

## Rapport de test

### Objectif :

Vérifier le bon fonctionnement de l'authentification des utilisateurs via le serveur RADIUS.

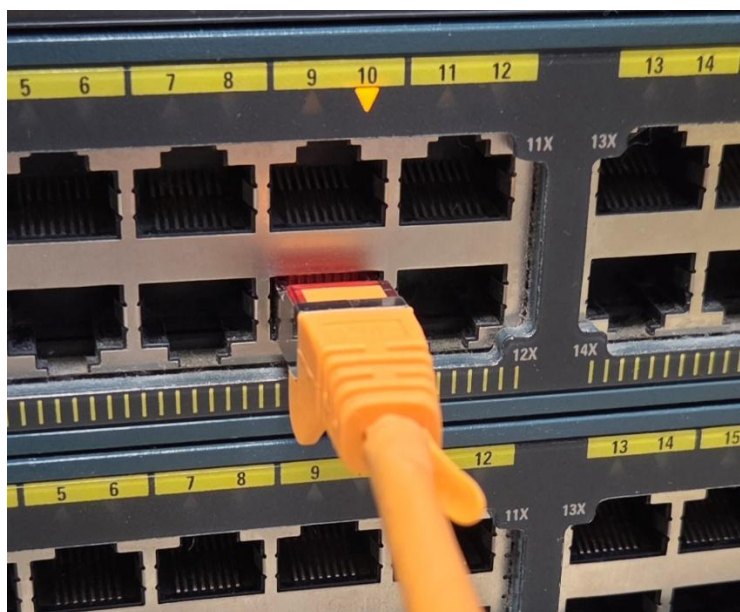
### Résultat attendu :

Nous devrions pouvoir nous connecter au compte de l'utilisateur sur le PC et recevoir une adresse IP dans le VLAN du nom du groupe de l'utilisateur

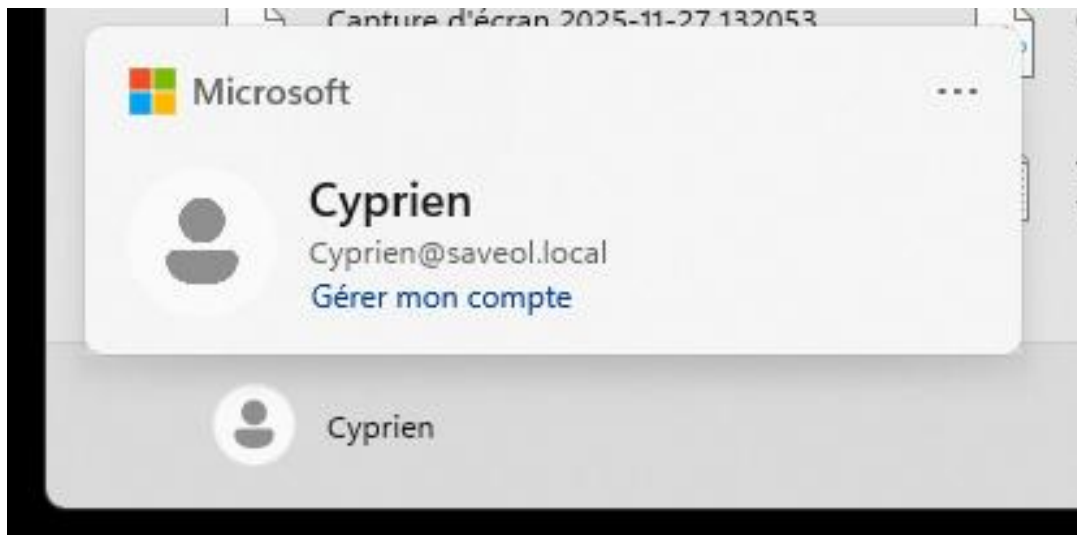
<b>Nom de la stratégie</b>	<b>Nom du groupe</b>	<b>Numéro du vlan</b>
Service Compta	Comptabilité	10
Service Marketing	Marketing	20
Service Conditionnement	Conditionnement	30
Service Livraison	Livraison	40
Service R&D	Recherche	50
Service IT	Admins du domaine	60
Service Direction RH	Direction	80

### Test :

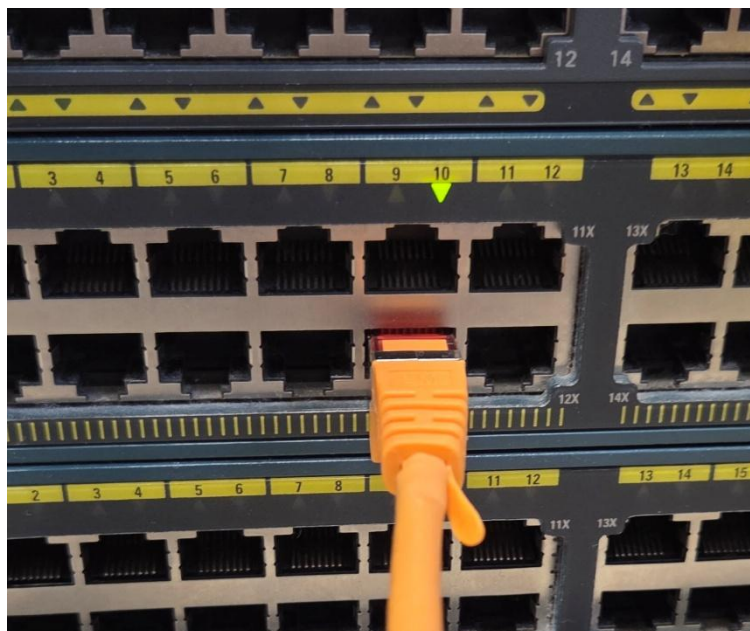
Avant l'authentification



Connexion à un utilisateur depuis le pc client



Après l'authentification



Vérification de la bonne attribution au VLAN approprié

*Résultat obtenu :*

Mon utilisateur « Cyprien » est membre de l'équipe IT.

Le numéro du VLAN est le 60, et j'ai bien reçu une adresse IP dans le VLAN 60, donc l'authentification des utilisateurs fonctionne bien avec le serveur RADIUS.

```

Carte Ethernet Ethernet :

Suffixe DNS propre à la connexion. . . . :
Adresse IPv6 de liaison locale. . . . . : fe80::5c14:5c33:c516:d795%2
Adresse IPv4. . . . . : 172.16.60.3
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . : 172.16.60.254

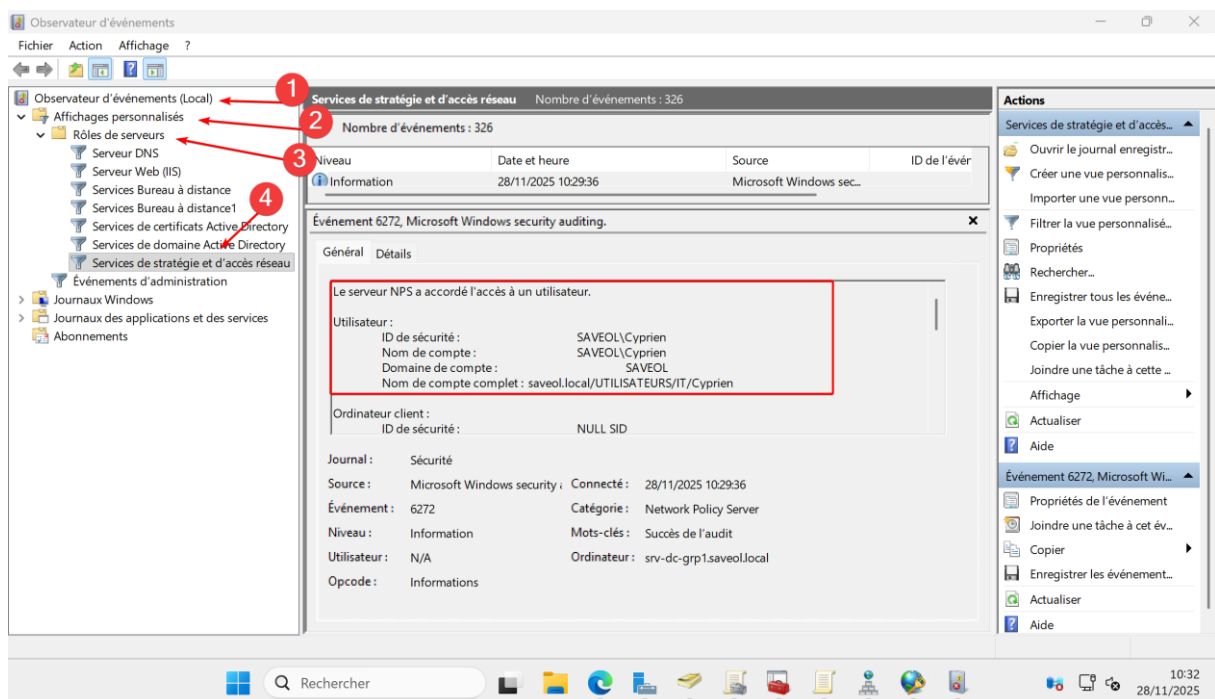
Carte Ethernet Connexion réseau Bluetooth :

Statut du média. . . . . : Média déconnecté
Suffixe DNS propre à la connexion. . . . :

C:\Users\Cyprien>

```

D'après l'observateur d'événements, nous pouvons constater que la connexion a bien réussi.

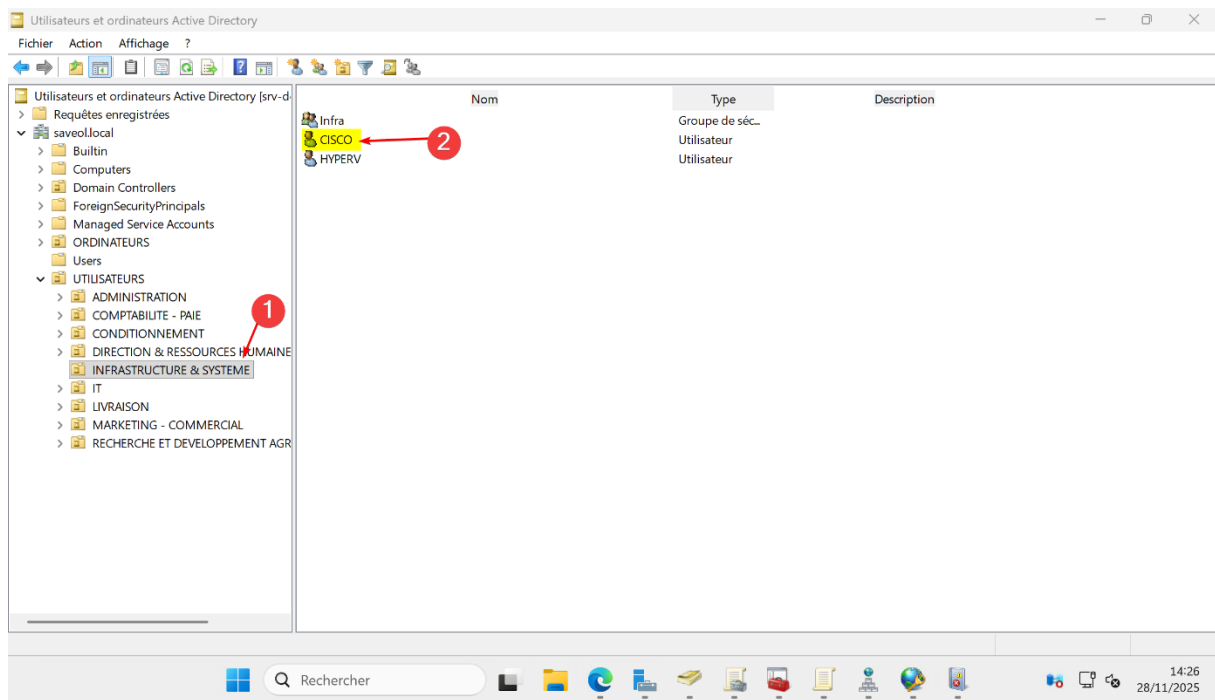


### Objectif :

Vérifier le bon fonctionnement de l'authentification des équipements réseaux avec le serveur radius

### Résultat attendu :

Avec un compte créé précédemment dans l'Active Directory L'authentification des équipements d'interconnexion devrais réussir.



### Test :

Test de connexion avec le compte « CISCO »

```
login as: CISCO
Keyboard-interactive authentication prompts from server:
Password:
End of keyboard-interactive prompts from server

• MobaXterm Personal Edition v25.2 •
(SSH client, X server and network tools)

> SSH session to CISCO@172.16.70.252
• Direct SSH : ✓
• SSH compression : ✗ (disabled or not supported by server)
• SSH-browser : ✗ (disabled for Cisco compatibility)
• X11-forwarding : ✗ (disabled for Cisco compatibility)

> For more info, ctrl+click on help or visit our website.

Switch_1e#
```

### Résultat obtenu :

Mon utilisateur « CISCO » a réussi à se connecter via RADIUS, comme le montre la capture d'écran de connexion.

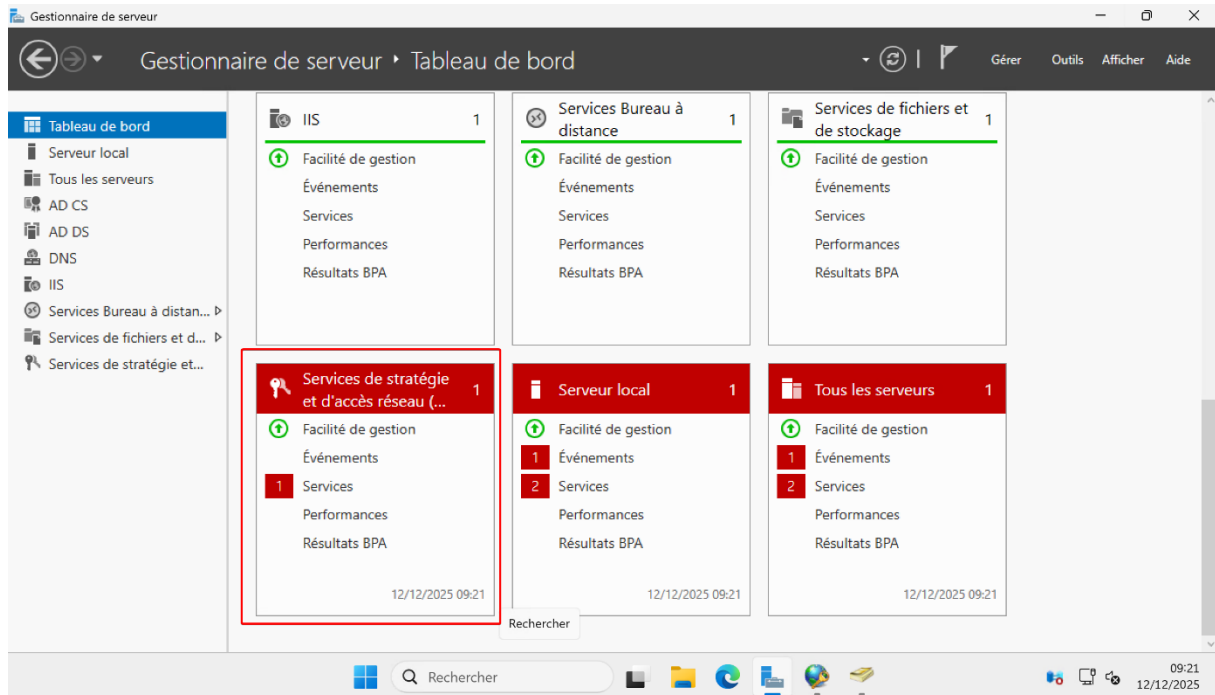
De plus, l'événement dans le rôle NPS confirme que la connexion a été autoriser pour le compte « CISCO ». Donc mon serveur ainsi que la configuration des équipements fonctionnent.

### Objectif :

Vérifier le bon fonctionnement de l'authentification des équipements réseau quand le serveur RADIUS est indisponible.

### Résultat attendu :

Avec un compte configuré localement sur le switch, je devrais être en mesure de m'authentifier, puisque le serveur RADIUS est éteint



(Le serveur a bien été éteint)

### Test :

Test de connexion avec le compte « admin »

```
login as: admin
Keyboard-interactive authentication prompts from server:
Password:
End of keyboard-interactive prompts from server

• MobaXterm Personal Edition v25.2 •
(SSH client, X server and network tools)

► SSH session to admin@172.16.70.252
• Direct SSH : ✓
• SSH compression : ✗ (disabled or not supported by server)
• SSH-browser : ✗ (disabled for Cisco compatibility)
• X11-forwarding : ✗ (disabled for Cisco compatibility)

► For more info, ctrl+click on help or visit our website.

Switch_1e>
```

*Résultat obtenu :*

Mon utilisateur « admin » a réussi à se connecter localement parce qu'il a envoyé une requête au serveur, qui n'a pas répondu, ce qui l'a amené à passer en mode d'authentification local. Donc l'authentification est fonctionnelle.