased,
- publickey,
- Keyboard-interactive
- PAM
- keyboard-interactive:pam

Uwierzytelnianie == OpenSSH

- password,
- hostbased,
- publickey,
- Keyboard-interactive
- PAM
- keyboard-interactive:pam

OpenSSH patterns

Host *.puchalak.???

IdentityFile ~/.ssh/id_puchalak

IdentitiesOnly yes

PreferredAuthentications publickey,password

Ansible patterns

```
~(web|db).*\.example\.com  
webservers[0:1]
```


Połączenie przez komputer pośredni

```
.ssh/config
```

```
...
```

```
Host hostB
```

```
    ProxyCommand ssh hostA nc %h %p
```

```
    HostName 10.1.8.31
```

```
Host hostA
```

```
    HostName 172.16.48.10
```

```
...
```

```
bash$ ssh hostB
```



Łączymy to co znamy.

Nowa jakość

Host unison

User puchalakd

Match Host unison exec "host -t A unison.net.puchalak"

HostName unison.net.puchalak

Host unison

HostName 192.168.1.125

ProxyCommand ssh pluton-remote nc %h %p

Nowa jakość

```
* * * * * flock -w 0 -n /root/.call.back ssh -i /root/.call.back  
-o BatchMode=yes -o ExitOnForwardFailure=yes -o  
StrictHostKeyChecking=no -R 12345:localhost:22  
puchalakd@somewhere.internet || exit 0
```

Host private.behind.nat

HostName 127.0.0.1

Port 12345

ProxyCommand ssh pluton-remote nc %h %p



Reusing Control Connection



Tylko jedno połączenie

Host *

ControlMaster auto

ControlPath ~/.ssh/ControlPath/%C

ControlPersist yes

Podnoszenie uprawnień.

become_method:

- sudo
- su
- pbrun
- pfexec
- doas
- dzdo
- ksu





Windows

Windows

winrm

Windows - winrm

Ustawić zmienne:

ansible_hosts: windows

ansible_user: Administrator

ansible_password: Pa\$\$w0rd

ansible_port: 5986

ansible_connection: winrm

when using default WinRM self-signed certificates:

ansible_winrm_server_cert_validation: ignore

Windows – przykład playbooka

```
---
#Based on:
# - https://baracoma.wordpress.com/2012/03/16/setting-windows-update-proxy-server-settings/
# - https://support.microsoft.com/en-us/kb/3084568

- name: Set registry to download updates but not install
  win_regedit:
    key: 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update'
    value: AUOptions
    data: 3
    datatype: dword
    state: present
  tags: [windows, windows_updates]

- name: Check if we have proxy defined
  raw: netsh winhttp show proxy
  register: windows_update_proxy_setting
  tags: [windows, windows_updates]
  changed_when: false

- name: Reset Windows Update Proxy
  raw: netsh winhttp reset proxy
  when: "'{{windows_updates_proxy}}' not in windows_update_proxy_setting.stdout"
  tags: [windows, windows_updates]

- name: Set new Windows Update Proxy
  raw: netsh winhttp set proxy {{windows_updates_proxy}}
  when: "'{{windows_updates_proxy}}' not in windows_update_proxy_setting.stdout"
  tags: [windows, windows_updates]
```




roles - check_mk

