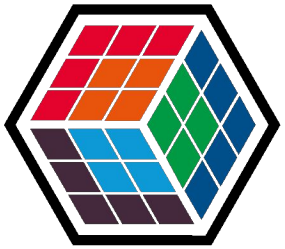
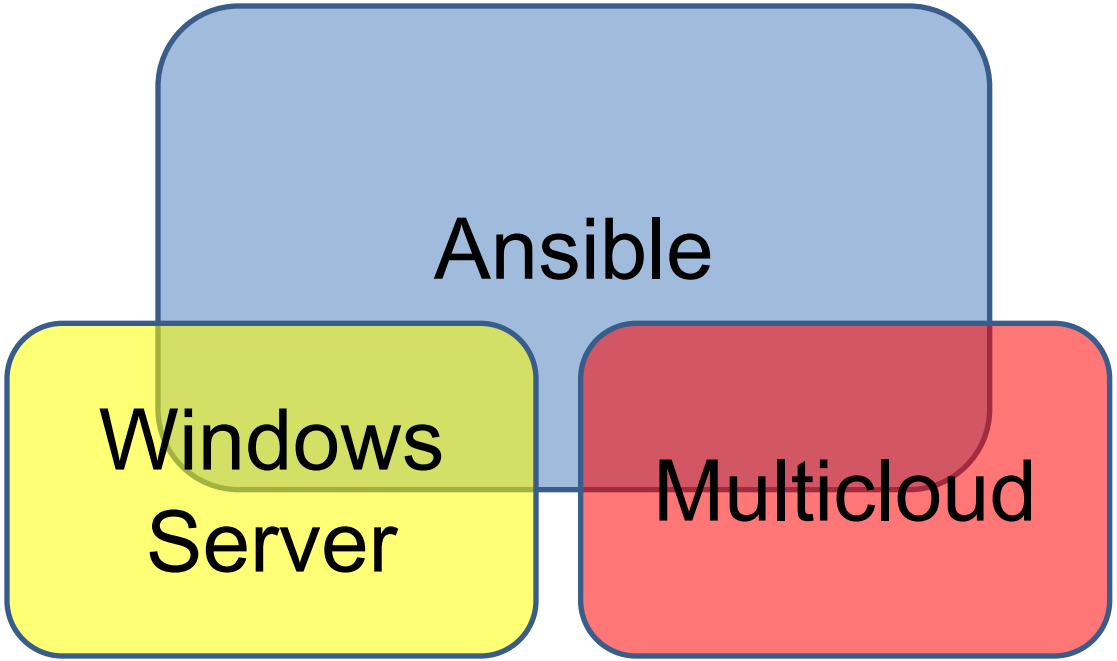


THE DEVELOPER'S CONFERENCE

Como o Ansible está ajudando a Nelogica A expandir um ambiente Multicloud Microsoft?

Pablo Soares
Analista de Infraestrutura e Redes


Ansible
Windows Server
Multicloud

Agenda

THE DEVELOPER'S CONFERENCE

- Introdução ao Ansible
- Entendendo o cenário
- Provisionando VMs
  - Criando os recursos
  - Configurando os novos hosts
- Ansible X AD GPOs?
- Dúvidas

Introdução ao Ansible

- Tecnologia *open source* para provisionamento e e gerenciamento de configuração.
- Versão inicial em 2012, comprada pela Red Hat em 2015.
- Utiliza SSH ou WinRM para gerenciar servidores e demais dispositivos.

Introdução ao Ansible

- Ou seja, é ***agentless***, sem necessidade de softwares instalados nos *hosts*.
- **Idempotente**
- Linguagem **declarativa**

Inventário

THE DEVELOPER'S CONFERENCE

- Descreve os hosts que podem ser acessados.
- Possibilita a organização de hosts em grupos.
- Sintaxe em diversos formatos como YAML e INI.

Exemplo

THE DEVELOPER'S CONFERENCE

```
mail.example.com

[webservers]
foo.example.com http_port=80
bar.example.com http_port=8080

[dbservers]
one.example.com
two.example.com
```

Exemplo

THE DEVELOPER'S CONFERENCE

```
mailserver

[webservers]
fooapp    # host_vars/fooapp.yml
barapp

[dbservers]
db1
db2
```

Playbooks

- Arquivos YAML simples que descrevem o estado desejado dos seus sistemas.
- Fáceis de escrever e manter.

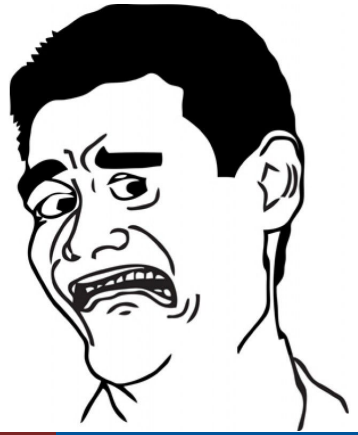
Exemplo

THE DEVELOPER'S CONFERENCE

```
- hosts: webservers
  gather_facts: no
  tasks:
    - name: Ensure user bob is absent
      win_user:
       name: bob
       state: absent
```

Não é SSH!

- WinRM (protocolo de shell remoto baseado em HTTP)
- sudo pip install pywinrm requests-credssp
- Microsoft OpenSSH?



Powershell

THE DEVELOPER'S CONFERENCE

- Já presente nas versões modernas de Windows
- Podemos usar .NET
- Powershell 3+ / Windows 7/2008+
- DSC via win_dsc

Cenário

- Fintech
- Necessidade de alta disponibilidade e baixa latência (=> estar perto da B3 em SP!)
- Regulamentos da B3 preveem ressarcimentos se clientes forem prejudicados

Cenário

THE DEVELOPER'S CONFERENCE

- Crescimento de 100% ao ano
- 80% do market share
- Projetos internacionais em andamento

Cenário

THE DEVELOPER'S CONFERENCE

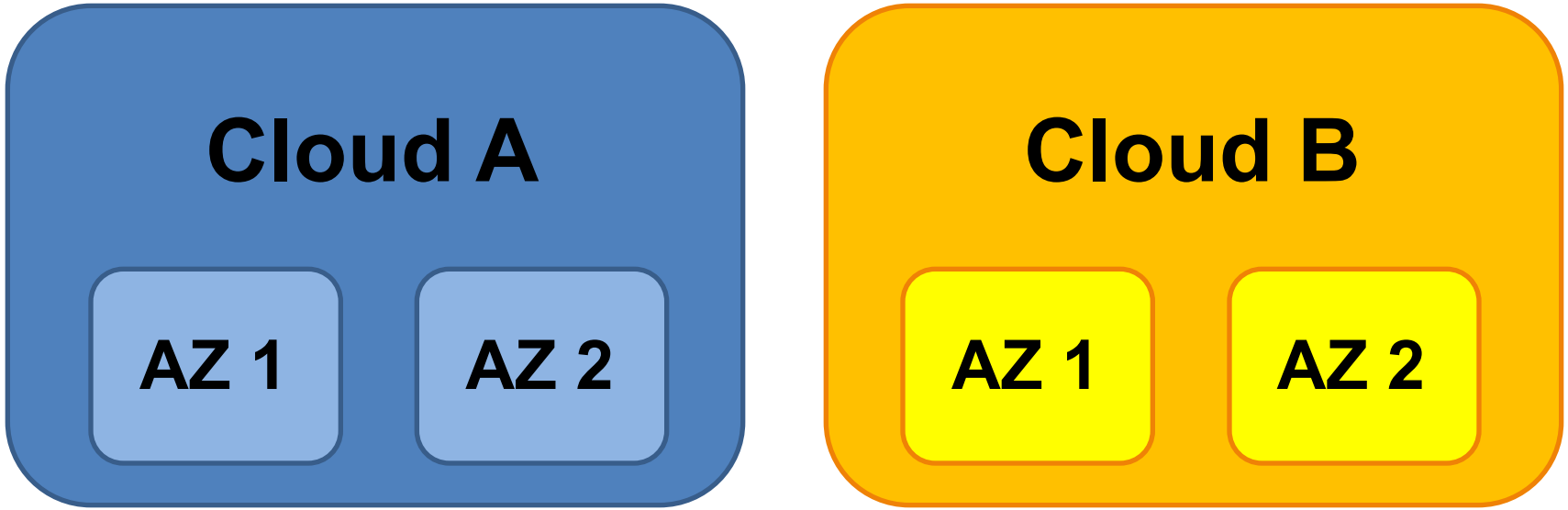
- P: Por que Windows?
- R: É o SO que suporta a stack da empresa. ☺

Cenário

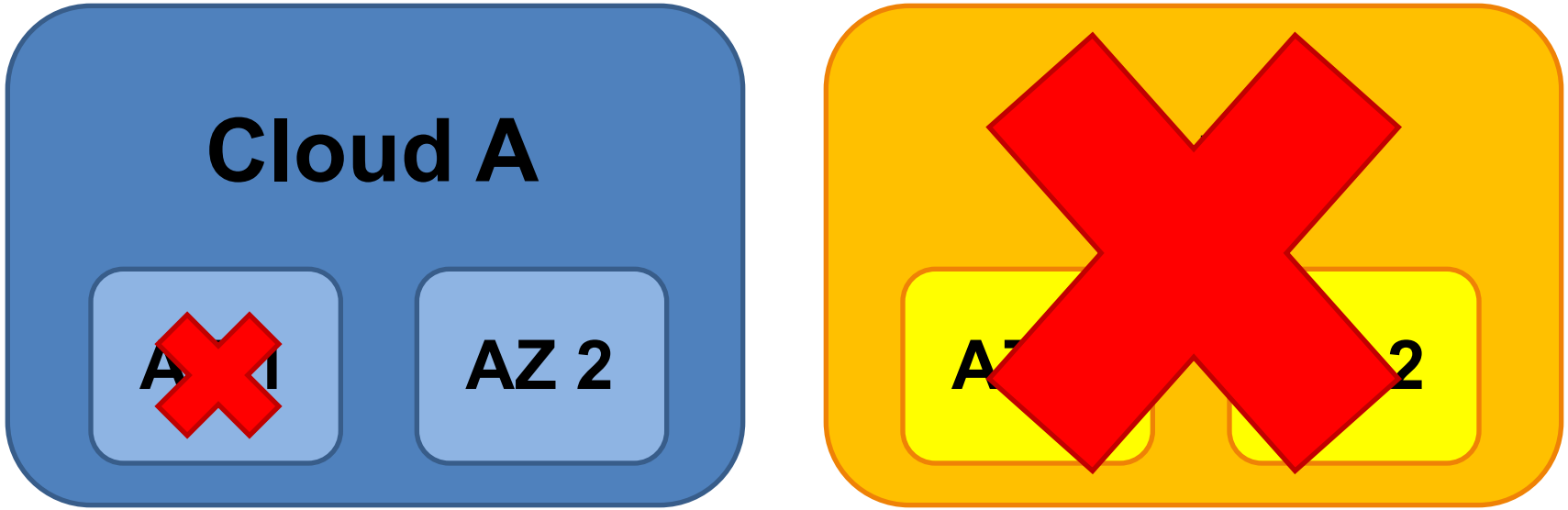
THE DEVELOPER'S CONFERENCE

- P: Por que Multicloud?
- R: Política de evitar vendor lock-in
- R: Quanto mais POPs, menor o impacto da queda de um POP

Cenário



Cenário



Problemas

THE DEVELOPER'S CONFERENCE

- Portais diferentes
- APIs diferentes
- Fluxo de ações equivalentes diferentes
- Processo extremamente manual


THIS IS FINE.

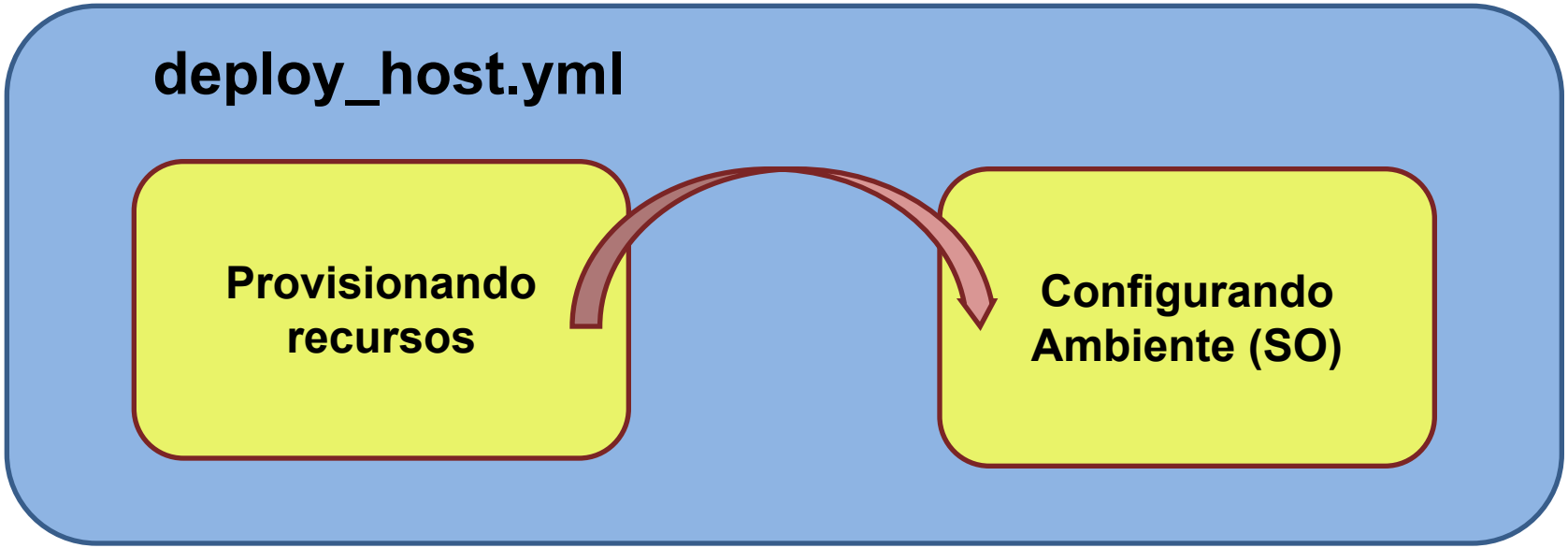

THIS IS
NOT
FINE!!

Cenário

THE DEVELOPER'S CONFERENCE

- P: Por que Ansible?
- R: Ferramenta madura com suporte a uma gama enorme de sistemas (SOs, devices...).
- R: Fácil deploy (agentless).
- IaC => Versionável (ex: GIT)

Provisionando VMs



```
[aws_webservers]
webapp1
webapp2

[azure_webservers]
webapp3

[gcp_webservers]
webapp4
```

THE DEVELOPER'S CONFERENCE

```
[webservers:children]
aws_webservers
azure_webservers
gcp_webservers

[aws:children]
aws_webservers

[azure:children]
azure_webservers

[gcp:children]
gcp_webservers
```

THE DEVELOPER'S CONFERENCE

```
hosts
host_vars/
    webapp1.yml
    ...
group_vars/
    aws.yml
    azure.yml
    gcp.yml
    webservers.yml
    aws_webservers.yml
    ...
```

THE DEVELOPER'S CONFERENCE

```
- hosts: "{{ target }}"
  connection: local
  gather_facts: no
  roles:
  - { role: aws_vm,
    when: inventory_hostname in group.aws }
  - { role: azure_vm,
    when: inventory_hostname in group.azure }
  - { role: gcp_vm,
    when: inventory_hostname in group.gcp }
```

THE DEVELOPER'S CONFERENCE

Modules & tips

THE DEVELOPER'S CONFERENCE

- AWS: ec2*
- Azure: azure_rm_*
- GCP: gcp_compute_*

```
- name: Wait 600s to WinRM be available
  wait_for_connection:
```

- azure_dns
- aws_dns
- host_file
- rdp_file
- zabbix
- netbox
- intra

THE DEVELOPER'S CONFERENCE

THE DEVELOPER'S CONFERENCE

- azure_dns
- aws_dns
- host_file
- rdp_file
- zabbix
- netbox
- intra

- azure_dns
- aws_dns
- host_file
- rdp_file
- zabbix
- netbox
- intra

THE DEVELOPER'S CONFERENCE

“Probleminhas”

- API da Azure lenta
- Autenticação API da Azure possui problemas com alguns caracteres (senha gerada pela Azure)
- GCP via Ansible não permite mudar SGs das VMs

THE DEVELOPER'S CONFERENCE

```
- hosts: "{{ target }}"
  gather_facts: no
  roles:
  - common
  - domain_computer
  - win_ntp
  - win_disk
  - { role: win_hyperv,
      when: inventory_hostname in groups.srv }
  - win_iis
```

Configurando conectividade

THE DEVELOPER'S CONFERENCE

```
ansible_connection: winrm
ansible_winrm_transport: credssp
ansible_port: 5986
ansible_winrm_server_cert_validation: ignore
ansible_user: "{{ ansible_user }}"
ansible_pass: "{{ ansible_pwd }}"
```

Configurando conectividade

THE DEVELOPER'S CONFERENCE

```
ansible_become_user: "{{ admin }}"
ansible_become_pass: "{{ admin_pwd }}"
ansible_become_method: runas
```

Instalando features

THE DEVELOPER'S CONFERENCE

```
- name: Install SNMP service
  win_feature:
    name: SNMP-Service
    include_management_tools: yes
    state: present
```

Setando timezone

THE DEVELOPER'S CONFERENCE

```
- name: Set timezone to GMT-3
  win_timezone:
    timezone: "{{ common_tz }}"
  become: yes
  become_user: "{{ admin }}"
```

Alterando nomes e rebootando

THE DEVELOPER'S CONFERENCE

```
- name: Change hostname
  win_hostname:
    name: "{{ hostname }}"
  register: res

- name: Reboot
  win_reboot:
  when: res.reboot_required
```

Ingressando no domínio

THE DEVELOPER'S CONFERENCE

```
- win_domain_membership:
    dns_domain_name: "{{ domain_name }}"
    hostname: "{{ hostname }}"
    domain_admin_user: "{{ da_user }}"
    domain_admin_password: "{{ da_pwd }}"
    state: domain
  register: domain_state
```

Configurando serviços

THE DEVELOPER'S CONFERENCE

```
- name: Configure NTP service
  win_service:
    name: ntp
    start_mode: auto
    state: restarted
    username: "{{ win_ntp_user }}"
    password:
```

Rodando scripts

THE DEVELOPER'S CONFERENCE

```
- name: Add network static routes
  win_shell: |
    route -p add "{{ item.net_ip }}" \
    mask "{{ item.mask }}" \
    "{{ item.gateway_ip }}"
  loop: "{{ net_routes }}"
```

“Probleminhas”

THE DEVELOPER’S CONFERENCE

- WinRM falha aleatoriamente
- Frequentemente o módulo win_shell é necessário
- Powershell gera processamento demasiado

Comando

THE DEVELOPER'S CONFERENCE

```
ansible-playbook deploy_host.yml \
  -i hosts --ask-vault-pass \
  --extra-vars "target=<target>"
```

Comando

THE DEVELOPER'S CONFERENCE

```
ansible-playbook deploy_host.yml \
  -i hosts --ask-vault-pass \
  --extra-vars "target=<target>"
```

```
./deploy_host.sh -t <target>
```

THE DEVELOPER'S CONFERENCE

```
[aws_webservers]
webapp1
webapp2

[azure_webservers]
webapp3

[gcp_webservers]
webapp4
webapp5
```

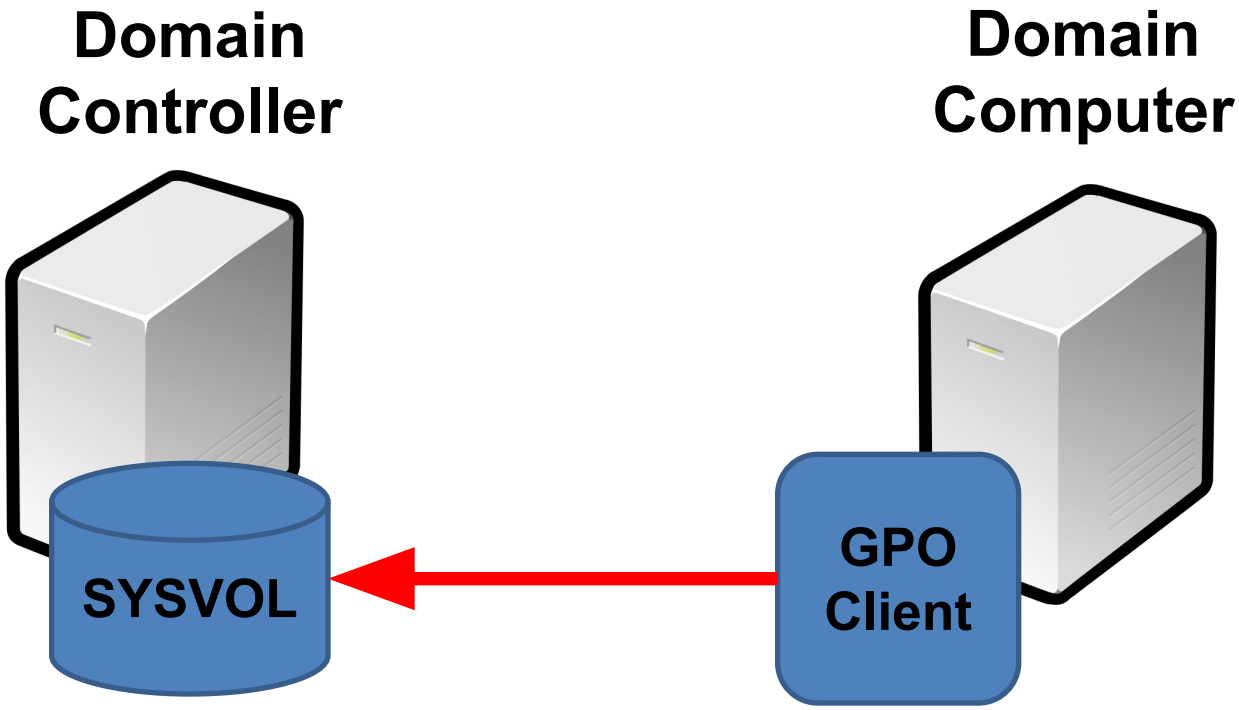
Comando

THE DEVELOPER'S CONFERENCE

```
./deploy_host.sh -t webapp5
```

THE DEVELOPER'S CONFERENCE

Ansible ou AD GPOs?


Domain Controller
Domain Computer
SYSVOL
GPO Client

Possibilidades com GPOs

THE DEVELOPER'S CONFERENCE

- Regras de FW
- Permissões sobre registros
- Permissões sobre sistema de arquivos
- Diversos direitos como: poder desligar, logar como serviço, aumentar prioridade de processos...
- Controlar acesso aos servidores
- Etc...

Conclusões

THE DEVELOPER'S CONFERENCE

- Enorme redução do tempo de operações de infra

  => De dias para minutos
- Melhor gerenciamento de diferenças entre plataformas de cloud
- Redução de erros nas entregas para corrigir posteriormente
- **+ tempo para inovação ;)**

THE DEVELOPER'S CONFERENCE

www.nelogica.com.br

Carreiras: **jobs.kenoby.com/nelogica**

linkedin.com/**company/nelogica**

rh@nelogica.com.br

Dúvidas? ☺