2025.10.29 - Bloc 2 - 2 - Contrôle d’accès centralisé avec un serveur RADIUS (AAA)

Cisco Packet Tracer avec Timothee pour Bloc 1 le mercredi 29 octobre 2025 en distanciel

Qui êtes-vous et qu’avez-vous le droit de faire ?

Imaginez que chaque porte de votre entreprise ait une serrure différente avec une clé unique. Pour donner l’accès à un nouvel employé, vous devriez copier des dizaines de clés. S’il part, vous devriez changer des dizaines de serrures ! C’est ingérable. La solution est un système de badge centralisé : vous créez un badge, vous lui donnez des droits, et il ouvre les portes autorisées. Si l’employé part, vous désactivez simplement son badge.

Dans un réseau, c’est le rôle du modèle **AAA** :

- **Authentication** (Authentification) : Qui êtes-vous ? (Prouvez-le avec un login/mot de passe).
- **Authorization** (Autorisation) : Qu’avez-vous le droit de faire ? (Accès simple utilisateur ou administrateur ?).
- **Accounting** (Comptabilité) : Qu’avez-vous fait ? (Journalisation des commandes et des connexions).

Le protocole **RADIUS** est l’un des standards les plus utilisés pour permettre à un équipement réseau (un commutateur, un routeur) de communiquer avec un serveur d’authentification central pour appliquer ce modèle.

Ce TP vous montrera comment configurer un commutateur pour qu’il demande la permission à un serveur RADIUS avant d’autoriser un administrateur à se connecter.

Objectifs

À la fin de ce laboratoire, vous serez capable de :

- Expliquer le modèle AAA et le rôle d’un serveur RADIUS.
- Configurer le service RADIUS sur un serveur dans Packet Tracer.
- Configurer un commutateur Cisco pour qu’il utilise ce serveur pour l’authentification.
- Mettre en place une méthode d’authentification de secours (fallback local).
- Valider la connexion à distance en utilisant les identifiants centralisés.

🧩 Étape 1 : Préparation du laboratoire

Objectif :
Mettre en place la topologie réseau de base qui servira à tester l'authentification centralisée via le protocole **RADIUS**.
Cette étape consiste à ajouter le matériel, réaliser le câblage et configurer les adresses IP pour permettre la communication entre tous les équipements.

⚙️ 1️⃣ Ajout des équipements

Matériel nécessaire :

- 1 Commutateur Cisco **2960**, nommé **SW1**
- 1 Serveur, nommé **RADIUS-SRV**
- 1 PC, nommé **PC-Admin**

🧠 *Rôle des équipements :*

- **RADIUS-SRV** : serveur d'authentification centralisé (AAA/RADIUS).
- **SW1** : client RADIUS (c'est lui qui interrogera le serveur pour valider les accès).
- **PC-Admin** : poste d'administration utilisé pour tester la connexion SSH au switch.

🔌 2️⃣ Câblage de la topologie

⚙️ Étapes précises :

1. Clique sur l'icône du **câble éclair** ⚡ dans la barre d'outils.
2. Sélectionne le câble **"Copper Straight-Through"** (*câble droit*).
3. Fais les connexions suivantes :
   - **SW1 (Fa0/1) → RADIUS-SRV (Fa0)**
   - **SW1 (Fa0/2) → PC-Admin (Fa0)**

🧠 *Pourquoi un câble droit ?*
Parce que tu relies des **équipements de type différent** (switch ↔ PC / switch ↔ serveur).
Les câbles croisés ne sont nécessaires qu'entre deux équipements de même type (ex : PC ↔ PC).

💡 *Vérifie les voyants verts* :
Quand le lien fonctionne, tu verras un petit voyant **vert** à chaque extrémité du câble.

🌐 3️⃣ Plan d'adressage IP

Voici le plan à respecter :

Équipement	Interface	Adresse IP	Masque	Passerelle par défaut
RADIUS-SRV	Fa0	192.168.1.100	255.255.255.0	192.168.1.1
PC-Admin	Fa0	192.168.1.10	255.255.255.0	192.168.1.1
SW1	VLAN 1 (gestion)	192.168.1.1	255.255.255.0	—

🧠 *Remarque :*
Le switch n'a pas de "vraie" interface Ethernet pour sa gestion.
L'adresse IP est configurée sur **l'interface virtuelle VLAN 1**, ce qui permet d'y accéder à distance (via Telnet ou SSH).

💻 4️⃣ Configuration des adresses IP

🔹 Étape A – Serveur **RADIUS-SRV**

1. Clique sur **RADIUS-SRV**.
2. Va dans **l'onglet Config**.
3. Dans le menu de gauche, sélectionne **FastEthernet0**.
4. Configure les paramètres suivants :

   `IP Address: 192.168.1.100 Subnet Mask: 255.255.255.0 Default Gateway: 192.168.1.1`
5. Vérifie que le bouton **Port Status** est sur **On**.
6. Pour vérifier, va dans l'onglet **Desktop** → **Command Prompt**, et tape :

   `ipconfig`

   ➜ Tu dois voir :

   `IP Address: 192.168.1.100 Subnet Mask: 255.255.255.0 Default Gateway: 192.168.1.1`

🔹 Étape B – PC **PC-Admin**

1. Clique sur **PC-Admin**.
2. Onglet **Config** → **FastEthernet0**.
3. Configure :

   `IP Address: 192.168.1.10 Subnet Mask: 255.255.255.0 Default Gateway: 192.168.1.1`
4. Vérifie que **Port Status = On**.
5. Vérifie avec **Desktop** → **Command Prompt** → **ipconfig** :

`IP Address: 192.168.1.10 Subnet Mask: 255.255.255.0 Default Gateway: 192.168.1.1`

🔹 Étape C – Switch **SW1**

1. Clique sur **SW1**.
2. Va dans **l'onglet CLI** (Command Line Interface).
3. Tape les commandes suivantes :

```
SW1> enable SW1# configure terminal SW1(config)# interface vlan 1 SW1(config-if)# ip address 192.168.1.1 255.255.255.0 SW1(config-if)# no shutdown SW1(config-if)# exit SW1(config)# end
```

🧠 *Explication :*

- `interface vlan 1` → on entre dans l'interface virtuelle utilisée pour la gestion.
- `ip address` → on assigne l'adresse IP de gestion du switch.
- `no shutdown` → on active l'interface VLAN (sinon elle reste "administratively down").

Vérifie ensuite :

```
SW1# show ip interface brief
```

Tu dois voir :

```
Vlan1 192.168.1.1 YES manual up up
```

🧪 5️⃣ Vérification de la connectivité

🔹 Depuis PC-Admin :

1. Clique sur **Desktop** → **Command Prompt**.
2. Tape les commandes suivantes :

```
ping 192.168.1.1 ping 192.168.1.100
```

✅ **Résultats attendus :**

```
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255 Reply from 192.168.1.100: bytes=32 time<1ms TTL=255
```

Cela confirme que :

- Le PC communique avec le switch,
- Le PC communique avec le serveur,
- Et donc que **toute la topologie fonctionne**.

🧠 Points à retenir pour l'examen

- Le **VLAN 1** est l'interface de gestion par défaut des switches Cisco.
- Toujours **activer (no shutdown)** l'interface VLAN sinon le ping échoue.
- Toujours **tester la connectivité avant d'ajouter des services (AAA, SSH, RADIUS)**.
- Une **passerelle par défaut** sur le serveur et le PC est nécessaire pour qu'ils puissent joindre d'autres sous-réseaux.

⚙️ Étape 2 : Configuration du serveur RADIUS

🎯 Objectif

Mettre en place et activer le **service AAA/RADIUS** sur le serveur **RADIUS-SRV** afin qu'il puisse authentifier les utilisateurs du réseau.
Ce serveur permettra de vérifier les identifiants lorsqu'un administrateur tentera de se connecter au commutateur **SW1**.

🧠 *Rappel conceptuel :*

- **AAA = Authentication, Authorization, Accounting**
  - **Authentication** → vérifie qui se connecte (login/mot de passe)
  - **Authorization** → définit ce qu'il a le droit de faire
  - **Accounting** → garde une trace de ce qu'il fait

Le protocole **RADIUS (Remote Authentication Dial-In User Service)** est celui qui permet au serveur et au switch de communiquer pour appliquer ces principes.

🧱 1️⃣ Accéder au serveur et au service AAA

1. Clique sur ton **serveur RADIUS-SRV** dans Packet Tracer.
2. Dans la fenêtre qui s'ouvre, clique sur **l'onglet "Services"** (en haut de la fenêtre).
3. Dans le menu de gauche, sélectionne **"AAA"**.
   👉 C'est ici que tu trouveras les paramètres du serveur RADIUS.

⚙️ 2️⃣ Activer le service RADIUS

- En haut de la section, tu verras un bouton intitulé **"Service On/Off"**.
- Coche **"On"** pour activer le service AAA/RADIUS.

💡 *Sans cette étape, ton serveur ne répondra pas aux requêtes d'authentification du switch.*

🧩 3️⃣ Configurer le client (le commutateur SW1)

Dans la section **"Client Setup"**, tu vas indiquer au serveur qui (quel équipement) est autorisé à l'utiliser.
Un "client" ici désigne un équipement réseau (switch, routeur, etc.) qui demande une authentification au serveur.

Remplis les champs suivants :

Champ	Valeur à entrer	Explication
Client Name	SW1	Nom du commutateur (pour s'y retrouver facilement)
Client IP	192.168.1.1	Adresse IP de l'interface VLAN 1 du switch
Secret	Cisco123	Clé partagée entre le serveur et le switch (doit être **identique** sur les deux équipements)

🧠 *Important :*

> Cette clé partagée est une sorte de "mot de passe" de communication entre le serveur et le switch.
> Si elle diffère d'un côté ou de l'autre, la communication RADIUS échouera.

Une fois les champs remplis, clique sur le bouton **"Add"**.
Le client **SW1** apparaît maintenant dans la liste des clients autorisés du serveur.

👤 4️⃣ Créer les comptes utilisateurs

Toujours sur la même page, repère la section **"User Setup"**.
C'est ici que tu définis les utilisateurs autorisés à s'authentifier via le serveur RADIUS.

Remplis les champs comme suit :

Champ	Valeur à entrer	Explication
Username	netadmin	Nom de l'administrateur réseau
Password	AdminPass	Mot de passe correspondant

Puis clique sur **"Add"** pour enregistrer le compte.

💡 *Tu peux créer plusieurs comptes ici si tu veux tester plusieurs profils d'utilisateurs, mais pour ce TP un seul suffit.*

🧪 5️⃣ Vérification de la configuration

Quand tu as ajouté ton client et ton utilisateur, tu dois voir :

- Ton **client SW1 (192.168.1.1)** listé dans la partie "Client Table".
- Ton **utilisateur netadmin** listé dans la partie "User Table".

✅ Cela signifie que :

- Le service AAA est activé.
- Le serveur connaît le switch autorisé à lui parler.
- Le compte administrateur "netadmin" est enregistré pour l'authentification.

🧠 Points à retenir pour l'examen

- Le **client RADIUS** (ici SW1) doit être déclaré sur le serveur, sinon il sera rejeté.
- Le **Secret partagé** doit être **strictement identique** des deux côtés.
- Le **nom d'utilisateur et le mot de passe** créés sur le serveur seront ceux utilisés pour la connexion SSH au switch.
- Le serveur RADIUS est l'équivalent du **"badge centralisé"** de ton entreprise : il détient toutes les clés d'accès.

⚙️ Étape 3 : Configuration du commutateur (Client AAA)

🎯 Objectif général

Configurer le commutateur **SW1** pour qu'il **ne gère plus localement les identifiants d'accès**, mais qu'il **interroge le serveur RADIUS-SRV** (192.168.1.100) à chaque tentative de connexion.
Avant de pouvoir communiquer avec le serveur, nous devons nous assurer que :

- Le switch dispose d'une **interface de gestion active (VLAN 1)**,
- Et qu'il est accessible **à distance via SSH** (connexion sécurisée).

PARTIE 1 — Configuration de base (IP et accès distant SSH)

🧠 Pourquoi cette étape ?

Pour que le serveur RADIUS puisse identifier et communiquer avec le switch, ce dernier doit :

- Avoir une **adresse IP sur son interface de gestion VLAN 1**,
- Être joignable en **SSH**, puisque c'est via SSH que l'administrateur se connectera pour être authentifié.

🔧 Étape A – Entrer en mode de configuration

1. Ouvre la **console de ton switch SW1**.
2. Tape les commandes suivantes :

```
SW1> enable SW1# configure terminal
```

💡 *Explication :*

- `enable` → permet de passer en mode privilégié (#).
- `configure terminal` → ouvre le mode de configuration globale du switch.

🔹 Étape B – Configurer l'interface de gestion (VLAN 1)

```
SW1(config)# interface vlan 1 SW1(config-if)# ip address 192.168.1.1 255.255.255.0
SW1(config-if)# no shutdown SW1(config-if)# exit
```

🧠 *Explication :*

- `interface vlan 1` → on entre dans l'interface virtuelle VLAN 1 (utilisée pour la gestion du switch).
- `ip address` → on assigne l'adresse IP du switch.
- `no shutdown` → on active l'interface.
- `exit` → on revient au mode de configuration globale.

Commande de vérification :

```
SW1# show ip interface brief
```

✅ **Résultat attendu :**

```
Vlan1 192.168.1.1 YES manual up up
```

🔹 Étape C – Configuration SSH (accès distant sécurisé)

Les connexions distantes (pour l'administration) doivent passer par SSH plutôt que Telnet, car SSH chiffre la communication.

Étapes à suivre :

```
SW1(config)# ip domain-name noob2pro.lab SW1(config)# crypto key generate rsa How many bits in the modulus [512]: 1024 SW1(config)# ip ssh version 2
```

🧠 *Explication détaillée :*

- `ip domain-name` → nécessaire pour générer une clé RSA (il faut un nom de domaine).
- `crypto key generate rsa` → crée la clé de chiffrement pour SSH.
  - Quand le switch te demande la taille, tape **1024** (plus sécurisé que 512).
- `ip ssh version 2` → force le switch à utiliser la version 2 d'SSH (plus sûre).

🔹 Étape D – Vérification du SSH

Tu peux t'assurer que le SSH est bien activé avec la commande :

```
SW1# show ip ssh
```

✅ **Résultat attendu :**

```
SSH Enabled - version 2.0 Authentication timeout: 120 secs; Authentication retries: 3
```

💡 Points clés à retenir pour l'examen

- L'accès distant **SSH** est indispensable pour tester l'authentification RADIUS.
- La commande `ip domain-name` est **obligatoire** avant de générer la clé RSA.
- Si le VLAN 1 est **administratively down**, le serveur ne pourra pas contacter le switch.
- On utilise **SSH** car il chiffre les identifiants et les commandes (contrairement à Telnet).

PARTIE 2 — Configuration du modèle AAA

🎯 Objectif

Mettre en place sur **SW1** le modèle **AAA** (Authentication, Authorization, Accounting) afin que l'authentification des connexions distantes (SSH) soit **déléguée au serveur RADIUS-SRV**. L'objectif est que le switch demande au serveur RADIUS de vérifier les identifiants des administrateurs, plutôt que de se baser sur sa propre base locale.

🧱 1️⃣ Activation du modèle AAA

Entre en mode de configuration globale sur le switch :

```
SW1# configure terminal SW1(config)# aaa new-model
```

🧠 *Explication :*

- La commande `aaa new-model` active la gestion avancée des accès (AAA).
- Une fois activée, le switch n'utilise plus la simple commande `login local`, mais un système de méthodes d'authentification centralisé.

⚠️ **Attention importante :**

> Si tu es connecté en SSH ou Telnet au moment où tu tapes cette commande, tu risques d'être déconnecté !
> Toujours faire cette configuration **depuis la console physique** du switch (port Console).

🧩 2️⃣ Déclaration du serveur RADIUS

Tu vas maintenant dire au switch **où se trouve le serveur RADIUS** et **quelle clé secrète** utiliser pour communiquer avec lui.

```
SW1(config)# radius server RADIUS-SRV SW1(config-radius-server)# address ipv4 192.168.1.100 SW1(config-radius-server)# key Cisco123 SW1(config-radius-server)# exit
```

🧠 *Explication :*

- `radius server RADIUS-SRV` → crée un profil nommé "RADIUS-SRV" (le nom est libre, mais garde-le cohérent avec le serveur).
- `address ipv4 192.168.1.100` → indique l'adresse IP du serveur RADIUS (celle du RADIUS-SRV).
- `key Cisco123` → clé partagée entre le switch et le serveur (elle doit être **identique** à celle configurée côté serveur à l'Étape 2).

💡 *Vérifie la configuration avec :*

```
SW1# show running-config | section radius
```

✅ **Résultat attendu :**

```
radius server RADIUS-SRV address ipv4 192.168.1.100 auth-port 1812 acct-port 1813 key Cisco123
```

🧰 3️⃣ Création d'une méthode d'authentification

On va maintenant dire au switch *comment* procéder lorsqu'un utilisateur tente de se connecter.

```
SW1(config)# aaa authentication login default group radius local
```

🧠 *Explication ligne par ligne :*

- `aaa authentication login` → définit la méthode d'authentification utilisée lors d'une connexion (login).
- `default` → applique cette méthode par défaut à toutes les lignes (console et SSH).
- `group radius` → indique que la 1re méthode est de **consulter le serveur RADIUS**.
- `local` → méthode de secours (fallback) : si le serveur RADIUS ne répond pas, alors le switch utilisera la base **locale**.

💡 *C'est une commande essentielle !*

> Elle crée une chaîne logique :
> - 🔹 Tente d'abord d'authentifier via **RADIUS**,
> - 🔹 Sinon, bascule sur la base **locale** (sauvegarde).

👤 4️⃣ Création d'un utilisateur local de secours

Pour garantir un accès d'urgence en cas de panne du serveur RADIUS, on crée **un compte local de secours**.

```
SW1(config)# username backupadmin secret BackupPass
```

🧠 *Explication :*

- `username` → nom de l'utilisateur local.
- `secret` → crée un mot de passe chiffré (plus sûr que `password`).
- `BackupPass` → mot de passe d'accès d'urgence.

💡 *Bonnes pratiques :*

- Toujours avoir **au moins un utilisateur local** configuré avant d'activer AAA.
- Ce compte est utilisé uniquement si le serveur RADIUS devient inaccessible.

🧪 5️⃣ Vérifications rapides

Afficher la configuration AAA :

```
SW1# show running-config | include aaa
```

✅ **Résultat attendu :**

```
aaa new-model aaa authentication login default group radius local
```

Afficher la configuration du serveur RADIUS :

```
SW1# show running-config | section radius
```

Afficher les utilisateurs locaux :

```
SW1# show running-config | include username
```


💡 Points clés à retenir (examen)

- **AAA** = Authentication / Authorization / Accounting.
- Le **serveur RADIUS** valide les identifiants des utilisateurs distants.
- Le **mot-clé "local"** dans la commande AAA permet une **méthode de secours**.
- Sans utilisateur local, tu risques de **te bloquer hors du switch** si le serveur RADIUS tombe.
- Toujours tester l'accès en **console physique** avant de tester en SSH.

Partie 3 — Appliquer la configuration aux lignes VTY

🎯 Objectif

Faire en sorte que le switch **utilise le serveur RADIUS (et non plus sa base locale)** pour authentifier les connexions SSH.
Pour cela, il faut **lier le modèle AAA que nous avons créé** aux **lignes VTY (Virtual Teletype)**, c'est-à-dire les ports logiques utilisés pour les connexions à distance (SSH ou Telnet).

🧱 1️⃣ Explication avant de configurer

- Les **lignes VTY** correspondent aux sessions virtuelles que les administrateurs utilisent pour se connecter au switch à distance.
- Par défaut, un switch autorise 16 connexions simultanées (de **VTY 0 à 15**).
- On doit donc appliquer la méthode AAA à toutes ces lignes pour que **toute connexion SSH passe par le serveur RADIUS**.

⚙️ 2️⃣ Commandes à entrer sur le switch

Ouvre la console du switch et saisis les commandes suivantes :

(Login : netadmin -- MDP : AdminPass)

```
SW1# configure terminal ! Appliquer la méthode d'authentification AAA aux lignes VTY
```
SW1(config)# line vty 0 15
```
SW1(config-line)# transport input ssh
```
SW1(config-line)# login authentication default
```
SW1(config-line)# exit
```
SW1(config)# end
```
SW1# write memory
```

🧠 Explications détaillées ligne par ligne

Commande	Rôle
`line vty 0 15`	Accède à la configuration de toutes les lignes virtuelles (VTY 0 à 15) utilisées pour SSH.
`transport input ssh`	Indique que seules les connexions **SSH** sont autorisées (et non Telnet, car non sécurisé).
`login authentication default`	Lie la méthode d'authentification **AAA** que nous avons créée (`default group radius local`) aux connexions SSH.
`exit`	Sort du mode configuration des lignes.
`end`	Quitte le mode configuration globale.
`write memory`	Sauvegarde la configuration dans la mémoire NVRAM (sinon elle serait perdue au redémarrage).

🧪 3️⃣ Vérification de la configuration

Affiche les paramètres des lignes VTY :

```
SW1# show running-config | section line vty
```

✅ **Résultat attendu :**

```
line vty 0 15 transport input ssh login authentication default
```

Affiche la méthode d'authentification active :

```
SW1# show aaa authentication
```

✅ **Résultat attendu :**

```
AAA authentication login default group radius local
```

⚠️ Erreurs fréquentes à éviter

- ❌ Oublier `transport input ssh` → cela autorise Telnet, ce qui est non sécurisé.
- ❌ Mettre `login local` au lieu de `login authentication` → cela désactive le modèle AAA.
- ❌ Ne pas sauvegarder (`write memory`) → tu perdras tout au redémarrage du switch.
- ❌ Tester AAA en SSH avant d'avoir créé ton utilisateur sur le serveur RADIUS → la connexion échouera systématiquement.

💡 Points importants pour l'examen

- La commande `login authentication default` fait le lien **entre AAA et les accès distants**.
- En entreprise, on désactive toujours Telnet (`transport input ssh`) pour des raisons de sécurité.
- La commande `write memory` ou `copy running-config startup-config` est **obligatoire** après toute configuration AAA.
- Si AAA est mal configuré, on risque de **se verrouiller hors du switch** → toujours tester depuis la **console** avant SSH.

🧩 Étape 4 : Vérification et test

🎯 Objectif

Vérifier que :

- Le **serveur RADIUS** authentifie correctement les connexions SSH au switch,
- Le **switch** applique bien la méthode d'authentification AAA,
- Le **mode de secours local (fallback)** fonctionne si le serveur RADIUS devient indisponible.

🧱 1️⃣ Préparation du test

1. Sur ton **PC-Admin**, clique sur **Desktop → Command Prompt**.
2. Vérifie d'abord que le PC peut toujours contacter le switch et le serveur :

```
ping 192.168.1.1 ping 192.168.1.100
```

✅ Les deux pings doivent répondre avant de continuer.

🔐 2️⃣ Connexion SSH avec l'utilisateur RADIUS

Depuis le **PC-Admin**, tape la commande suivante dans le terminal :

```
ssh -l netadmin 192.168.1.1
```

Quand le mot de passe est demandé, entre :

```
AdminPass
```

✅ **Résultat attendu :**

```
Password: SW1>
```

🎉 La connexion réussit !
Le commutateur a transmis les identifiants au serveur **RADIUS-SRV**, qui les a validés.
L'utilisateur `netadmin` est maintenant connecté à **SW1** grâce à l'authentification centralisée RADIUS.

🧠 *Ce test prouve que le modèle AAA et la liaison RADIUS fonctionnent correctement.*

❌ 3️⃣ Test avec un mot de passe erroné

Déconnecte-toi du switch :

```
exit
```

Puis tente à nouveau une connexion SSH avec un mauvais mot de passe :

```
ssh -l netadmin 192.168.1.1
```

Quand le mot de passe est demandé, entre volontairement une mauvaise valeur (ex : `WrongPass`).

✅ **Résultat attendu :**

```
Password authentication failed
```

🧠 *Le serveur RADIUS rejette logiquement la connexion car les identifiants ne correspondent pas à ceux stockés dans sa base AAA.*

🧰 4️⃣ Simulation de panne du serveur RADIUS

Pour vérifier que la méthode **de secours locale** fonctionne, tu vas simuler une coupure du serveur.

1. Clique sur **RADIUS-SRV**.
2. Va dans **Services** → **AAA**.
3. Désactive le service AAA en mettant le bouton **Service** → **Off**.

💡 Cela simule une panne du serveur RADIUS.
Le switch ne peut plus contacter le serveur d'authentification.

🧪 5️⃣ Test de connexion pendant la panne du serveur

Retourne sur le **PC-Admin**, puis retente une connexion SSH avec le même utilisateur RADIUS :

```
ssh -l netadmin 192.168.1.1
```

✅ **Résultat attendu :**

- Le terminal **“hésite” quelques secondes**, car le switch essaie de contacter le serveur RADIUS.
- Puis, le message d’échec apparaît :

```
Password authentication failed
```

🧠 *Le switch ne trouve pas le serveur RADIUS, il passe automatiquement à la méthode locale — mais comme `netadmin` n’existe pas localement, la connexion échoue.*

👨‍🔧 6️⃣ Test de la méthode locale (utilisateur de secours)

Toujours depuis **PC-Admin**, connecte-toi cette fois avec **l’utilisateur local de secours** :

```
ssh -l backupadmin 192.168.1.1
```

Entre le mot de passe :

```
BackupPass
```

✅ **Résultat attendu :**

```
Password: SW1>
```

🎉 La connexion réussit !
Le commutateur, ne parvenant pas à joindre le serveur RADIUS, a basculé automatiquement sur la **méthode de secours locale** et a validé `backupadmin`.

🧠 *Ce test prouve que ton infrastructure est résiliente : même si le serveur RADIUS tombe, tu gardes un accès d’urgence au switch.*

📝 7️⃣ Réactivation du serveur RADIUS

Une fois les tests terminés :

1. Retourne sur **RADIUS-SRV → Services → AAA**.
2. Réactive le service en cliquant sur **“On”**.

Tu pourras à nouveau te reconnecter avec l’utilisateur RADIUS (`netadmin / AdminPass`).

💡 Points clés à retenir (examen)

- Le protocole **RADIUS (UDP 1812/1813)** est le standard pour l’authentification centralisée.
- Le modèle **AAA** permet une gestion fine :
  - **Authentication** : qui se connecte

    - **Authorization** : que peut-il faire
    - **Accounting** : que fait-il
- Toujours configurer un **utilisateur de secours local** avant d'activer AAA.
- La commande `aaa authentication login default group radius local` permet au switch de basculer automatiquement vers le local si le serveur RADIUS ne répond plus.
- Tester la **résilience** (fallback) est indispensable dans toute configuration AAA en production.