# Sessão 6: Gestão de configuração

## 1) Instalação do Ansible

Clonar template para `ansible`, 10.0.42.5/24. Renomear e integrar no LDAP/SSH-ca como de costume. Criar entradas no DNS direto/reverso para `ansible.intnet`.

Como `root@ldap`, crie um usuário para o Ansible, membro dos grupos `setup` e `fwadm`:

```
# ldapadduser ansible setup
# ldapaddusertogroup ansible setup
# ldapaddusertogroup ansible fwadm
```

Como `root@nfs`, permita ao usuário `ansible` executar quaisquer comandos como `root` sem digitar senha:

```
# grep ansible /config/sudoers
ansible   ALL=(ALL:ALL)    NOPASSWD: ALL
```

Como `root@ansible`, instale o Ansible no servidor:

```
# echo "deb http://ppa.launchpad.net/ansible/ansible/ubuntu trusty main" >
/etc/apt/sources.list.d/ansible.list
# apt-get install dirmngr
# apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 93C4A3FD7BB9C367
# apt-get update
# apt-get install ansible
```

## 2) Execução de comandos simples

Como `ansible@ansible`, assine um par de chaves para logar nos servidores integrados no sistema LDAP/SSH-CA:

```
$ bash scripts/sshsign_user.sh
(sshca@10.0.42.2) Enter passphrase:
# 10.0.42.2:22 SSH-2.0-OpenSSH_7.4p1 Debian-10+deb9u4

(CA private key) Enter passphrase: seg10_user_ca
Signed user key id_rsa-cert.pub: id "ansible" serial 0 for ansible valid from 2018-11-
06T13:25:23 to 2021-11-05T12:30:23
```

Crie um diretório `~/ansible`, e um arquivo de hosts identificando as máquinas a gerenciar.

```
$ mkdir ~/ansible
$ cd ~/ansible
```

```
$ nano ~/ansible/hosts
(...)
```

```
$ cat ~/ansible/hosts
[srv]
fw
ldap
nfs
log
ansible
```

Execute um comando simples em todas as máquinas gerenciadas pelo Ansible.

```
$ ansible -i ~/ansible/hosts srv -b --become-user=root -m shell -a 'hostname ; whoami'
ansible | CHANGED | rc=0 >>
ansible
root

fw | CHANGED | rc=0 >>
fw
root

ldap | CHANGED | rc=0 >>
ldap
root

nfs | CHANGED | rc=0 >>
nfs
root

log | CHANGED | rc=0 >>
log
root
```

# 3) Uso de roles no Ansible

Vamos usar roles (papéis) no Ansible para configurar o sudo de forma local, mais segura. Crie o diretório `~/ansible/roles`, e inicialize o papel `sudoers`:

```
$ mkdir ~/ansible/roles
$ cd ~/ansible/roles/
```

```
$ ansible-galaxy init sudoers
- sudoers was created successfully
```

```
$ ls -R sudoers/
sudoers/:
defaults  files  handlers  meta  README.md  tasks  templates  tests  vars

sudoers/defaults:
main.yml

sudoers/files:

sudoers/handlers:
main.yml

sudoers/meta:
main.yml

sudoers/tasks:
main.yml

sudoers/templates:

sudoers/tests:
inventory  test.yml

sudoers/vars:
main.yml
```

Copie o arquivo `sudoers` do NFS para a pasta `files`:

```
$ cp /config/sudoers ~/ansible/roles/sudoers/files/
```

Observe as permissões do arquivo `sudoers` original. Com isso em mente, edite o arquivo `~/ansible/roles/sudoers/tasks/main.yml` como se segue:

```
$ ls -ld /etc/sudoers.old
-r--r----- 1 root root 669 jun  5  2017 /etc/sudoers.old
```

```
$ cat ~/ansible/roles/sudoers/tasks/main.yml
---
- name: Propagate sudoers configuration
  become: yes
  become_user: root
  copy:
    src: sudoers
    dest: /etc
    owner: root
    group: root
    mode: 0440
```

Crie o arquivo `~/ansible/srv.yml` para amarrar os hosts à nova role.

```
$ cat ~/ansible/srv.yml
---
- hosts: srv
  roles:
    - sudoers
```

Execute a role.

```
$ ansible-playbook -i ~/ansible/hosts ~/ansible/srv.yml

PLAY [srv] *********************************************************************

TASK [Gathering Facts] *********************************************************
ok: [nfs]
ok: [ldap]
ok: [fw]
ok: [ansible]
ok: [log]

TASK [sudoers : Propagate sudoers configuration] *******************************
changed: [fw]
changed: [ldap]
changed: [nfs]
changed: [ansible]
changed: [log]

PLAY RECAP *********************************************************************
ansible                    : ok=2    changed=1    unreachable=0    failed=0
fw                         : ok=2    changed=1    unreachable=0    failed=0
ldap                       : ok=2    changed=1    unreachable=0    failed=0
log                        : ok=2    changed=1    unreachable=0    failed=0
nfs                        : ok=2    changed=1    unreachable=0    failed=0
```

Verifique que o arquivo `/etc/sudoers` é lido localmente, agora.

```
$ ls -ld /etc/sudoers
-r--r----- 1 root root 1392 nov  6 13:50 /etc/sudoers
```

# 4) Versionamento de configuração com git