

Spécialité : Réseaux Intelligents et Cybersécurité

Présenté par : COULIBALY DAOUDA DAVID & WAHID Moncef

ANSIBLE

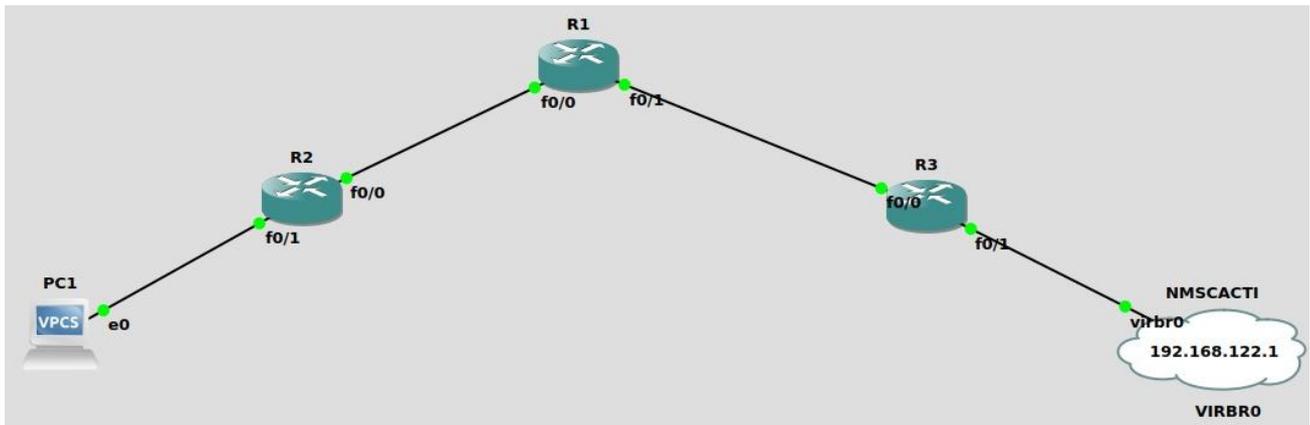
Encadré par:

Pr. Jihane JABRANE

ENSA Khouribga

Année universitaire :2024/2025

Mettons la topologie sur GNS3 :



Après installé ansible par ces trois commandes :

```
apt-add-repository ppa:ansible/ansible
apt update
Apt install ansible
```

```
packages can be upgraded. run 'apt list --upgradable' to see them.
david@david-virtual-machine:~$ sudo apt install ansible
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
ansible-core python-babel-localedata python3-babel python3-bcrypt
python3-jinja2 python3-jmespath python3-kerberos python3-markupsafe
python3-ntlm-auth python3-packaging python3-paramiko
python3-requests-kerberos python3-requests-ntlm python3-resolvelib
python3-winrm python3-xmltodict sshpass
```

Vérifions ansible est bien installé :

```
david@david-virtual-machine:~$ ls /etc/ansible
ansible.cfg  hosts  roles
david@david-virtual-machine:~$ ipconfig
Command 'ipconfig' not found, did you mean:
  command 'iconfig' from deb ipmiutil (3.18-1)
```

Configuration des 3 Routers :

```
laviEnter configuration commands, one per line. End with CNTL/Z.
[sudR1(config)#int F1/0
ReadR1(config-if)#ip addr 192.168.122.7 255.255.255.0
BuildR1(config-if)#no shutdown
ReadR1(config-if)#
The *Mar 1 00:01:40.503: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state t
DCO UP
```

Test de connectivité :

```
david@david-virtual-machine:~$ ping 192.168.122.7
PING 192.168.122.7 (192.168.122.7) 56(84) bytes of data.
64 bytes from 192.168.122.7: icmp_seq=1 ttl=255 time=21.2 ms
64 bytes from 192.168.122.7: icmp_seq=2 ttl=255 time=11.7 ms
64 bytes from 192.168.122.7: icmp_seq=3 ttl=255 time=5.64 ms
64 bytes from 192.168.122.7: icmp_seq=4 ttl=255 time=0.689 ms
64 bytes from 192.168.122.7: icmp_seq=5 ttl=255 time=3.45 ms
```

Configurons SSH dans R1 :

```
R1
R3 x R1 x R2 x
R1(config)#crypto key generate rsa
The name for the keys will be: R1.monreseau.local
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#
*Mar 1 00:38:12.355: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#username admin privilege 15 secret password
R1(config)#ip ssh version 2
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)#exit
R1(config)#exit
R1#w
*Mar 1 00:40:10.203: %SYS-5-CONFIG_I: Configured from console by console
R1#wr
Building configuration...
[OK]
R1#
```

Configurons SSH dans R3 :

```
R3 x R1 x R2 x
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ip domain-name monreseau.local
R3(config)#crypto key generate rsa
The name for the keys will be: R3.monreseau.local
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

R3(config)#
*Mar 1 00:19:19.039: %SSH-5-ENABLED: SSH 1.99 has been enabled
R3(config)#username admin privilege 15 secret password
R3(config)#ip ssh version 2
R3(config)#line vty 0 4
R3(config-line)#login local
R3(config-line)#transport input ssh
R3(config-line)#exit
R3(config)#wr
```

Configurons SSH dans R2 :

```
R2
R3 x R1 x R2 x
R2(config)#crypto key generate rsa
The name for the keys will be: R2.monreseau.local
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

R2(config)#
*Mar 1 00:23:26.399: %SSH-5-ENABLED: SSH 1.99 has been enabled
R2(config)#username admin privilege 15 secret password
R2(config)#ip ssh version 2
R2(config)#line vty 0 4
R2(config-line)#login local
R2(config-line)#transport input ssh
R2(config-line)#exit
R2(config)#exit
R2#w
*Mar 1 00:25:00.999: %SYS-5-CONFIG_I: Configured from console by console
R2#wr
Building configuration...
[OK]
R2#
```

Vérifié SSH est bien installé dans R1:

```

moR1#show running-config | i ssh
The ip ssh version 2
nc transport input ssh
0 upR1#
Need*Mar 1 00:22:18.767: SSH2 0: no matching cipher found: client chacha20-poly1305
Afte@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,
Do yR1#ping 192.168.122.1
Get:
ver Type escape sequence to abort.

```

Modifions fichier ssh_config dans Ansible pour que les deux mettre en d'accord sur des critères de chiffrement :

```

david@david-virtual-machine: /etc/ansible x david@david-virtual-machine: /etc/ssh x
GNU nano 6.2 ssh config
# IdentityFile ~/.ssh/id_dsa
# IdentityFile ~/.ssh/id_ecdsa
# IdentityFile ~/.ssh/id_ed25519
Port 22
Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc
# MACs hmac-md5,hmac-sha1,umac-64@openssh.com
# EscapeChar ~
# Tunnel no
# TunnelDevice any:any
# PermitLocalCommand no
# VisualHostKey no
# ProxyCommand ssh -q -W %h:%p gateway.example.com
# RekeyLimit 1G 1h
# UserKnownHostsFile ~/.ssh/known_hosts.d/%k
SendEnv LANG LC_*
HashKnownHosts yes
GSSAPIAuthentication yes
KexAlgorithms +diffie-hellman-group1-sha1
HostKeyAlgorithms +ssh-rsa
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^_ Go To Line

```

Testons la connectivité SSH vers les 3 routeurs :

```

david@david-virtual-machine: /etc/ansible$ ssh admin@192.168.2.2
The authenticity of host '192.168.2.2 (192.168.2.2)' can't be established.
RSA key fingerprint is SHA256:EMXZCgh6EAIBfm/IvREL9Vu/c4sXq36gtYQnx+yf3F8.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.2.2' (RSA) to the list of known hosts.
(admin@192.168.2.2) Password:

R2#exit
Connection to 192.168.2.2 closed.
david@david-virtual-machine: /etc/ansible$ ssh admin@192.168.1.1
The authenticity of host '192.168.1.1 (192.168.1.1)' can't be established.
RSA key fingerprint is SHA256:cbrEpQ/inLdMpMdUuABDi1r26riuxAZhgPQw2WFnc/4.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.1' (RSA) to the list of known hosts.
(admin@192.168.1.1) Password:

R3#exit
Connection to 192.168.1.1 closed.
david@david-virtual-machine: /etc/ansible$ ssh admin@192.168.122.2
The authenticity of host '192.168.122.2 (192.168.122.2)' can't be established.
RSA key fingerprint is SHA256:cbrEpQ/inLdMpMdUuABDi1r26riuxAZhgPQw2WFnc/4.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:3: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.122.2' (RSA) to the list of known hosts.
(admin@192.168.122.2) Password:

```

Ajoutons les routeurs au inventaires d'Ansible :

```
david@david-virtual-machine:/etc/ssh$ cd /etc/ansible
david@david-virtual-machine:/etc/ansible$ sudo nano hosts
```

```
GNU nano 6.2 hosts
# You can also use ranges for multiple hosts:
## db-[99:101]-node.example.com

# Ex 3: A collection of database servers in the 'dbservers' group:
## [dbservers]
##
## db01.intranet.mydomain.net
## db02.intranet.mydomain.net
## 10.25.1.56
## 10.25.1.57

# Ex4: Multiple hosts arranged into groups such as 'Debian' and 'openSUSE':
## [Debian]
## alpha.example.org
## beta.example.org

## [openSUSE]
## green.example.com
## blue.example.com

#Collection des hotes routeurs Cisco
[cisco_routers]
R1 ansible_host=192.168.1.2
R2 ansible_host=192.168.2.2
R3 ansible_host=192.168.122.2
#Collection des variables
[cisco_routers: vars]
ansible_network_os=ios
ansible_user=admin
ansible_password=password
ansible_connection=network_cli
```

Vérifions que les routeurs été bien ajouté :

```
david@david-virtual-machine:/etc/ansible$ sudo ansible-inventory --list
{
  "_meta": {
    "hostvars": {
      "R1": {
        "ansible_connection": "network_cli",
        "ansible_host": "192.168.1.2",
        "ansible_network_os": "ios",
        "ansible_password": "password",
        "ansible_user": "admin"
      },
      "R2": {
        "ansible_connection": "network_cli",
        "ansible_host": "192.168.2.2",
        "ansible_network_os": "ios",
        "ansible_password": "password",
        "ansible_user": "admin"
      },
      "R3": {
        "ansible_connection": "network_cli",
        "ansible_host": "192.168.122.2",
        "ansible_network_os": "ios",
        "ansible_password": "password",
        "ansible_user": "admin"
      }
    }
  },
  "all": {
    "children": [
      "ungrouped",
      "cisco_routers"
    ]
  },
  "cisco_routers": {
    "hosts": [
      "R1",
      "R2",
      "R3"
    ]
  }
}
david@david-virtual-machine:/etc/ansible$
```

Testons la connectivité au Routeurs depuis Ansible :

```
david@david-virtual-machine:/etc/ansible$ sudo ansible cisco_routers -m ping
[WARNING]: ansible-pylibssh not installed, falling back to paramiko
R3 | SUCCESS => {
  "changed": false,
  "ping": "pong"
}
R2 | SUCCESS => {
  "changed": false,
  "ping": "pong"
}
R1 | SUCCESS => {
  "changed": false,
  "ping": "pong"
}
david@david-virtual-machine:/etc/ansible$
```

Créons un nouveau playbook :

```
GNU nano 6.2 cisco playbook.yaml
--
- name: une description de Uptime routers Cisco ios
  hosts: R1-router
  gather_facts: false

  tasks:
    - name: afficher Uptime
      ios_command:
        commands: show version | include uptime
      register: output

    - name: result
      debug:
        msg: "{{ output.stdout_lines }}"
```

Lançons le PLAYBOOK :

```

david@david-virtual-machine:/etc/ansible$ ls
ansible.cfg  cisco_playbook.yaml  hosts  roles
david@david-virtual-machine:/etc/ansible$ sudo nano cisco_playbook.yaml
david@david-virtual-machine:/etc/ansible$ sudo nano cisco_playbook.yaml
david@david-virtual-machine:/etc/ansible$ sudo ansible-playbook cisco_playbook.yaml
sudo: ansible-playbook: command not found
david@david-virtual-machine:/etc/ansible$ sudo ansible-playbook cisco_playbook.yaml

PLAY [Vérification de l'uptime des routeurs Cisco] *****

TASK [Afficher l'uptime des routeurs Cisco] *****
[WARNING]: ansible-pylibssh not installed, falling back to paramiko
ok: [R3]
ok: [R1]
ok: [R2]

TASK [Afficher le résultat] *****
ok: [R1] => {
  "msg": [
    [
      "R1 uptime is 1 hour, 10 minutes"
    ]
  ]
}
ok: [R2] => {
  "msg": [
    [
      "R2 uptime is 52 minutes"
    ]
  ]
}
ok: [R3] => {
  "msg": [
    [
      "R3 uptime is 57 minutes"
    ]
  ]
}

PLAY RECAP *****
R1      : ok=2    changed=0    unreachable=0    failed=0    skipped=0    rescue=0
changed=0    ignored=0
R2      : ok=2    changed=0    unreachable=0    failed=0    skipped=0    rescue=0
changed=0    ignored=0
R3      : ok=2    changed=0    unreachable=0    failed=0    skipped=0    rescue=0
changed=0    ignored=0
Show Applications
david@david-virtual-machine:/etc/ansible$

```

BONUS :

MODIFIONS Playbook pour changer @ ip de Router :

```

--
- name: Configurer une interface Cisco
  hosts: R1-router
  gather_facts: false

  tasks:
    - name: Changer l'adresse IP de l'interface FastEthernet1/0
      ios_config:
        lines:
          - ip address 192.168.1.2 255.255.255.0
          - no shutdown # Active l'interface si elle est désactivée
        parents: interface FastEthernet1/0
      notify: Sauvegarder la configuration

  handlers:
    - name: Sauvegarder la configuration
      ios_config:
        save_when: modified

```

Lançons Playbook & testons la connectivité au ancien @IP:

The offending line appears to be:

```

tasks:
^ here
david@david-virtual-machine:/etc/ansible$ sudo nano cisco_playbook.yaml
david@david-virtual-machine:/etc/ansible$ sudo nano cisco_playbook.yaml
david@david-virtual-machine:/etc/ansible$ sudo ansible-playbook cisco_playbook.yaml
[WARNING]: Invalid characters were found in group names but not replaced, use -vvvv to see
details

PLAY [Configurer une interface Cisco] *****

TASK [Changer l'adresse IP de l'interface FastEthernet1/0] *****
[WARNING]: ansible-pylibssh not installed, falling back to paramiko
Fatal: [R1]: FAILED! => {"changed": false, "module_stderr": "timeout value 30 seconds reached while trying to send command: b'ip address 192.168
ILURE\nSee stdout/stderr for the exact error"}

PLAY RECAP *****
R1                : ok=0    changed=0    unreachable=0    failed=1    skipped=0    rescued=0    ignored=0

david@david-virtual-machine:/etc/ansible$ ping 192.168.122.7
PING 192.168.122.7 (192.168.122.7) 56(84) bytes of data:
From 192.168.122.1 icmp_seq=1 Destination Host Unreachable
From 192.168.122.1 icmp_seq=2 Destination Host Unreachable
From 192.168.122.1 icmp_seq=3 Destination Host Unreachable
From 192.168.122.1 icmp_seq=4 Destination Host Unreachable
^C
--- 192.168.122.7 ping statistics ---
5 packets transmitted, 0 received, +4 errors, 100% packet loss, time 5152ms
pipe 4
david@david-virtual-machine:/etc/ansible$ sudo ansible-playbook cisco_playbook.yaml
[WARNING]: Invalid characters were found in group names but not replaced, use -vvvv to see
details

PLAY [Configurer une interface Cisco] *****

TASK [Changer l'adresse IP de l'interface FastEthernet1/0] *****
[WARNING]: ansible-pylibssh not installed, falling back to paramiko
^C [ERROR]: User interrupted execution
david@david-virtual-machine:/etc/ansible$ sudo nano cisco_playbook.yaml
david@david-virtual-machine:/etc/ansible$

```