# Ansible-RadiusSSH

## Compte rendu : Installation et configuration d'Ansible pour la gestion des switchs Cisco

Anthony GRASSET
Yassine DEMATOS

**Objectif** : Installer Ansible sur une VM, configurer l'accès SSH aux switchs, tester le déploiement automatique sur les switchs.

---

## 🔹 1. Installation d'Ansible sur la VM Ubuntu 24.04

> **VM utilisée :** Ubuntu Server 24.04

## Étapes :

1. **Mettre à jour le système**

```
sudo apt update && sudo apt upgrade -y
```

2. **Installer Ansible et ses dépendances**

```
sudo apt install -y ansible sshpass
```

3. **Vérifier l'installation**

```
ansible --version
```

```
ansible [core 2.17.9]
  config file = /etc/ansible/ansible.cfg
  configured module search path = ['/root/.ansible/plugins/modules', '/usr/share/ansible/plugins/modules']
  ansible python module location = /usr/lib/python3/dist-packages/ansible
  ansible collection location = /root/.ansible/collections:/usr/share/ansible/collections
  executable location = /usr/bin/ansible
  python version = 3.12.3 (main, Feb  4 2025, 14:48:35) [GCC 13.3.0] (/usr/bin/python3)
  jinja version = 3.1.2
  libyaml = True
```

## 🔹 2. Configuration des switchs pour l'accès SSH

> **Les switchs doivent être accessibles en SSH**

## Sur chaque switch Cisco :

1. **Créer un utilisateur Ansible avec accès `enable` ou utiliser ceux existant**

```
conf t
username gady privilege 15 secret gady
enable secret admin
```

2. **Activer SSH**

```
ip domain-name SATOMAS
crypto key generate rsa modulus 2048
ip ssh version 2
```

3. **Configurer l'accès SSH sur les lignes VTY**

```
line vty 0 4
transport input ssh
login local
privilege level 15
exit
```

4. **Sauvegarder la configuration**

```
write memory
```

---

## 🔹 3. Configuration d'Ansible pour gérer les switchs

> **Fichier d'inventaire :** `/etc/ansible/inventory.yml`

## Création du fichier `inventory.yml`

Ansible a besoin d'un **fichier d'inventaire** ( `inventory.yml` ) qui liste tous les switchs à gérer. Ce fichier définit :

- L'**adresse IP** de chaque switch.
- Les **identifiants SSH** pour s'y connecter.
- Les **paramètres réseau** spécifiques à Cisco IOS.

```
switches:
  hosts:
    switchRDC:
      ansible_host: 172.17.70.1
      ansible_user: gady
      ansible_password: gady
      ansible_become_password: admin
      ansible_network_os: cisco.ios
      ansible_ssh_common_args: '-o StrictHostKeyChecking=no -
UserKnownHostsFile=/dev/null'
      ansible_connection: network_cli
      ansible_become: yes
      ansible_become_method: enable
      ansible_command_timeout: 90
      gather_facts: no

    switchE1:
      ansible_host: 172.17.70.2
      ansible_user: gady
      ansible_password: gady
      ansible_become_password: admin
      ansible_network_os: cisco.ios
      ansible_ssh_common_args: '-o StrictHostKeyChecking=no -o
UserKnownHostsFile=/dev/null'
      ansible_connection: network_cli
      ansible_become: yes
      ansible_become_method: enable
      ansible_command_timeout: 90
      gather_facts: no
```

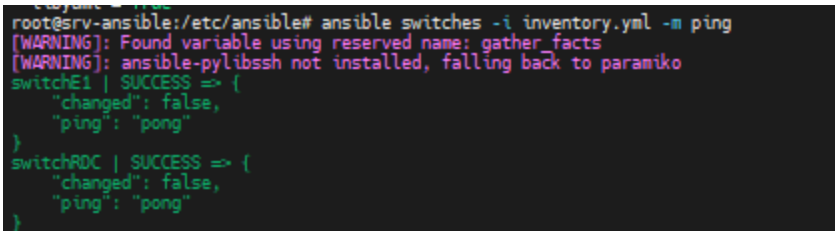
**Options importantes** :

- `ansible_become_password` : Mot de passe `enable`
- `ansible_connection: network_cli` : Utilisation du module Cisco
- `ansible_ssh_common_args: '-o StrictHostKeyChecking=no -o UserKnownHostsFile=/dev/null'` → Désactive la vérification de clé SSH pour éviter les erreurs.

## Tester la connexion SSH avec Ansible

```
ansible switches -i inventory.yml -m ping
```

### Résultat :




---

# 🔹 4. Récupérer la version des switchs

## Création du fichier `check_switch_version.yml`

```
- name: Vérifier la version des switchs Cisco
  hosts: switches
  gather_facts: no
  tasks:

    - name: Récupérer la version du système
      cisco.ios.ios_command:
        commands:
          - show version | include (Cisco IOS Software|Model number)
      register: version_output

    - name: Afficher la version et le modèle du switch
      debug:
        msg: "{{ version_output.stdout_lines | join(' ') }}"
```

## Exécuter le Playbook

```
ansible-playbook -i inventory.yml check_switch_version.yml
```

**Résultat :**

```
root@srv-ansible:/etc/ansible# ansible-playbook -i inventory.yml check_switch_version.yml

PLAY [Vérifier la version des switchs Cisco] ***********************************************************************************************************************************************************
[WARNING]: Found variable using reserved name: gather_facts

TASK [Récupérer la version du système] *****************************************************************************************************************************************************************
[WARNING]: ansible-pylibssh not installed, falling back to paramiko
ok: [switchE1]
ok: [switchRDC]

TASK [Afficher la version du switch] *******************************************************************************************************************************************************************
ok: [switchRDC] => {
    "version_output.stdout_lines": [
        [
            "Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.2(2)E7, RELEASE SOFTWARE (fc3)",
            "Technical Support: http://www.cisco.com/techsupport",
            "Copyright (c) 1986-2017 by Cisco Systems, Inc.",
            "Compiled Wed 12-Jul-17 15:29 by prod_rel_team",
            "",
            "ROM: Bootstrap program is C2960 boot loader",
            "BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M) Version 15.0(2r)EZ1, RELEASE SOFTWARE (fc1)",
            "",
            "SwRDC uptime is 8 hours, 34 minutes",
            "System returned to ROM by power-on",
            "System restarted at 02:51:16 CEST Thu Mar 13 2025",
            "System image file is \"flash:/c2960-lanbasek9-mz.152-2.E7/c2960-lanbasek9-mz.152-2.E7.bin\"",
            "Last reload reason: power-on",
            "",
            "",
            "",
            "This product contains cryptographic features and is subject to United",
            "States and local country laws governing import, export, transfer and",
            "use. Delivery of Cisco cryptographic products does not imply",
            "third-party authority to import, export, distribute or use encryption.",
            "Importers, exporters, distributors and users are responsible for",
            "compliance with U.S. and local country laws. By using this product you",
            "agree to comply with applicable laws and regulations. If you are unable",
            "to comply with U.S. and local laws, return this product immediately.",
            "",
            "A summary of U.S. laws governing Cisco cryptographic products may be found at:",
            "http://www.cisco.com/wwl/export/crypto/tool/stqrg.html",
            "",
            "If you require further assistance please contact us by sending email to",
            "export@cisco.com.",
            "",
            "cisco WS-C2960+24TC-L (PowerPC405) processor (revision J0) with 131072K bytes of memory.",
            "Processor board ID FCW2204A4UE",
            "Last reset from power-on",
            "2 Virtual Ethernet interfaces",
            "24 FastEthernet interfaces",
            "2 Gigabit Ethernet interfaces",
            "The password-recovery mechanism is enabled.",
            "",
            "64K bytes of flash-simulated non-volatile configuration memory.",
            "Base ethernet MAC Address       : 00:BF:77:C5:A4:80",
            "Motherboard assembly number     : 73-15620-01",
            "Power supply part number        : 341-0097-03",
            "Motherboard serial number       : FOC22035W5L",
            "Power supply serial number      : DCA215083U0",
            "Model revision number           : J0",
            "Motherboard revision number     : B0",
            "Model number                    : WS-C2960+24TC-L",
            "System serial number            : FCW2204A4UE",
            "Top Assembly Part Number        : 800-40261-02",
            "Top Assembly Revision Number    : D0",
            "Version ID                      : V02",
            "CLEI Code Number                : CMMKV00ARB",
            "Hardware Board Revision Number  : 0x0B",
            "",
            "",
            "Switch Ports Model                     SW Version          SW Image                ",
            "------ ----- -----                     ----------          ----------              ",
            "*    1 26    WS-C2960+24TC-L           15.2(2)E7           C2960-LANBASEK9-M       ",
            "",
            "",
            "Configuration register is 0xF"
        ]
    ]
}
```

```
ok: [switchE1] => {
    "version_output.stdout_lines": [
        [
            "Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 12.2(55)SE5, RELEASE SOFTWARE (fc1)",
            "Technical Support: http://www.cisco.com/techsupport",
            "Copyright (c) 1986-2012 by Cisco Systems, Inc.",
            "Compiled Thu 09-Feb-12 19:11 by prod_rel_team",
            "Image text-base: 0x00003000, data-base: 0x01900000",
            "",
            "ROM: Bootstrap program is C2960 boot loader",
            "BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(53r)SEY3, RELEASE SOFTWARE (fc1)",
            "",
            "SwE1 uptime is 8 hours, 34 minutes",
            "System returned to ROM by power-on",
            "System image file is \"flash:/c2960-lanbasek9-mz.122-55.SE5/c2960-lanbasek9-mz.122-55.SE5.bin\"",
            "",
            "",
            "This product contains cryptographic features and is subject to United",
            "States and local country laws governing import, export, transfer and",
            "use. Delivery of Cisco cryptographic products does not imply",
            "third-party authority to import, export, distribute or use encryption.",
            "Importers, exporters, distributors and users are responsible for",
            "compliance with U.S. and local country laws. By using this product you",
            "agree to comply with applicable laws and regulations. If you are unable",
            "to comply with U.S. and local laws, return this product immediately.",
            "",
            "A summary of U.S. laws governing Cisco cryptographic products may be found at:",
            "http://www.cisco.com/wwl/export/crypto/tool/stqrg.html",
            "",
            "If you require further assistance please contact us by sending email to",
            "export@cisco.com.",
            "",
            "cisco WS-C2960-24TT-L (PowerPC405) processor (revision R0) with 65536K bytes of memory.",
            "Processor board ID FCQ1632X5UD",
            "Last reset from power-on",
            "2 Virtual Ethernet interfaces",
            "24 FastEthernet interfaces",
            "2 Gigabit Ethernet interfaces",
            "The password-recovery mechanism is enabled.",
            "",
            "64K bytes of flash-simulated non-volatile configuration memory.",
            "Base ethernet MAC Address       : 88:75:56:F3:7E:00",
            "Motherboard assembly number     : 73-12600-06",
            "Power supply part number        : 341-0097-03",
            "Motherboard serial number       : FCQ163208GG",
            "Power supply serial number      : ALD1623B108",
            "Model revision number           : R0",
            "Motherboard revision number     : A0",
            "Model number                    : WS-C2960-24TT-L",
            "System serial number            : FCQ1632X5UD",
            "Top Assembly Part Number        : 800-32797-02",
            "Top Assembly Revision Number    : A0",
            "Version ID                      : V11",
            "CLEI Code Number                : COMBL00BRF",
            "Hardware Board Revision Number  : 0x0A",
            "",
            "",
            "Switch Ports Model             SW Version          SW Image                ",
            "------ ----- -----             ----------          ----------              ",
            "*    1 26    WS-C2960-24TT-L   12.2(55)SE5         C2960-LANBASEK9-M       ",
            "",
            "",
            "Configuration register is 0xF"
        ]
    ]
}

PLAY RECAP *********************************************************************************************************************************************************************************************
switchE1                   : ok=2    changed=0    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
switchRDC                  : ok=2    changed=0    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
```

Notre script renvoie bien les commandes que l'on a effectuée comme afficher sur le PLAY RECAP on peut désormais créer d'autres script pour autre configuration et faire de même pour

les inventaires.

---

# Intégration Radius SSH sur Équipements Réseaux Cisco

## Objectif

Mettre en place une authentification centralisée via **Radius** permettant aux administrateurs du domaine Active Directory de se connecter en **SSH** sur les équipements réseaux Cisco avec des privilèges élevés (niveau 15). Cette solution renforce la sécurité et simplifie la gestion des accès.

---

## Contexte Technique

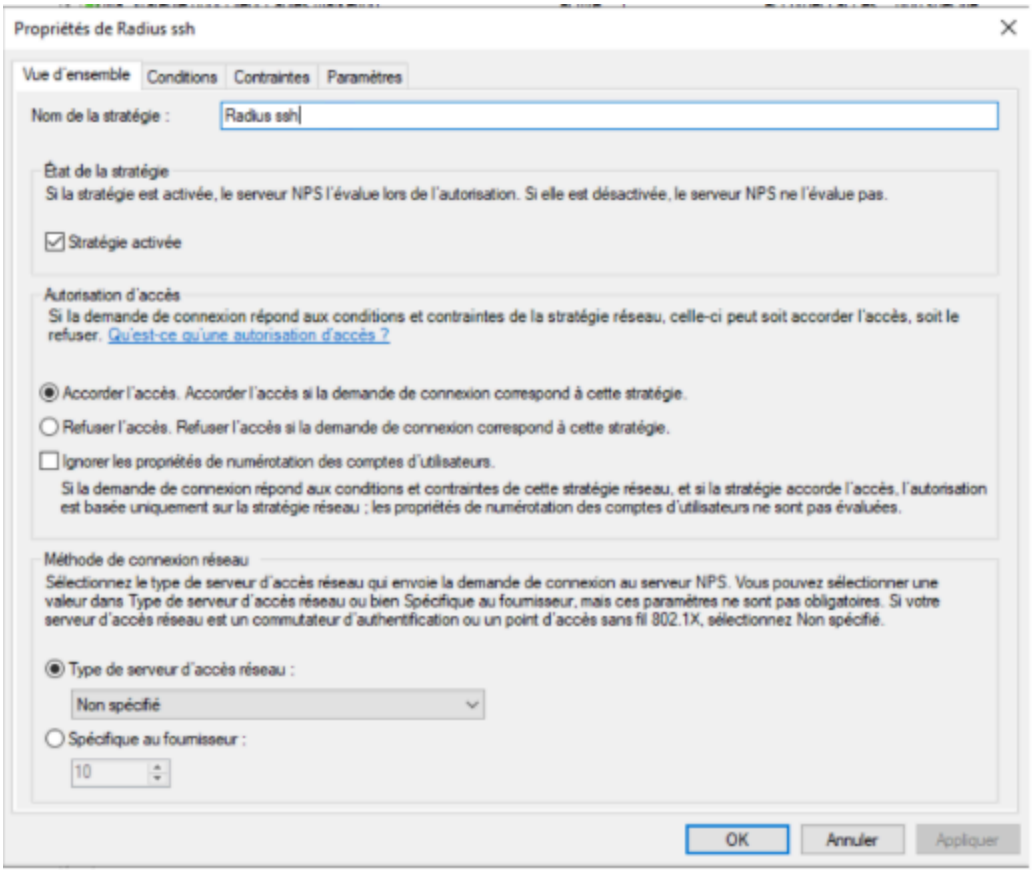
- **Équipements Réseaux** : Switchs Cisco
- **Serveur Radius** : Contrôleur de domaine Active Directory (IP : 172.17.100.2)
- **Authentification SSH** : Comptes administrateurs du domaine Active Directory
- **Outil de connexion** : MobaXterm pour les tests

---

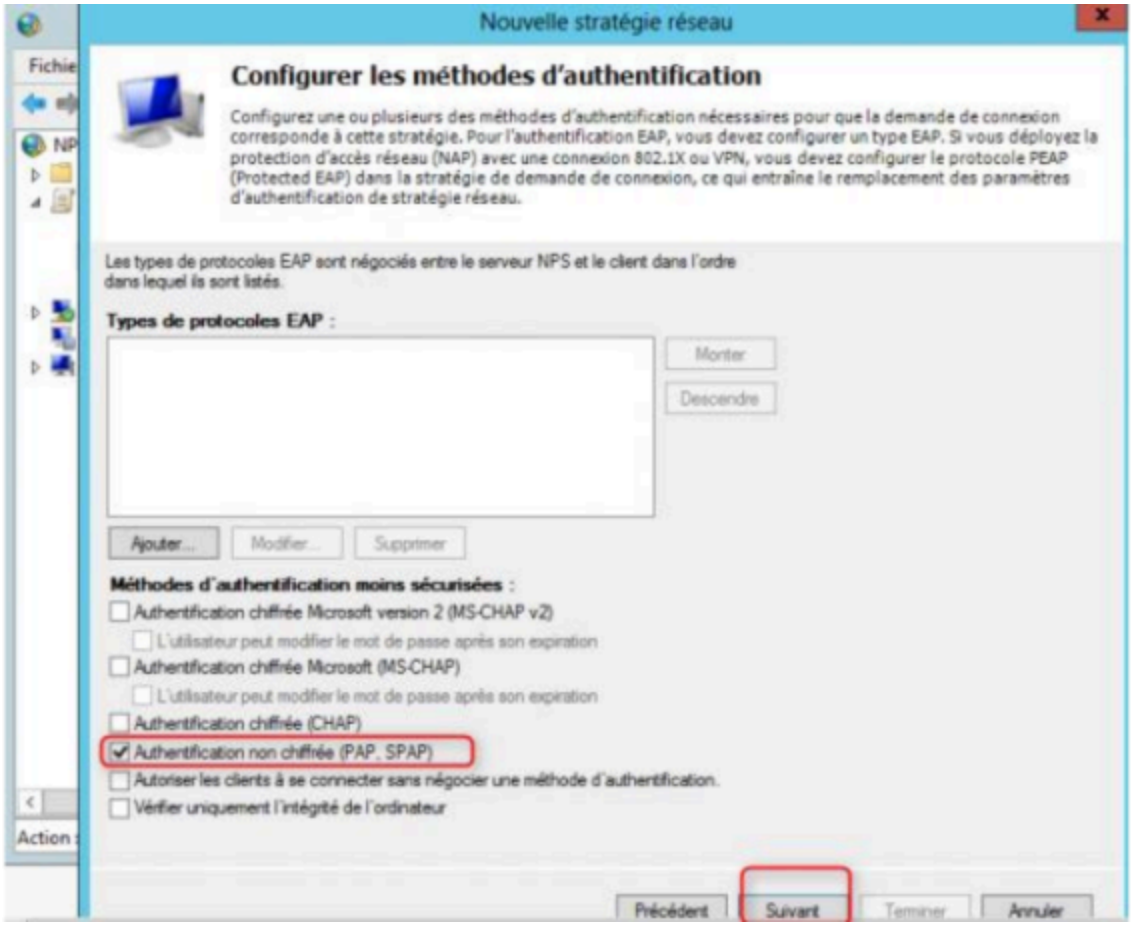
## Démarche de mise en œuvre

### 1. Configuration du Serveur Radius (Active Directory)

- Création d'une **stratégie de connexion réseau** nommée "Radius SSH" :




- Autorisation d'accès : *Accorder l'accès*.
- Méthode d'authentification : *PAP/SPAP* (Authentification non chiffrée).



- Condition d'accès : Groupe Windows → **Admins du domaine**.
- Ajout d'un attribut :
  - **Service-Type** : *login*.
- Configuration fournisseur spécifique (Cisco) :
  - Définir un attribut permettant d'octroyer le niveau de privilège 15 (accès administrateur complet) aux membres du groupe **Admins du domaine**.

---

## 2. Configuration des Équipements Réseaux (Cisco)

- **Définition du serveur Radius** :
  - Adresse IP du serveur Radius : 172.16.100.2.
  - Clé secrète partagée pour sécuriser les échanges.
- **Configuration SSH et AAA** :

```
aaa authentication login default group radius local
aaa authentication login console local
aaa authorization exec default group radius local
```

- **Explication** :
  - La commande `aaa authentication login default group radius local` permet d'utiliser le Radius pour l'authentification SSH, avec un fallback sur les comptes locaux si le serveur Radius est indisponible.
  - La ligne console ( `line con 0` ) reste accessible avec les comptes locaux pour garantir un accès de secours.

---

## 3. Tests de Connexion

- **Connexion SSH via MobaXterm** :
  - Test réalisé depuis un poste personnel avec un compte **Admin du domaine**.
  - Résultat : Connexion SSH réussie avec privilèges administrateur sur le switch Cisco.
- **Connexion de secours (local)** :
  - Test de la connexion en mode console (serial).
  - Résultat : Accès possible avec les comptes locaux en cas de défaillance du Radius.

--