

# Procédure Borne Wifi et Activation RADIUS

## Procédure RDS

### ASSURMER

Montpellier, Occitanie, France

Ezequiel VARELA-MONTEIRO

Kévin BOULIER

SISR 2B



Version	Date version	Auteur	Validateur et date	Destinataires	Diffusion document	Nbr. de pages	Commentaires
2	25/11/24	BOULIER KEVIN	Aucun	Service DSI	Interne via Teams	29	Document entier



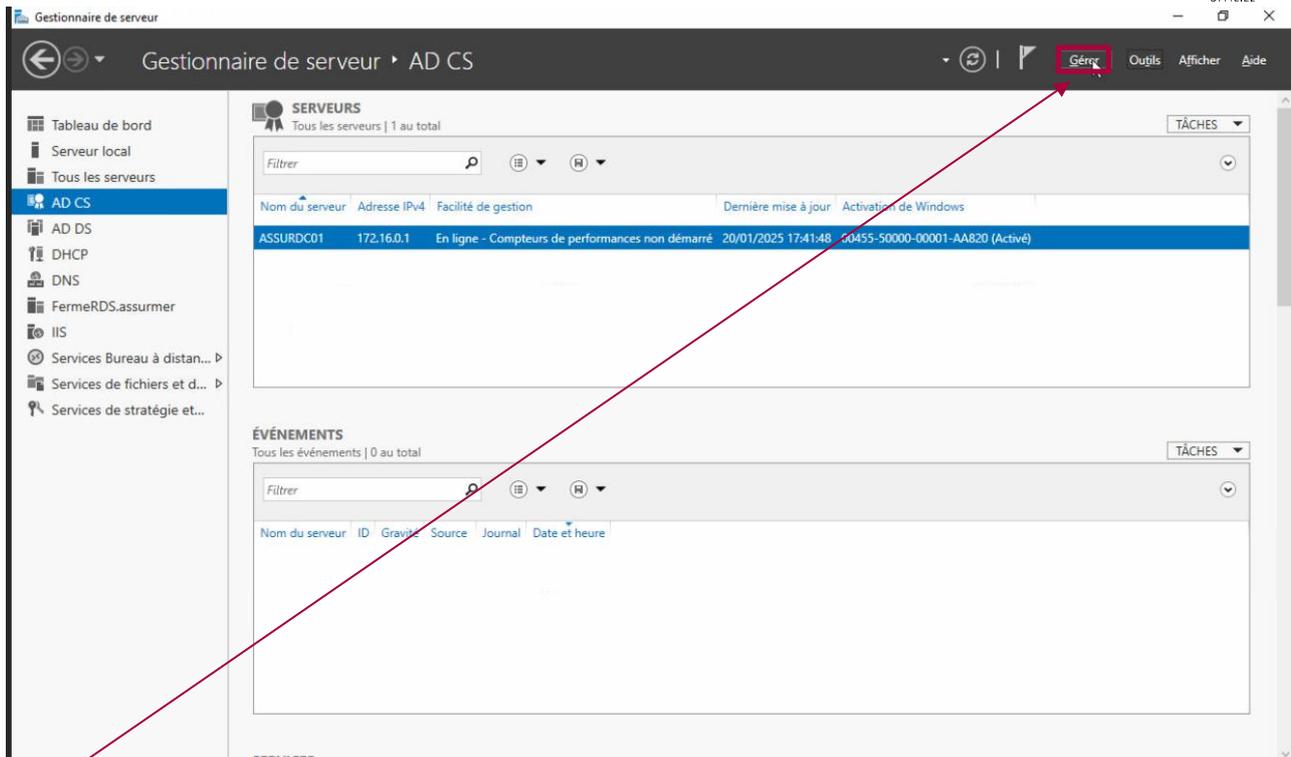
## Table des matières

Introduction.....	3
Début de la Procédure w .....	4

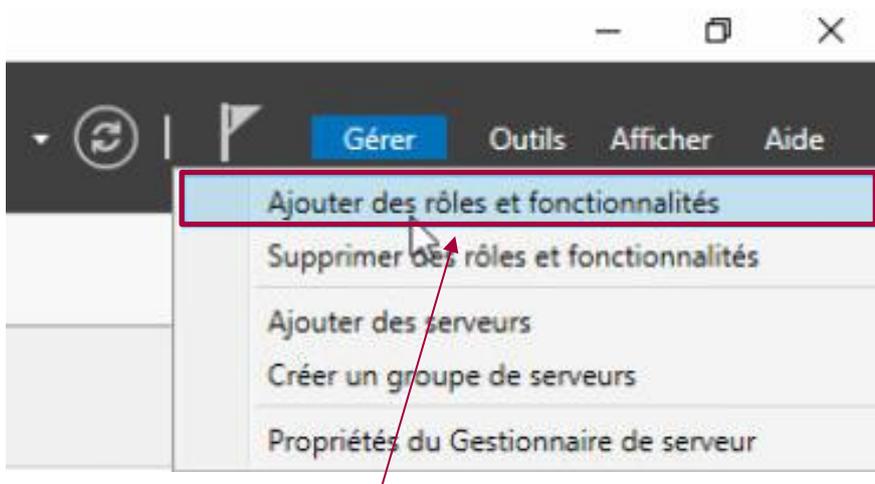
# Introduction

## *Présentation de Radius*

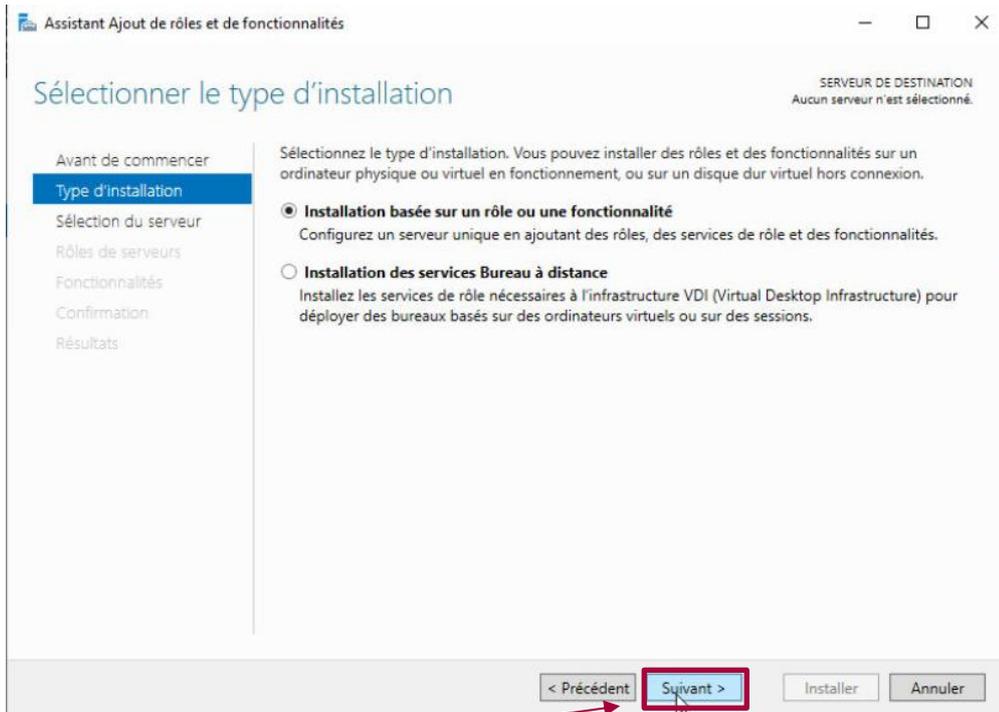
Un serveur RADIUS, NPS sous Windows agit comme une « autorité centrale » d'authentification. Il reçoit les demandes d'authentification depuis des équipements ici un point d'accès Wi-Fi et prend la décision d'accepter ou de rejeter la connexion, en s'appuyant sur notre Active Directory.



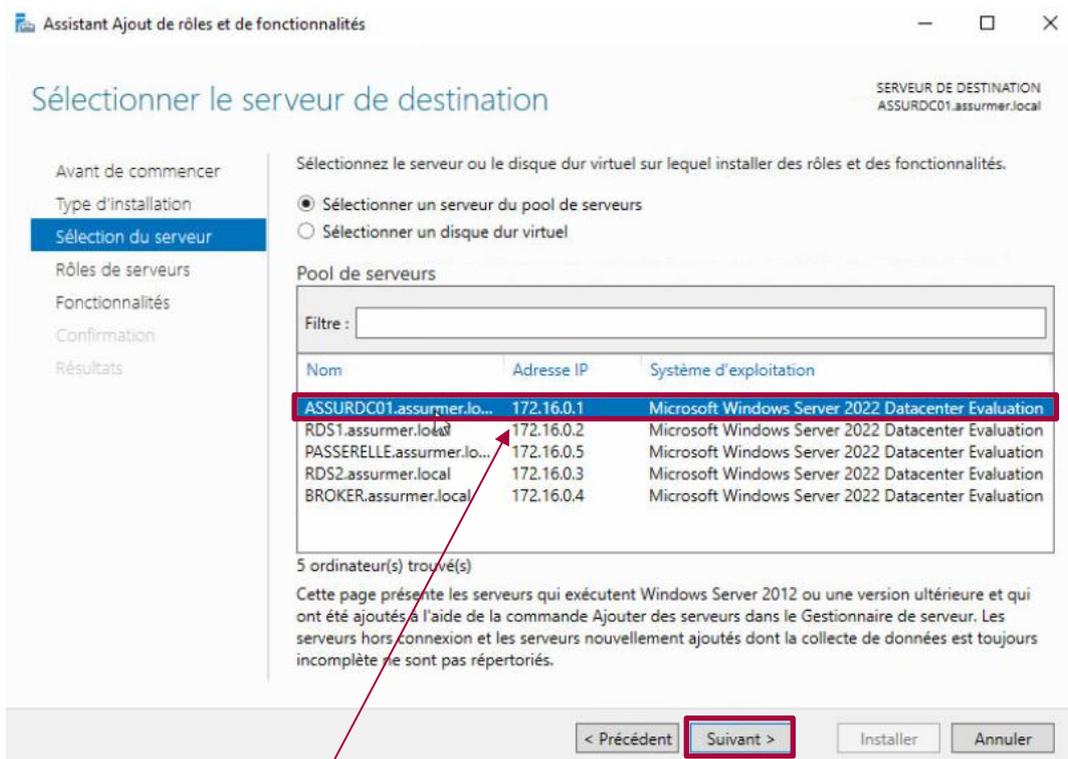
Pour commencer on va installer le service NPS sur notre serveur AD



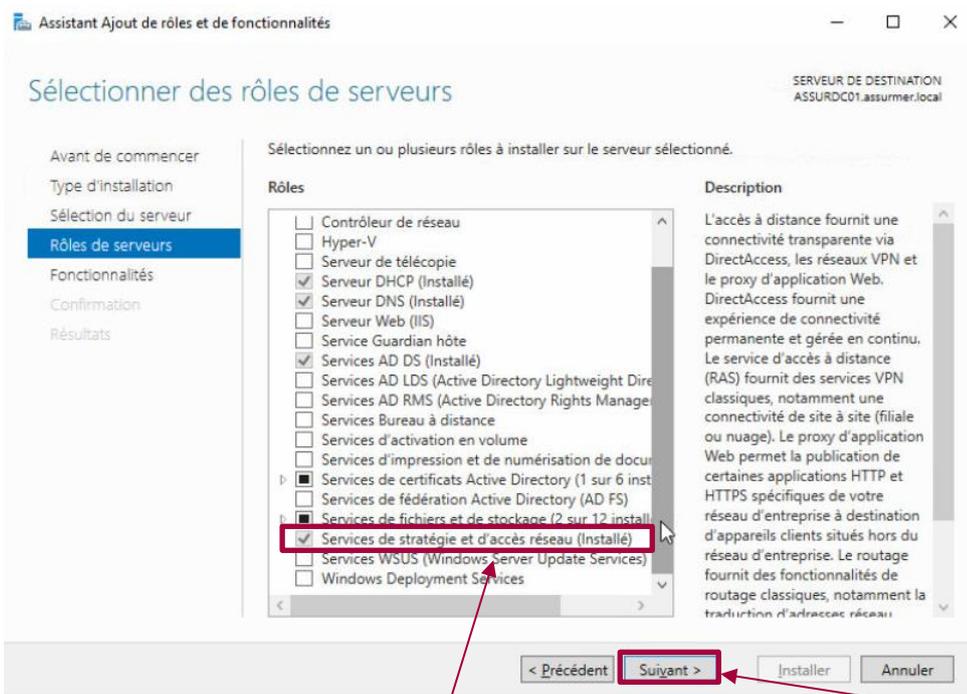
On va sur Ajouter des rôles et fonctionnalités



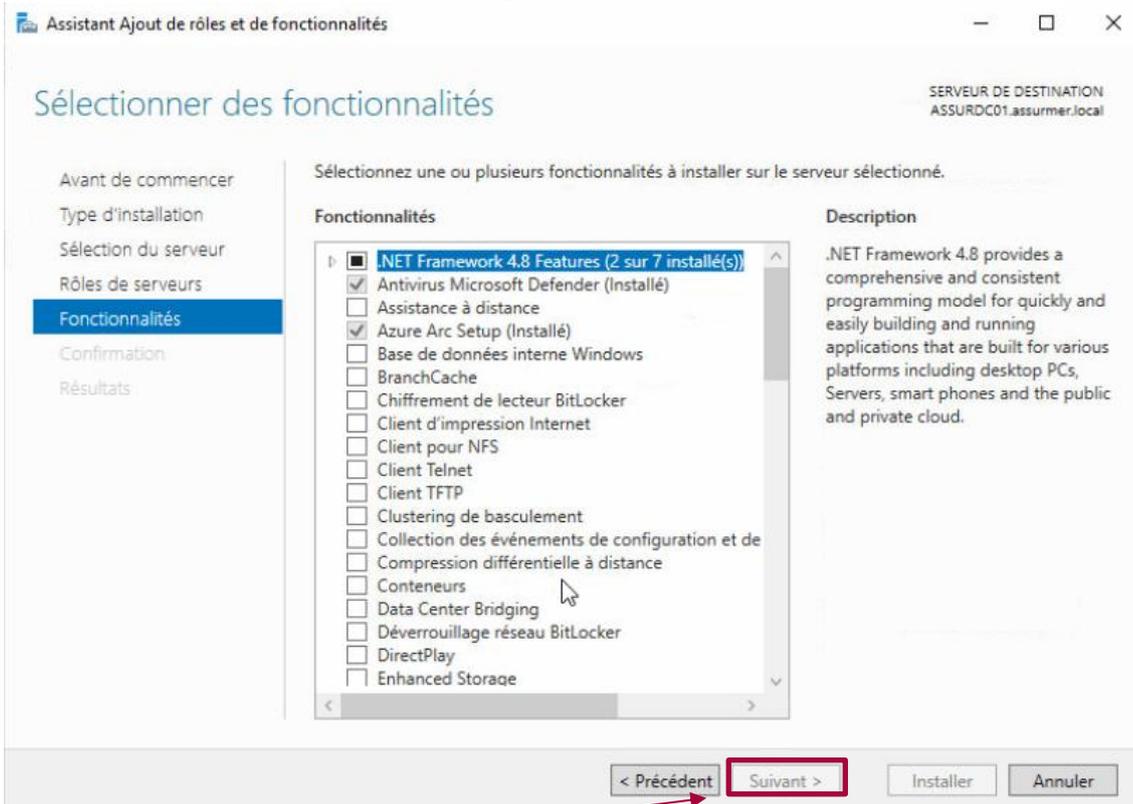
On fait suivant



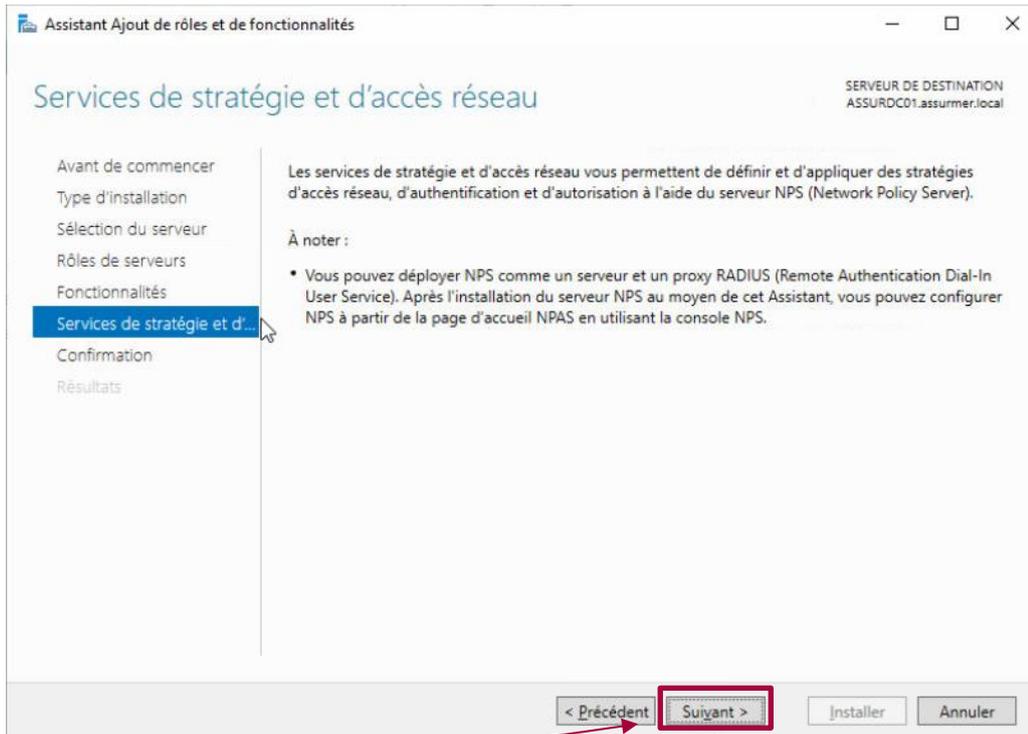
On va choisir notre server AD puis faire suivant



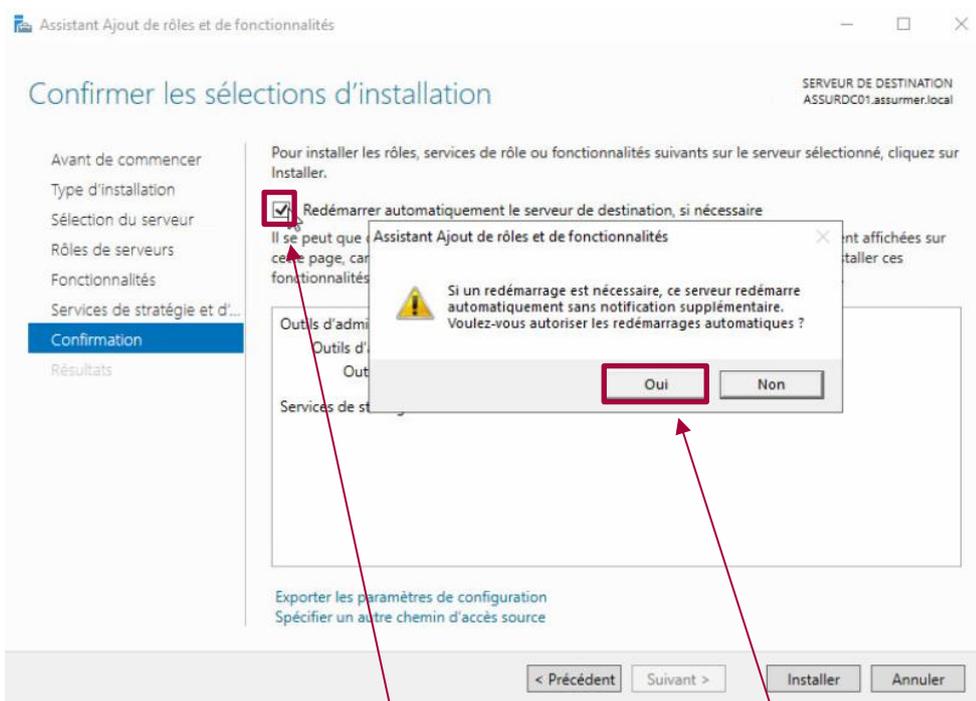
On va choisir le « Service de stratégie et d'accès réseau » puis on fait suivant



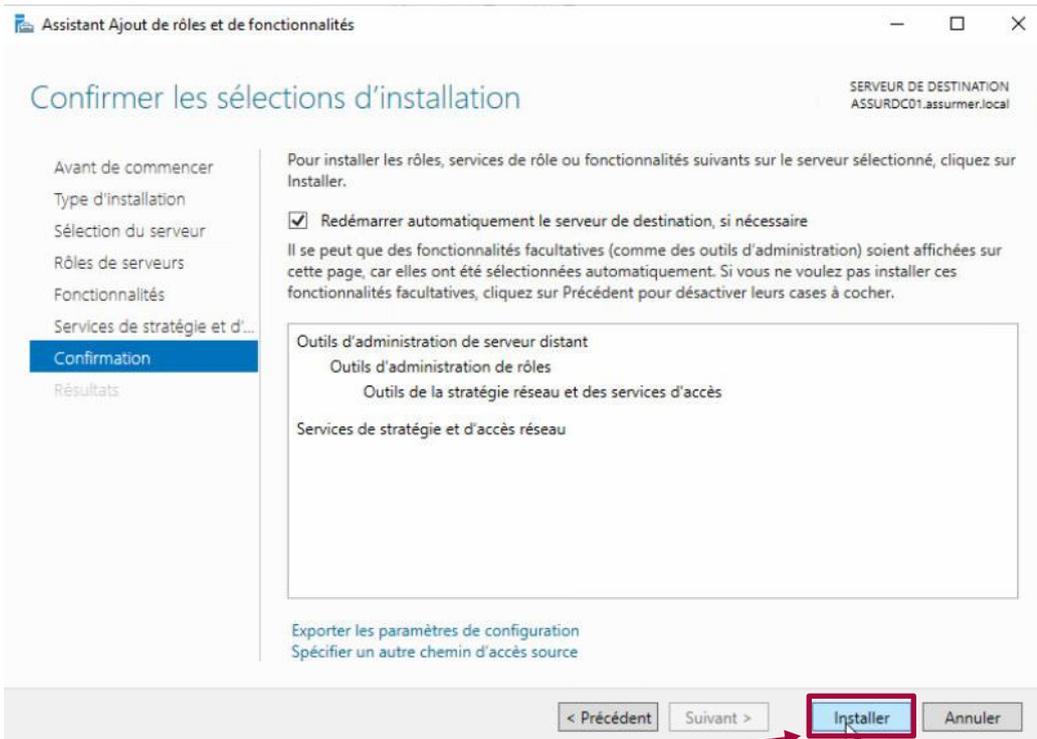
On fait Suivant



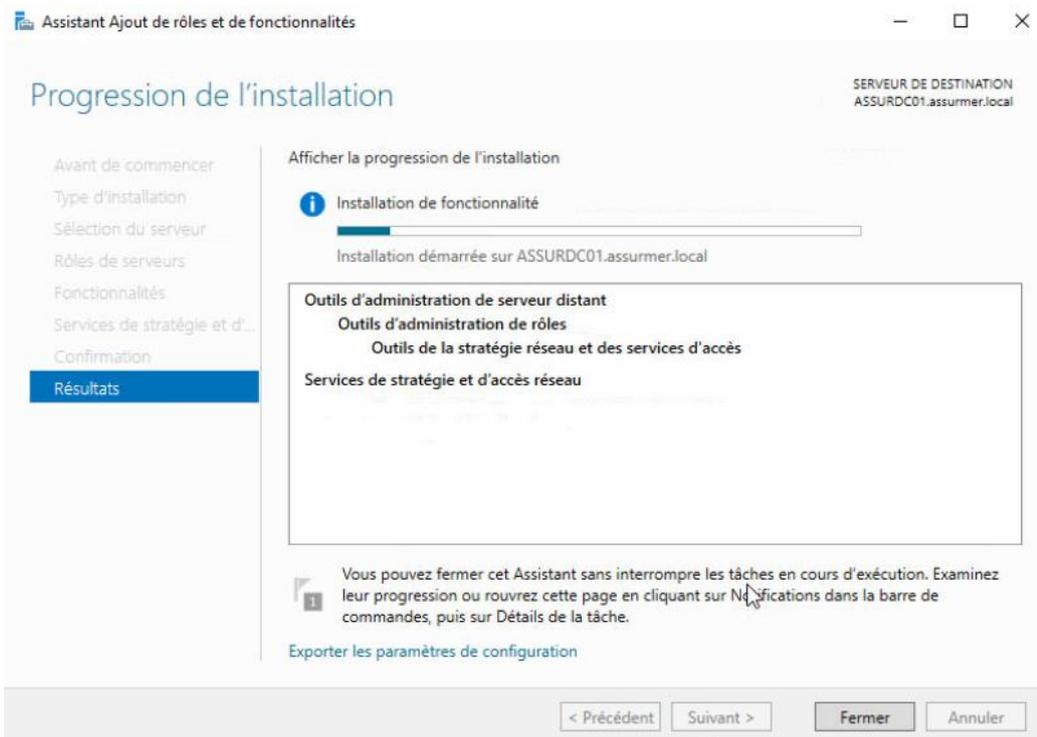
On fait Suivant

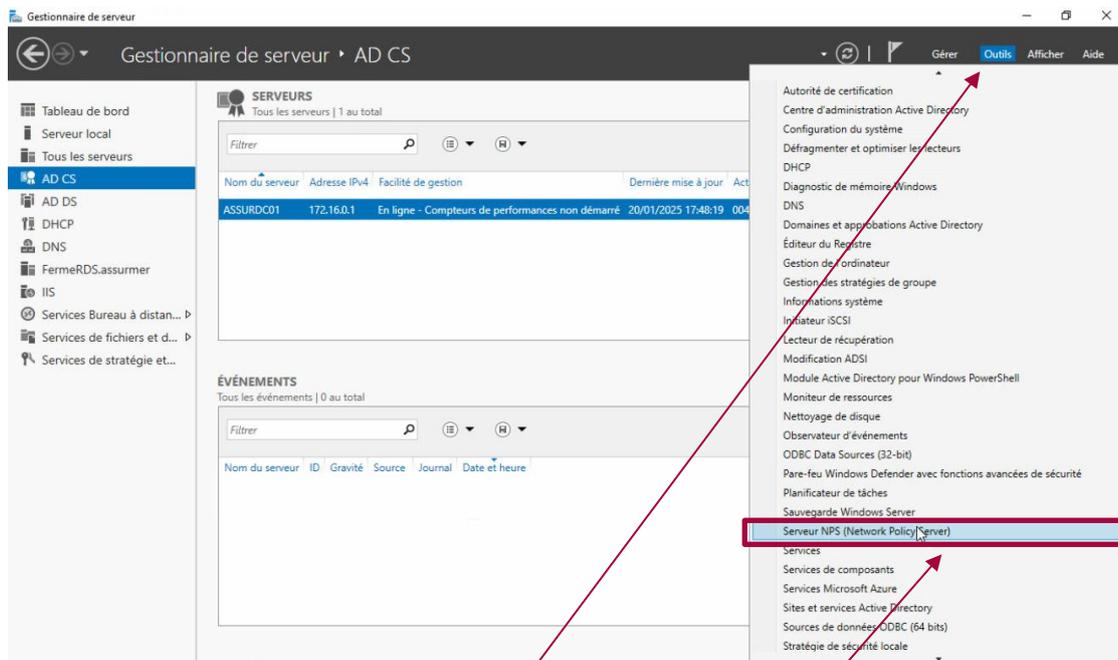


Dans la prochaine étape on check le redémarrage automatique

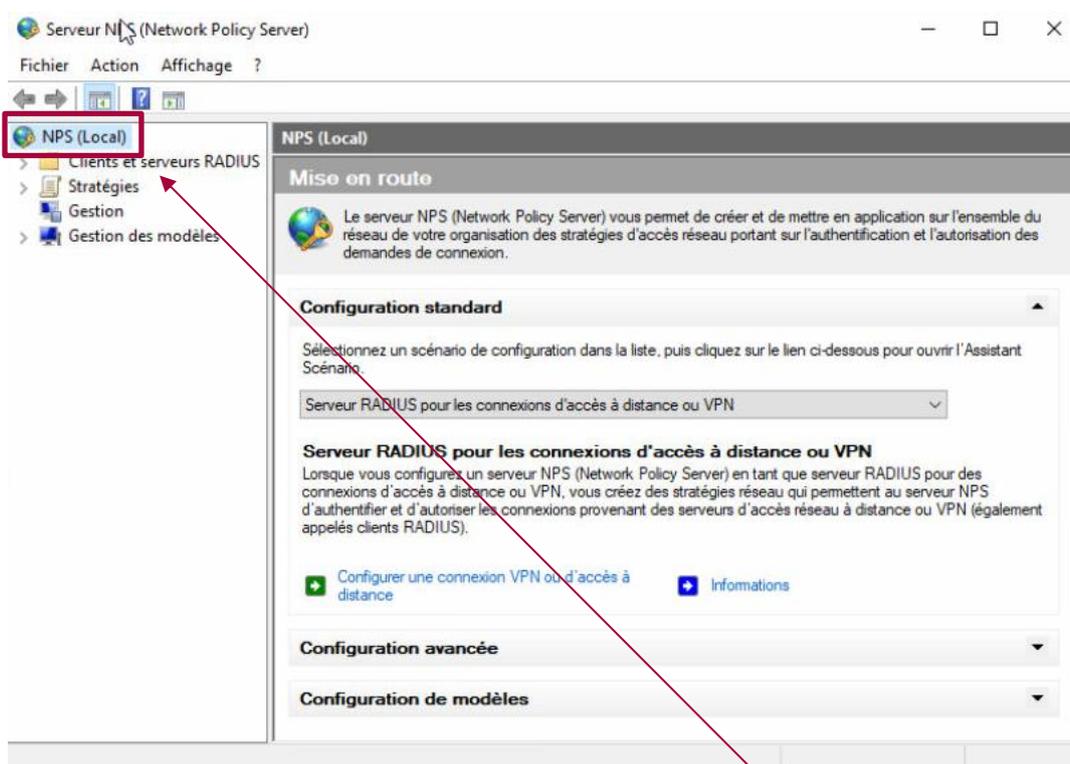


## Enfin on fait installer

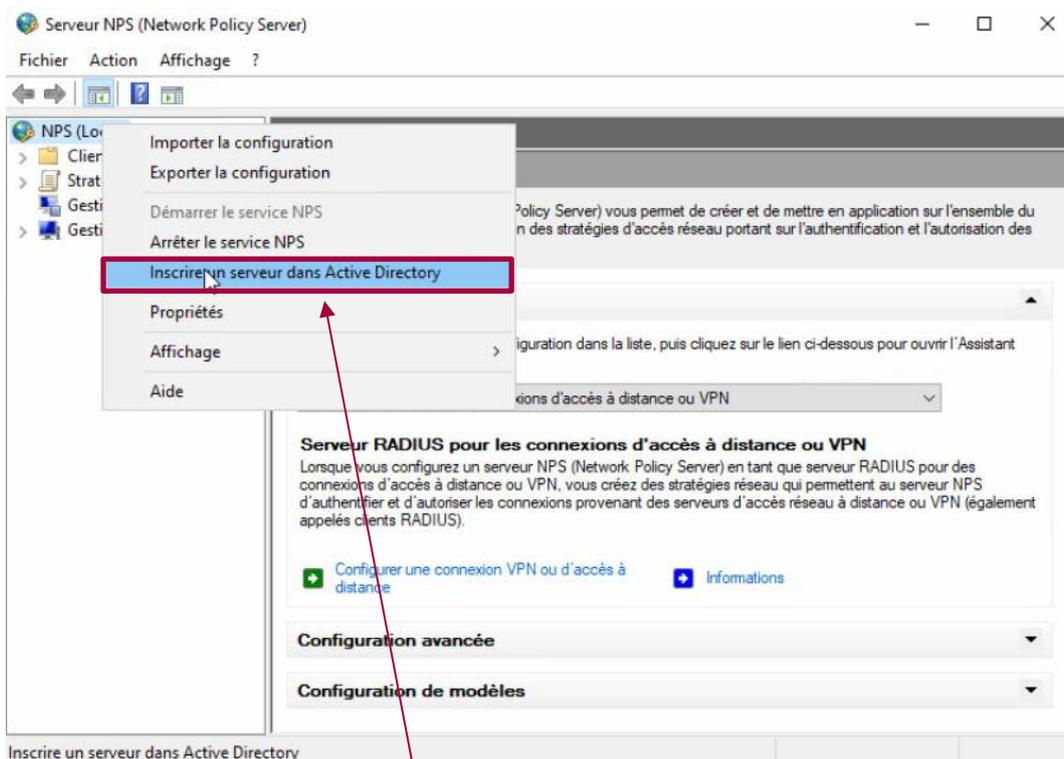




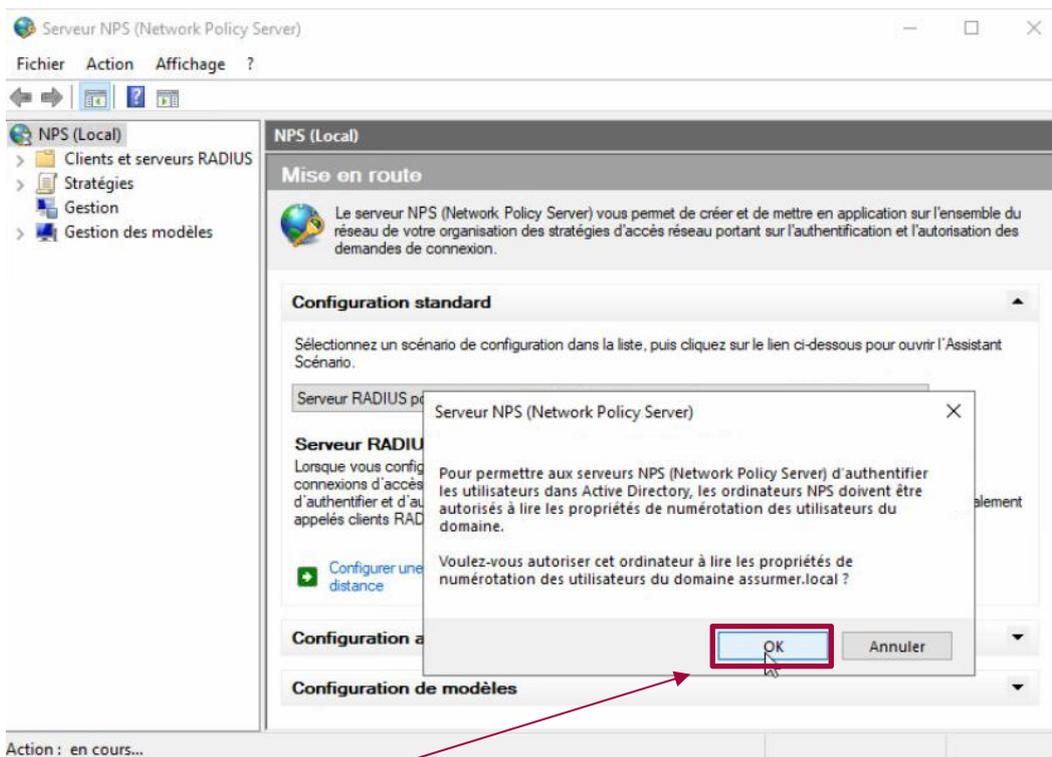
On retourne dans notre gestionnaire de serveur et on va chercher notre service NPS



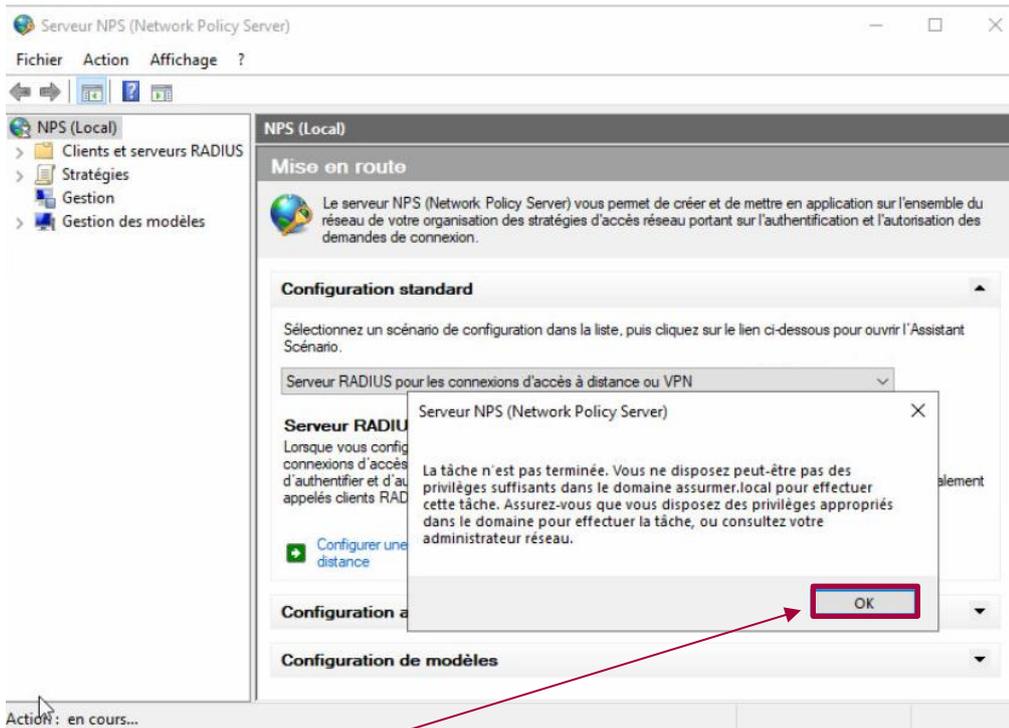
Dans la nouvelle fenêtre on va faire un click droit sur NPS local



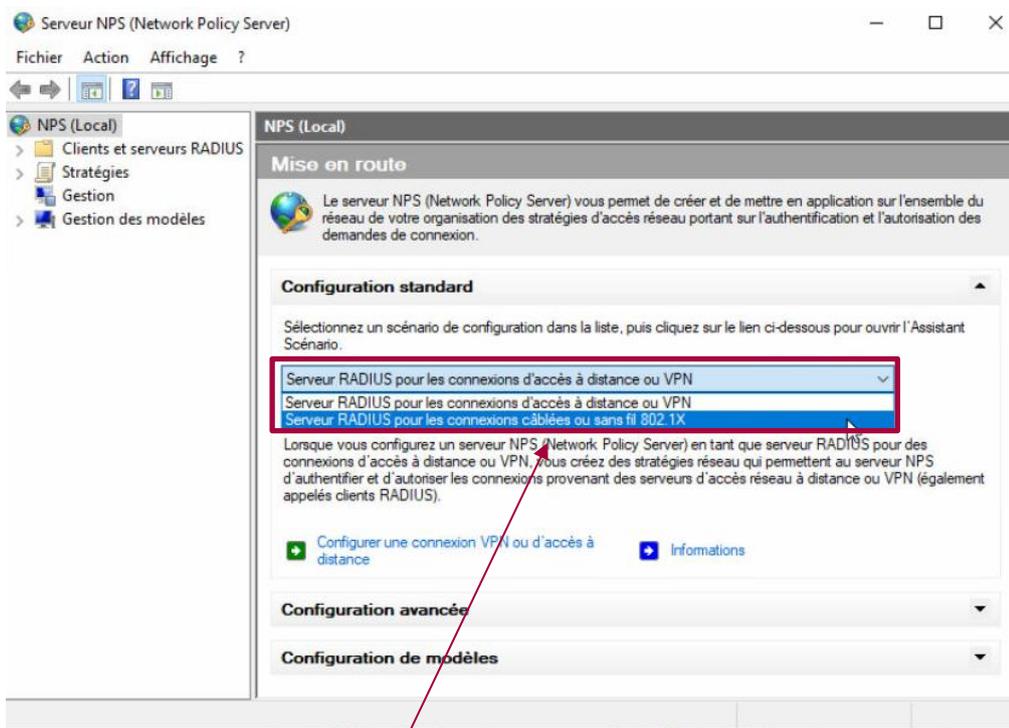
On va inscrire notre serveur dans l'AD



On clique sur Ok



On clique sur Ok



On va choisir les connexions sans fils 802.1x

Configurer 802.1X

### Sélectionner le type de connexions 802.1X

**Type de connexions 802.1X :**

Connexions sans fil sécurisées  
Lorsque vous déployez des points d'accès sans fil 802.1X sur votre réseau, le serveur NPS (Network Policy Server) peut authentifier et autoriser les demandes de connexion effectuées par les clients sans fil qui se connectent via ces points d'accès.

Connexions câblées (Ethernet) sécurisées  
Lorsque vous déployez des commutateurs d'authentification 802.1X sur votre réseau, le serveur NPS (Network Policy Server) peut authentifier et autoriser les demandes de connexion effectuées par les clients Ethernet qui se connectent via ces commutateurs.

**Nom :**  
Ce texte par défaut est utilisé pour composer le nom de chacune des stratégies créées à l'aide de cet Assistant. Vous pouvez vous servir du texte par défaut ou le modifier.

ASSWIFI

Précédent Suivant Terminer Annuler

On va choisir la connexion sans fils, choisir un Nom et enfin cliquer sur Suivant

Configurer 802.1X

### Spécifier les commutateurs 802.1X

Spécifiez les commutateurs ou points d'accès sans fil 802.1X (clients RADIUS)

Les clients RADIUS sont des serveurs d'accès réseau, à l'image des commutateurs d'authentification et des points d'accès sans fil. Les clients RADIUS ne sont pas des ordinateurs clients.

Pour spécifier un client RADIUS, cliquez sur Ajouter.

**Clients RADIUS :**

Ajouter...  
Modifier...  
Supprimer

Précédent Suivant Terminer Annuler

Ensuite on clique sur Ajouter

Propriétés de ASSDC01

Paramètres

Sélectionner un modèle existant :

Nom et adresse

Nom convivial :  
ASSDC01

Adresse (IP ou DNS) :  
172.16.0.1

Secret partagé

Sélectionnez un modèle de secrets partagés existant :  
Aucun

Pour taper manuellement un secret partagé, cliquez sur Manuel. Pour générer automatiquement un secret partagé, cliquez sur Générer. Vous devez configurer le client RADIUS avec le même secret partagé entré ici. Les secrets partagés respectent la casse.

Manuel  Générer

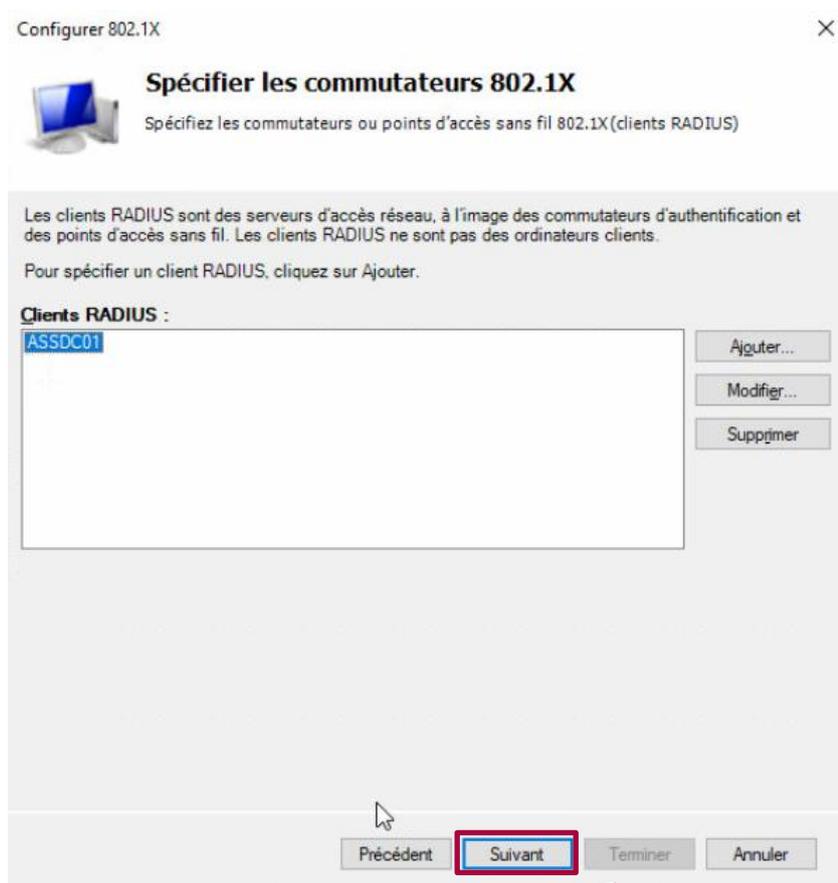
Secret partagé :  
●●●●●●●●

Confirmez le secret partagé :  
●●●●●●●●

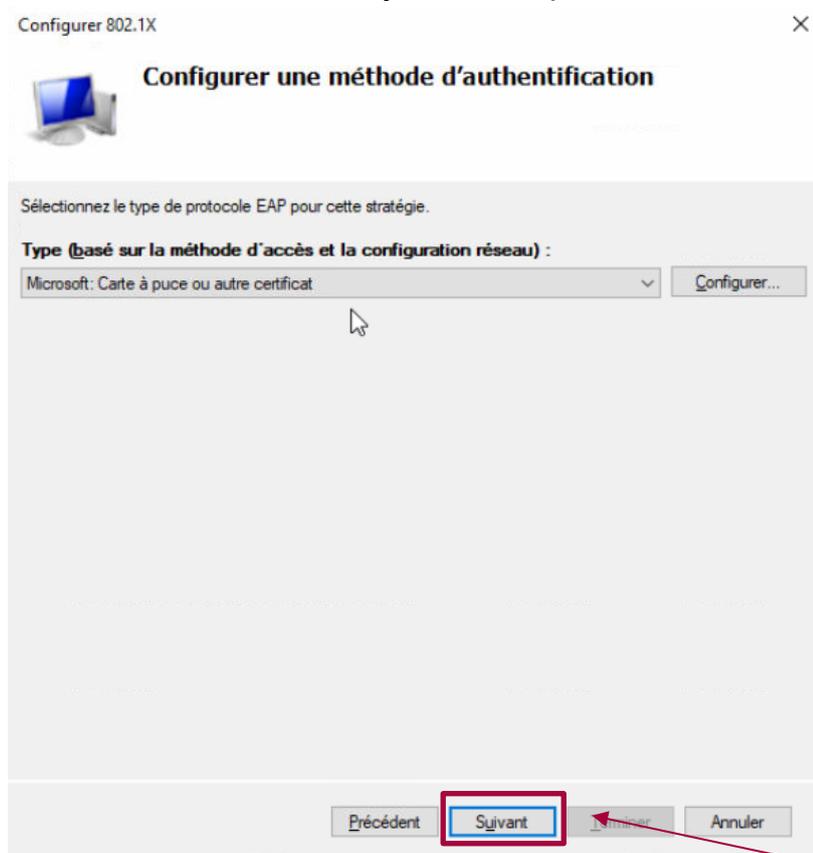
Dans cette fenêtre on doit remplir toutes les informations

Le nom convivial est le nom de notre server AD, on suit par son IP

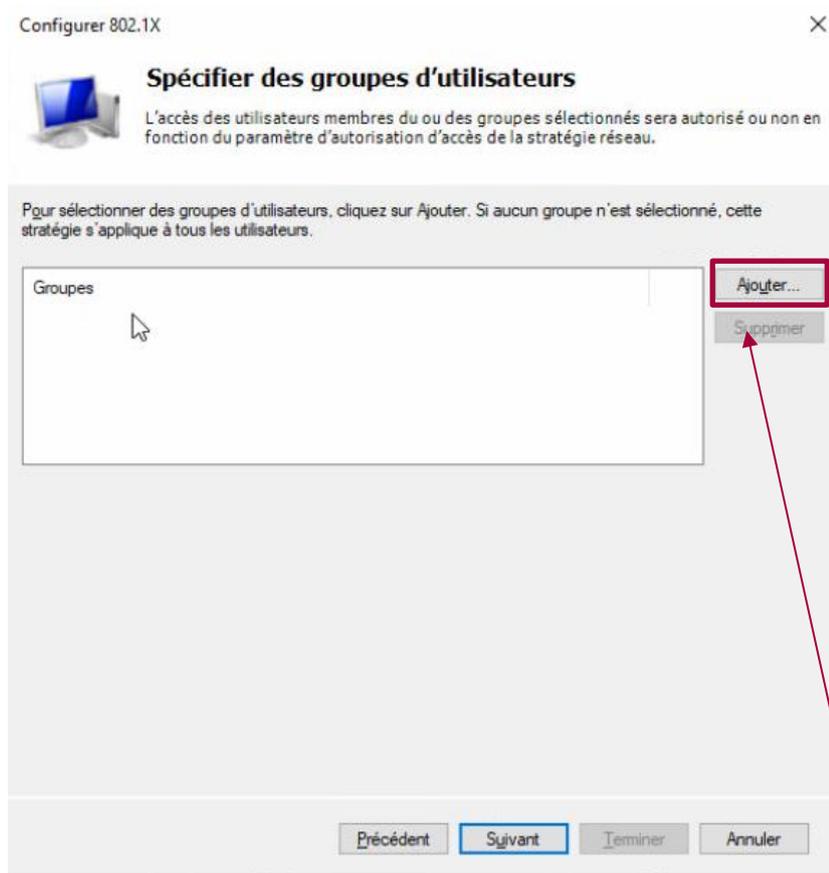
Enfin on met un MDP sécurise



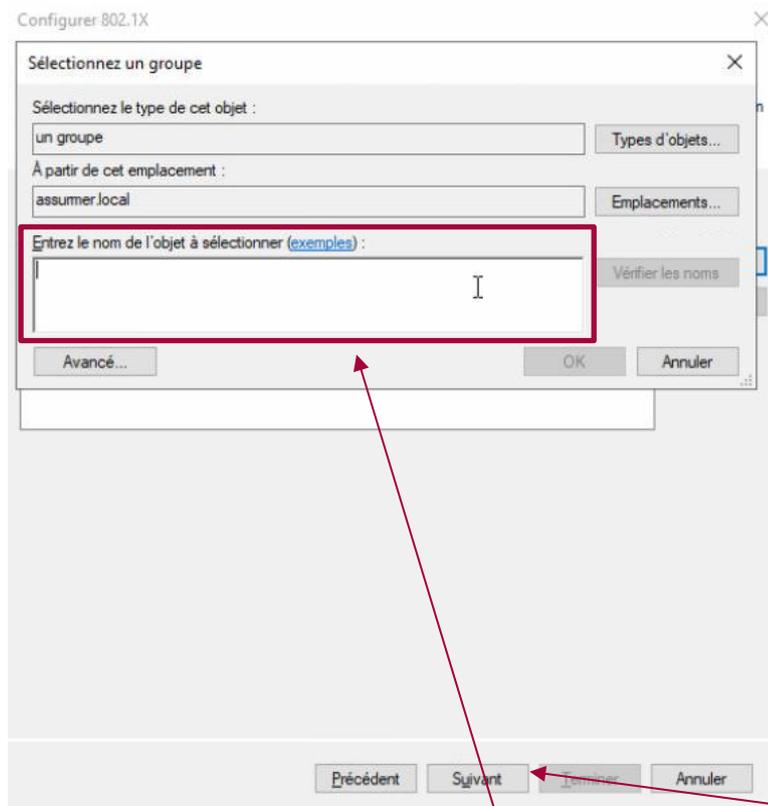
Notre server AD est bien ajoute on clique sur suivant



On clique sur suivant le certificat sera généré et géré dans une autre étape



Ici nous allons rajouter un groupe ou une OU qui aura les droits pour accéder au wifi



On doit taper le nom exact de l'OU ou du groupe et on fait suivant

Configurer 802.1X



## Spécifier des groupes d'utilisateurs

L'accès des utilisateurs membres du ou des groupes sélectionnés sera autorisé ou non en fonction du paramètre d'autorisation d'accès de la stratégie réseau.

Pour sélectionner des groupes d'utilisateurs, cliquez sur Ajouter. Si aucun groupe n'est sélectionné, cette stratégie s'applique à tous les utilisateurs.

Groupes

ASSURMER\Wifi-user

Ajouter...

Supprimer

Précédent

Suivant

Terminer

Annuler

On fait suivant

Configurer 802.1X ✕

## Configurer les contrôles du trafic

Utilisez des réseaux locaux virtuels (VLAN) et des listes de contrôle d'accès (ACL) pour contrôler le trafic réseau.

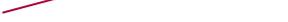
Si vos clients RADIUS (commutateurs d'authentification et points d'accès sans fil) prennent en charge l'affectation de contrôles de trafic à l'aide d'attributs de tunnel RADIUS, vous pouvez configurer ces attributs ici. Si vous configurez ces attributs, le serveur NPS invite les clients RADIUS à appliquer ces paramètres pour les demandes de connexion authentifiées et autorisées.

Si vous n'utilisez pas de contrôles du trafic ou si vous souhaitez les configurer ultérieurement, cliquez sur Suivant.

### Configuration du contrôle du trafic

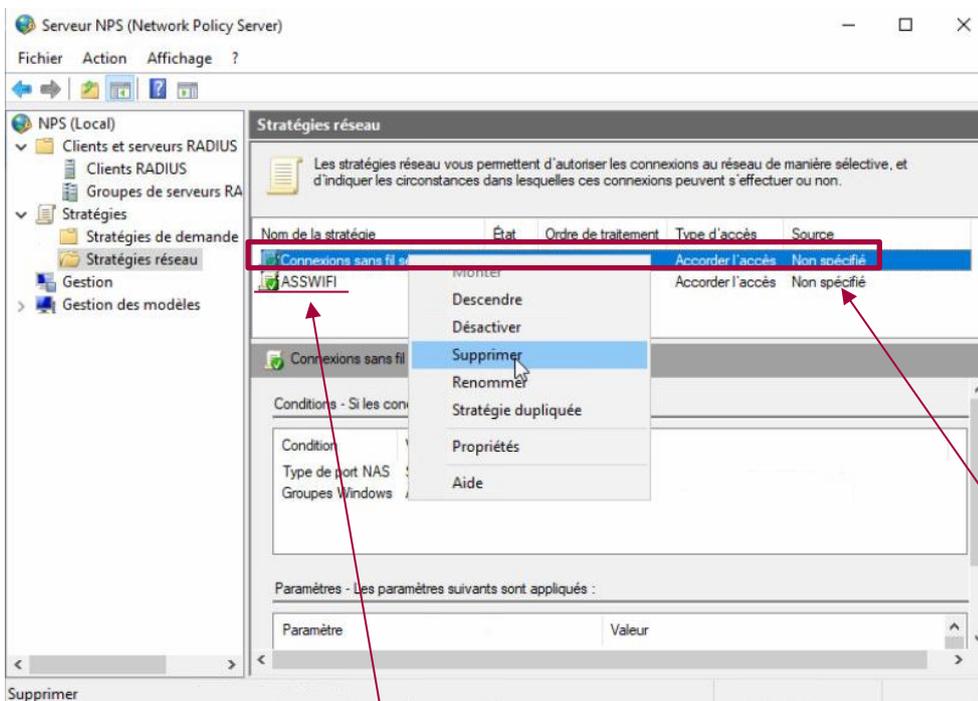
Pour configurer les attributs de contrôle du trafic, cliquez sur Configurer.

[Configurer...](#)[Précédent](#)[Suivant](#)[Terminer](#)[Annuler](#)

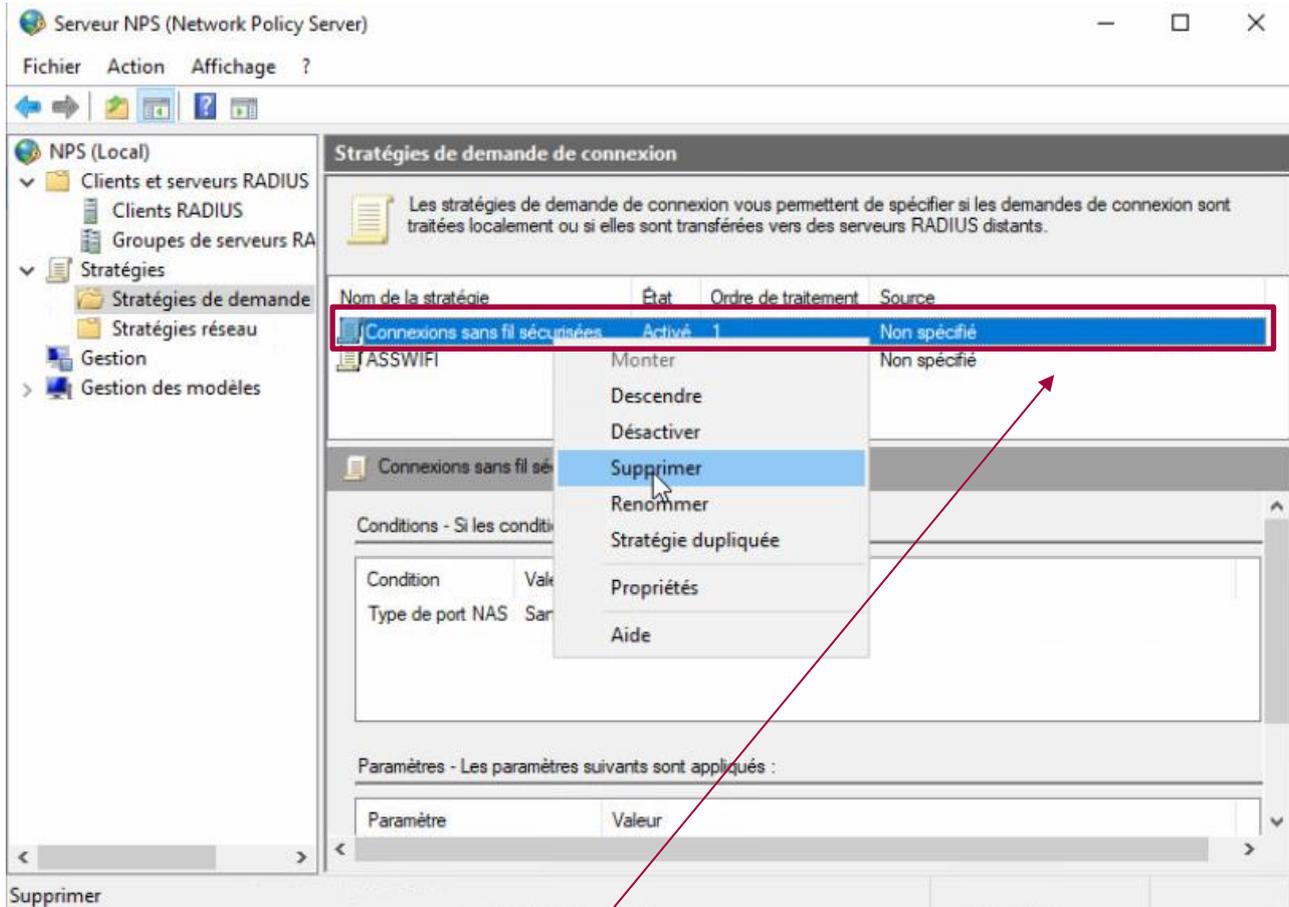
On clique sur suivant 



On fait Terminer



De retour sur l'interface NPS dans Stratégies réseau on vas supprimer le(s) Stratégie(s) qui n'ont pas le nom de notre stratégie



De même pour les Stratégie de demande