



# PROJET ASSURMER

2025

**AUTEURS :**

**DATE :**

DE CARVALHO LOPES Bruno  
BELAHA Sidahmed  
LE CLAINCHE Killian

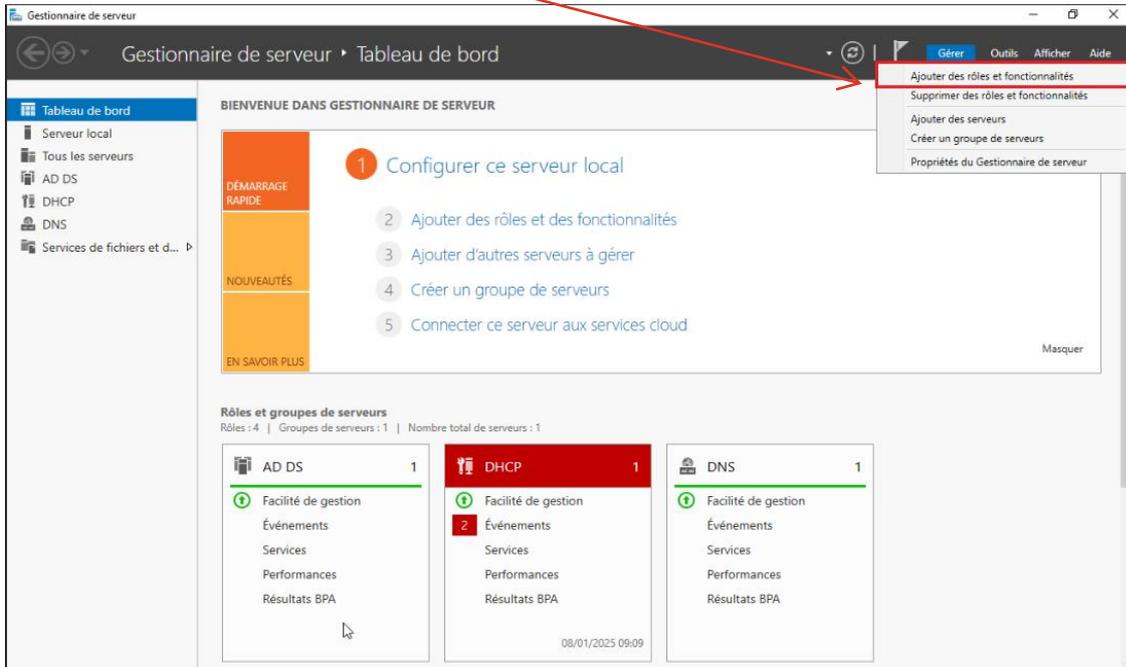
07/01/2025

## Sommaire

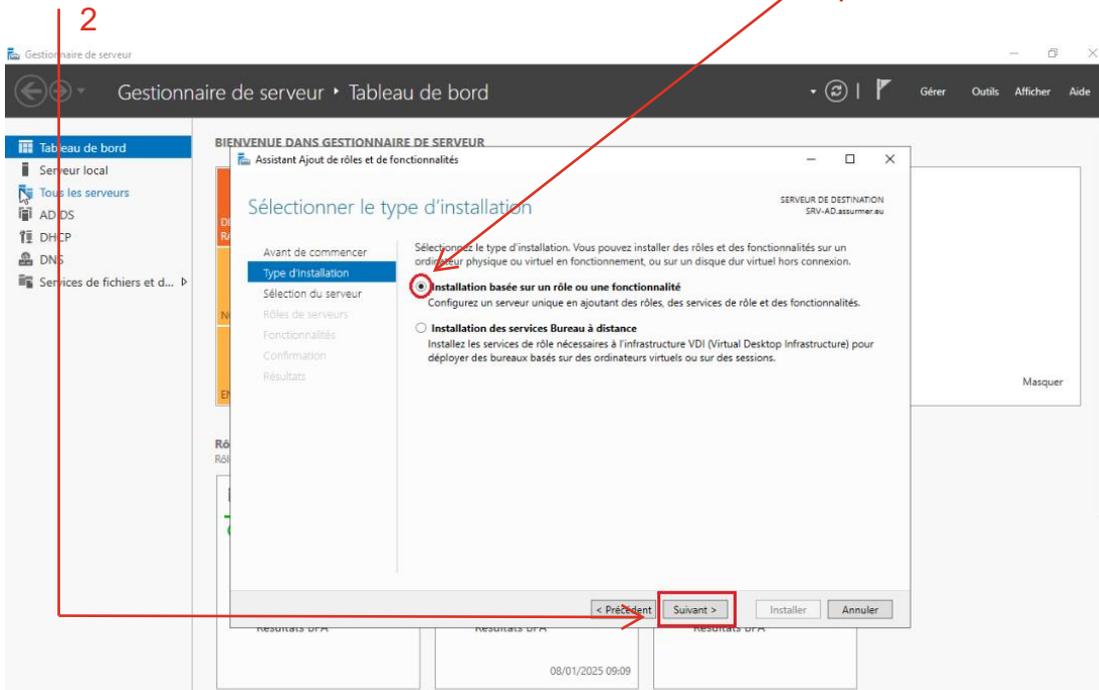
|      |   |    |
|------|---|----|
| I.   | Installation du serveur NPS .....                                   | 3  |
| II.  | Configuration du serveur RADIUS .....                               | 10 |
| III. | Installation du rôle requis pour l'autorité de certifications ..... | 16 |
| IV.  | Configuration du serveur RADIUS + Certificats .....                 | 22 |

## I. Installation du serveur NPS

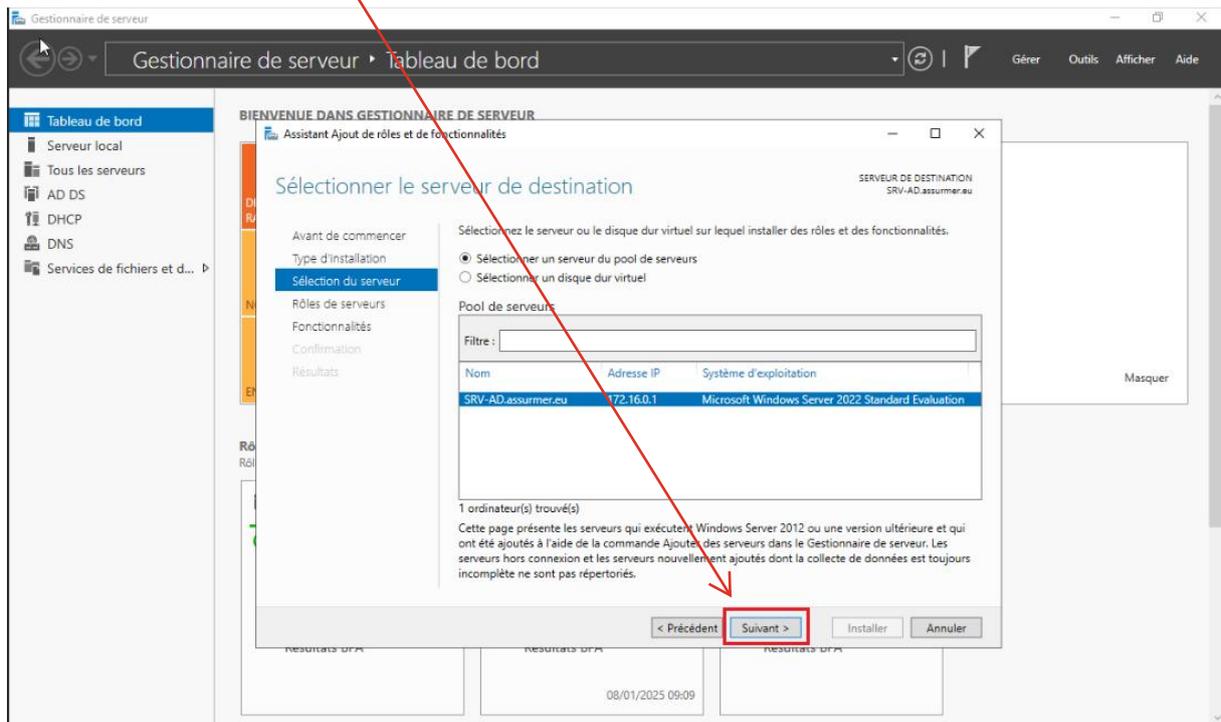
**Etape 1 :** Cliquez sur « ajouter des rôles et fonctionnalités » :



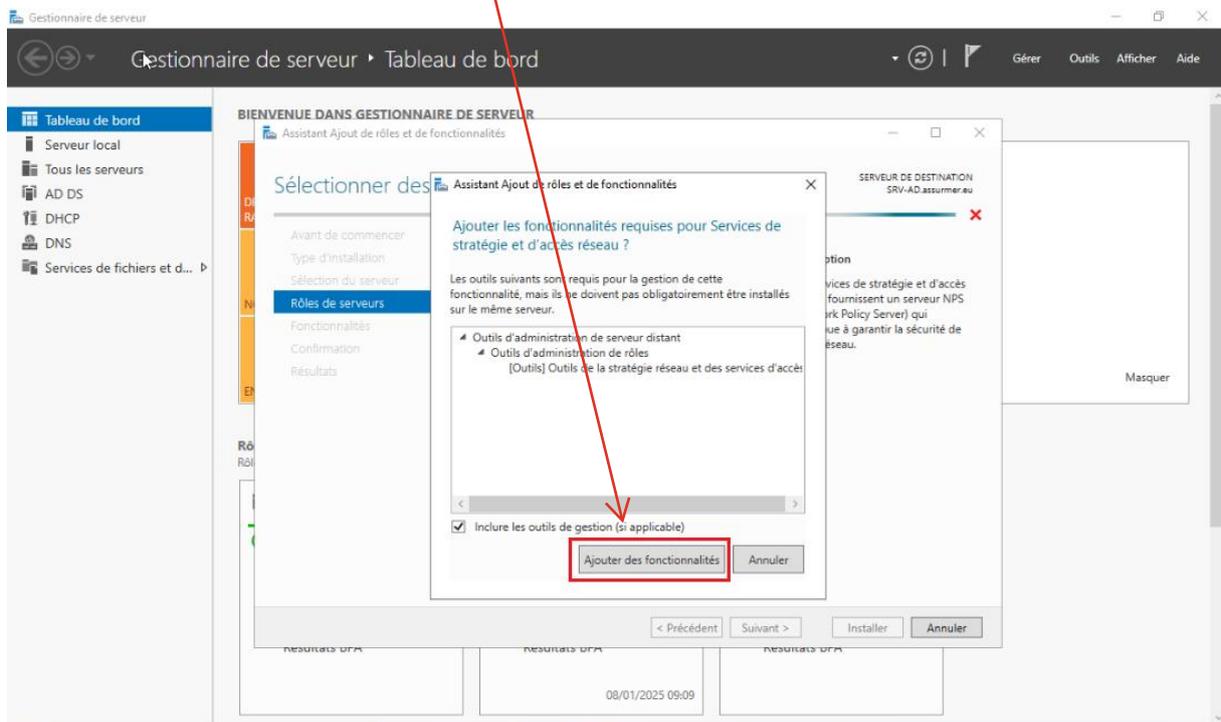
**Etape 2 :** Cochez « Installation basée sur un rôle ou une fonctionnalité », puis cliquez sur « Suivant »



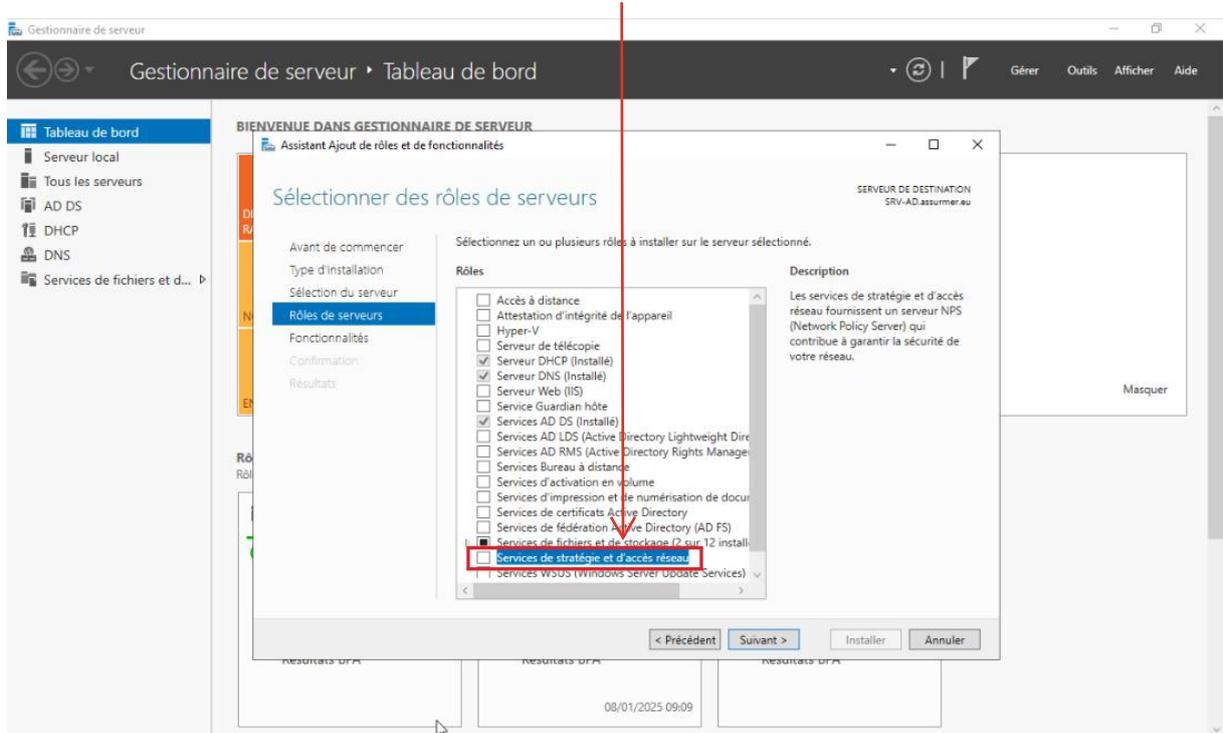
### Etape 3 : Cliquez sur « Suivant » :



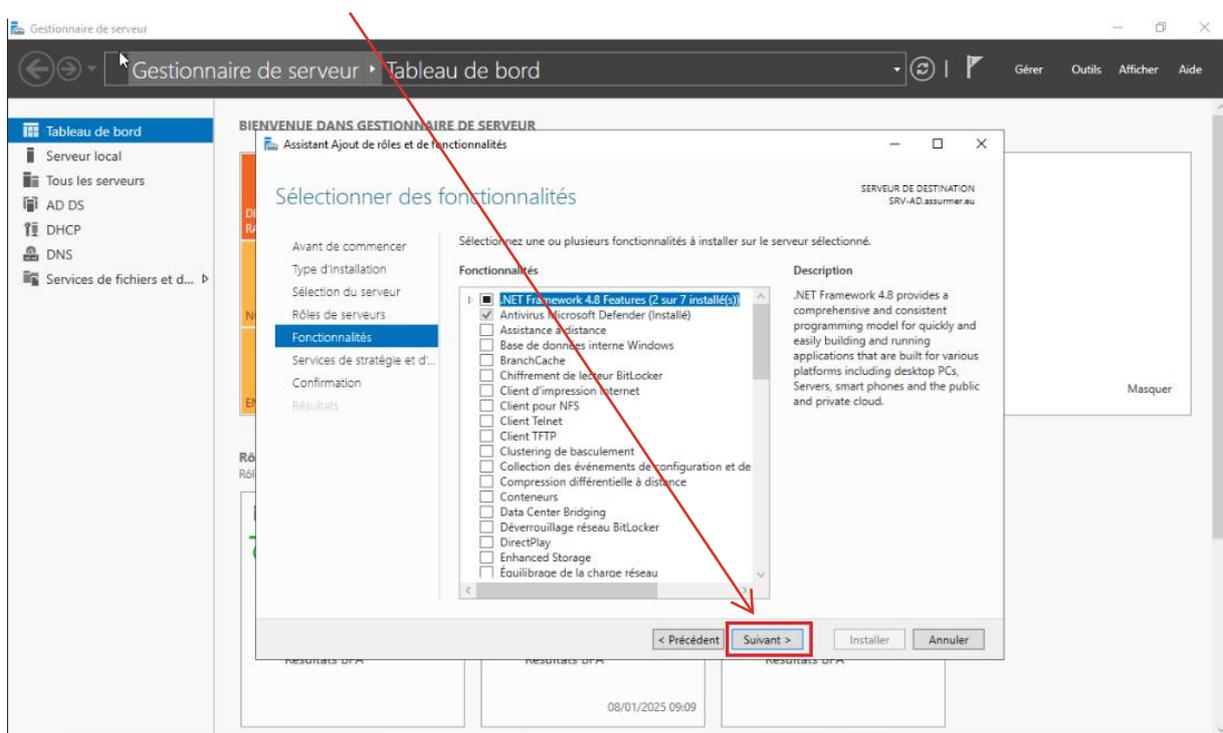
### Etape 4 : Cliquez sur « Ajouter des fonctionnalités » :



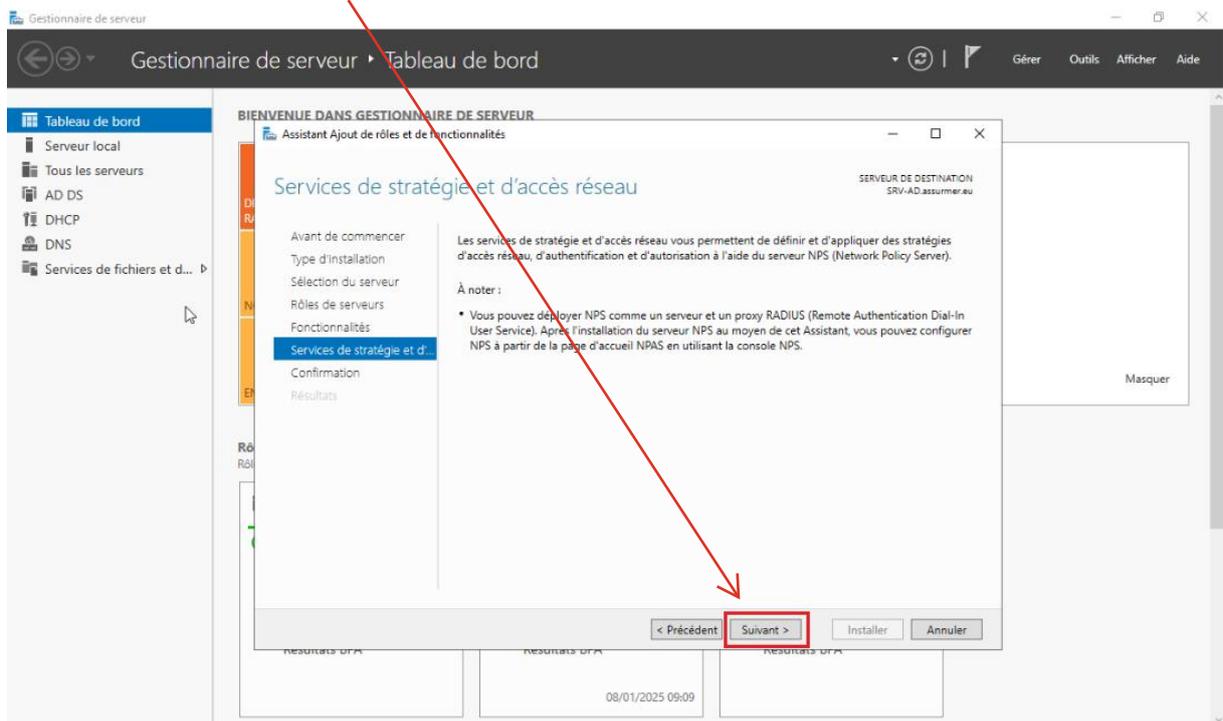
## Etape 5 : Cochez la case « Services de stratégie et d'accès réseau » :



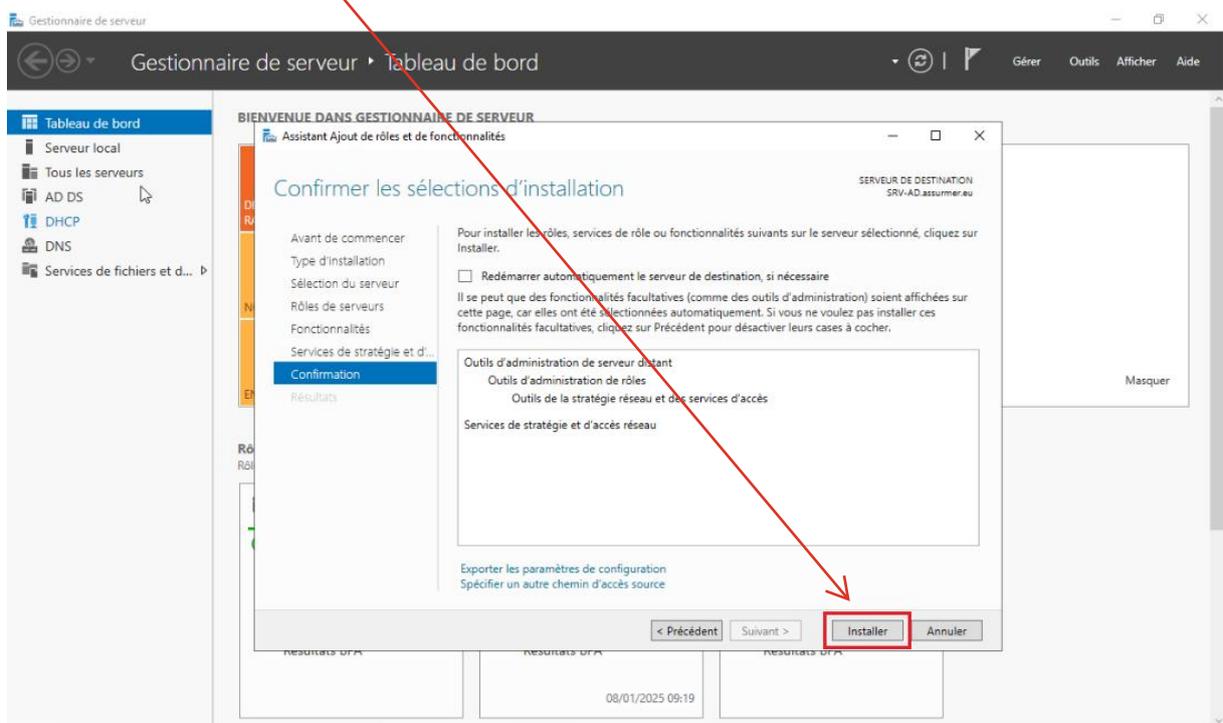
## Etape 6 : Cliquez sur « Suivant » :



## Etape 7 : Cliquez sur « Suivant » :

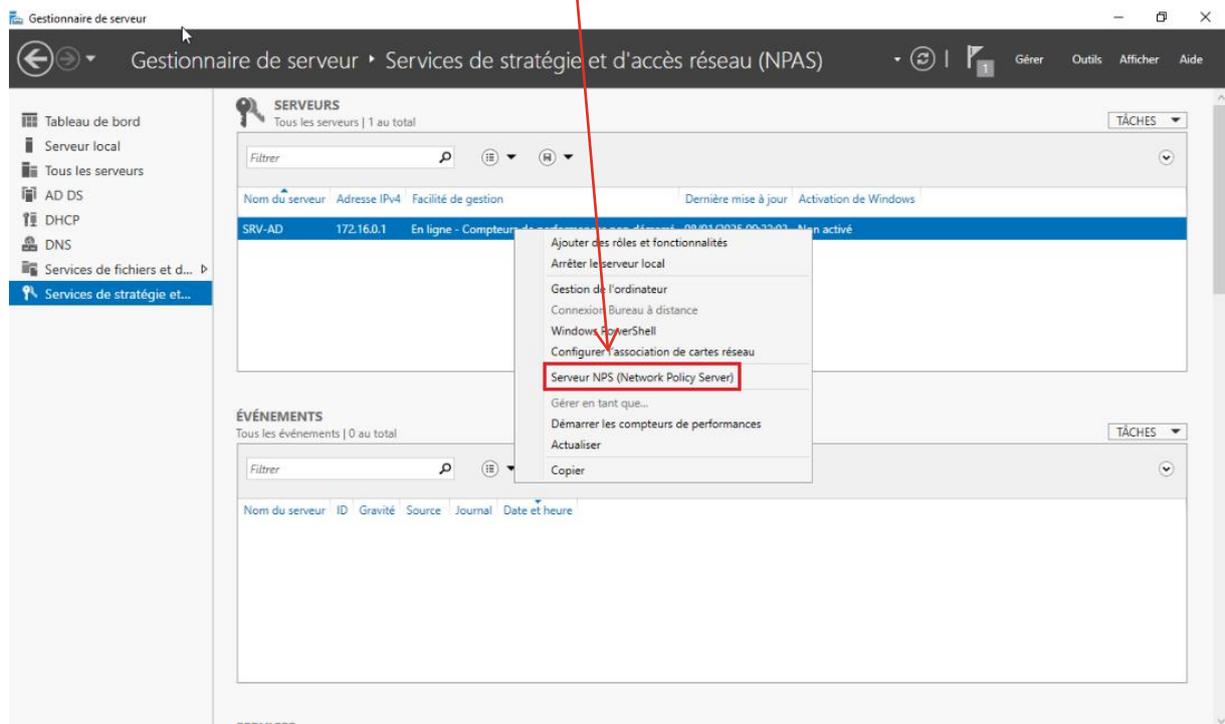


## Etape 8 : Cliquez sur « Suivant » :

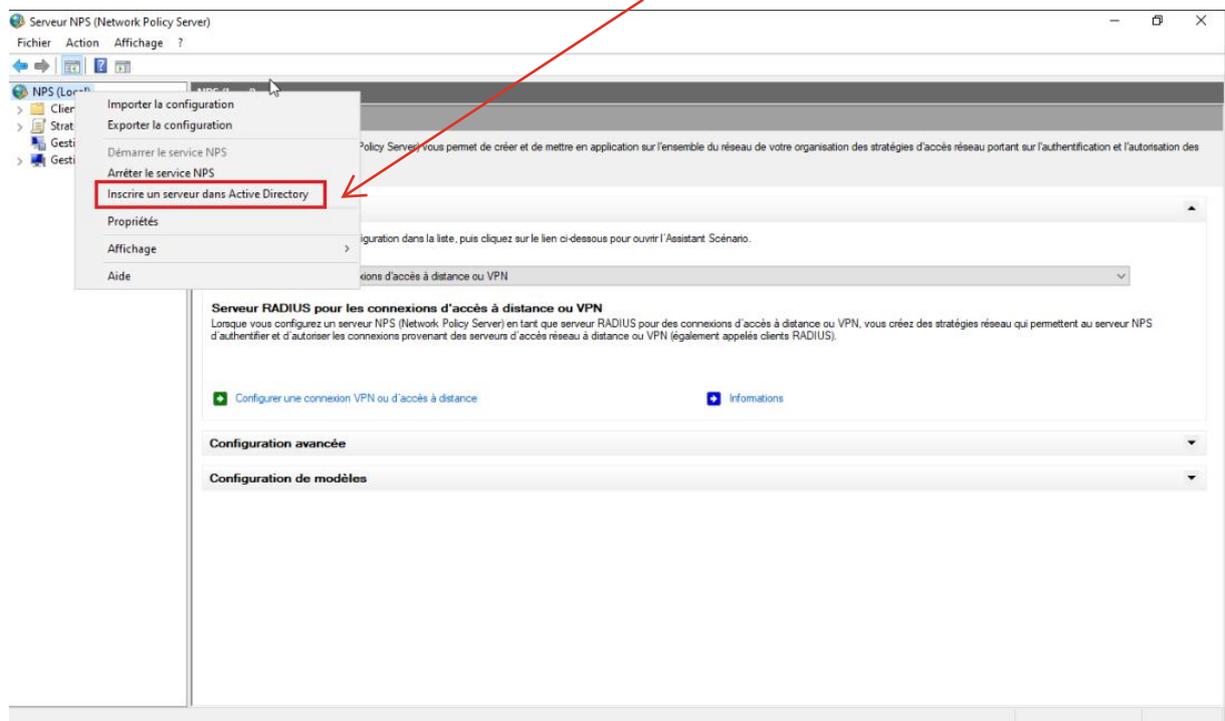




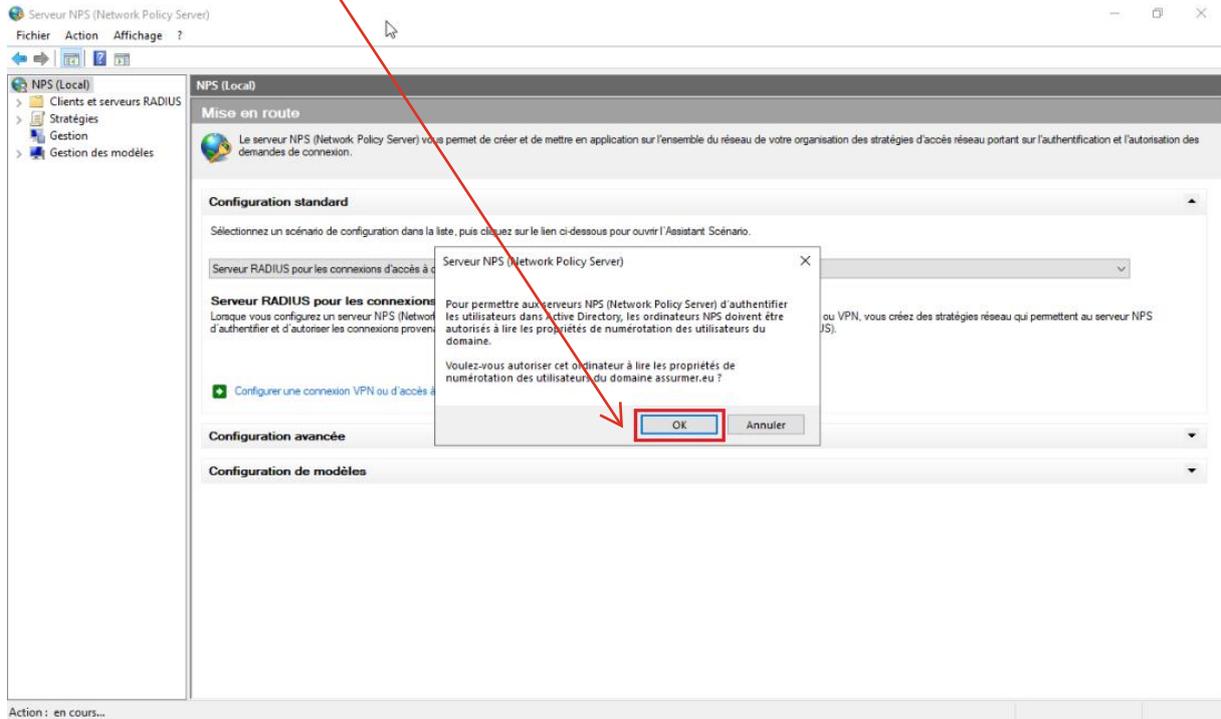
## Etape 11 : Cliquez sur « Serveur NPS (Network Policy Server) » :



## Etape 12 : Cliquez sur « Inscrire un serveur Active Directory » :

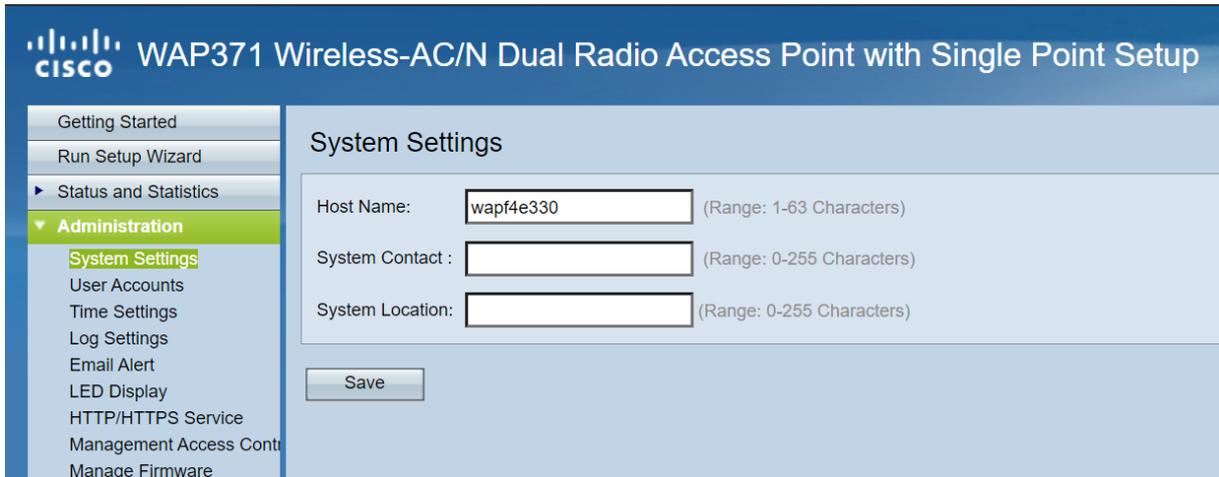


### Etape 13 : Cliquez sur « OK » :



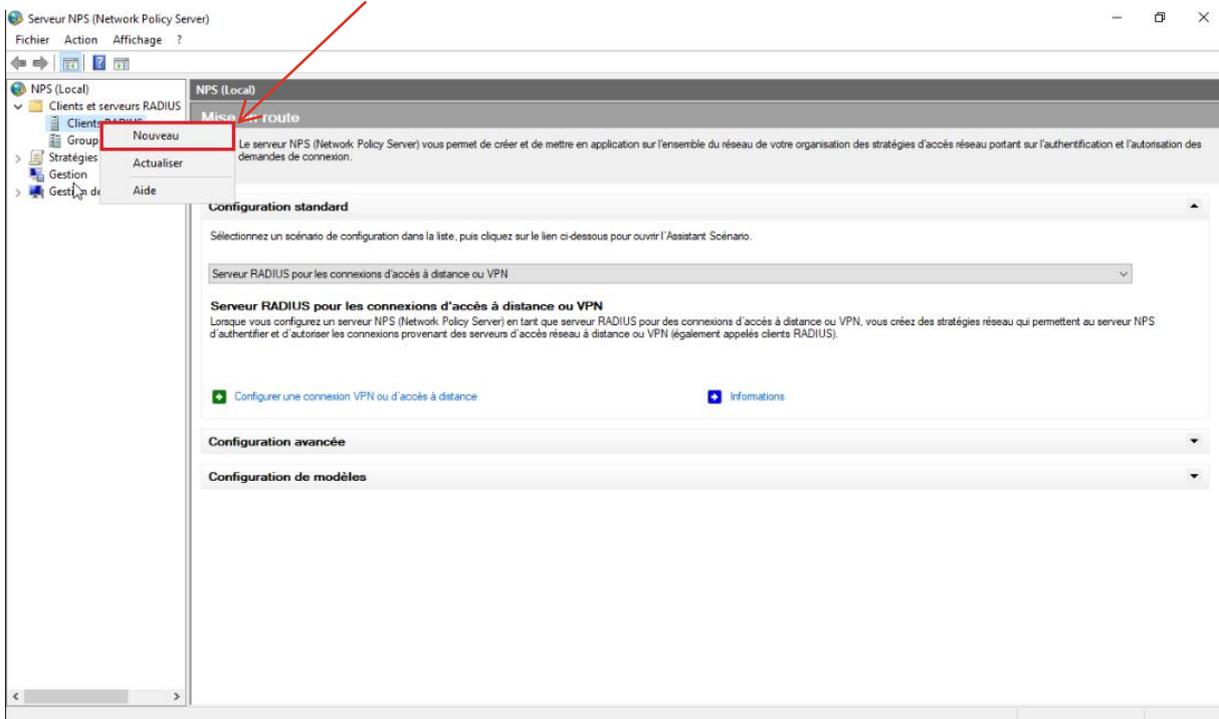
## II. Configuration du serveur RADIUS

### Etape 1 :



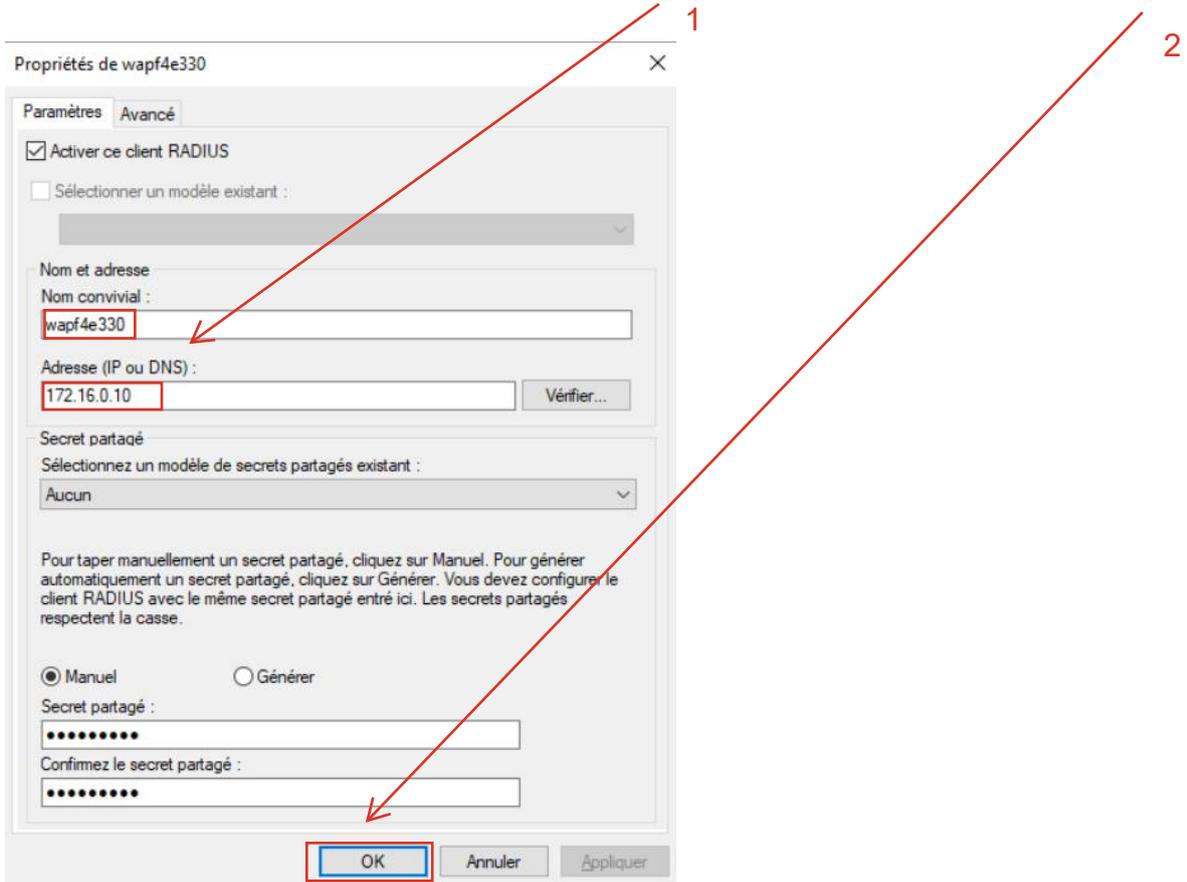
The screenshot shows the Cisco WAP371 configuration interface. The title bar reads "WAP371 Wireless-AC/N Dual Radio Access Point with Single Point Setup". On the left, a navigation menu is visible with "Administration" expanded and "System Settings" selected. The main area is titled "System Settings" and contains three input fields: "Host Name" with the value "wapf4e330", "System Contact", and "System Location". Each field has a range constraint in parentheses: "(Range: 1-63 Characters)", "(Range: 0-255 Characters)", and "(Range: 0-255 Characters)" respectively. A "Save" button is located below the fields.

### Etape 2 : Cliquez sur « Nouveau » :

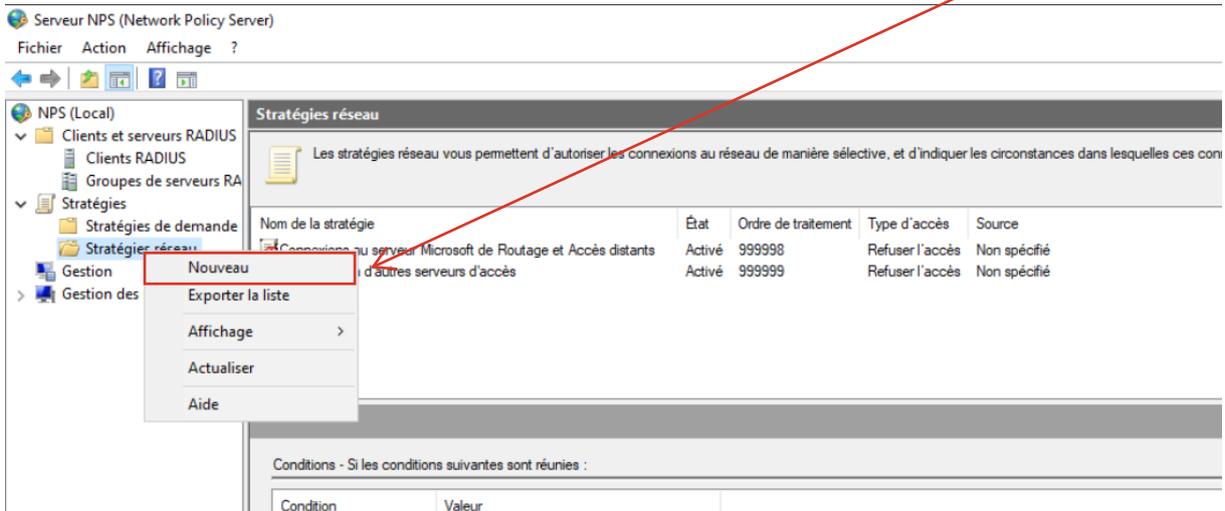


The screenshot shows the Windows Network Policy Server (NPS) console. The window title is "Serveur NPS (Network Policy Server)". The left-hand tree view shows "Clients et serveurs RADIUS" expanded, with "Nouveau" (New) highlighted in a red box. A red arrow points from the text "Cliquez sur « Nouveau »" to this button. The main pane shows the "Configuration standard" section, which includes a dropdown menu for "Serveur RADIUS pour les connexions d'accès à distance ou VPN" and a description of the server's role. Below this, there are sections for "Configuration avancée" and "Configuration de modèles".

**Etape 3 :** Renseignez le host en fonction des paramètres de la borne, puis cliquez sur « **OK** » :



**Etape 4 :** Dans stratégie de réseau, faites un clic droit puis cliquez sur « **Nouveau** »



## Etape 5 : Entrez le nom de la stratégie « SSID » :

Nouvelle stratégie réseau

**Spécifier le nom de la stratégie réseau et le type de connexion**

Vous pouvez spécifier le nom de votre stratégie réseau ainsi que le type des connexions auxquelles la stratégie s'applique.

**Nom de la stratégie :**  
SSID

Méthode de connexion réseau  
Sélectionnez le type de serveur d'accès réseau qui envoie la demande de connexion au serveur NPS. Vous pouvez sélectionner une valeur dans Type de serveur d'accès réseau ou bien Spécifique au fournisseur, mais ces paramètres ne sont pas obligatoires. Si votre serveur d'accès réseau est un commutateur d'authentification ou un point d'accès sans fil 802.1X, sélectionnez Non spécifié.

Type de serveur d'accès réseau :  
Non spécifié

Spécifique au fournisseur :  
10

Précédent Suivant Terminer Annuler

## Etape 6 : Cliquer sur « Ajouter... » :

Nouvelle stratégie réseau

**Spécifier les conditions**

Spécifiez les conditions qui déterminent si cette stratégie réseau est évaluée pour une demande de connexion. Au minimum, une condition est nécessaire.

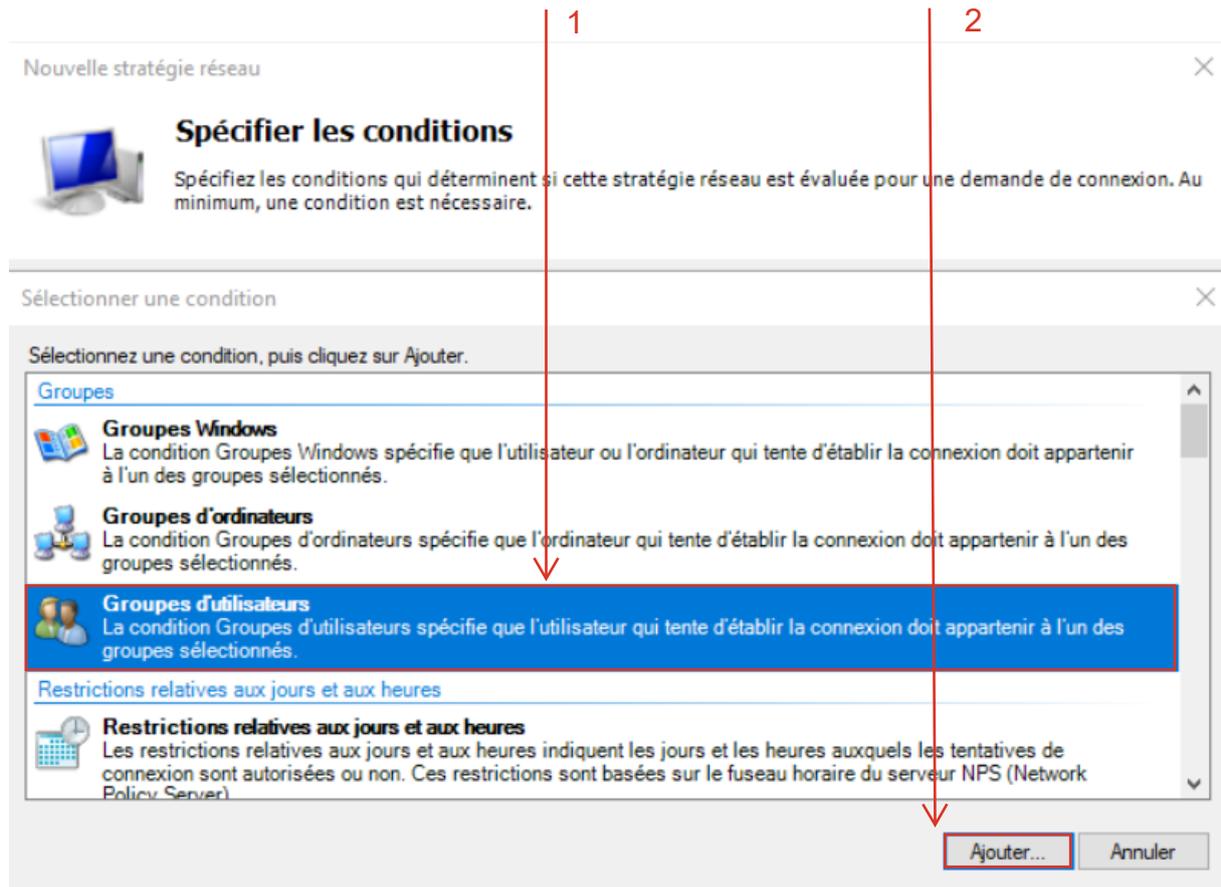
| Condition | Valeur |
|-----------|--------|
|-----------|--------|

Description de la condition :

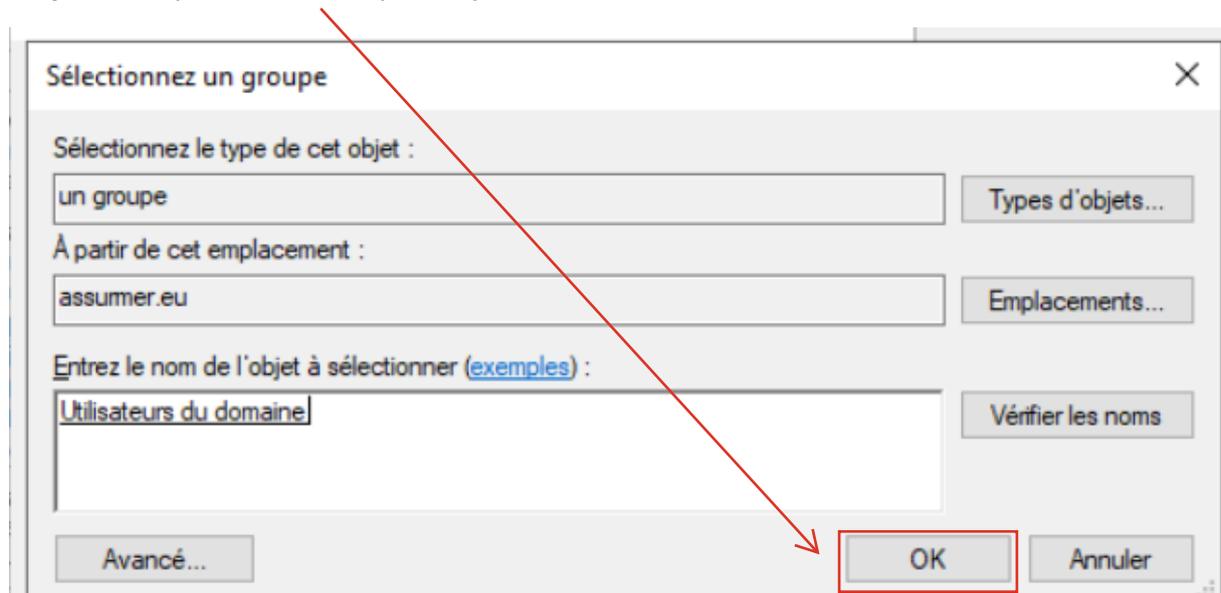
Ajouter... Modifier... Supprimer

Précédent Suivant Terminer Annuler

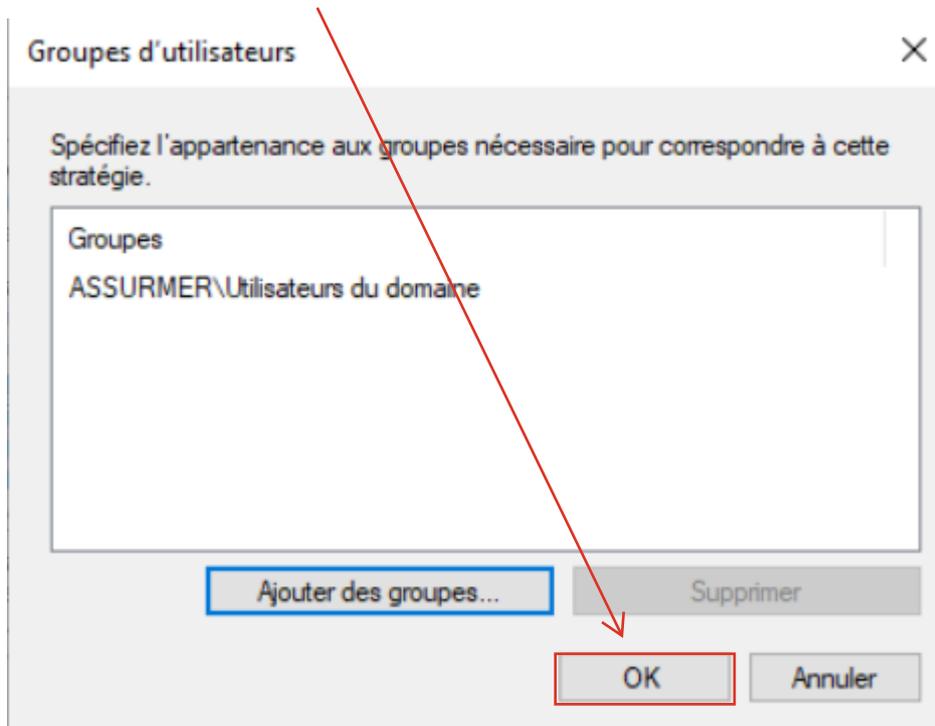
**Etape 7 :** Sélectionnez « **Groupe d'utilisateurs** », puis cliquez sur « **Ajouter** » :



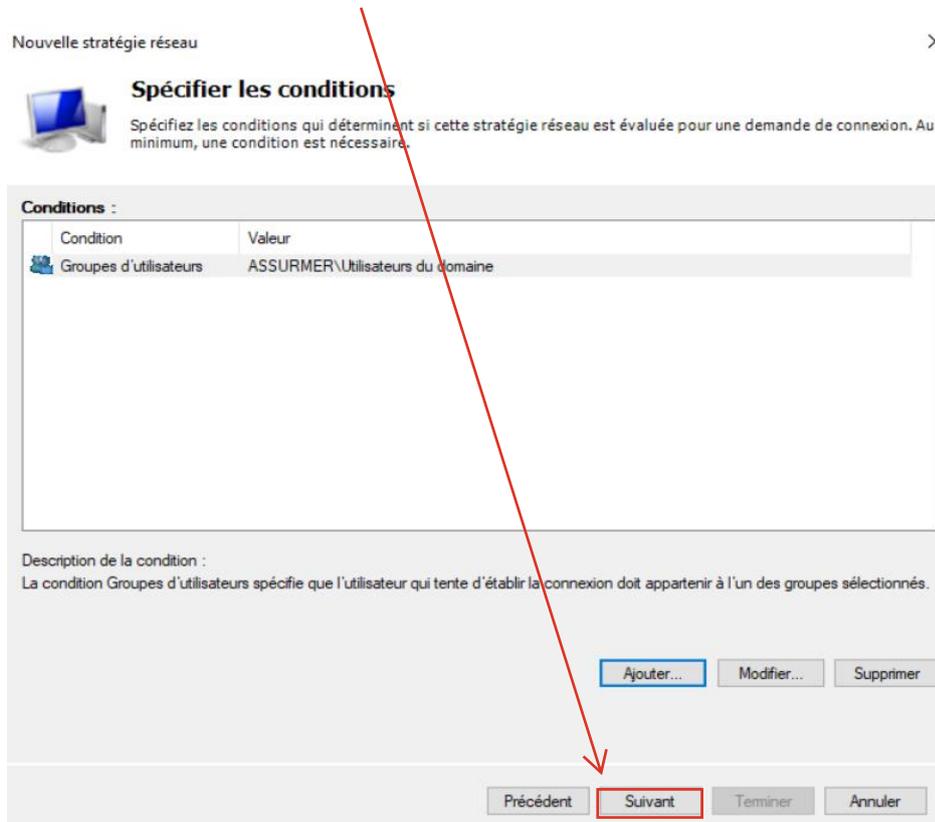
**Etape 8 :** Cliquez sur « **OK** » après l'ajout des utilisateurs du domaine :



**Etape 9 :** Cliquez sur « **OK** » :



**Etape 10 :** Cliquez sur « **Suivant** » :



**Etape 11** : Cochez la case « **Accès accordé** », puis cliquez sur « **Suivant** » :

Nouvelle stratégie réseau ×

**Spécifier l'autorisation d'accès**

Effectuez la configuration nécessaire pour accorder ou refuser l'accès réseau si la demande de connexion correspond à cette stratégie.

**Accès accordé**  
Accordez l'accès si les tentatives de connexion des clients répondent aux conditions de cette stratégie.

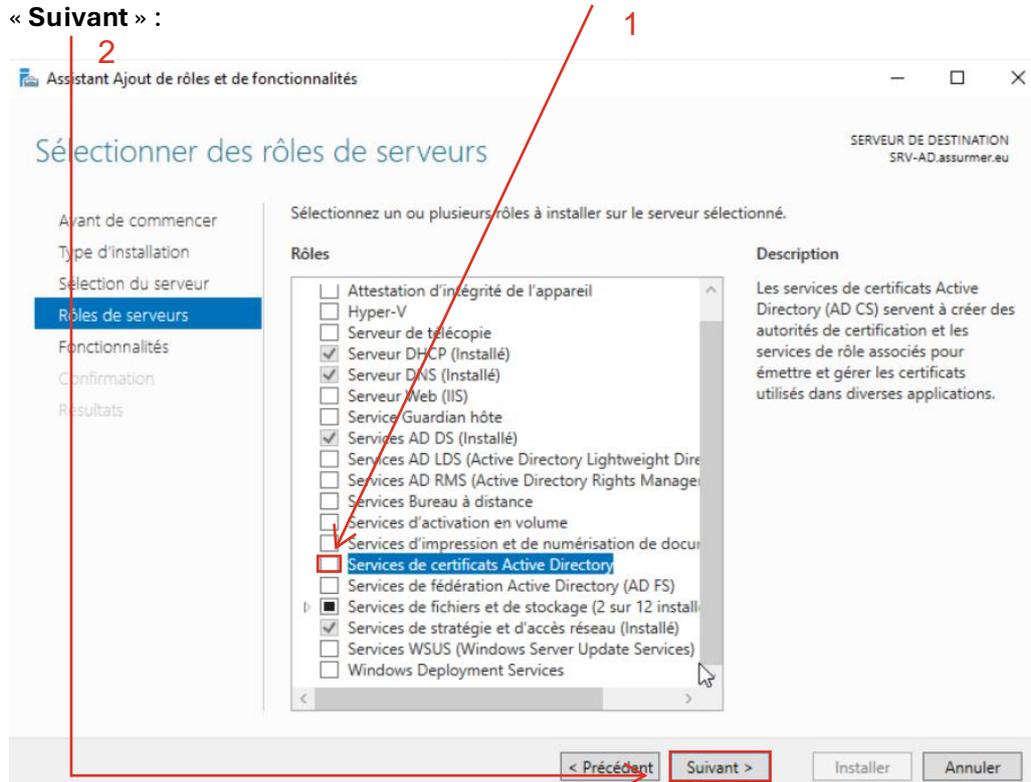
**Accès refusé**  
Refusez l'accès si les tentatives de connexion des clients répondent aux conditions de cette stratégie.

**L'accès est déterminé par les propriétés de numérotation des utilisateurs (qui remplacent la stratégie NPS)**  
Choisissez selon les propriétés de numérotation utilisateur si les tentatives de connexion des clients répondent aux conditions de la stratégie.

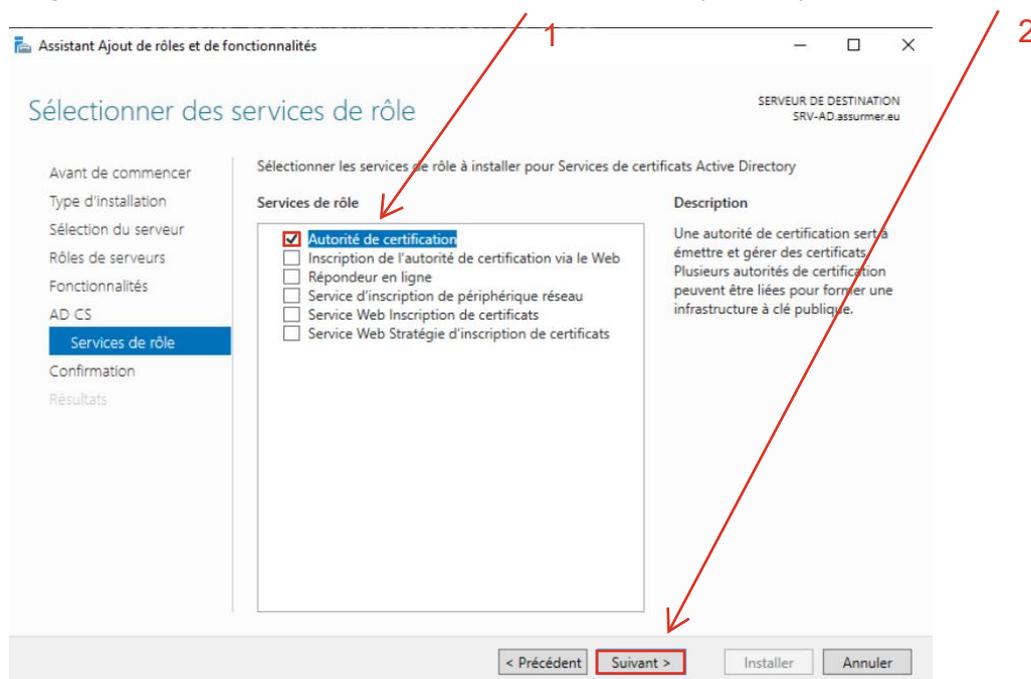
Précédent **Suivant** Terminer Annuler

### III. Installation du rôle requis pour l'autorité de certifications

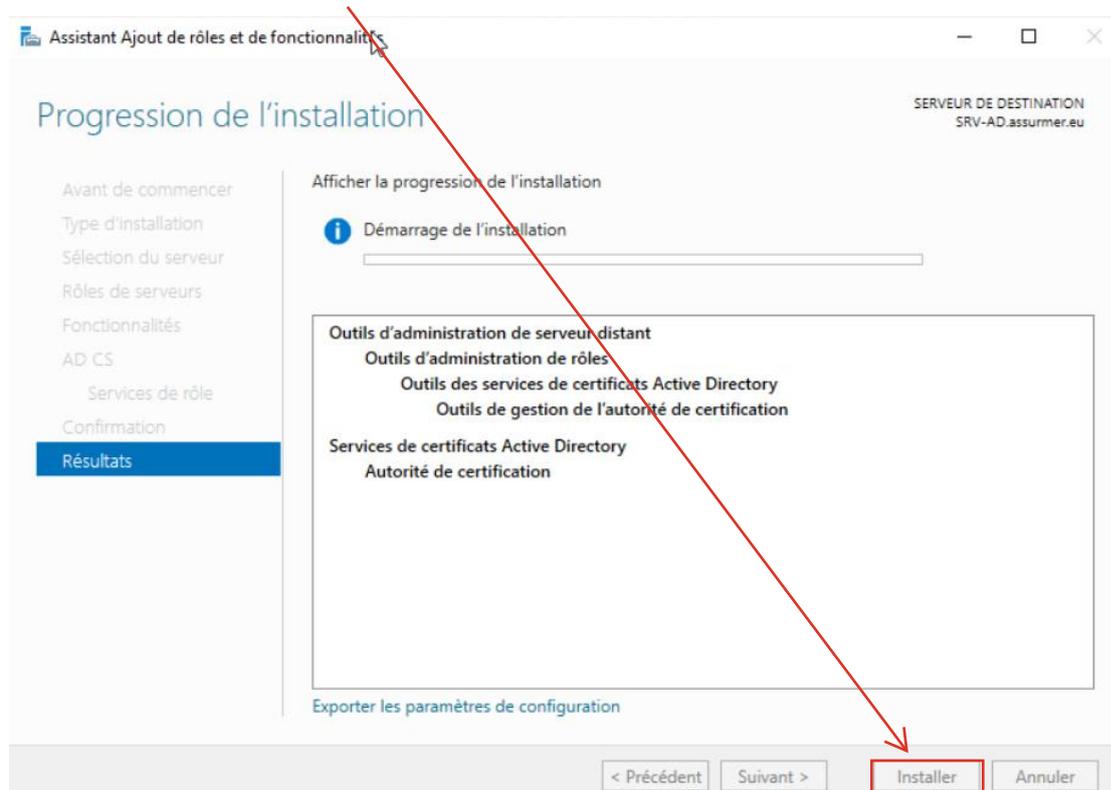
**Etape 1 :** Cochez la case « **Services de certificats Active Directory** », puis cliquez sur « **Suivant** » :



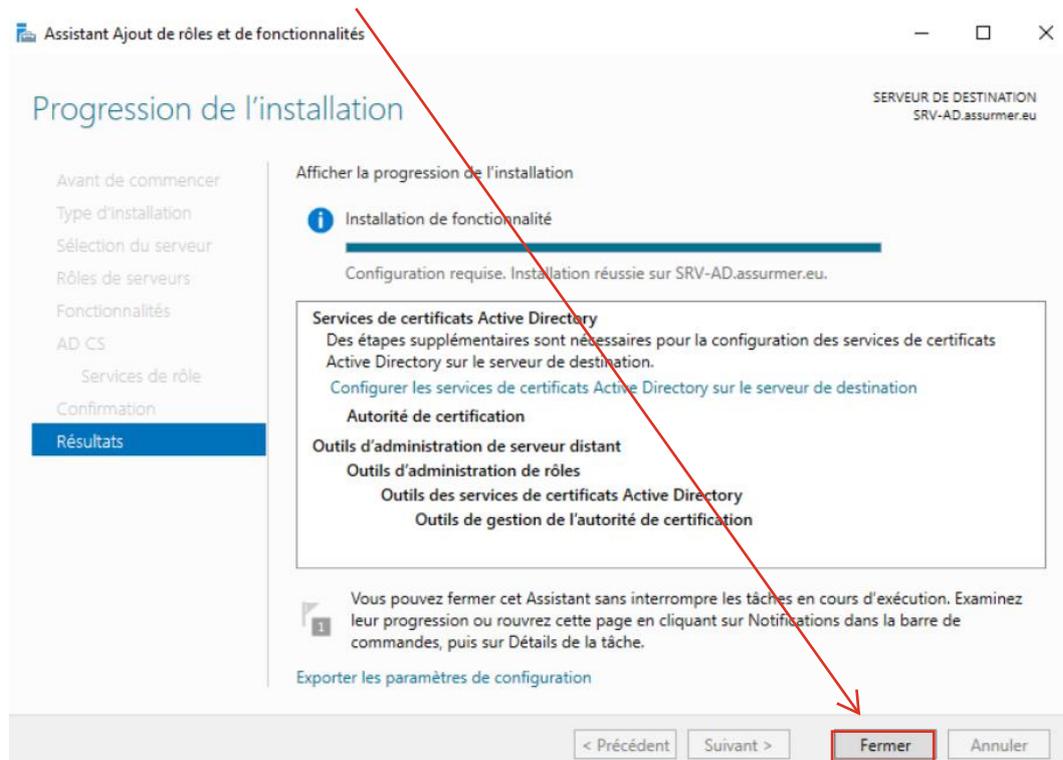
**Etape 2 :** Cochez la case « **Autorité de certification** », puis cliquez sur « **Suivant** » :



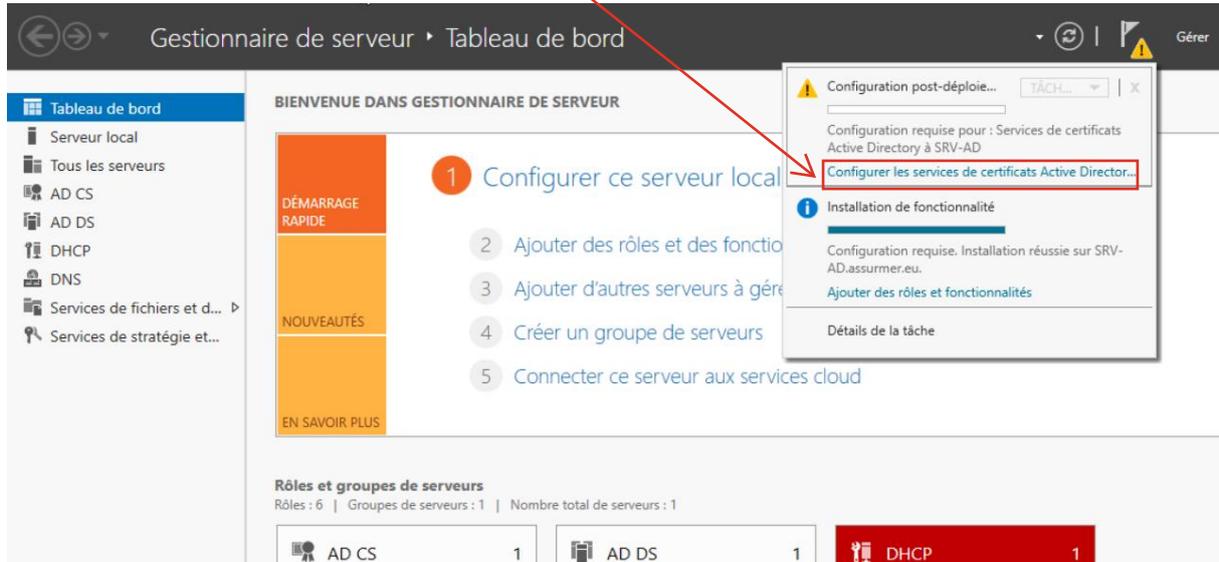
### Etape 3 : Cliquez sur « Installer » :



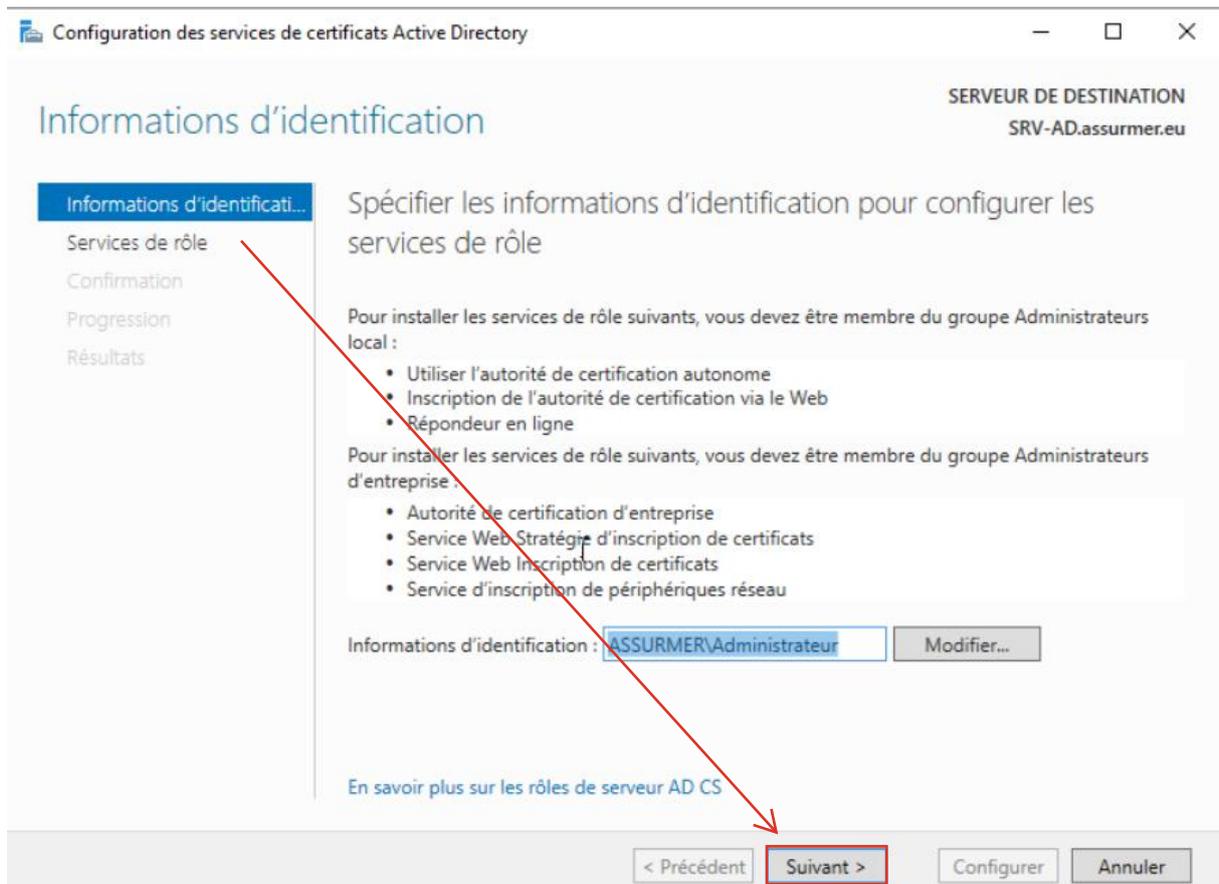
### Etape 4 : Cliquez sur « Fermer » :



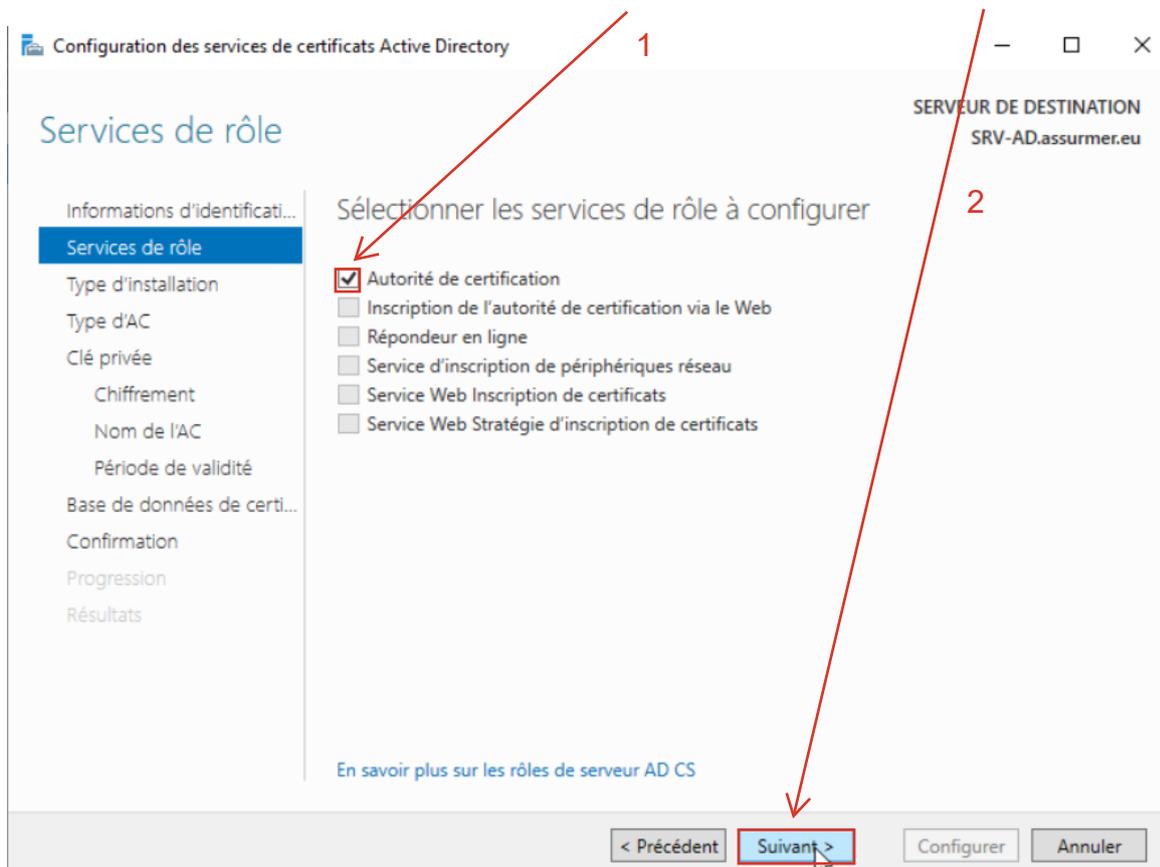
**Etape 5 : Cliquez sur « Configurer les services de certificats Active Directory »**



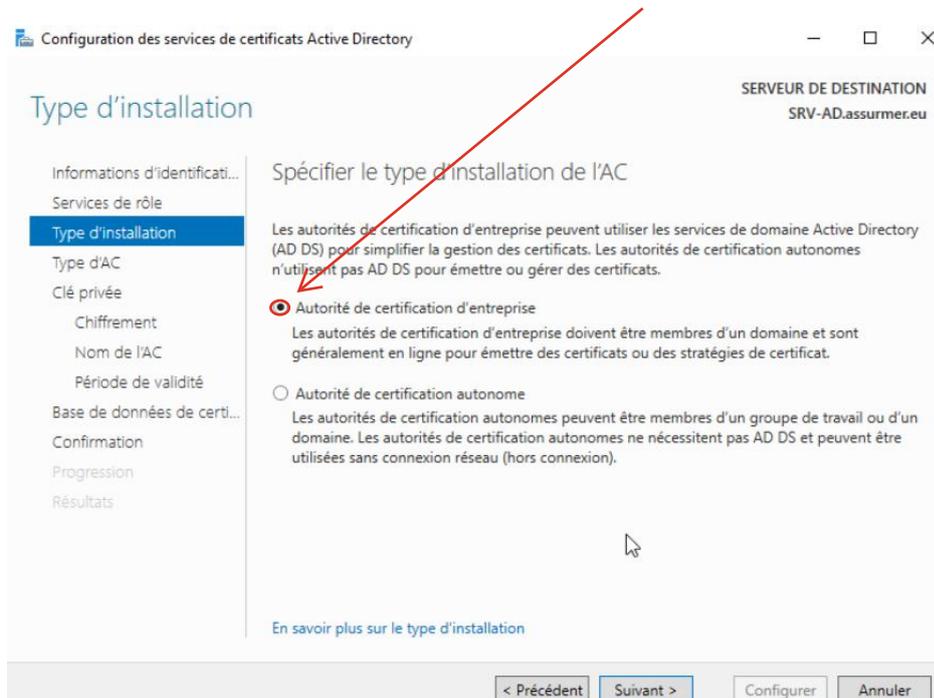
**Etape 6 : Cliquez sur “Suivant”**



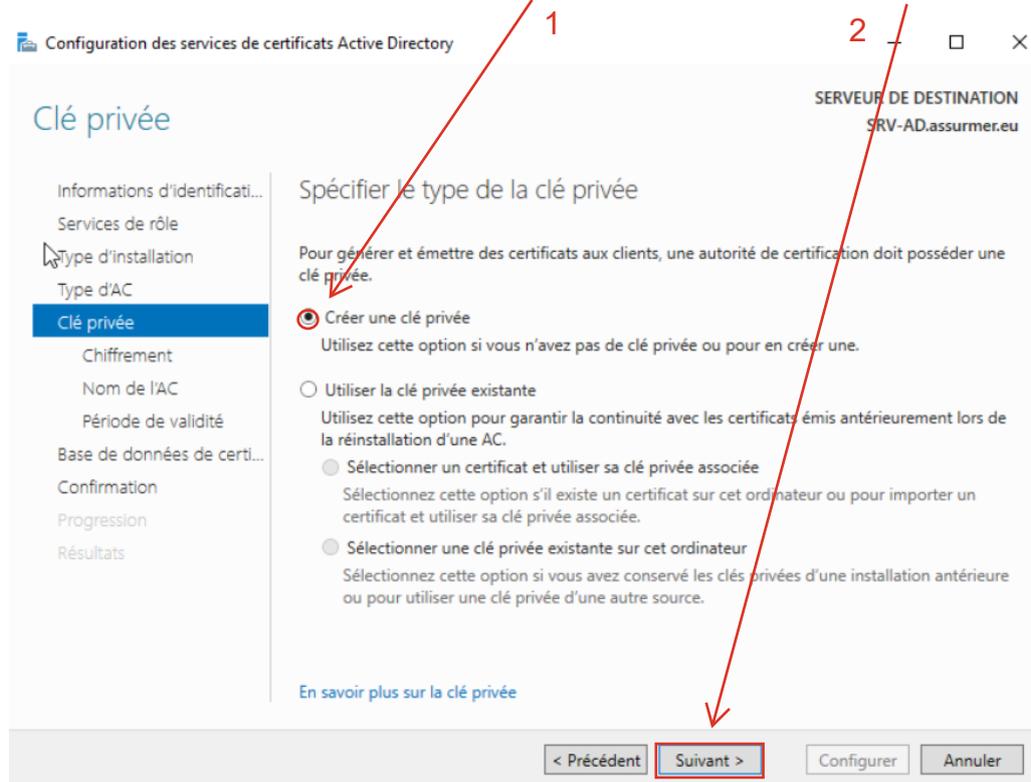
**Etape 7 :** Cochez la case « **Autorité de certification** », puis cliquez sur « **Suivant** » :



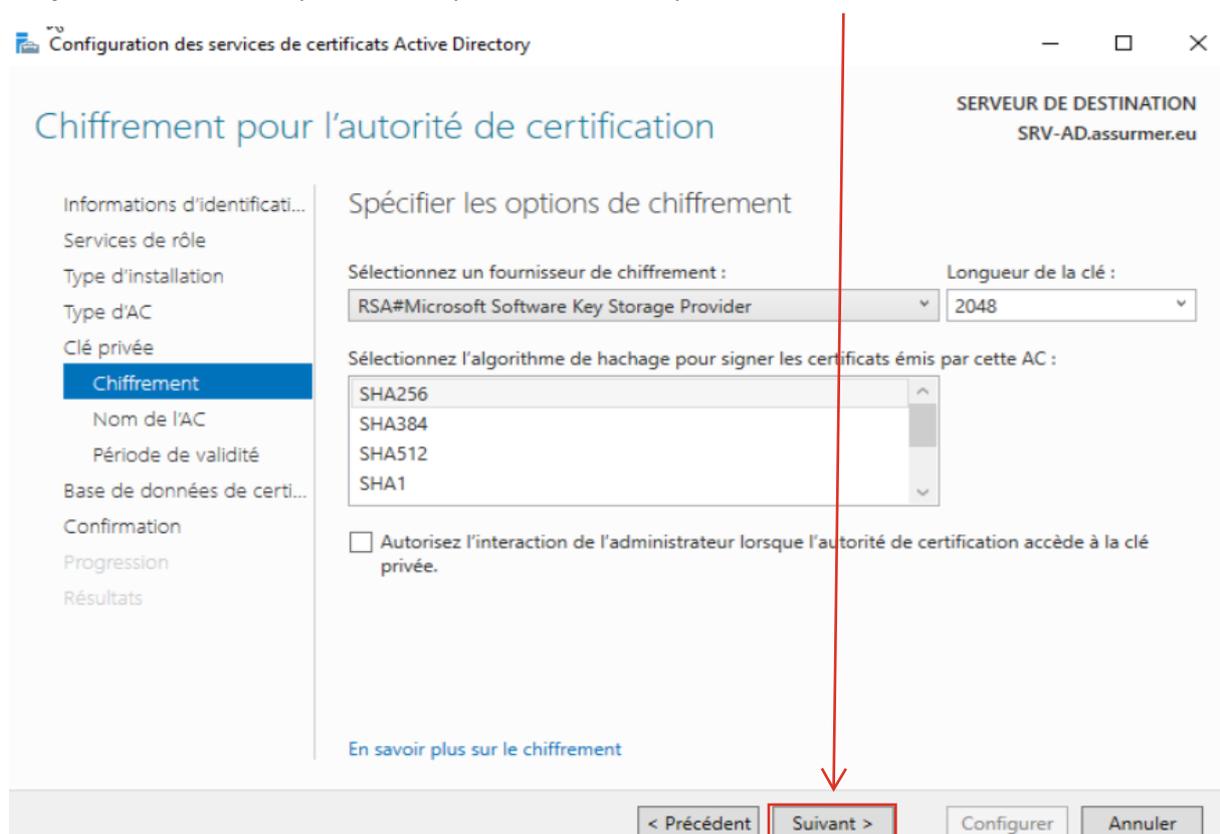
**Etape 8 :** Cochez la case « **Autorité de certification d'entreprise** » :



**Etape 9 :** Coche la case « **Créer une clé privée** », puis cliquez sur « **Suivant** » :



**Etape 10 :** Laissez les paramètres par défaut et cliquez sur « **Suivant** »



**Etape 11 : Cliquez sur « Suivant » :**

Configuration des services de certificats Active Directory

SERVEUR DE DESTINATION  
SRV-AD.assurmer.eu

### Nom de l'autorité de certification

Informations d'identificati...  
Services de rôle  
Type d'installation  
Type d'AC  
Clé privée  
Chiffrement  
**Nom de l'AC**  
Période de validité  
Base de données de certi...  
Confirmation  
Progression  
Résultats

#### Spécifier le nom de l'AC

Tapez un nom commun pour identifier cette autorité de certification. Ce nom est ajouté à tous les certificats émis par l'autorité de certification. Les valeurs des suffixes du nom unique sont générées automatiquement, mais elles sont modifiables.

Nom commun de cette AC :

Suffixe du nom unique :

Aperçu du nom unique :

[En savoir plus sur le nom de l'autorité de certification](#)

< Précédent **Suivant >** Configurer Annuler

**Etape 12 : Cliquez sur « Suivant » :**

Configuration des services de certificats Active Directory

SERVEUR DE DESTINATION  
SRV-AD.assurmer.eu

### Période de validité

Informations d'identificati...  
Services de rôle  
Type d'installation  
Type d'AC  
Clé privée  
Chiffrement  
Nom de l'AC  
**Période de validité**  
Base de données de certi...  
Confirmation  
Progression  
Résultats

#### Spécifier la période de validité

Sélectionnez la période de validité du certificat généré pour cette autorité de certification :

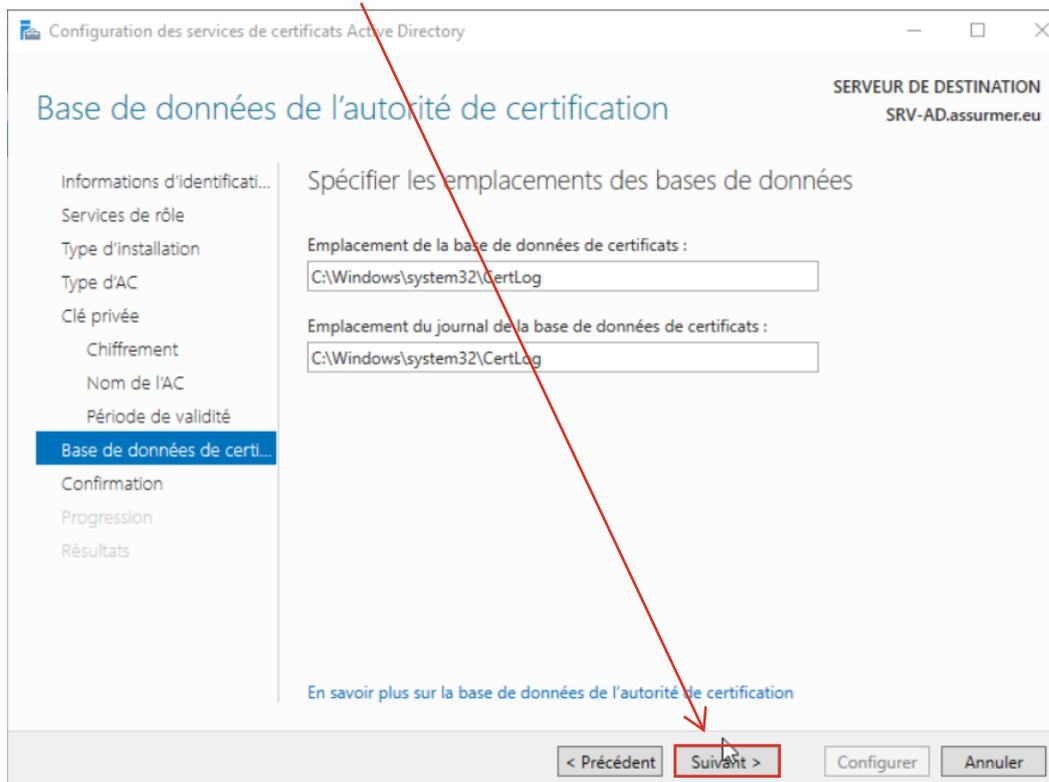
Date d'expiration de l'AC : 08/01/2030 10:58:00

La période de validité configurée pour ce certificat d'autorité de certification doit dépasser la période de validité pour les certificats qu'elle émettra.

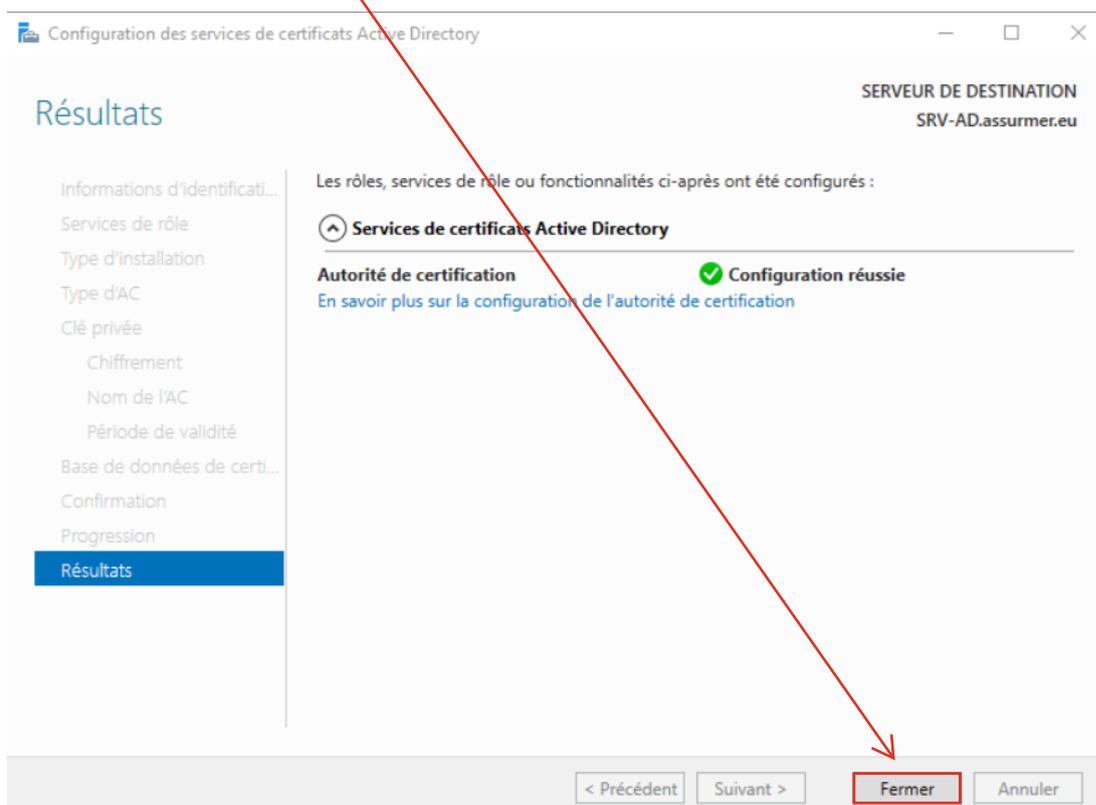
[En savoir plus sur la période de validité](#)

< Précédent **Suivant >** Configurer Annuler

**Etape 13 :** Cliquez sur « **Suivant** » :

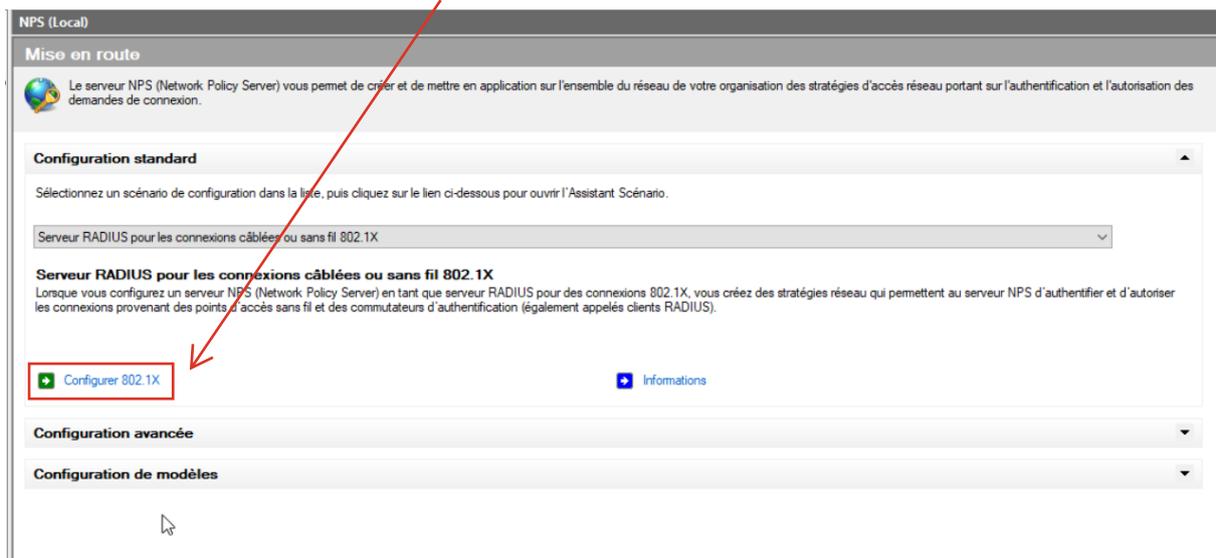


**Etape 14 :** Cliquez sur « **Fermer** » :



#### **IV. Configuration du serveur RADIUS + Certificats**

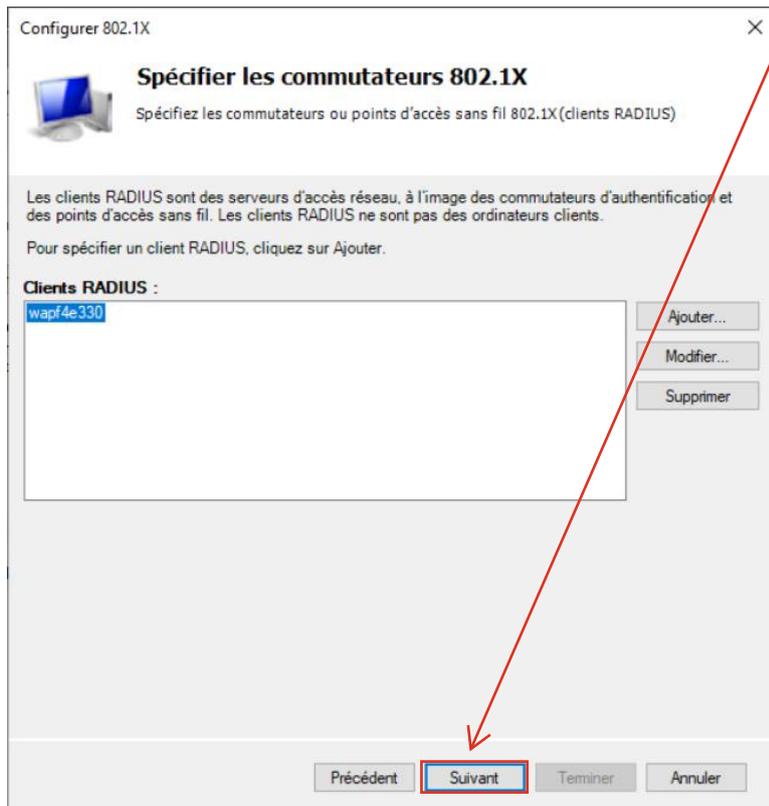
## Etape 1 : Cliquez sur « Configurer 802.1X » :



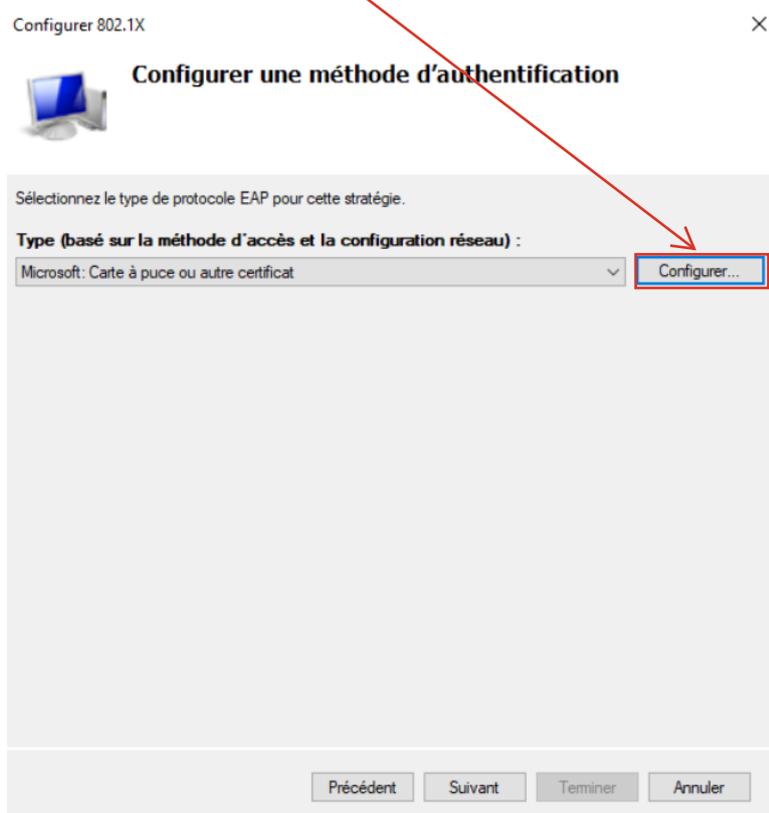
## Etape 2 : Sélectionnez la case « Connexion sans fil sécurisées », puis cliquez sur « Suivant » :



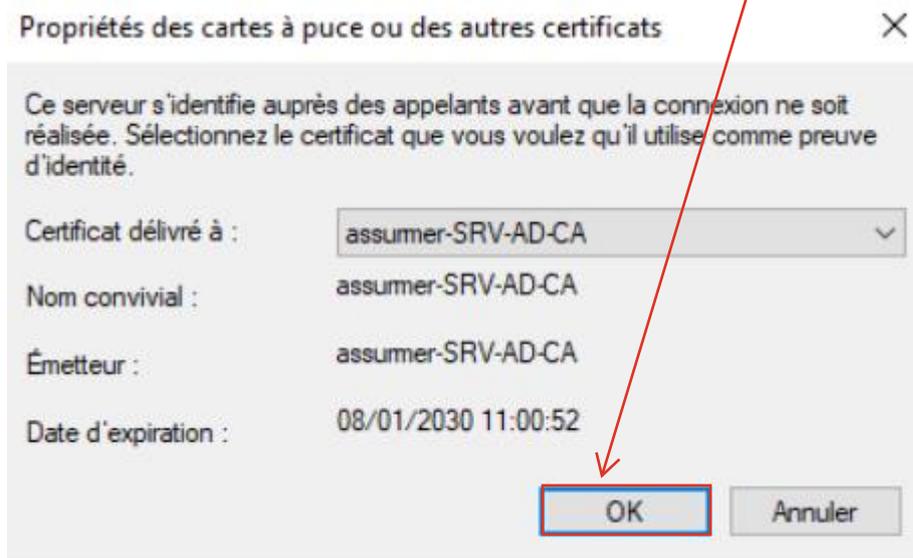
## Etape 3 : Confirmez le client RADIUS préalablement ajouter, puis cliquez sur « Suivant » :



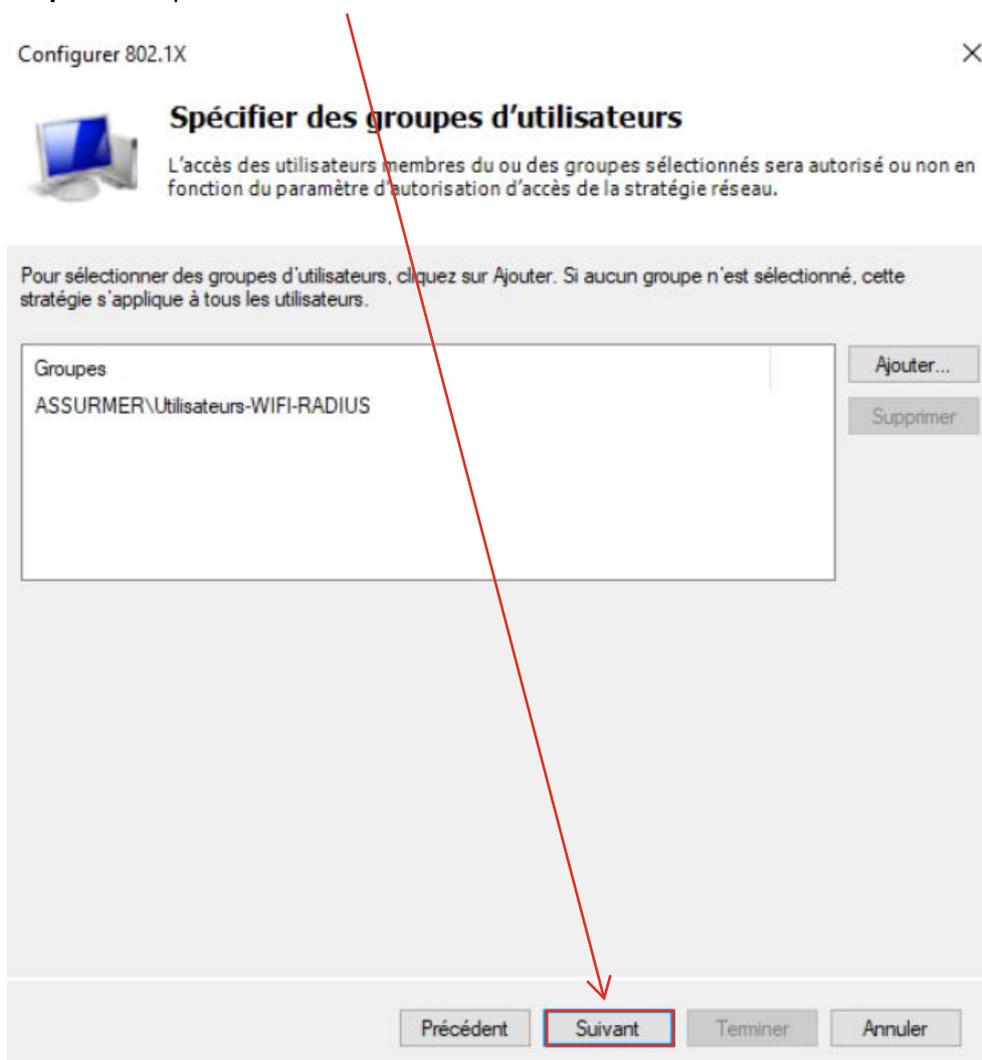
**Etape 4 :** Cliquez sur « **Configurer...** »



**Etape 5 :** Sélectionnez l'AD impacter par l'ajout, puis cliquez sur « **OK** » :



**Etape 6 :** Cliquez sur « **Suivant** » :



## Etape 7 : Cliquez sur « 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

## Etape 8 : Cliquez sur « Terminer » :

Configurer 802.1X

### Fin de la configuration des nouvelles connexions câblées/sans fil sécurisées IEEE 802.1X et des clients RADIUS

Vous avez créé les stratégies suivantes et configuré les clients RADIUS ci-dessous.

- Pour afficher les détails de la configuration dans votre navigateur, cliquez sur Détails de la configuration.
- Pour modifier la configuration, cliquez sur Précédent.
- Pour enregistrer la configuration et fermer cet Assistant, cliquez sur Terminer.

**Stratégie de demande de connexion :**  
RADIUS-WIFI

**Stratégies réseau :**  
RADIUS-WIFI

[Détails de la configuration](#)

Précédent Suivant **Terminer** Annuler

**Etape 9 :** Se rediriger vers l'interface web du réseau wifi dans la page network.

Cliquez sur « **Edit** »

Select the radio interface first, and then enter the configuration parameters.

Radio:  Radio 1 (5 GHz)  
 Radio 2 (2.4 GHz)

|                                     | VAP No. | Enable                              | VLAN ID | SSID Name    | SSID Broadcast                      | Security     | MAC Filter | Channel Isolation        | Band Steer               |
|-------------------------------------|---------|-------------------------------------|---------|--------------|-------------------------------------|--------------|------------|--------------------------|--------------------------|
| <input checked="" type="checkbox"/> | 0       | <input checked="" type="checkbox"/> | 1       | Assumer-LSD5 | <input checked="" type="checkbox"/> | WPA Personal | Disabled   | <input type="checkbox"/> | <input type="checkbox"/> |

[Show Details](#)

**Etape 10 :** Cliquez sur « **Use global RADIUS settings** »

Select the radio interface first, and then enter the configuration parameters.

Radio:  Radio 1 (5 GHz)  
 Radio 2 (2.4 GHz)

|                                     | VAP No. | Enable                              | VLAN ID | SSID Name    | SSID Broadcast                      | Security       | MAC Filter | Channel Isolation        | Band Steer               |
|-------------------------------------|---------|-------------------------------------|---------|--------------|-------------------------------------|----------------|------------|--------------------------|--------------------------|
| <input checked="" type="checkbox"/> | 0       | <input checked="" type="checkbox"/> | 1       | Assumer-LSD5 | <input checked="" type="checkbox"/> | WPA Enterprise | Disabled   | <input type="checkbox"/> | <input type="checkbox"/> |

[Hide Details](#)

WPA Versions:  WPA-TKIP  WPA2-AES  
 Enable pre-authentication  
MFP:  Not Required  Capable  Required

**Use global RADIUS server settings**

Server IP Address Type:  IPv4  IPv6

Server IP Address-1:  (xxx.xxx.xxx.xxx)  
Server IP Address-2:  (xxx.xxx.xxx.xxx)  
Server IP Address-3:  (xxx.xxx.xxx.xxx)  
Server IP Address-4:  (xxx.xxx.xxx.xxx)

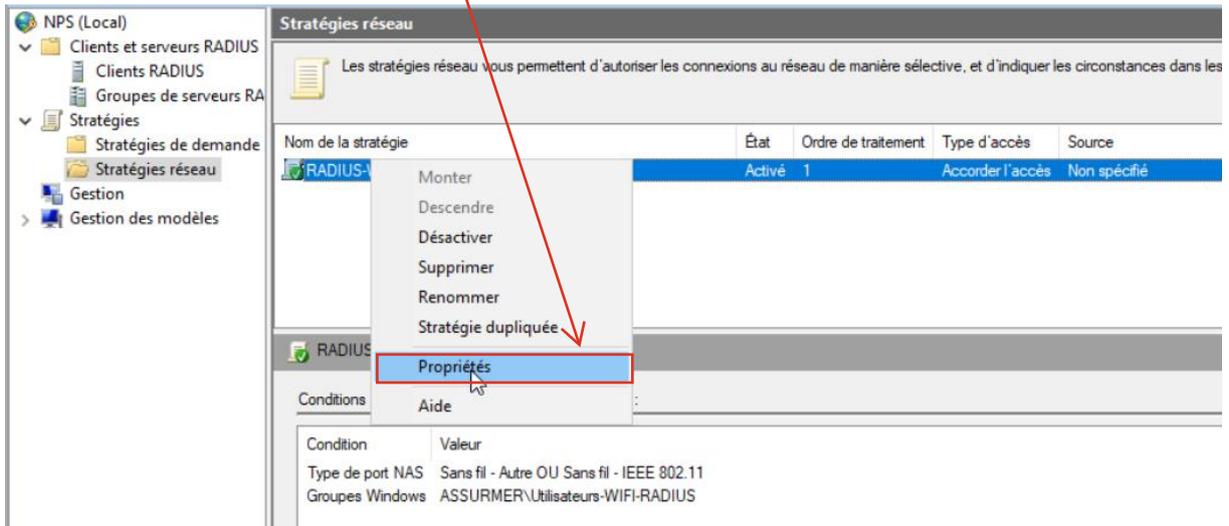
Key-1:  (Range: 1-64 Characters)  
Key-2:  (Range: 1-64 Characters)  
Key-3:  (Range: 1-64 Characters)  
Key-4:  (Range: 1-64 Characters)

Enable RADIUS Accounting

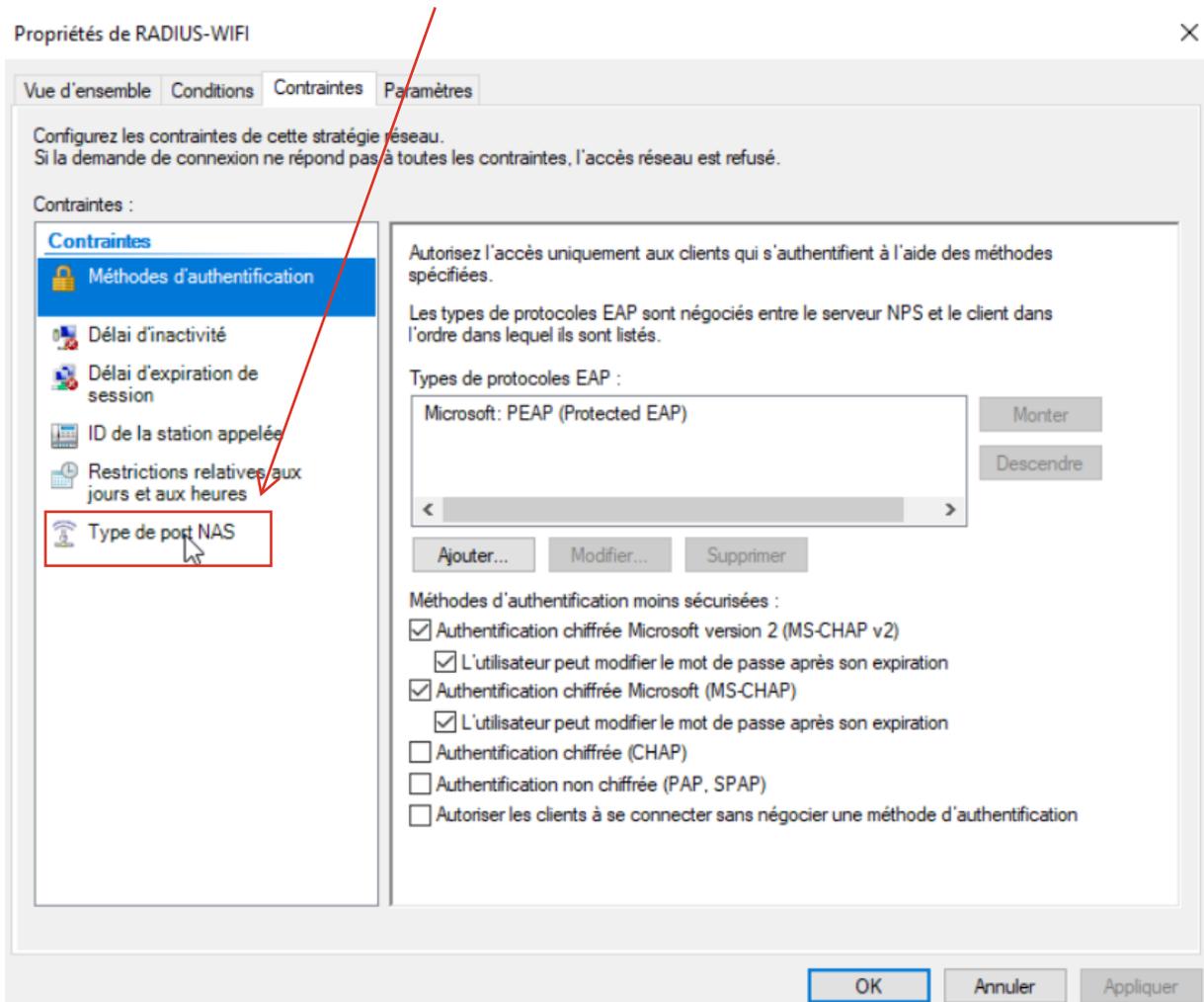
Active Server:

Broadcast Key Refresh Rate:  Sec (Range: 0-86400, 0 = Disable, Default: 86400)  
Session Key Refresh Rate:  Sec (Range: 30-86400, 0 = Disable, Default: 0)

## Etape 11 : Se diriger vers les “propriétés” de la stratégies réseau



## Etape 12 : Cliquer sur “Type de port NAS”



### Etape 13 : Sélectionner uniquement “sans fil – IEEE 802.11”

Propriétés de RADIUS-WIFI

Vue d'ensemble Conditions Contraintes Paramètres

Configurez les contraintes de cette stratégie réseau.  
Si la demande de connexion ne répond pas à toutes les contraintes, l'accès réseau est refusé.

Contraintes :

- Contraintes
- Méthodes d'authentification
- Délai d'inactivité
- Délai d'expiration de session
- ID de la station appelée
- Restrictions relatives aux jours et aux heures
- Type de port NAS

Spécifier les types de médias d'accès nécessaires pour correspondre à cette stratégie

Types de tunnels pour connexions d'accès à distance et VPN standard

- Asynchrone (Modem)
- RNIS synchrone
- Synchrone (ligne T1)
- Virtuel (VPN)

Types de tunnels pour connexions 802.1X standard

- Ethernet
- FDDI
- Sans fil - IEEE 802.11
- Token Ring

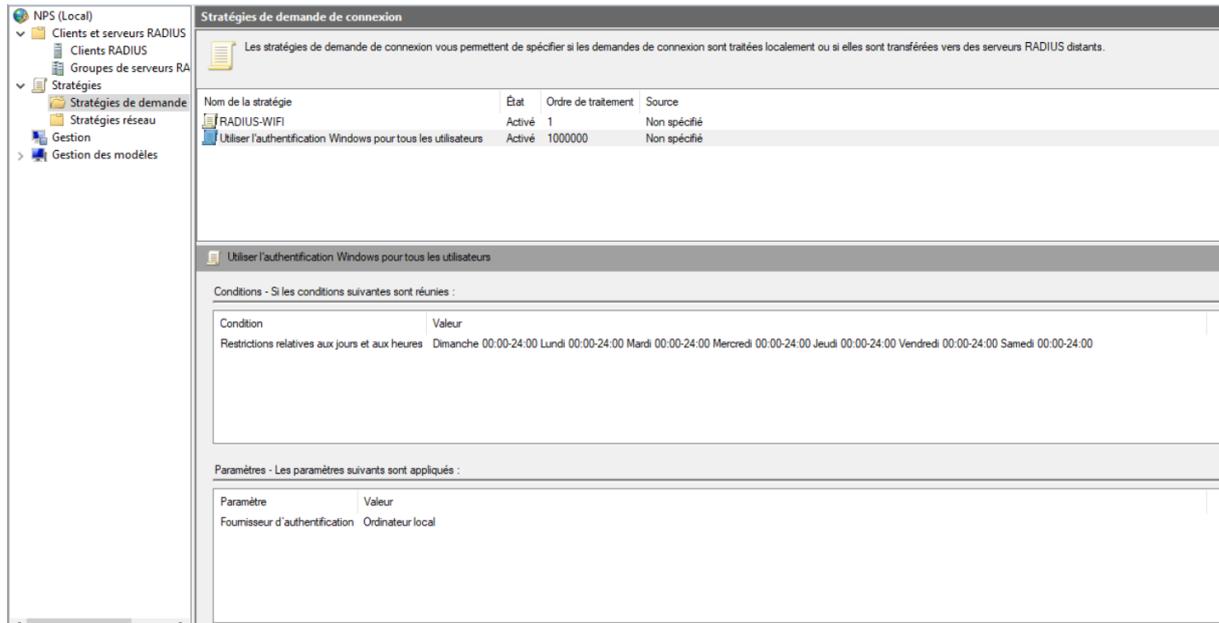
Autres

- ADSL-CAP - Modulation de phase d'amplitude sans porteuse DSL asymétrique
- ADSL-DMT - Multi-tonalité discrète DSL asymétrique
- Asynchrone (Modem)
- Câble

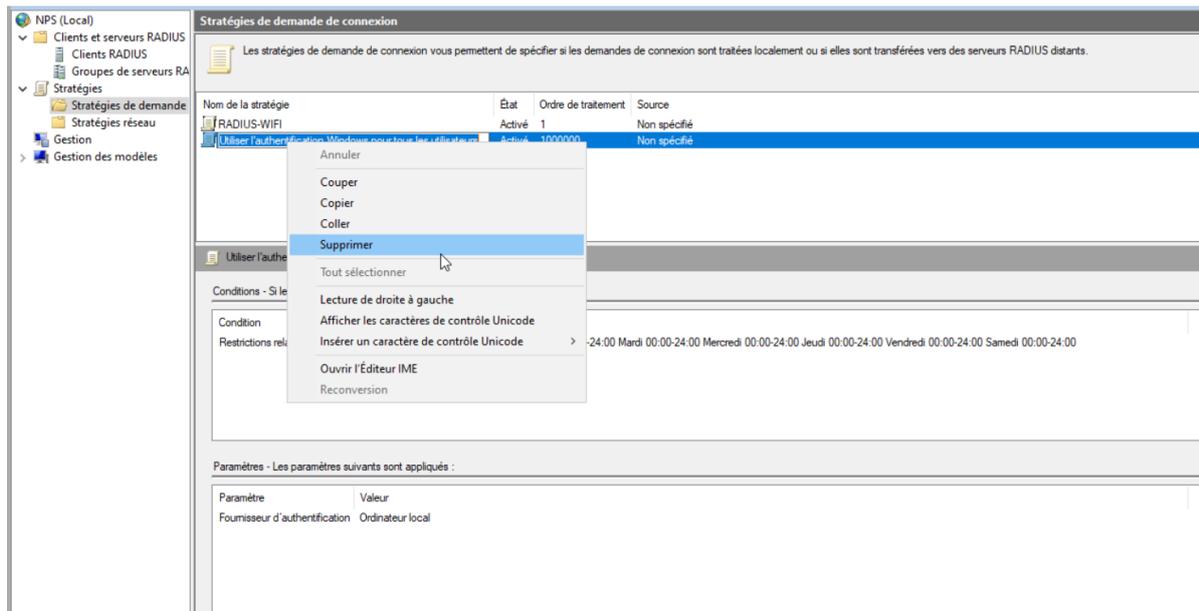
OK Annuler Appliquer

La configuration du RADIUS est terminée pour que cela fonctionne bien, certains paramètres sont à ajuster.

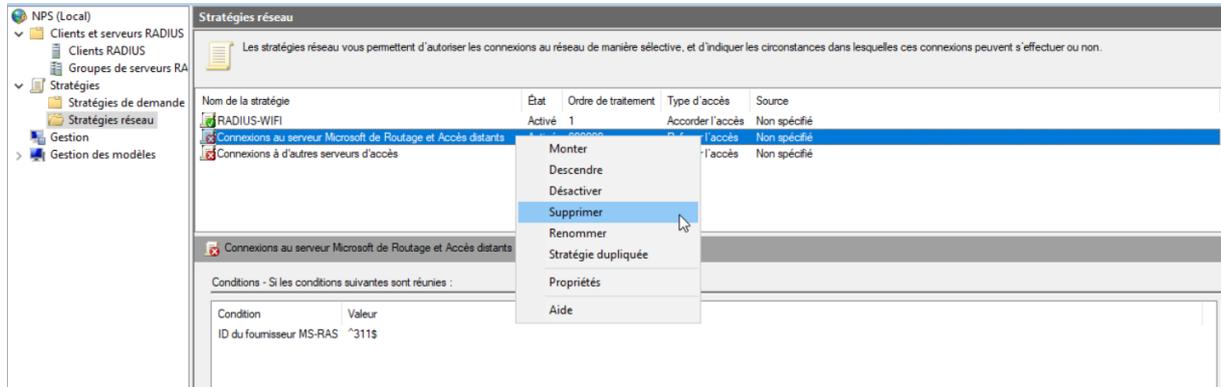
### Etape Annexe 1 : Supprimez les autres stratégies de réseaux



### Etape Annexe 2 :



### Etape Annexe 3 :



### Etape Annexe 4 :

