**Documentation**

**Technique**

ligne horizontale

**Serveur RADIUS**

ligne horizontale

# 

**25/04/2025**

**Gabriel PFISTER, Quentin PARC**

**Sommaire**

ligne horizontale

[**Contexte 3**](#_yqc3zntowln1)

[**Mise en place 3**](#_q0xtv7r3f5yl)

[Installation du rôle NPS (Network Policy Server) 3](#_jr36e6wo0htx)

[Inscription du serveur dans l’Active Directory 6](#_tvim4ld2v89m)

[Création d’une stratégie réseau (Network Policy) 9](#_pekcwhmsjb82)

# 

# Contexte



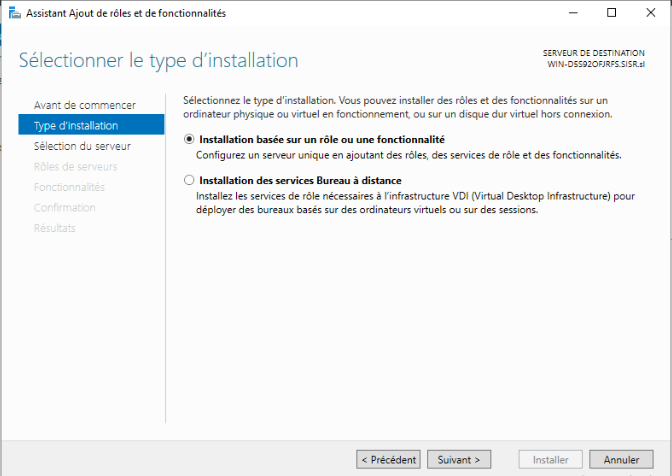
Un serveur RADIUS base son fonctionnement sur le protocole [UDP (User Datagram Protocol)](https://www.fortinet.com/fr/resources/cyberglossary/user-datagram-protocol-udp) et il s’agit généralement d’une application démon qui s’exécute sur une machine Windows ou UNIX. Un démon est un programme qui s’exécute en arrière-plan. Le serveur RADIUS collecte des informations d’identification sur toutes les informations d’identification de ses utilisateurs. Le serveur attend d’obtenir une demande d’un client ou d’un NAS, qui peut être des appareils ou des systèmes tels que des points d’accès sans fil ou des réseaux privés virtuels (RPV)

# Mise en place

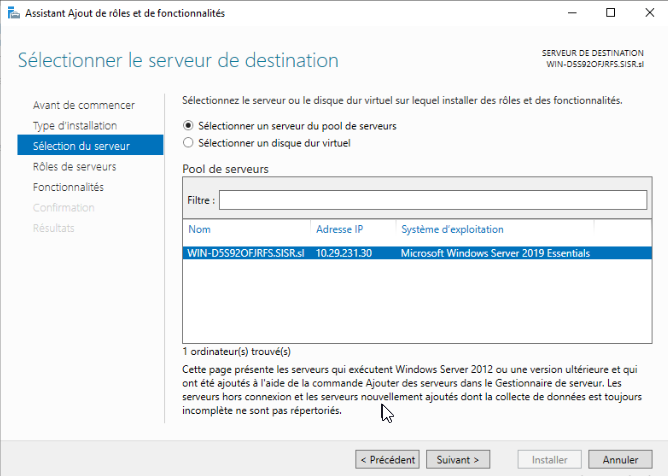


## Installation du rôle NPS (Network Policy Server)

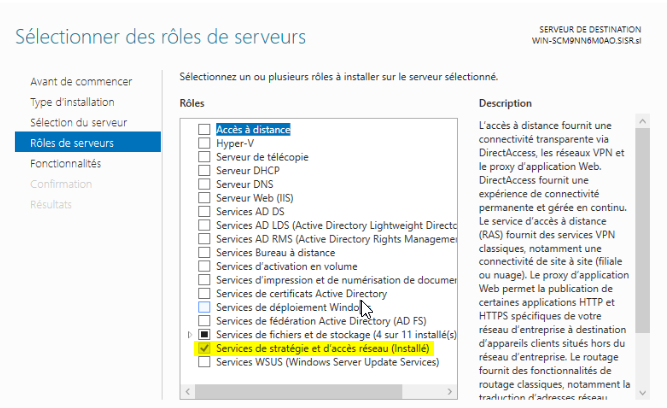
1. Ouvrir le Gestionnaire de serveur.
2. Aller dans Gérer > Ajouter des rôles et fonctionnalités.
3. Suivre l’assistant jusqu'à l’étape Rôles de serveurs.



*Image 1 : Installation de Radius dans l’Assistant - Ajout de rôles et de fonctionnalités*



*Image 2 : Sélectionner le serveur du pool de serveurs*



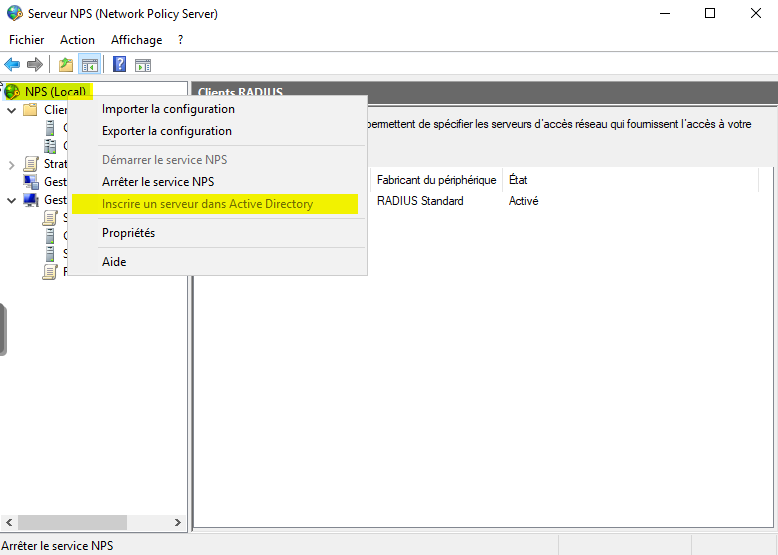
*Image 3 : Rôle de serveurs - Services de stratégie et d’accès réseau*

## 

## **Inscription du serveur dans l’Active Directory**

Dans le Serveur NPS :

* Faire un clic droit sur "NPS (Local)" et cliquer sur "Inscrire un Serveur dans Active Directory".
* Confirmer l’inscription.

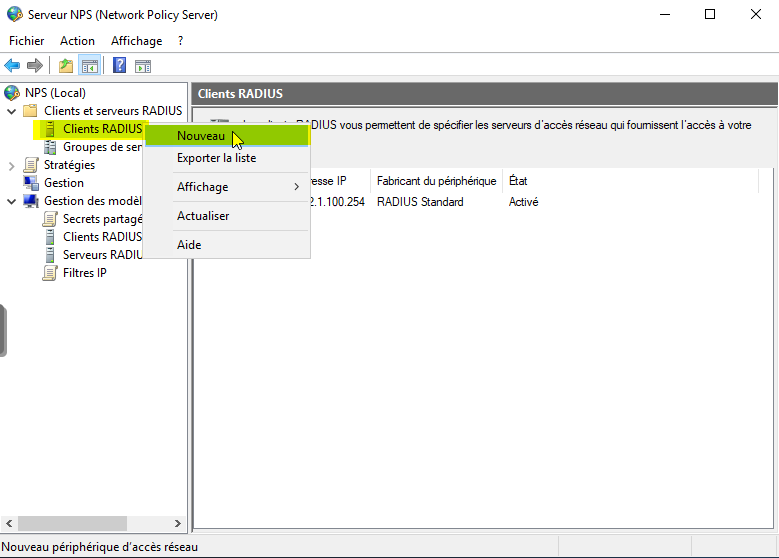


*Image 4 : Mise en place du serveur dans Active Directory*

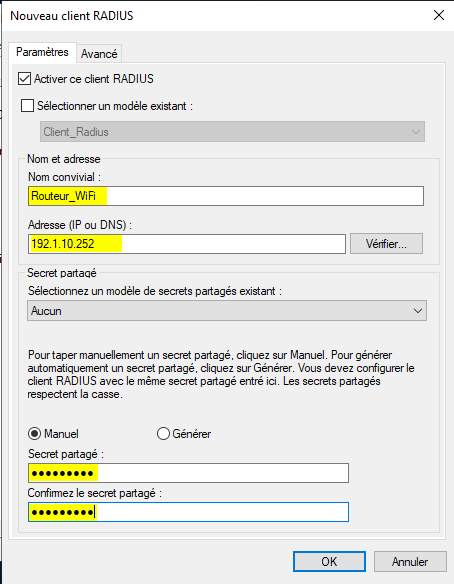
**Ajout des clients RADIUS**

Dans le dossier “Clients et serveurs RADIUS” :

* Faire un clic droit sur “Clients RADIUS” puis choisir “Nouveau”



*Image 5 : Ajout d’un Nouveau client sur le serveur RADIUS*



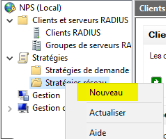
*Image 6 : Configuration du nouveau client*

Le Secret est Azerty123.

## Création d’une stratégie réseau (Network Policy)

Dans la partie “Stratégies” :

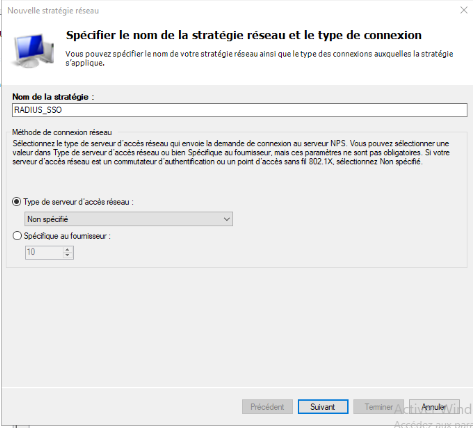
* Faire un clic droit sur “Stratégies réseau” puis “Nouveau”.

****

*Image 6 : Création de la nouvelle stratégie*

Ajout du nom de la stratégie :

* Ici, le nom sera “RADIUS\_SSO”

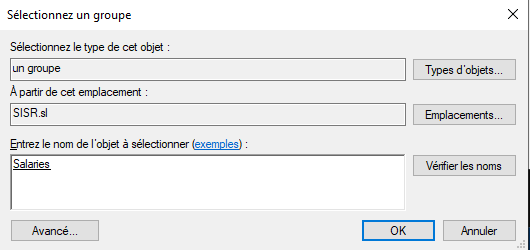


*Image 6 : Mise en place de la nouvelle stratégie*

Ajout de conditions et de contraintes dans la stratégie :

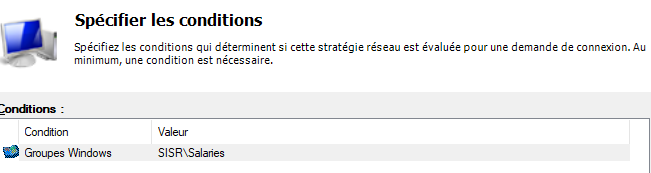
Condition :

* Création d’une condition à partir du groupe “Salaries” dans l’Active Directory.

****

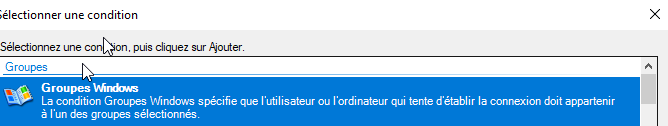
*Image 7 : Mise en place de la condition sur les groupes*

Dans cette situation, la politique s’applique pour le groupe Salariés de l’active Directory

****

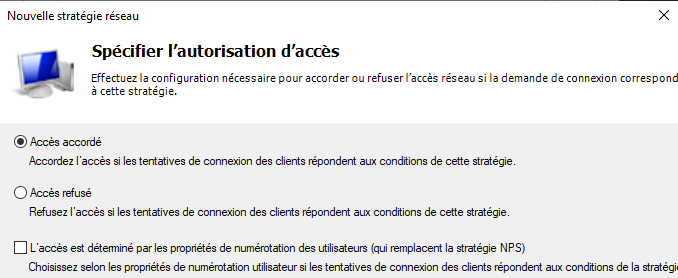
*Image 8 : Condition des groupes*

Ajout d’un groupe Windows, dépendamment de ce qui est voulu :

****

*Image 9 : Mise en place de la condition sur les groupes*

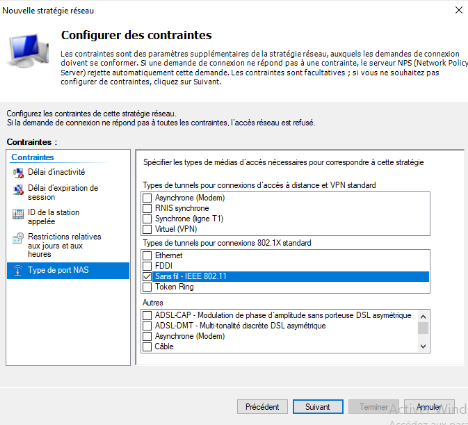
Accordé l’accès à “si les tentatives de connexion des clients répondent aux conditions de cette stratégie”.

****

*Image 10 : Spécifier l’autorisation d’accès*

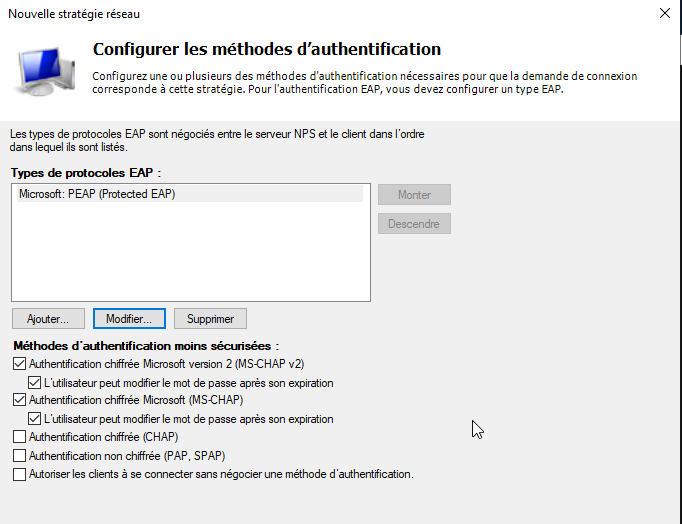
Ajout des contraintes :

Ici, dans “Type de port NAS”, cocher “Sans fil - IEEE 8.0.11”

****

*Image 11 : Ajout de la contrainte dans “Type de port NAS”*

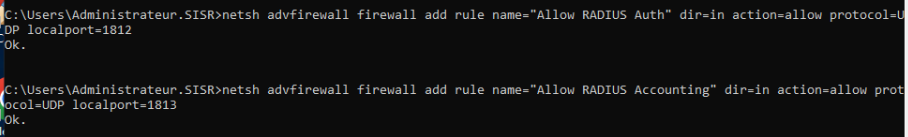
Configuration des méthodes d’authentification :

****

*Image 12 : Configuration des méthodes d’authentification*

Pour autoriser le trafic RADIUS via le pare-feu Windows, sur une invite de commande :

| netsh advfirewall firewall add rule name="Allow RADIUS Auth" dir=in action=allow protocol=UDP localport=1812  netsh advfirewall firewall add rule name="Allow RADIUS Accounting" dir=in action=allow protocol=UDP localport=1813 |
| --- |

****

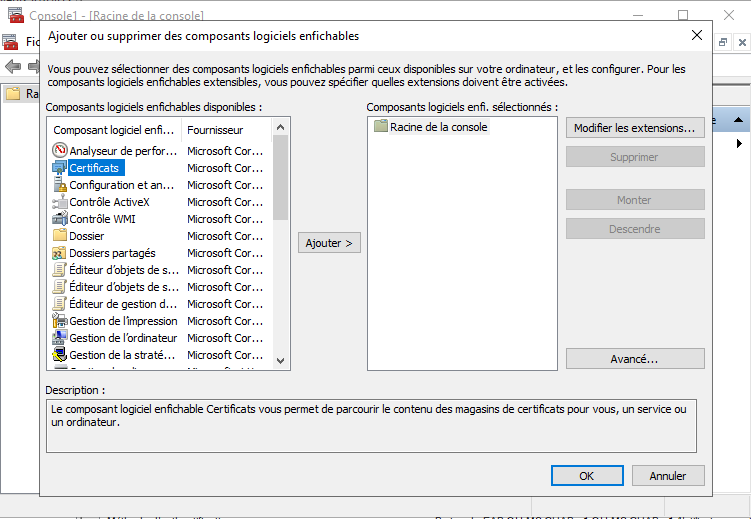
*Image 13 : Ajout des autorisations RADIUS*

#### Elles permettent :

* 1812 (Auth) : Autoriser les requêtes d’authentification RADIUS entrantes.
* 1813 (Accounting) : Autoriser les messages de comptabilité RADIUS (journalisation des connexions, etc.).

Enfin, pour ajouter un Certificats, aller dans “Ajouter ou supprimer des composants logiciels enfichables”.

* Ouvrir la console MMC (Microsoft Management Console).
* Cliquer sur Fichier puis Ajouter/Supprimer un composant logiciel enfichable.
* Dans la liste des composants, sélectionner “Certificats”, puis cliquer sur Ajouter

****

*Image 14 : Ajout des certificats*

**Mise en place d’une GPO pour activer le SSO sur les clients**