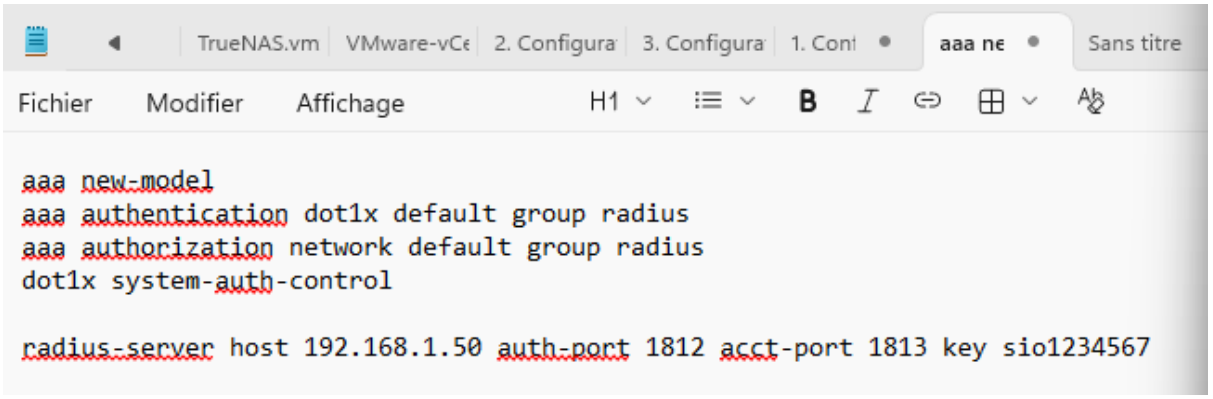
# TP1 – Mise en oeuvre d'une infrastructure 802.1x : connexions câblées

# Table des Matières :

# Annexe 1 : Commutateur Cisco 2960 et authentification 802.1x

▪ Configuration appliquée sur le switch en aval.

```
vlan 2
name Pedagogie
vlan 3
name Administration
vlan 4
name Serveurs
vlan 99
name Gestion

interface Fa0/1
switchport mode trunk
switchport trunk allowed vlan 1,2,3,4,99

interface vlan 1
ip address 192.168.0.2 255.255.255.248
no shutdown

interface Fa0/2
switchport access vlan 4
switchport mode access

interface Fa0/19
switchport mode trunk
```




```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
dot1x system-auth-control

radius-server host 192.168.1.50 auth-port 1812 acct-port 1813 key sio1234567
```

▪ Interfaces fa0/7 et fa0/8 :

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int fa0/7
Switch(config-if)#switchport mode access
Switch(config-if)#authentication port-control auto
Switch(config-if)#dot1x pae authenticator
Switch(config-if)#
```

```
Switch(config-if)#int fa0/8
Switch(config-if)#switchport mode access
Switch(config-if)#authentication port-control auto
Switch(config-if)#dot1x pae authenticator
Switch(config-if)#
```

▪ Copie du run vers le start :

```
Switch#copy run
Switch#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Switch#
```

▪ Configuration routeur :

```
Router(config)#interface G0/0
Router(config-if)# no shutdown
Router(config-if)#
```

```
Router(config)#
Router(config)#interface G0/0.1
Router(config-subif)# encapsulation dot1Q 1
Router(config-subif)# ip address 192.168.0.1 255.255.255.248
Router(config-subif)#
Router(config-subif)#interface G0/0.2
Router(config-subif)# encapsulation dot1Q 2
Router(config-subif)# ip address 192.168.1.1 255.255.255.240
Router(config-subif)#
Router(config-subif)#interface G0/0.3
Router(config-subif)# encapsulation dot1Q 3
Router(config-subif)# ip address 192.168.1.17 255.255.255.240
Router(config-subif)#
Router(config-subif)#interface G0/0.4
Router(config-subif)# encapsulation dot1Q 4
Router(config-subif)# ip address 192.168.1.49 255.255.255.248
Router(config-subif)#
Router(config-subif)#
```

```
Router(config)#ip dhcp excluded-address 192.168.1.1
Router(config)#ip dhcp excluded-address 192.168.1.17
Router(config)#ip dhcp excluded-address 192.168.1.33
Router(config)#
Router(config)#ip dhcp pool VLAN2_PEDAGO
Router(dhcp-config)# network 192.168.1.0 255.255.255.240
Router(dhcp-config)# default-router 192.168.1.1
Router(dhcp-config)# dns-server 192.168.1.50
Router(dhcp-config)#
Router(dhcp-config)#ip dhcp pool VLAN3_ADMIN
Router(dhcp-config)# network 192.168.1.16 255.255.255.240
Router(dhcp-config)# default-router 192.168.1.17
Router(dhcp-config)# dns-server 192.168.1.50
Router(dhcp-config)#
Router(dhcp-config)#
```

▪ Copie du run vers le start :

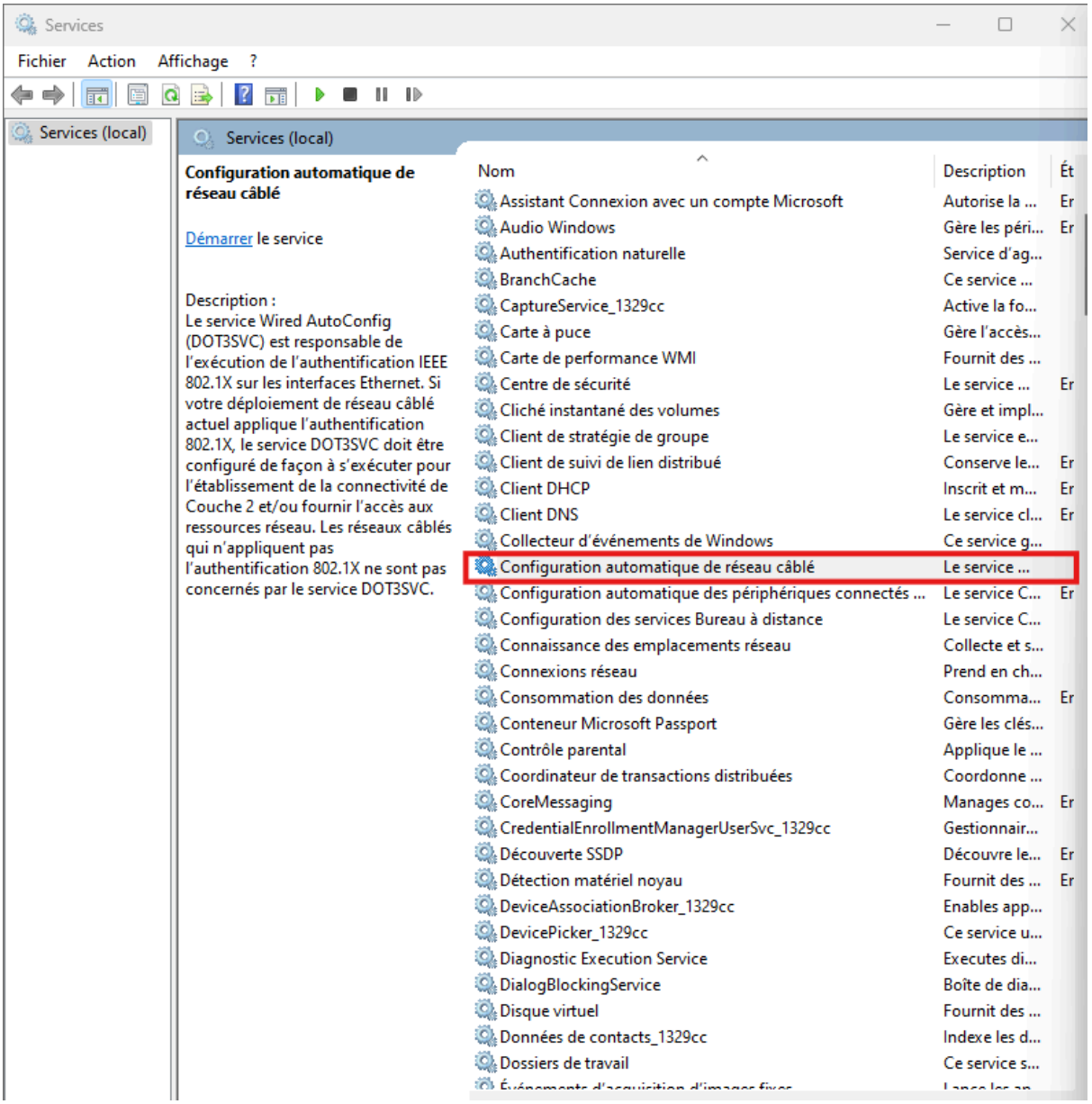
```
Router#
Router#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
```

▪ Affichage des informations sur l'authentification 802.1x avec deux commandes différentes : show dot1x all et show dot1x all summary

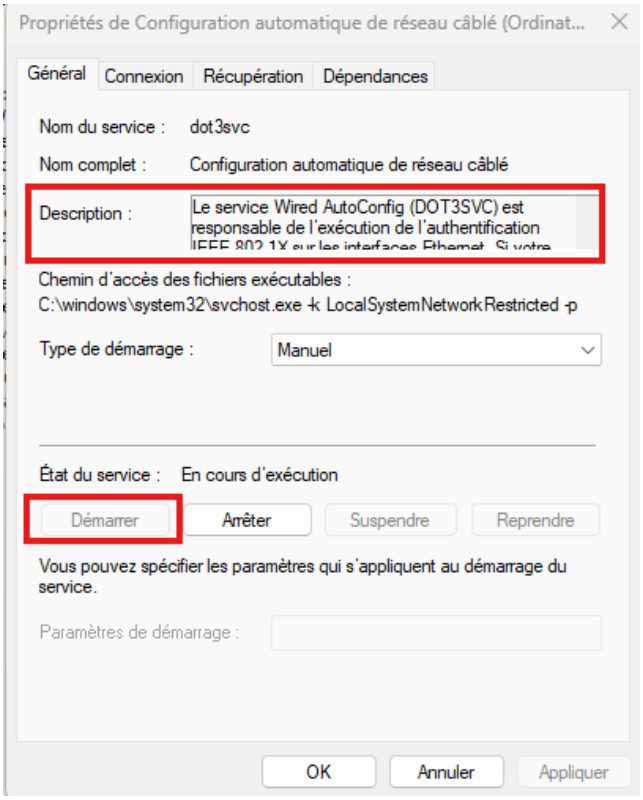
```
Switch#show dot1
Switch#show dot1x al
Switch#show dot1x all
Sysauthcontrol              Enabled
Dot1x Protocol Version            3

Dot1x Info for FastEthernet0/7
----------------------------------
PAE                       = AUTHENTICATOR
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30

Dot1x Info for FastEthernet0/8
----------------------------------
PAE                       = AUTHENTICATOR
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30

Switch#
```

```
Switch#show dot1x all summ
Switch#show dot1x all summary
Interface        PAE     Client          Status
---------------------------------------------------------
Fa0/7            AUTH    none            UNAUTHORIZED
Fa0/8            AUTH    none            UNAUTHORIZED
Switch#
```

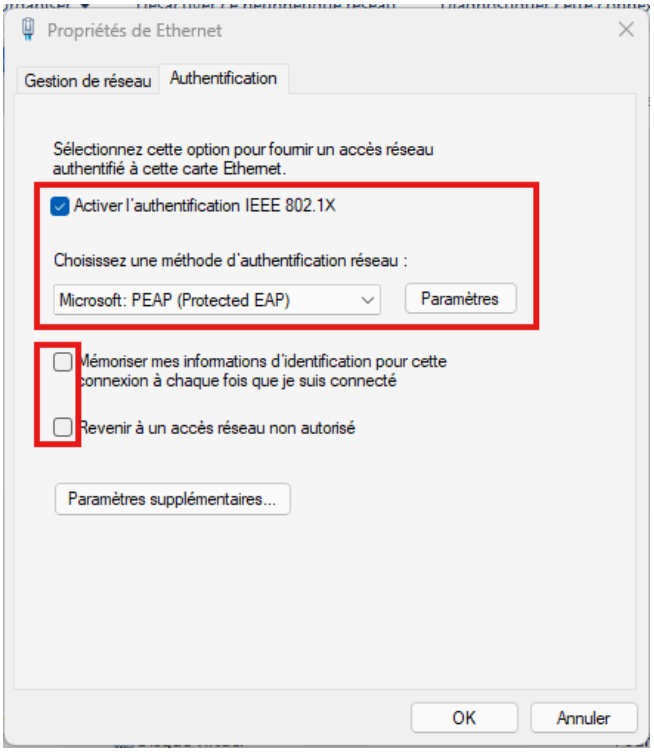
▪ Configuration du second pc :



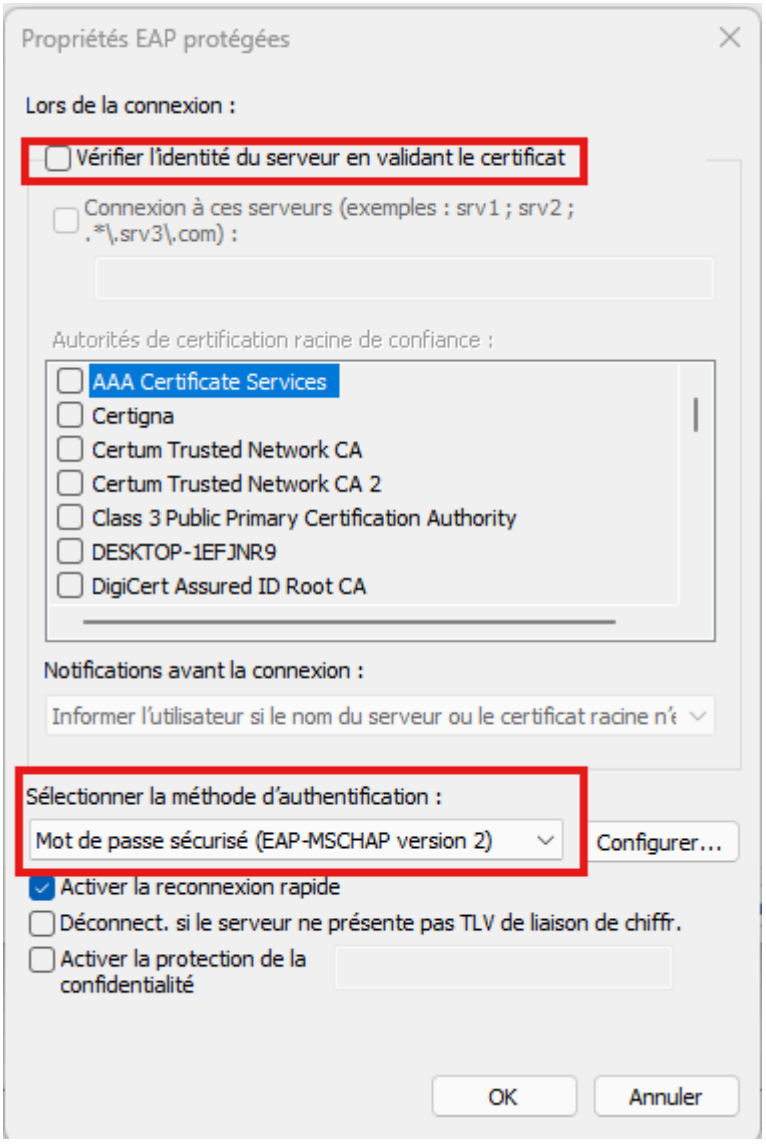
▪ Nous lançons le service de configuration automatique du réseau câblé.



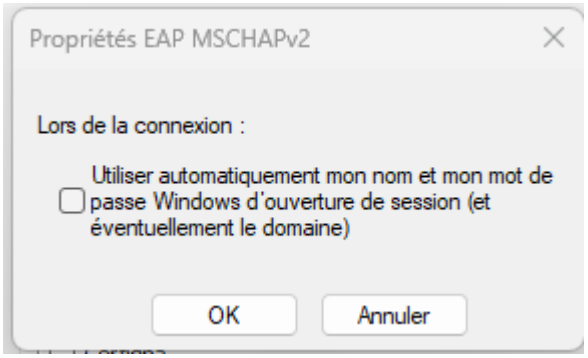

▪ Apparition de l'onglet authentification dans les propriétés de la carte réseau.



▪ Nous ouvrons l'écran Propriétés EAP protégées en cliquant sur "Paramètres"



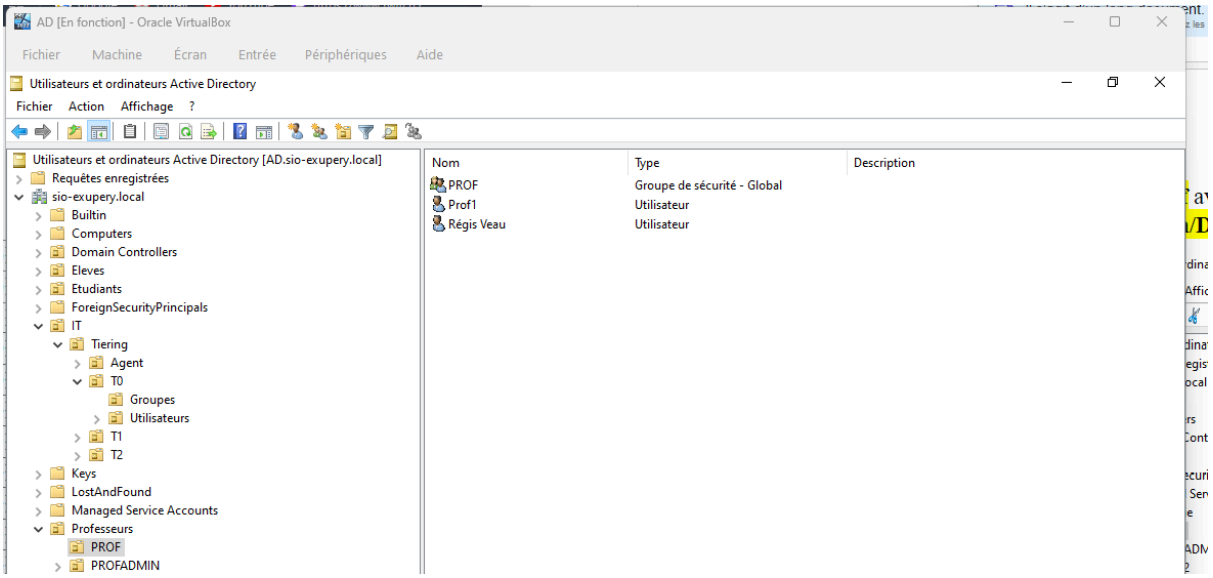

▪ Nous cliquons sur le bouton "Configurer"



# Annexe 2 : Mise en place du serveur RADIUS (service NPS)

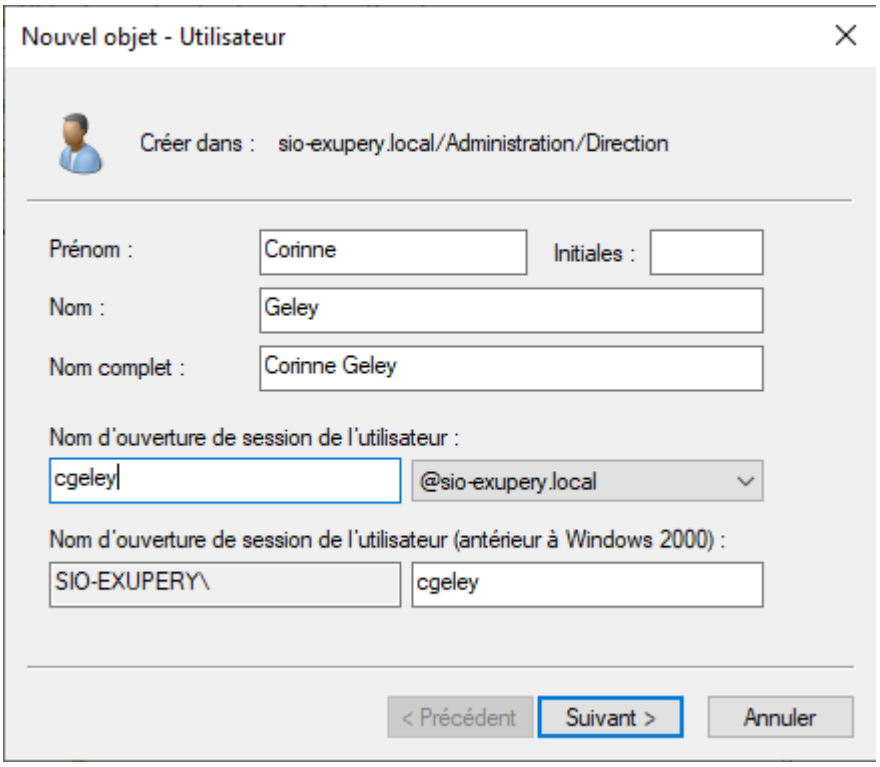
## 2.1 Situation de départ

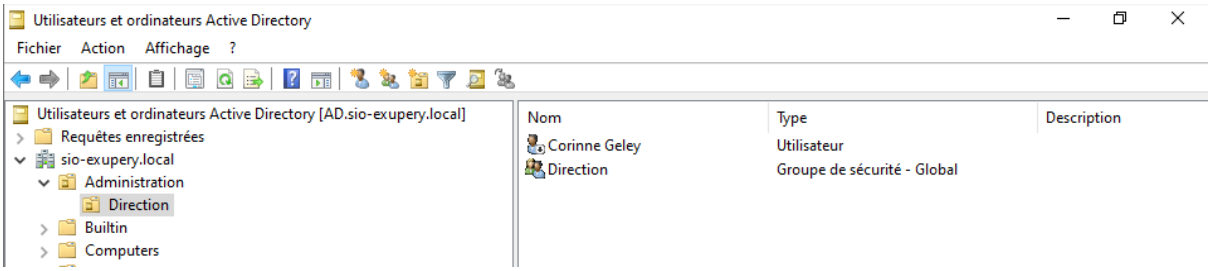
▪ Création du compte utilisateur Régis Veau puis nous ajoutons au groupe Prof :



▪ Unité d'organisation "Administration" créé au préalable puis nous avions créé "Direction"

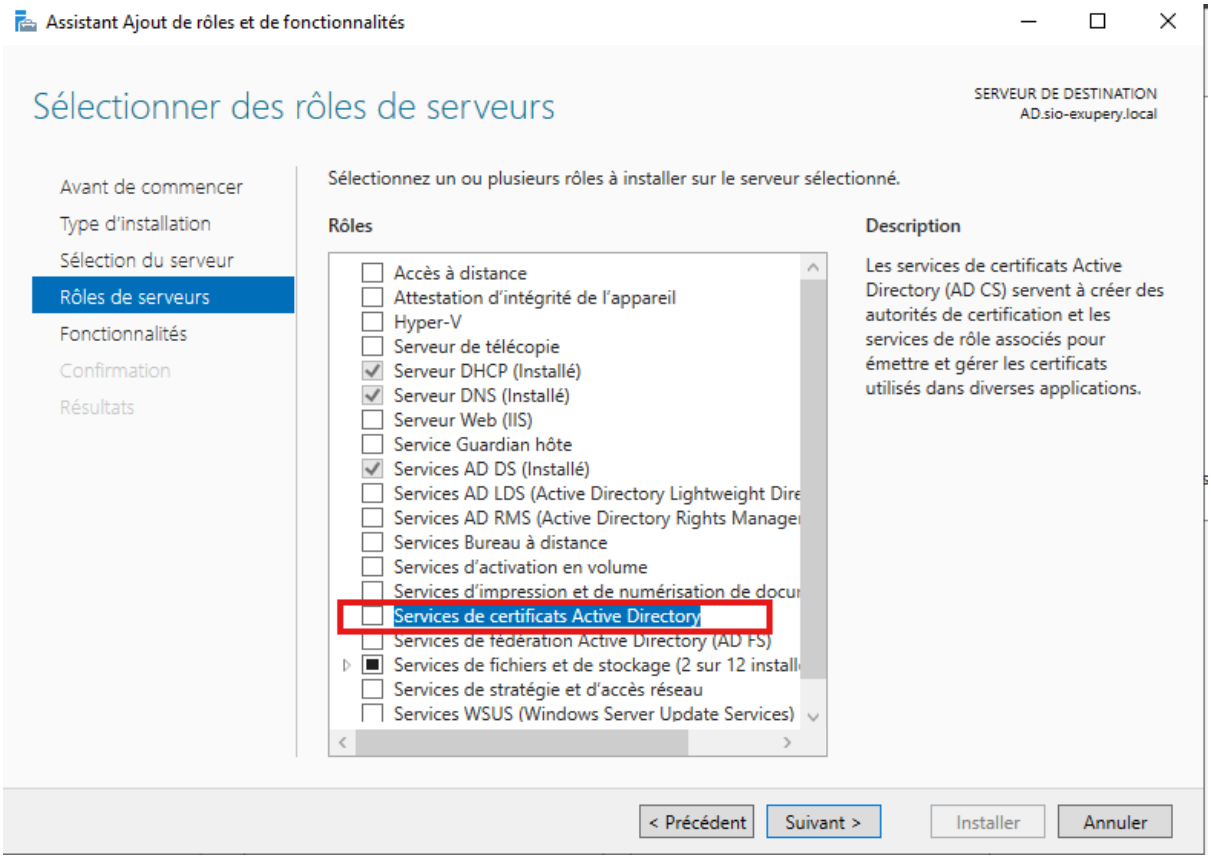
- Création du compte utilisateur Corinne Geley



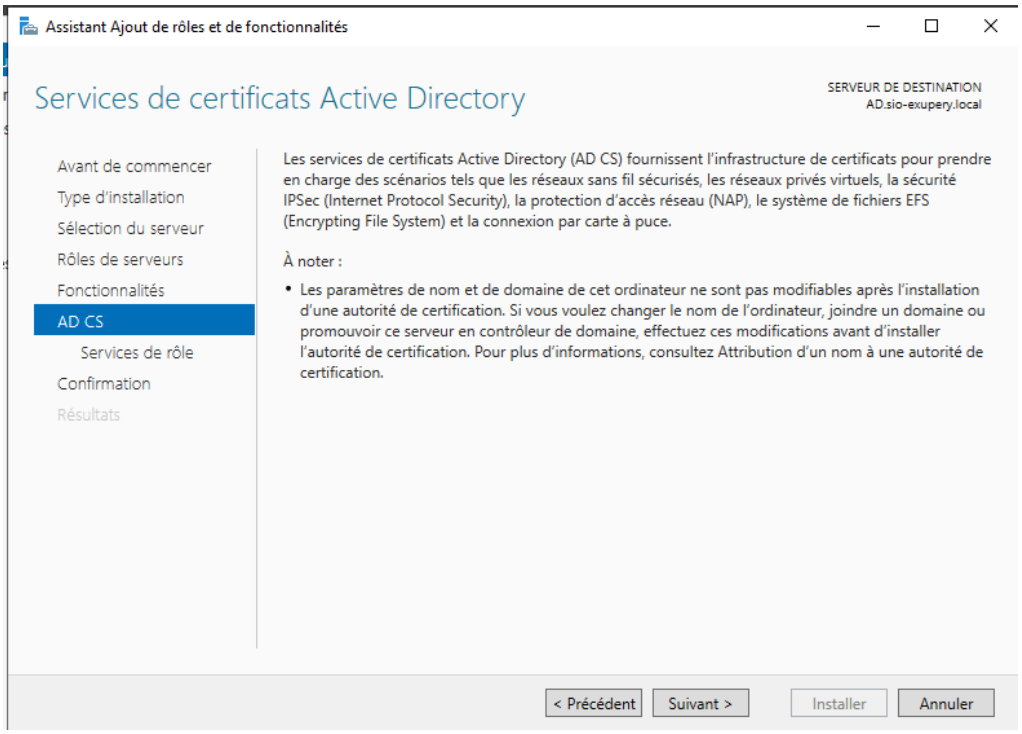



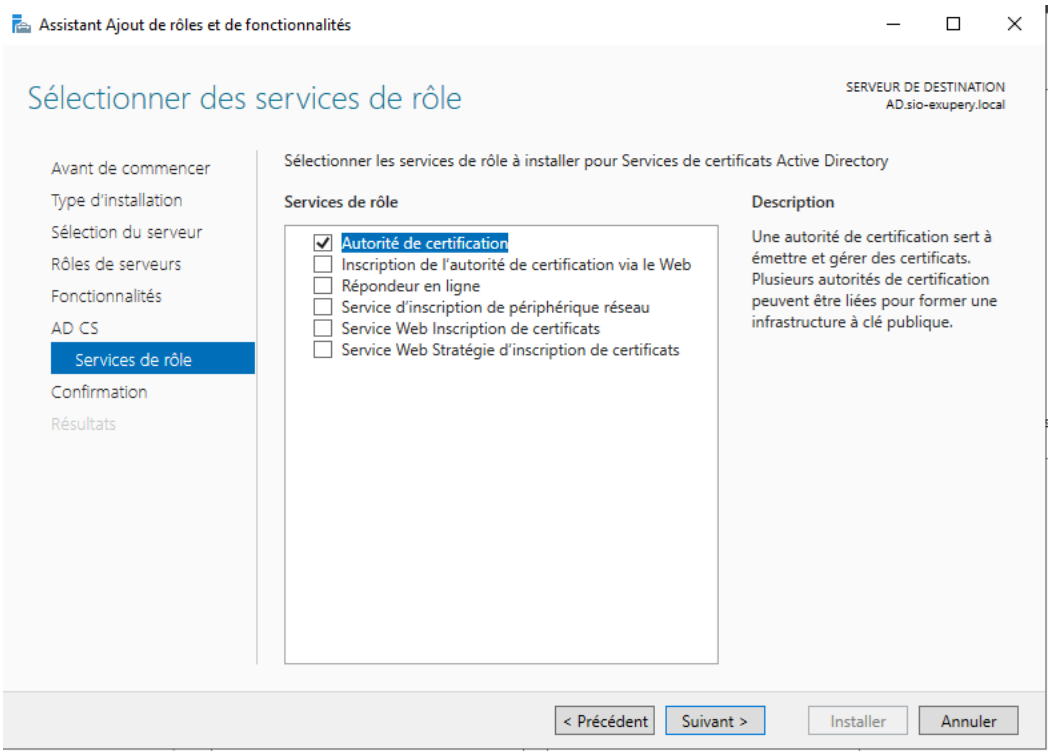
## 2.2 Ajout du rôle Services de certificats Active Directory

▪ Nous ajoutons le rôle Service de certificats Active Directory.

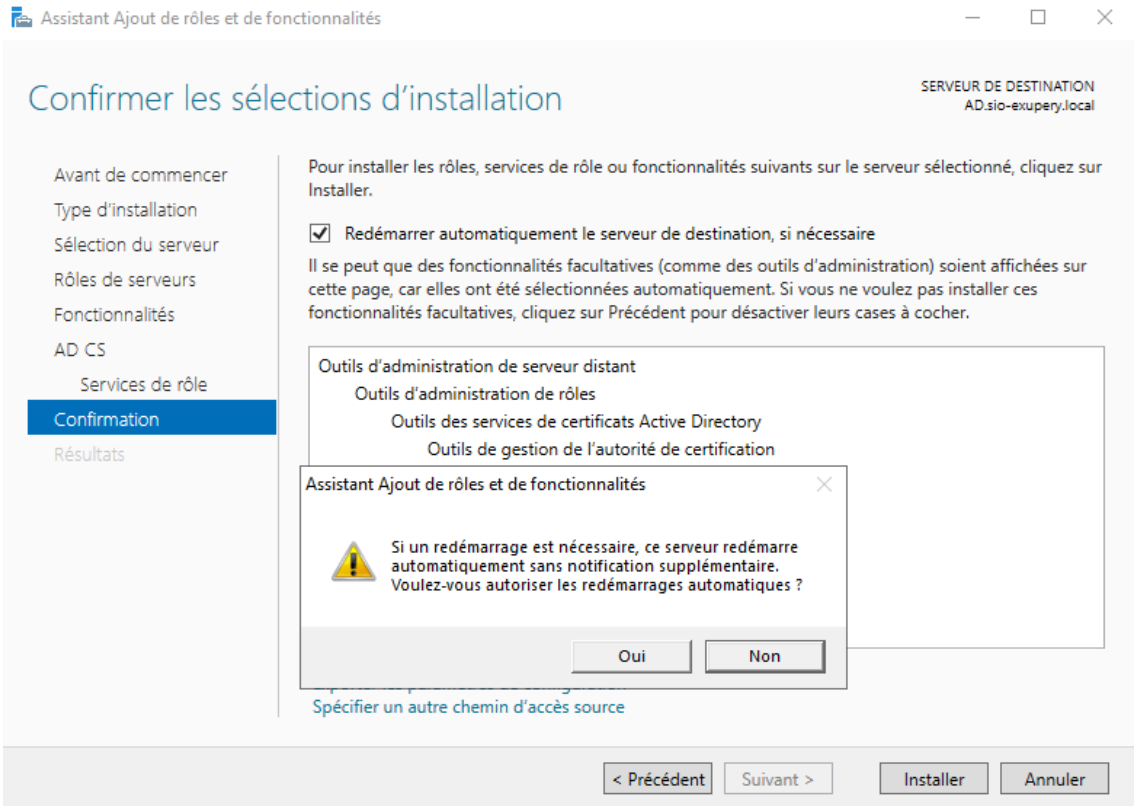



▪ Nous prenons connaissance des informations sur la page d'information AD CS et nous cliquons sur le bouton Suivant.

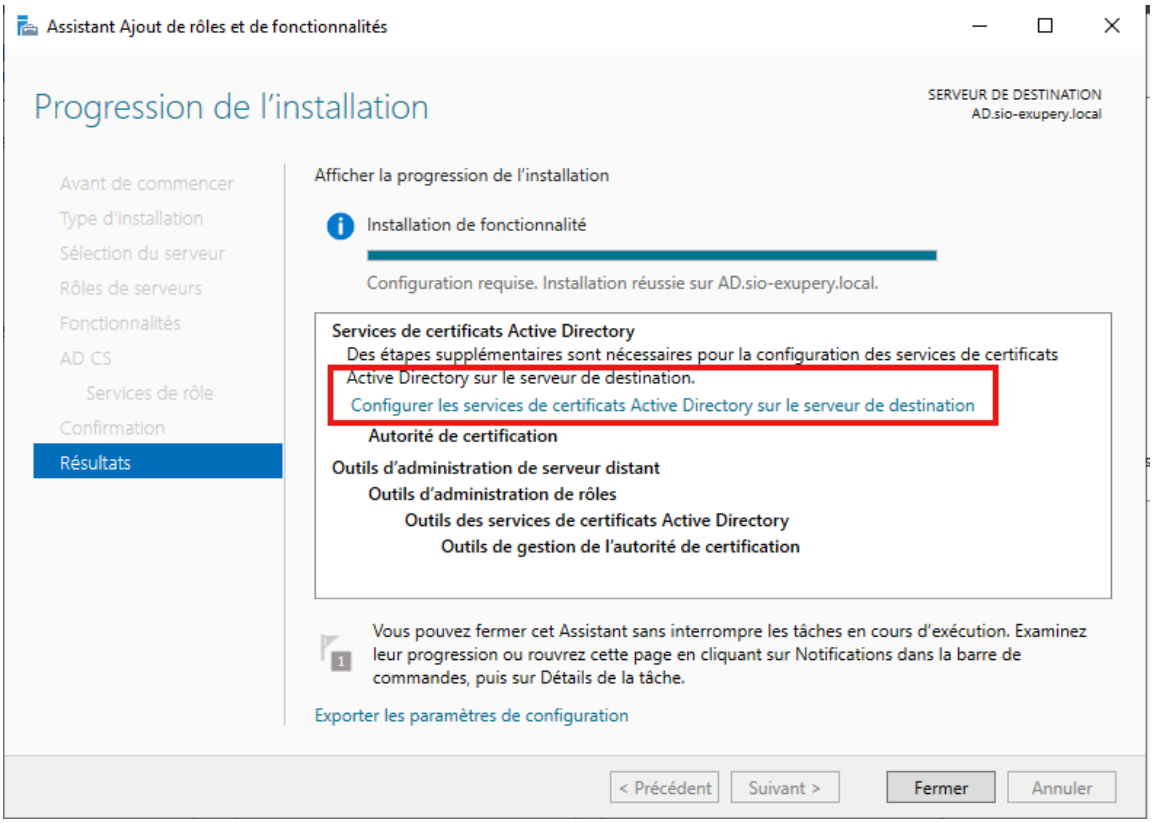


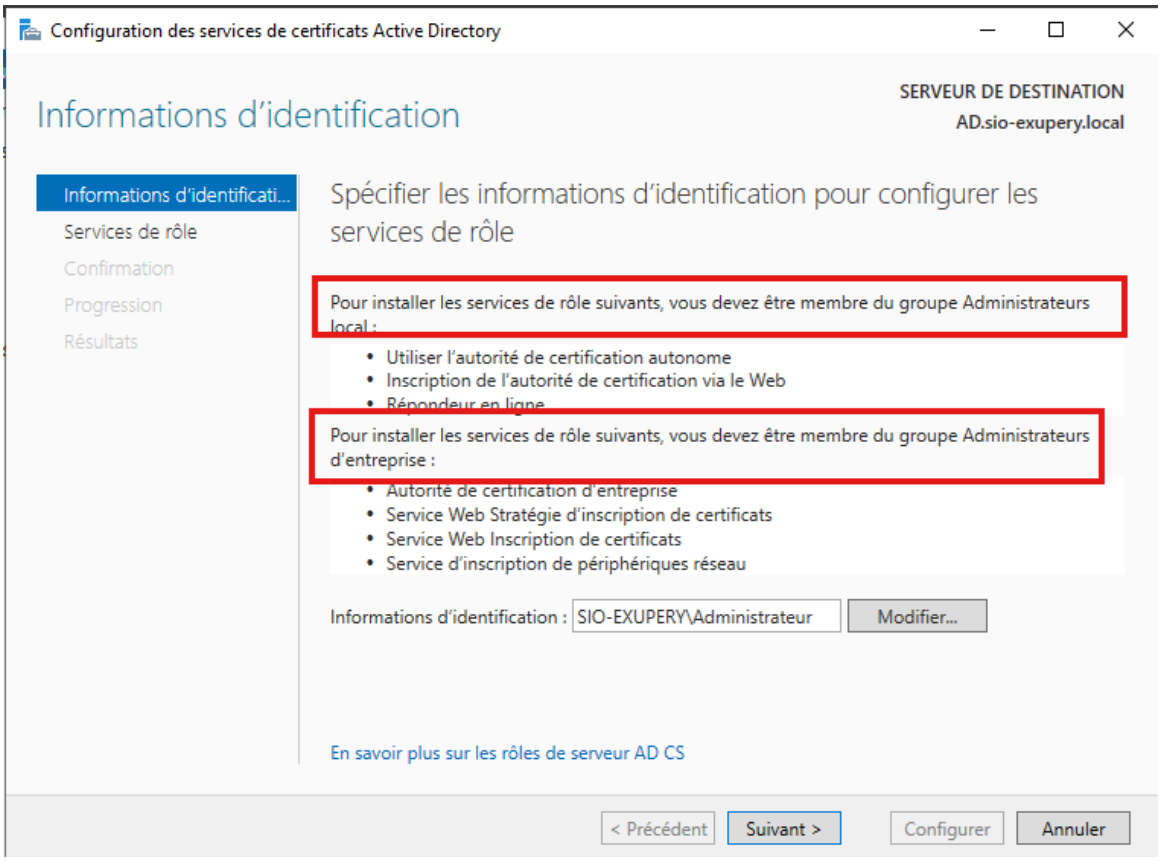



- Nous cochons la case

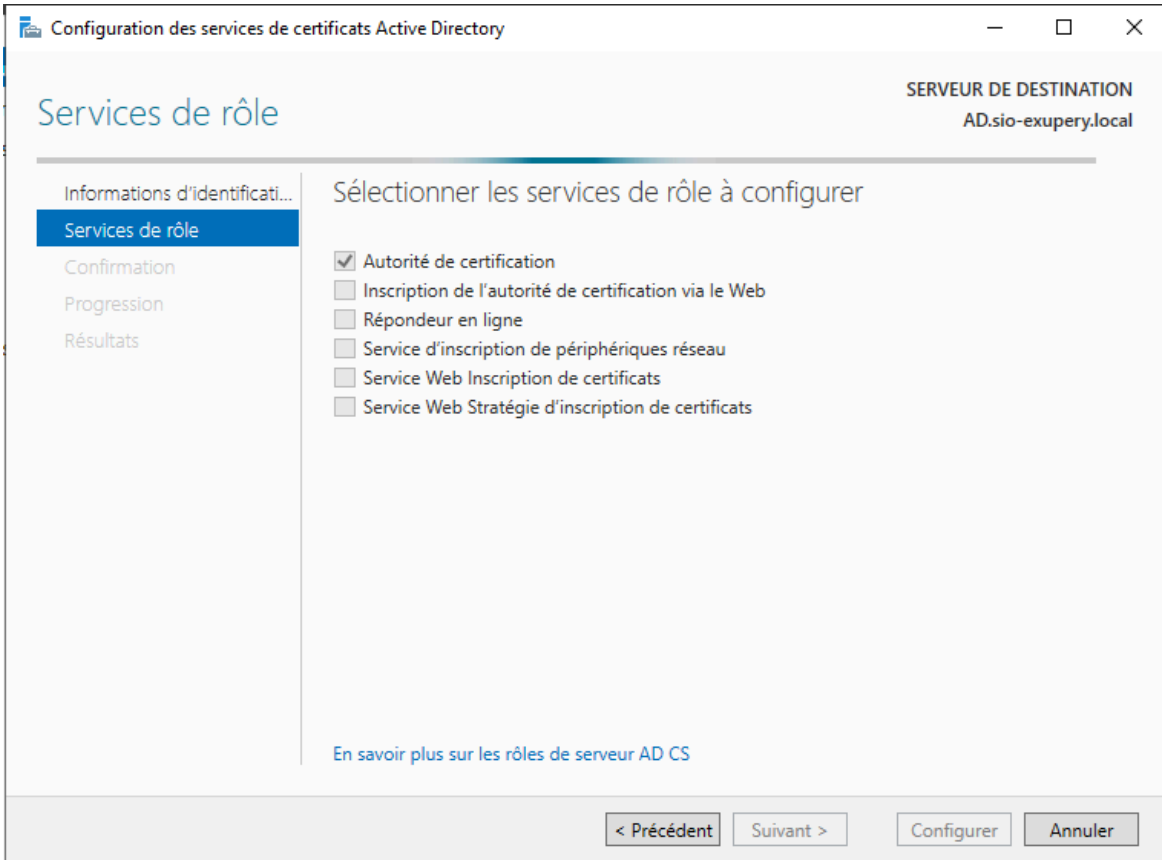


- Nous cliquons sur le lien encadré encadré en rouge ci-dessous

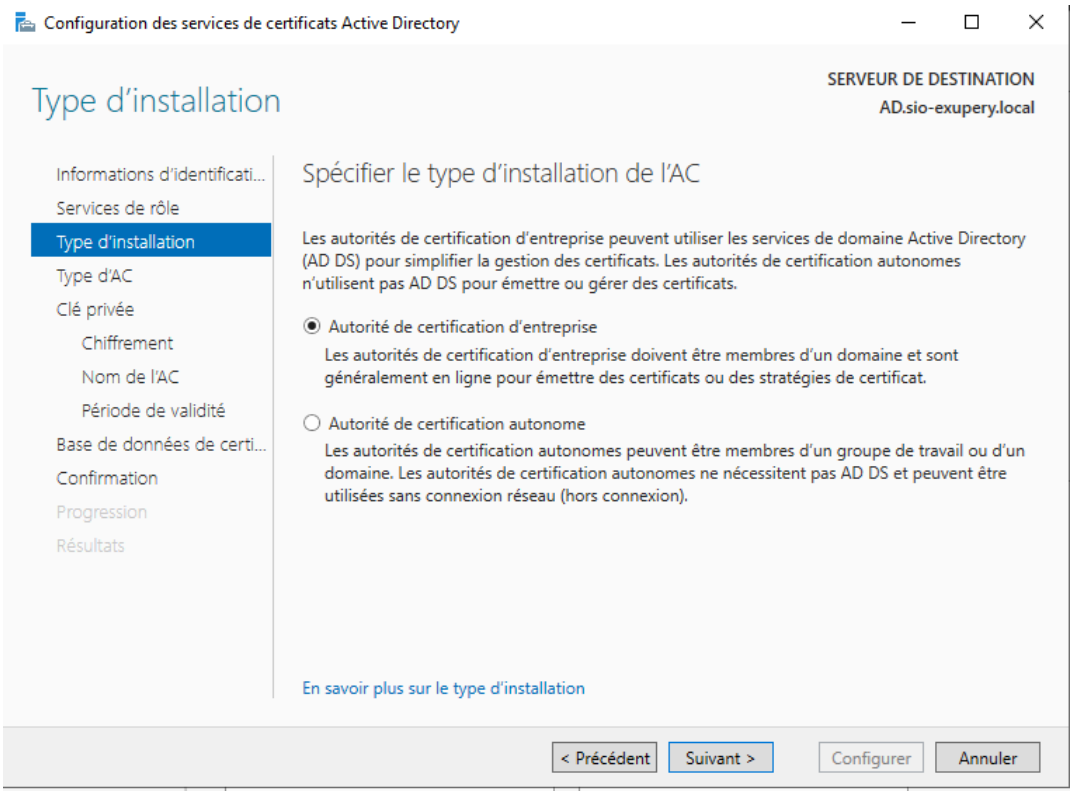


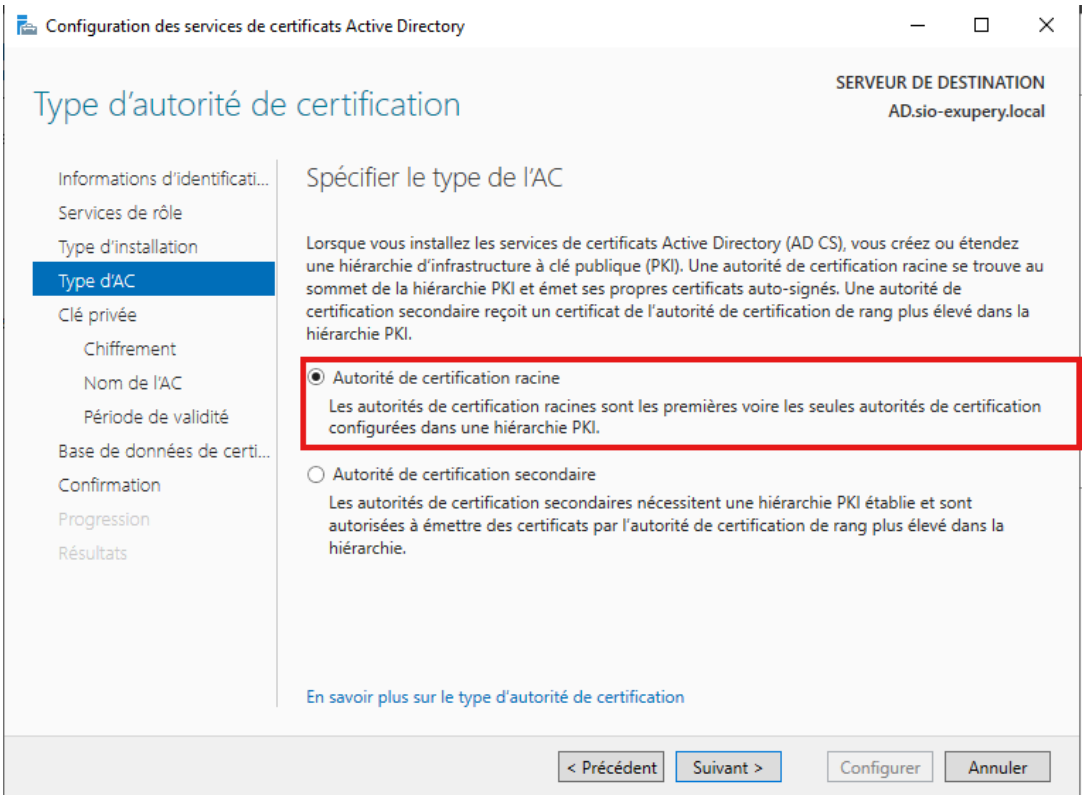
▪ Nous cochons la case Autorité de certification pour configurer ce rôle.



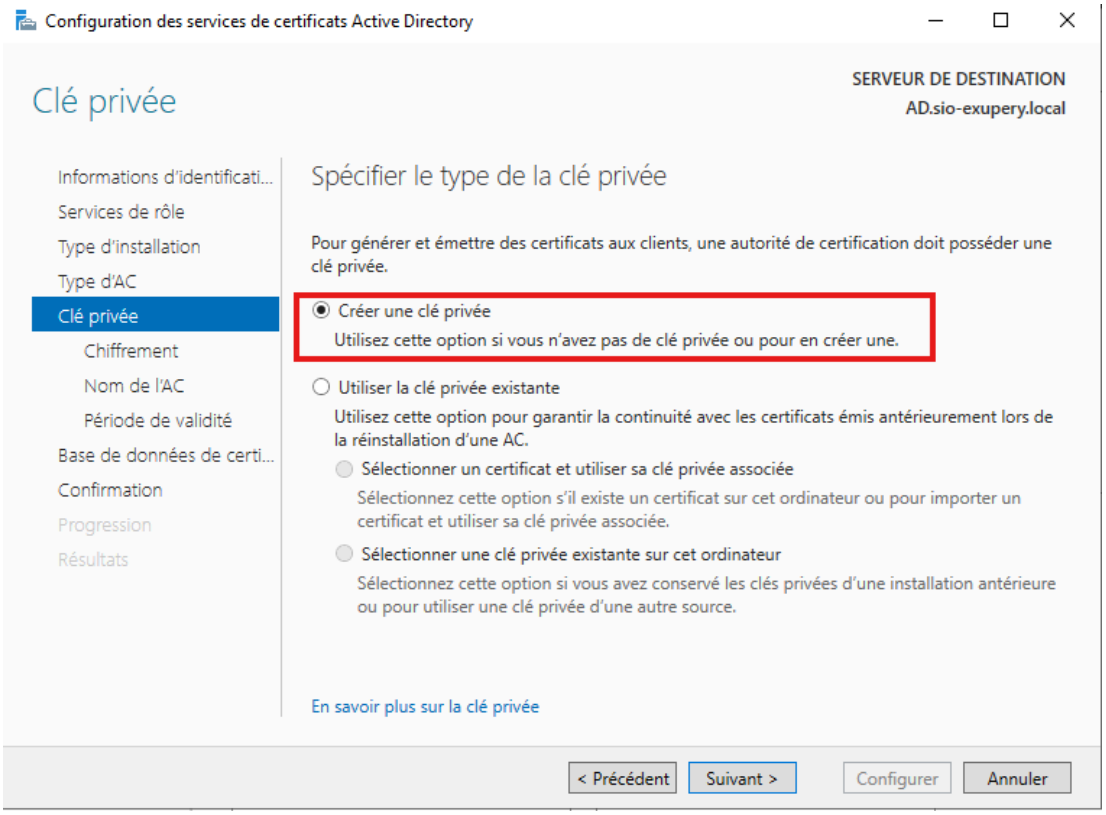

▪ Nous sélectionnons Autorité de certification d'entreprise.



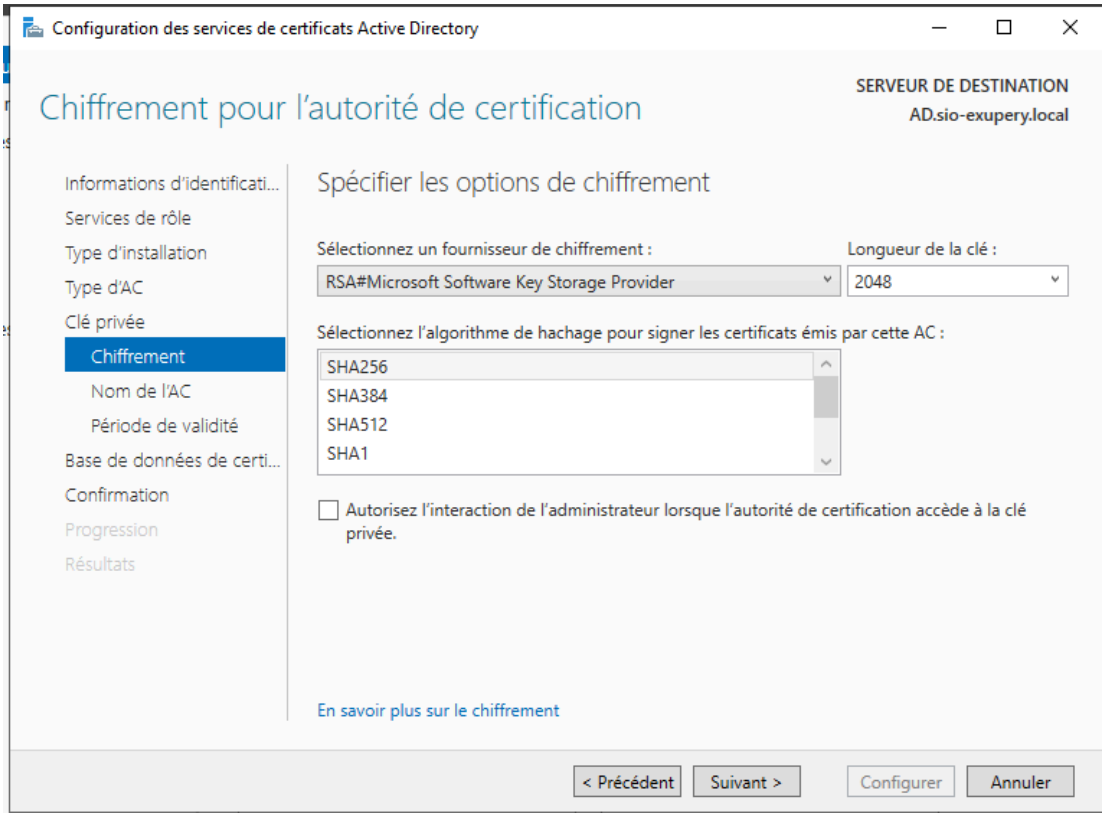
▪ Nous sélectionnons Autorité de certification racine :



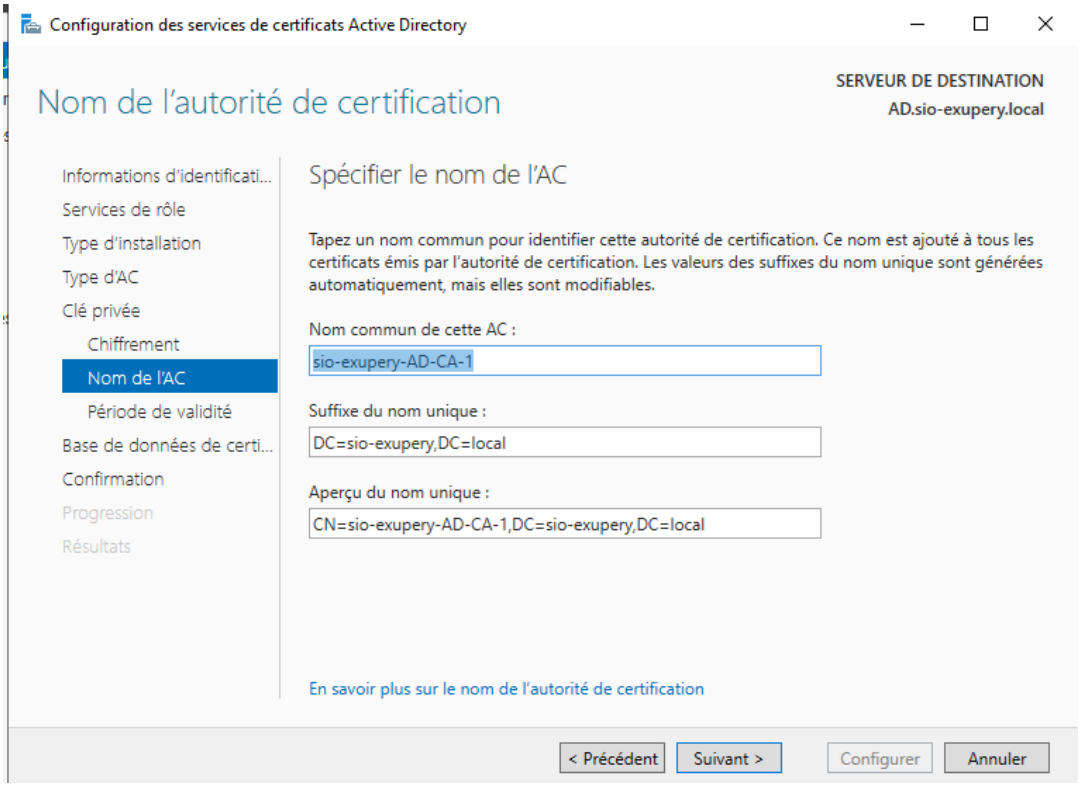

▪ On sélectionne Créer une nouvelle clé privée.



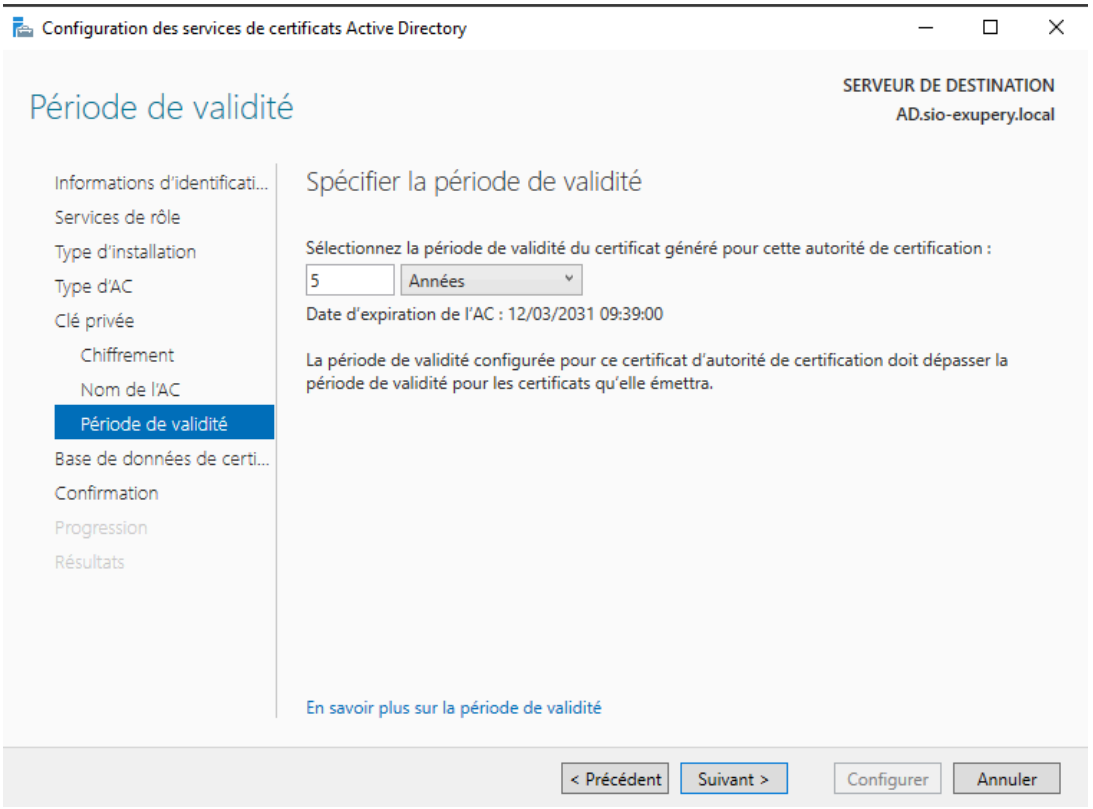
▪ On choisit l'algorithme de chiffrement ainsi que de hachage par défaut.



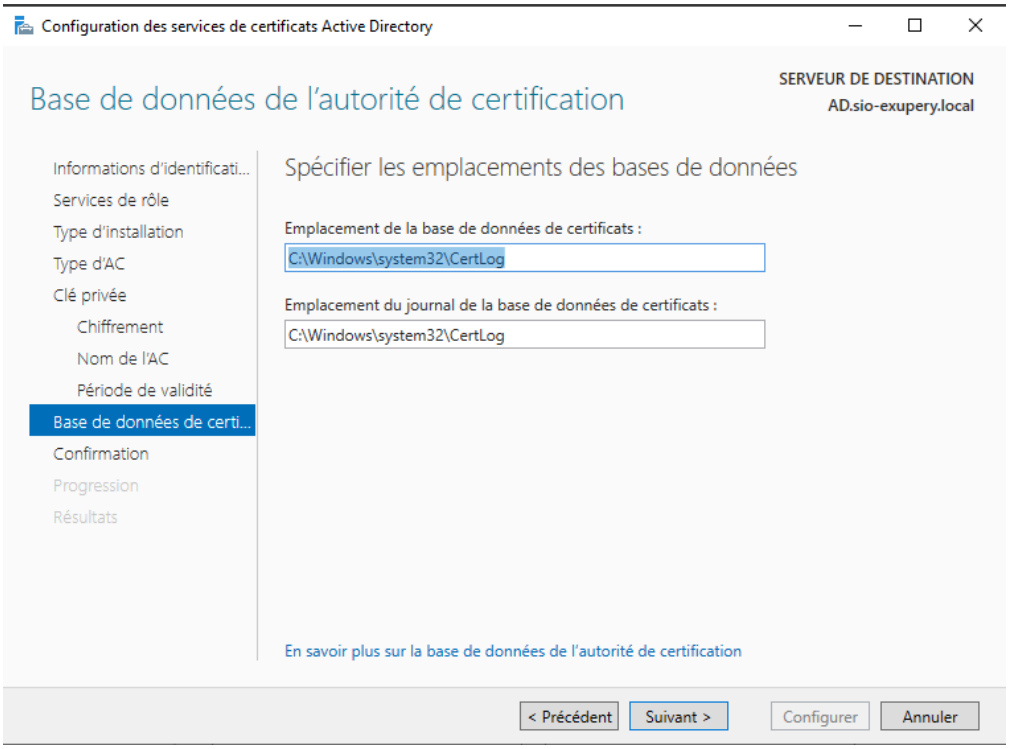

▪ Par défaut, l'assistant nomme l'autorité de certification avec le nom de domaine suivi du nom de machine : sio-exupery-AD-CA.



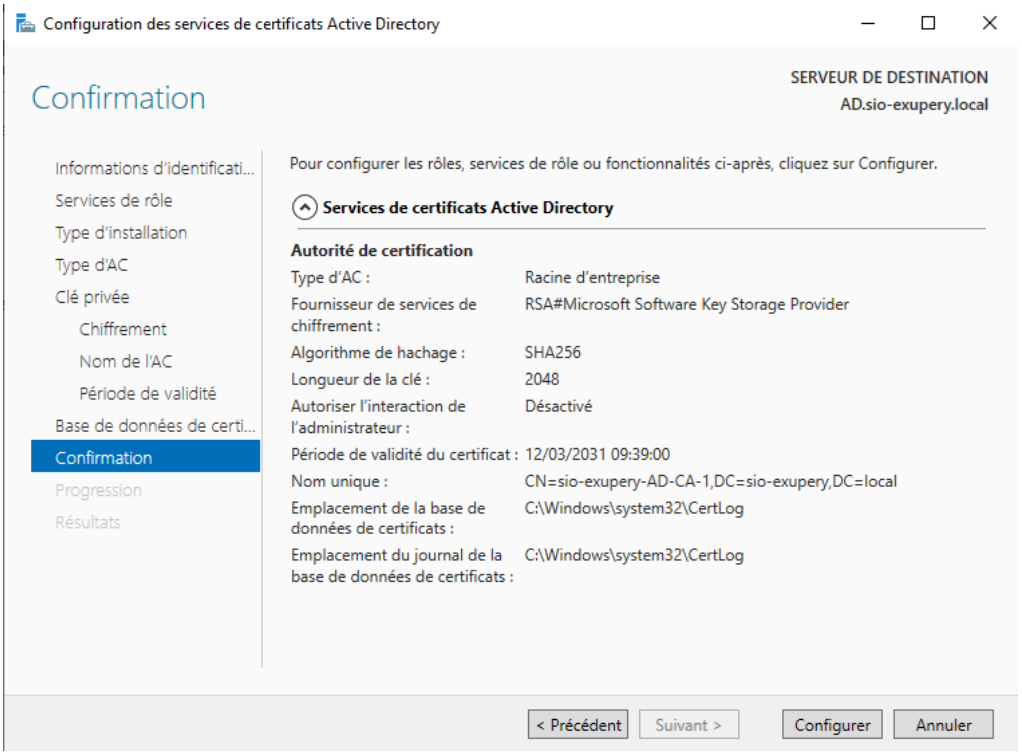
▪ On laisse la période de validité par défaut.



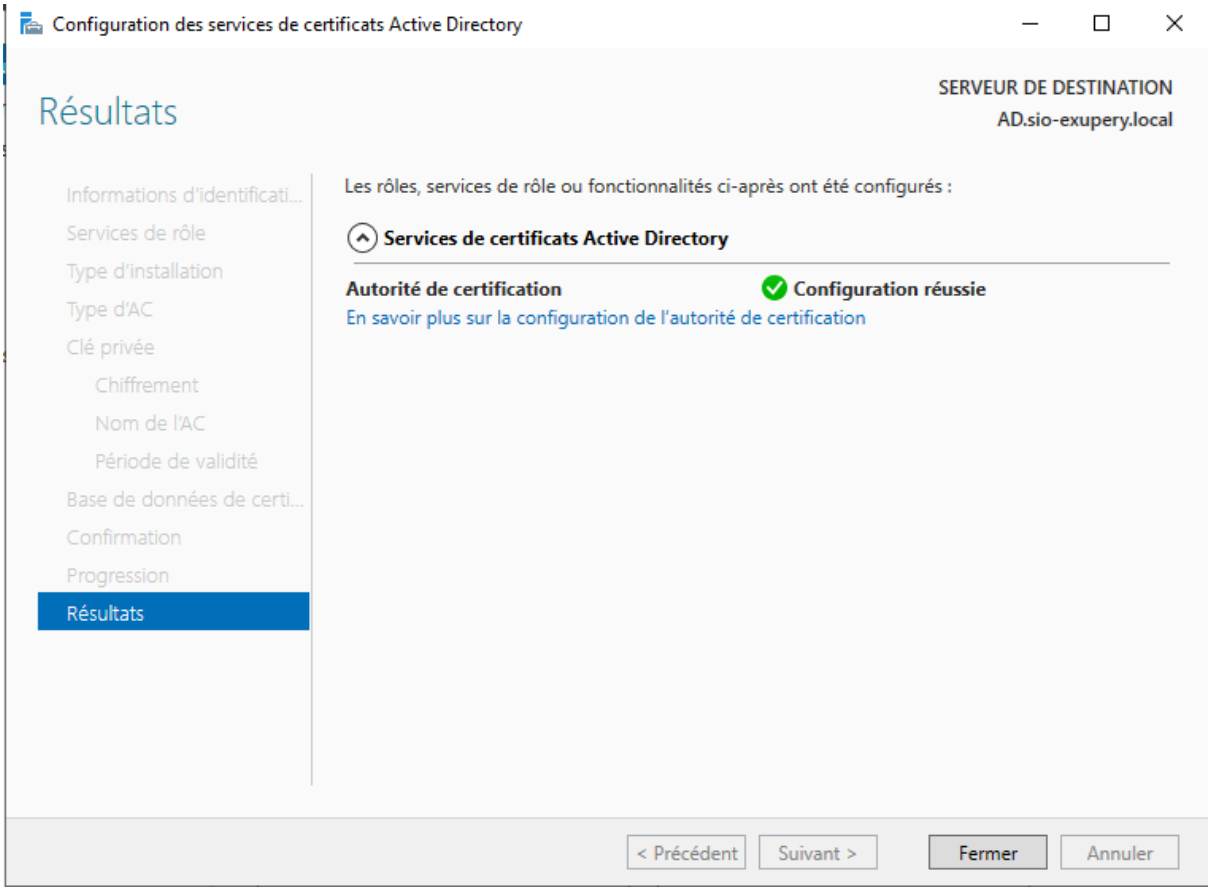

▪ On laisse également les dossiers des bases de données, par défaut.



- Nous cliquons sur Configurer.

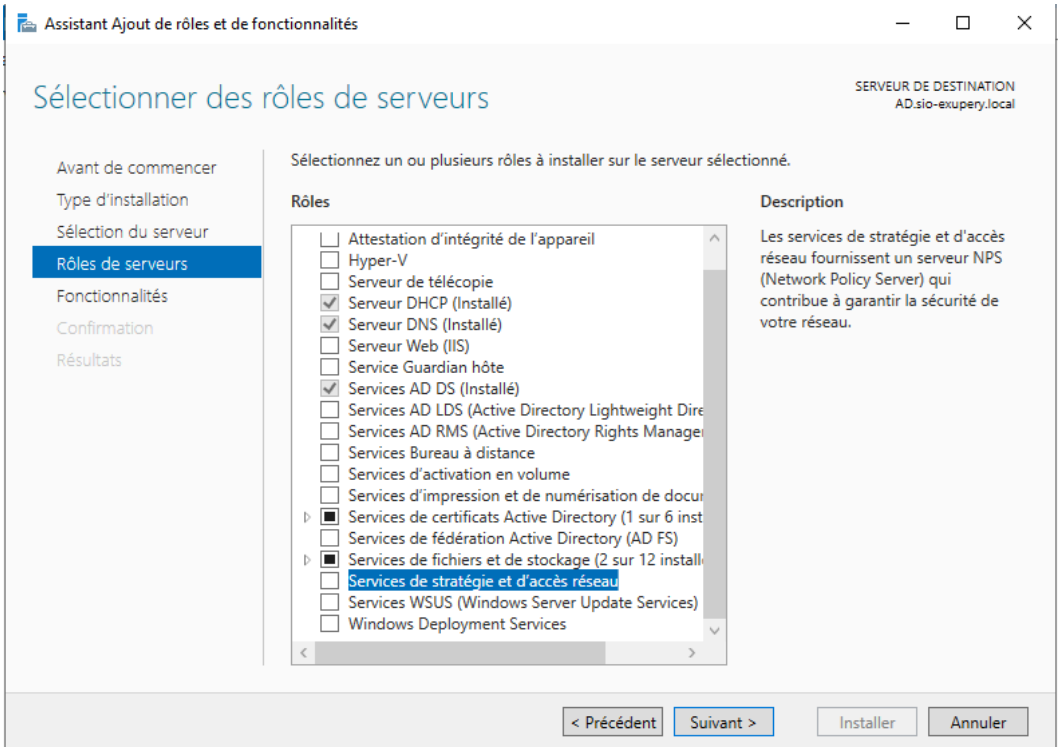



- Notre autorité de certification est maintenant installée et configurée.
  - Nous cliquons sur Fermer.

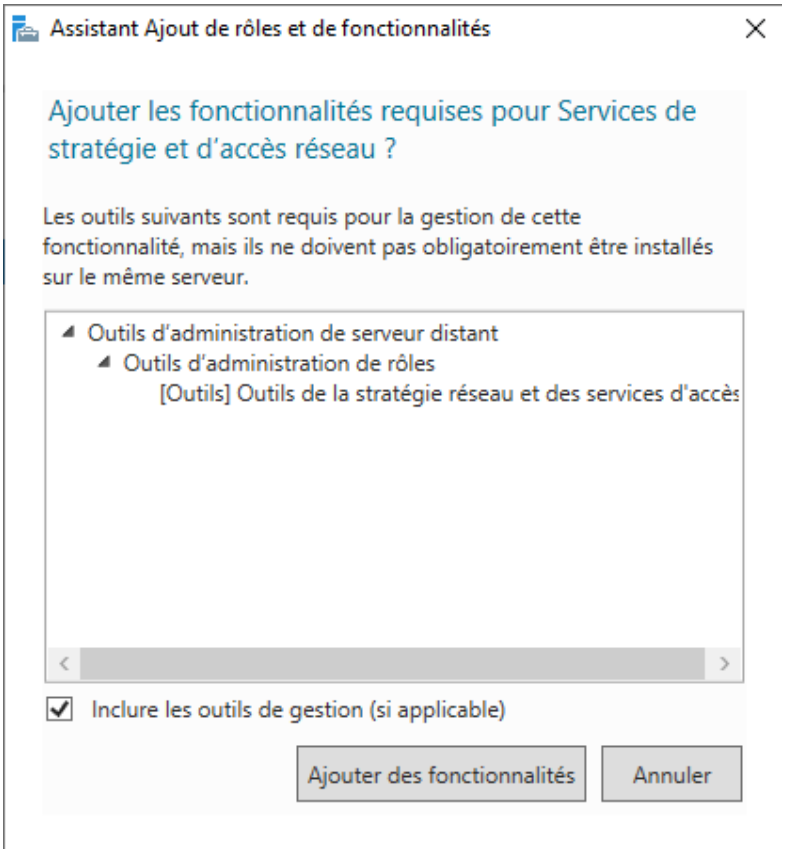


## 2.3 Installation du service NPS

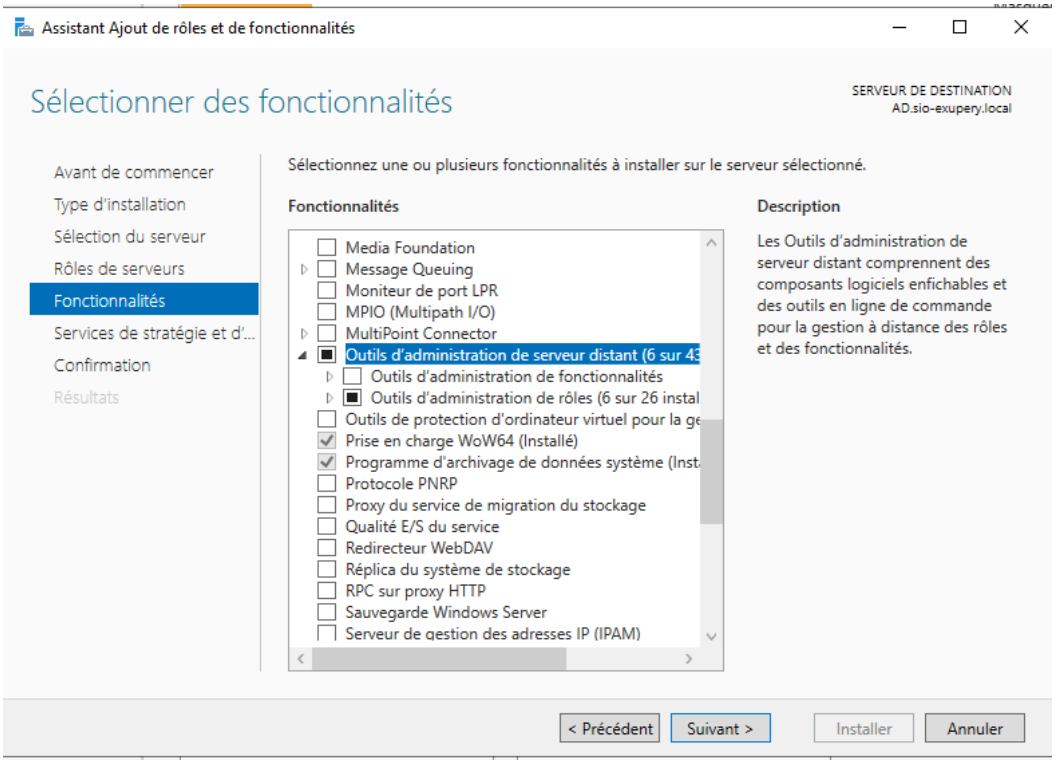
▪ On ajoute le rôle Services de stratégie et d'accès réseau.



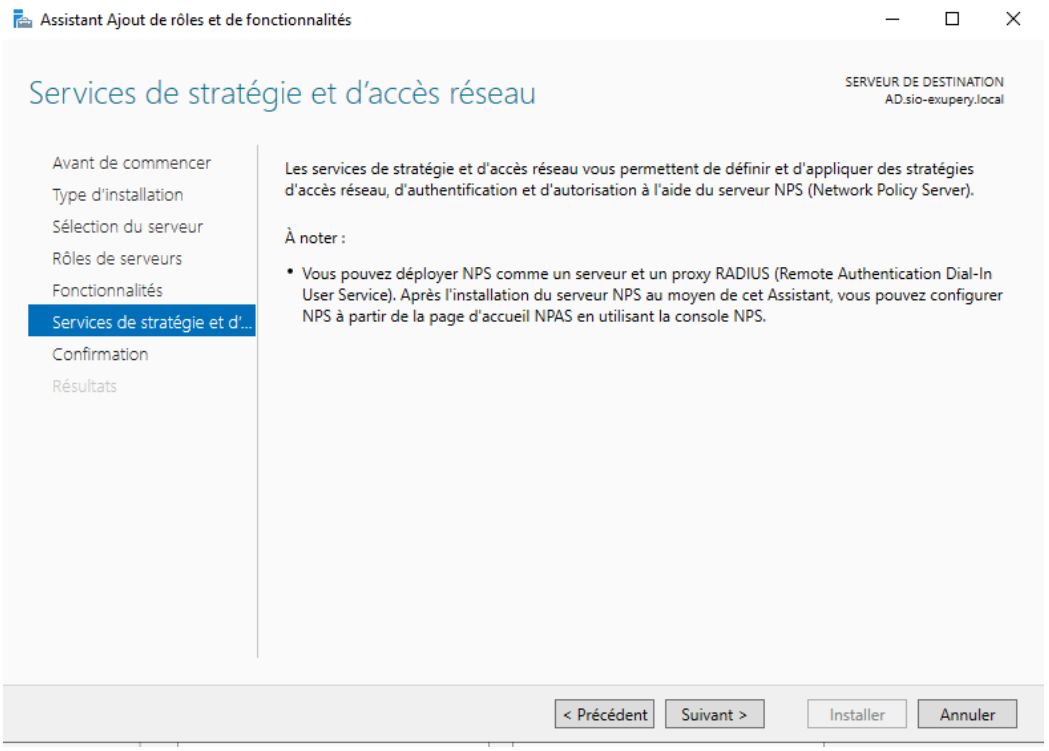

▪ Nous cliquons sur le bouton Ajouter des fonctionnalités.



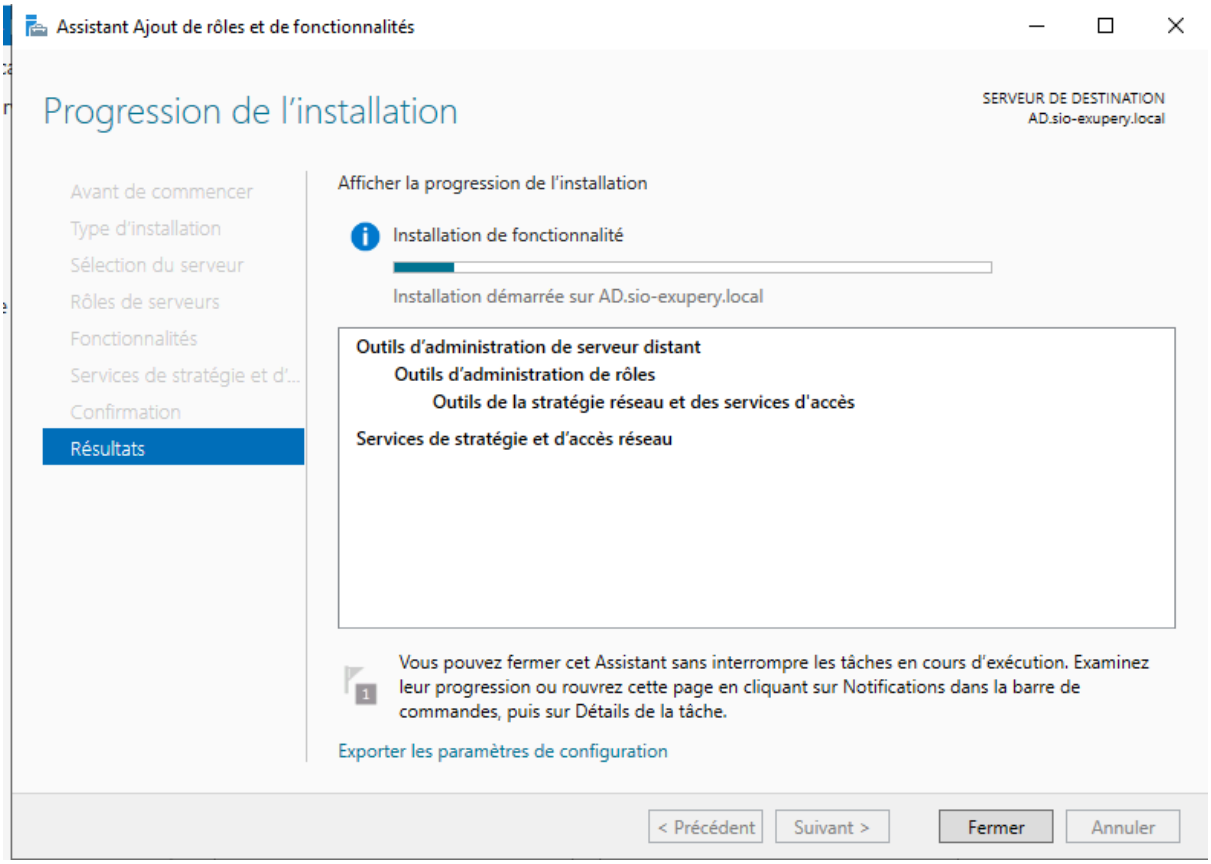
▪ On clique sur le bouton Suivant.



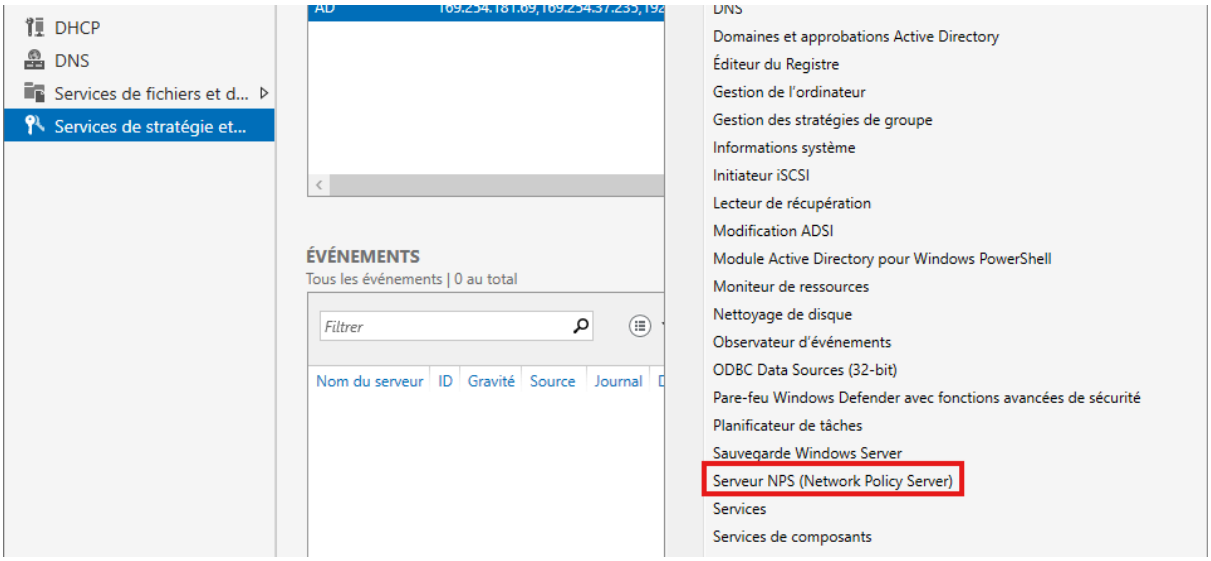

▪ De nouveau, on clique sur suivant :
- Puis nous allons cliquer sur installer.



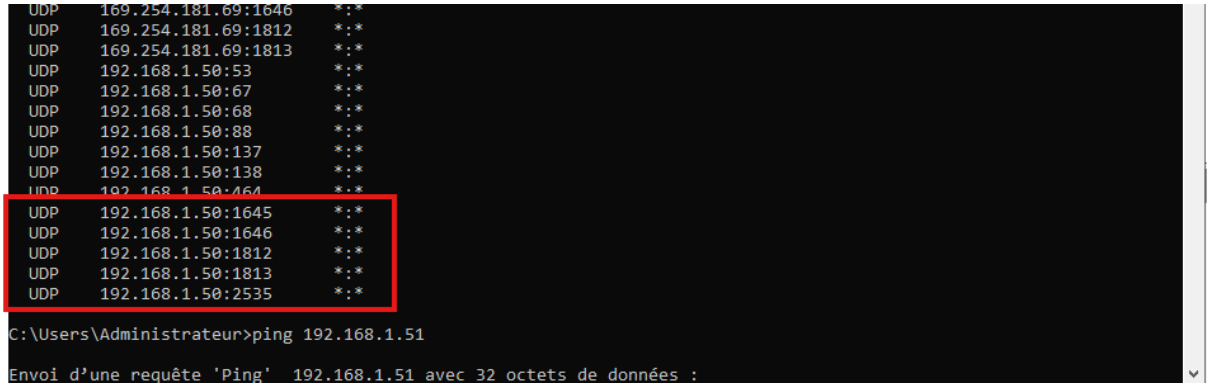
▪ Une fois terminé, nous allons cliquer sur le bouton Fermer




▪ Nous constatons la présence de la console Serveur NPS.

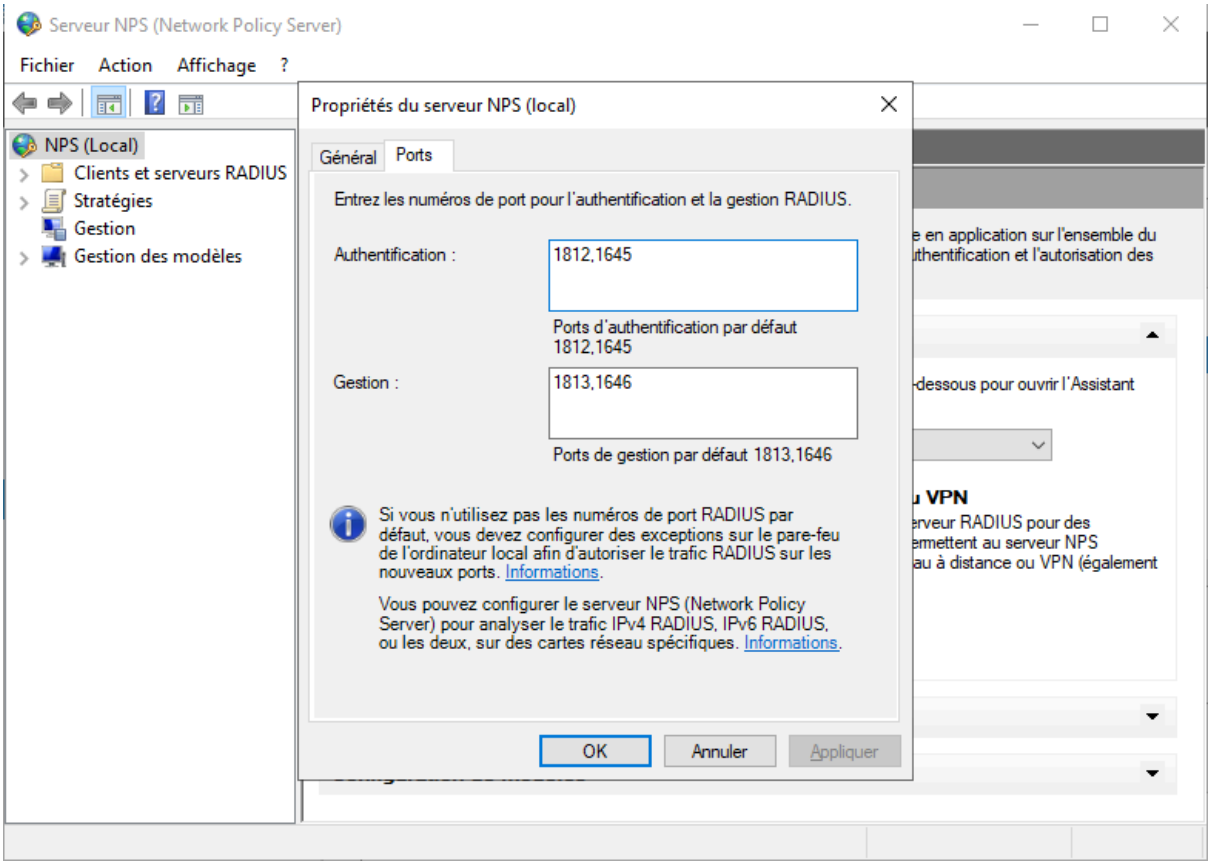


▪ Afin de vérifier le bon fonctionnement du service NPS sur le serveur, nous affichons les ports en écoute sur celui-ci avec la commande netstat -a -p udp :



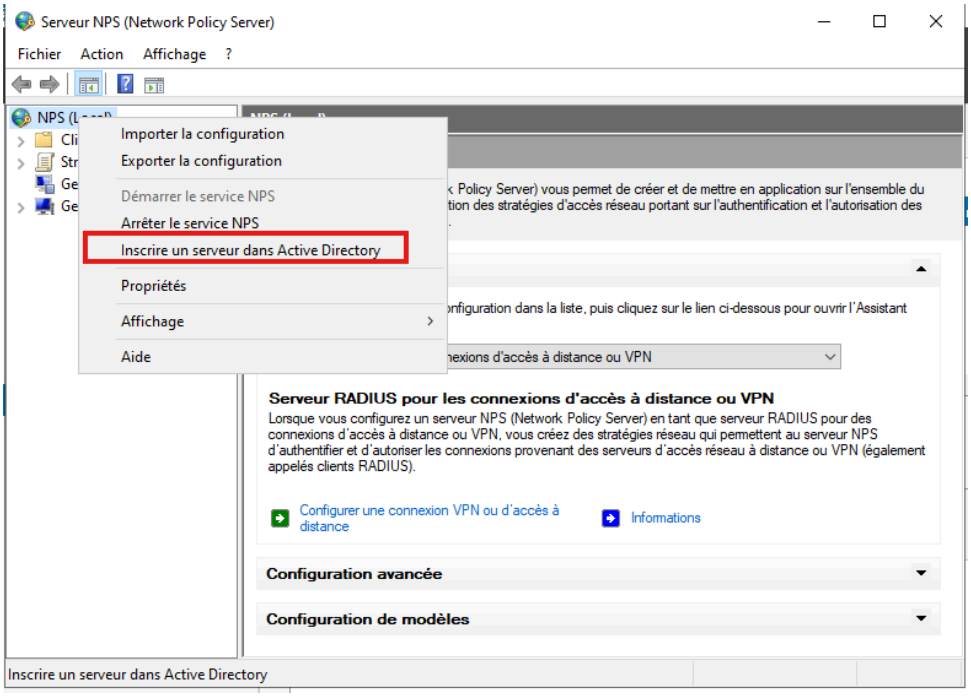

▪ Ouverture de la console du Serveur NPS :

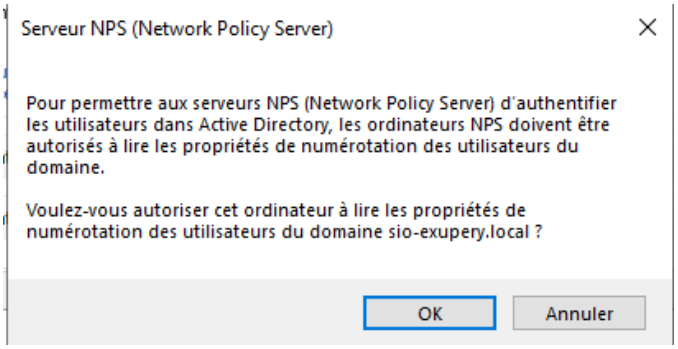
- Liste des ports dans les propriétés du serveur NPS :

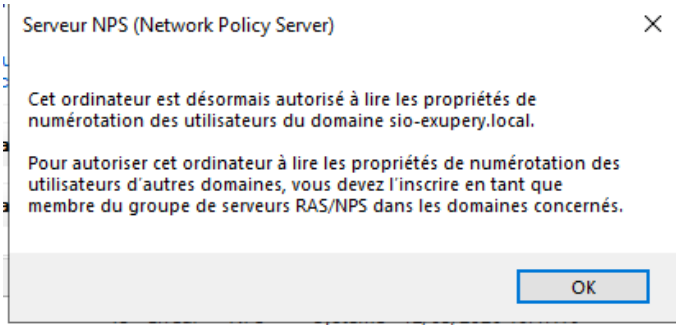


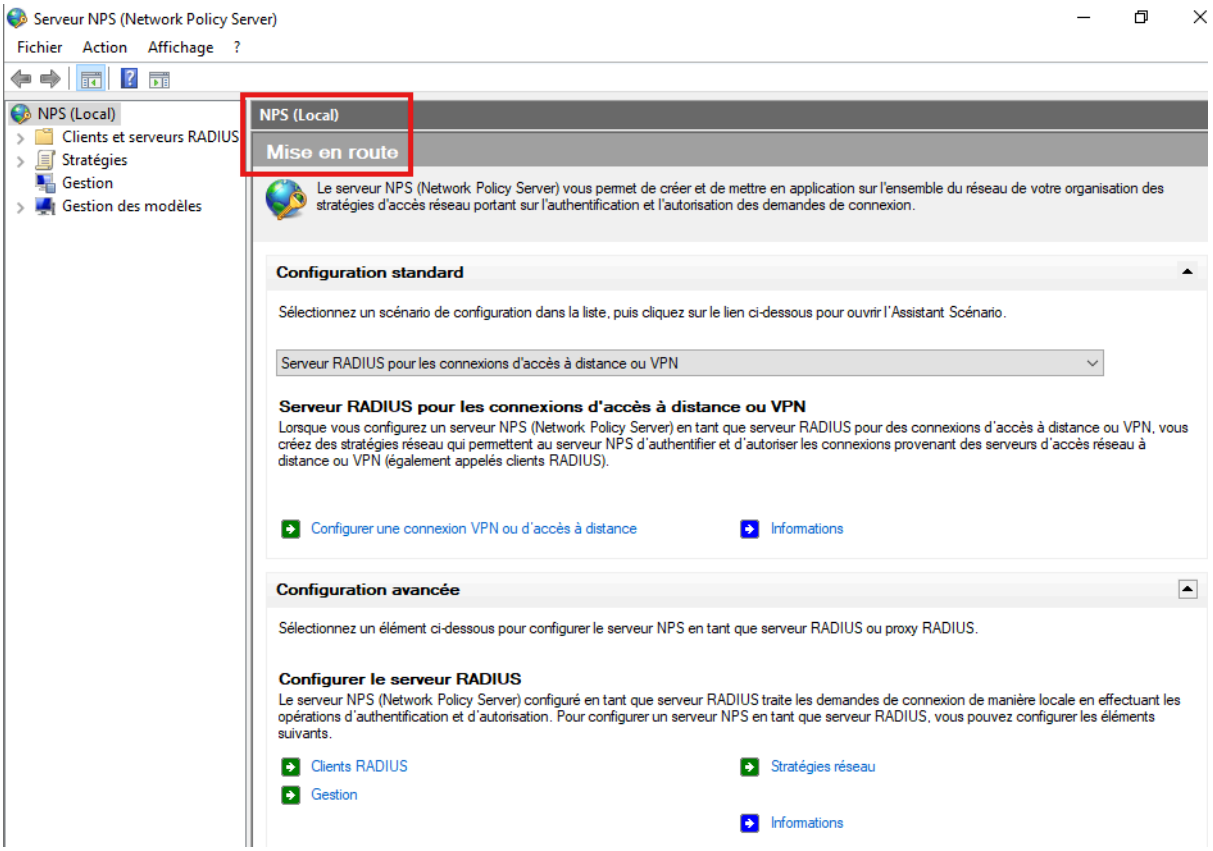
## 2.4 Configuration du serveur RADIUS NPS

▪ Nous cliquons depuis le menu Action sur Inscrire un serveur dans Active Directory, afin d'inscrire NPS dans Active Directory pour lui permettre d'interroger la base des utilisateurs.



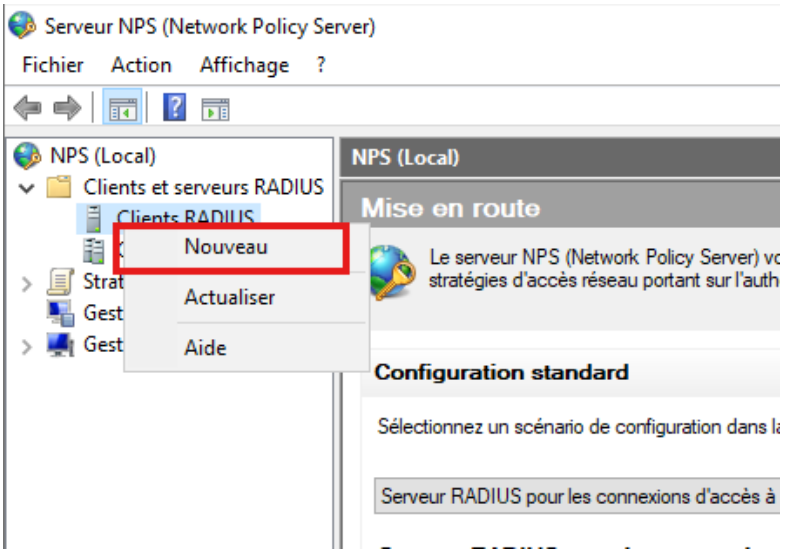



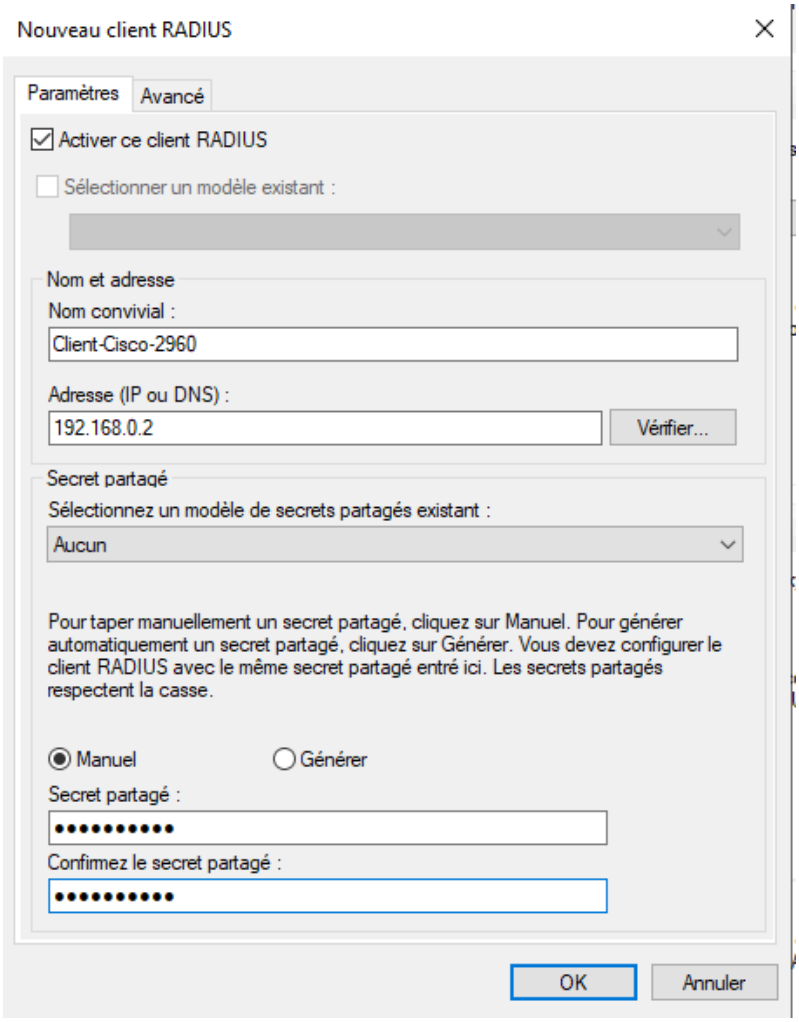




Serveur NPS (Network Policy Server)
Fichier Action Affichage ?
NPS (Local)
Clients et serveurs RADIUS
Stratégies
Gestion
Gestion des modèles
NPS (Local)
Mise en route
Le serveur NPS (Network Policy Server) vous permet de créer et de mettre en application sur l'ensemble du réseau de votre organisation des stratégies d'accès réseau portant sur l'authentification et l'autorisation des demandes de connexion.
Configuration standard
Sélectionnez un scénario de configuration dans la liste, puis cliquez sur le lien ci-dessous pour ouvrir l'Assistant Scénario.
Serveur RADIUS pour les connexions d'accès à distance ou VPN
Serveur RADIUS pour les connexions d'accès à distance ou VPN
Lorsque vous configurez un serveur NPS (Network Policy Server) en tant que serveur RADIUS pour des connexions d'accès à distance ou VPN, vous créez des stratégies réseau qui permettent au serveur NPS d'authentifier et d'autoriser les connexions provenant des serveurs d'accès réseau à distance ou VPN (également appelés clients RADIUS).
Configurer une connexion VPN ou d'accès à distance
Informations
Configuration avancée
Sélectionnez un élément ci-dessous pour configurer le serveur NPS en tant que serveur RADIUS ou proxy RADIUS.
Configurer le serveur RADIUS
Le serveur NPS (Network Policy Server) configuré en tant que serveur RADIUS traite les demandes de connexion de manière locale en effectuant les opérations d'authentification et d'autorisation. Pour configurer un serveur NPS en tant que serveur RADIUS, vous pouvez configurer les éléments suivants.
Clients RADIUS
Stratégies réseau
Gestion
Informations

## 2.4.1 Déclaration du client RADIUS

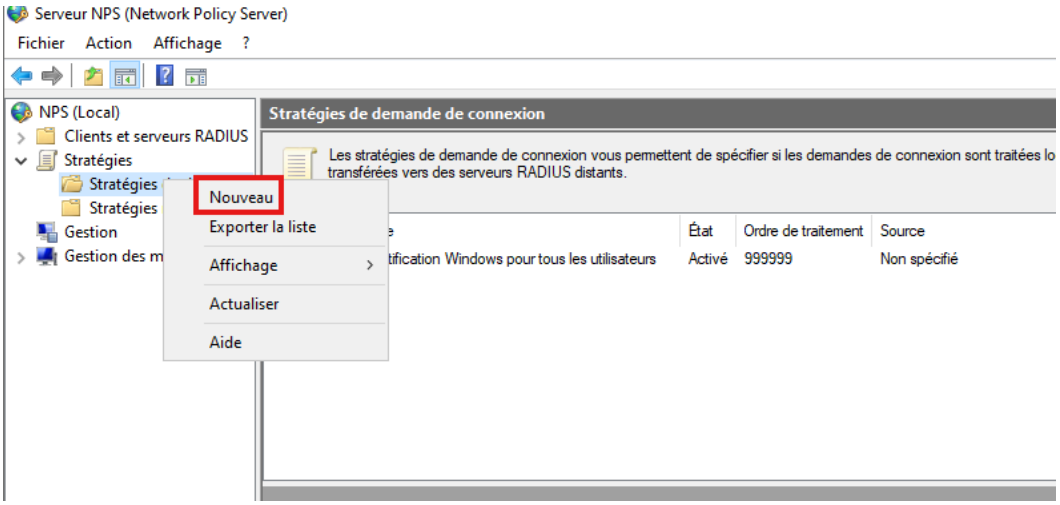
▪ Nous effectuons un clic droit sur l'entrée Clients RADIUS puis nous sélectionnons “Nouveau”.



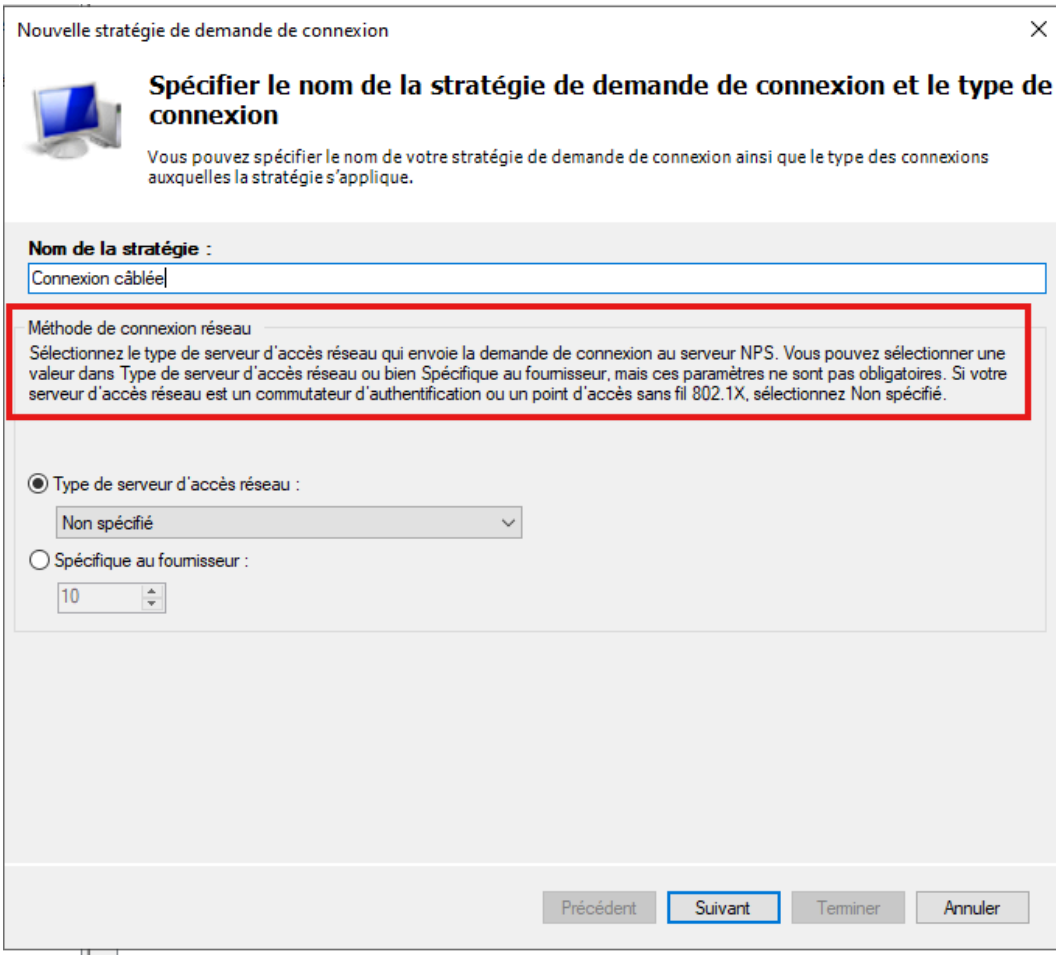
## 2.4.2 Déclaration d'une stratégie de demande de connexion

▪ Nous cliquons droit sur l'entrée Stratégies de demande de connexion et on sélectionne "Nouveau".

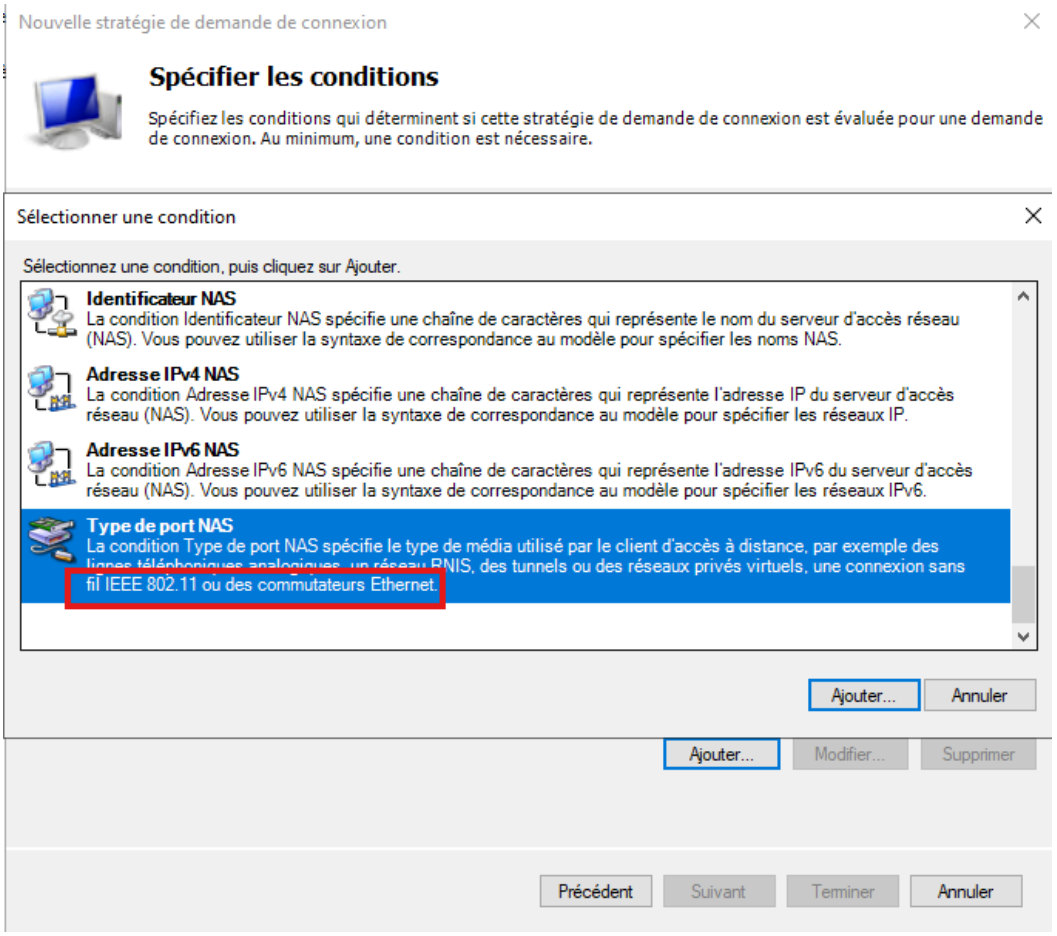


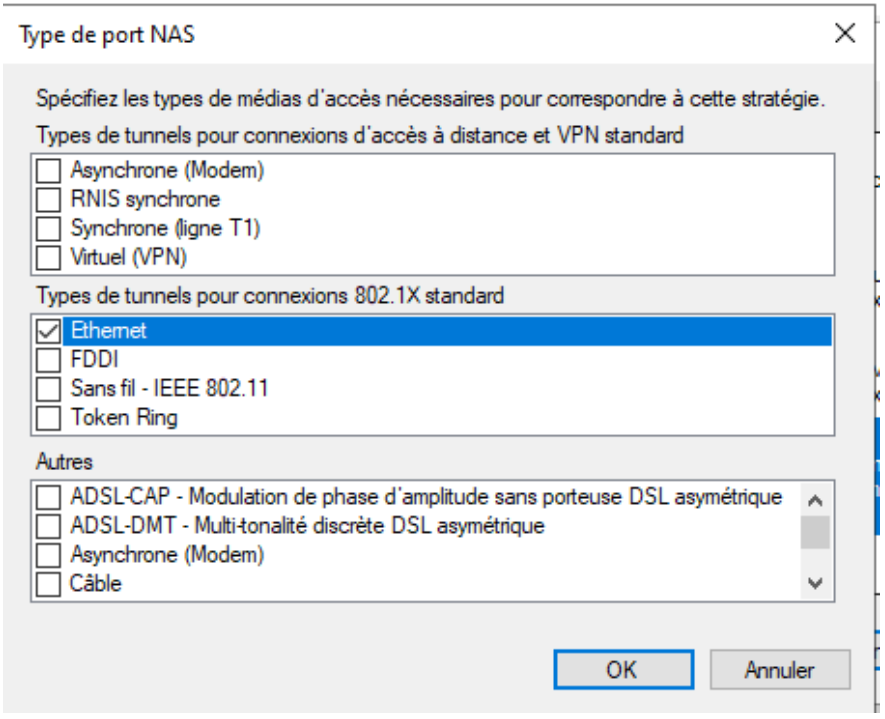

▪ Nous y spécifions un nom de stratégie (Connexion câblée).

- On laisse le type de serveur d'accès réseau sur non spécifié car nous utilisons un commutateur en tant que client Radius.

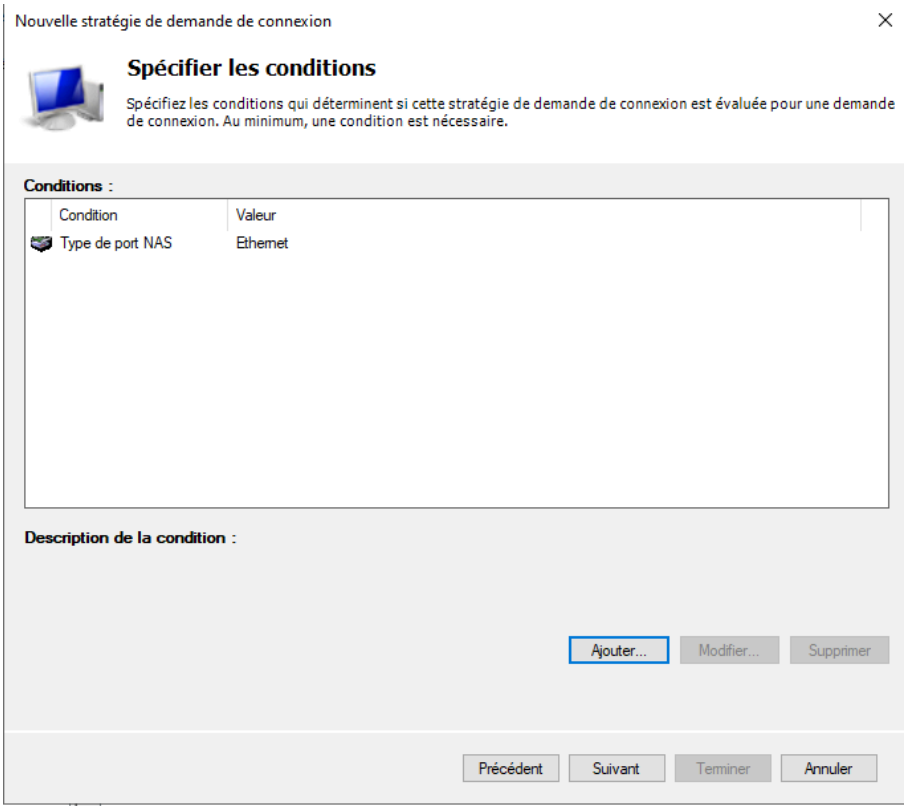


▪ On déclare une stratégie de demande de connexion pour Ethernet.

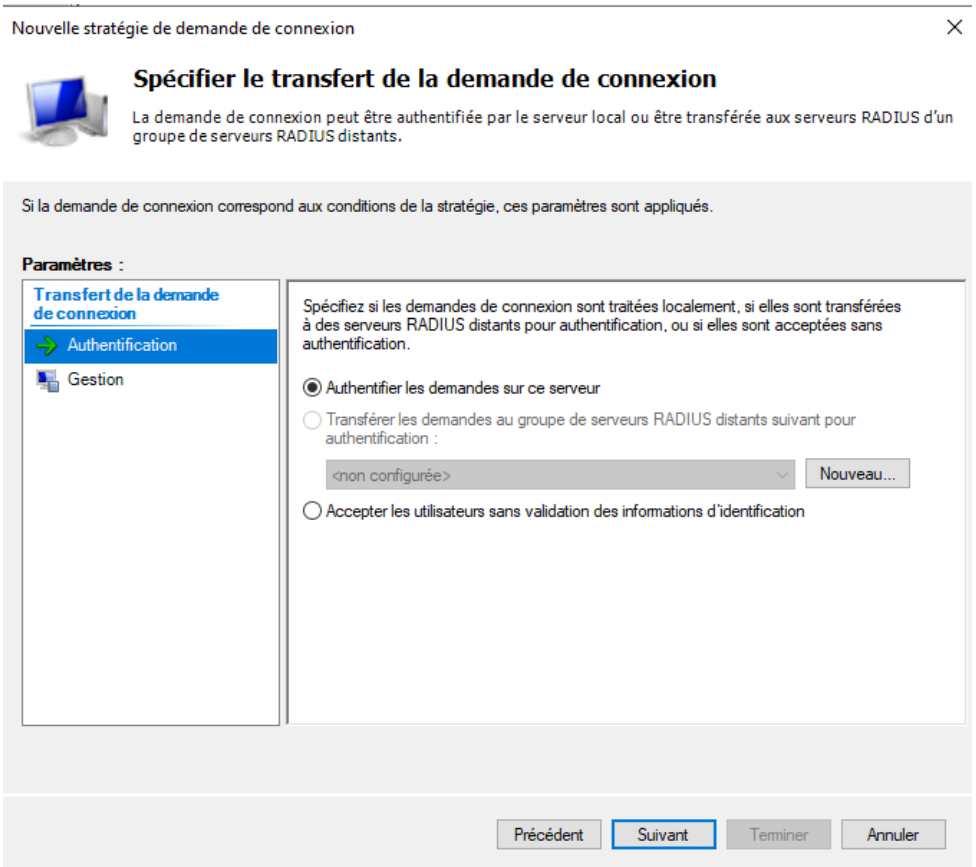


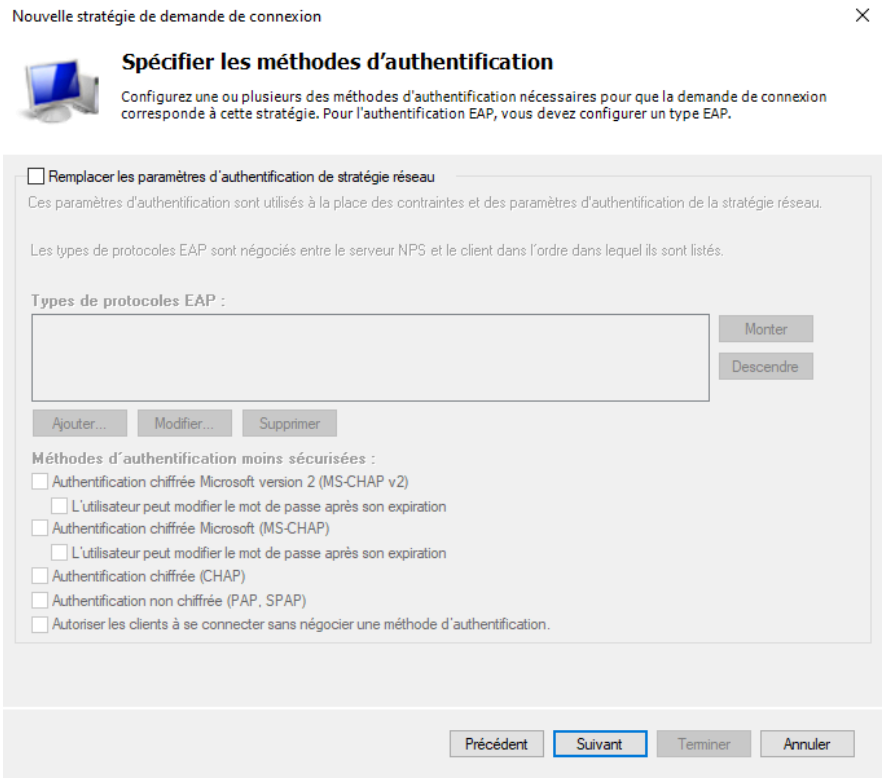
Nous cliquons sur le bouton Suivant.



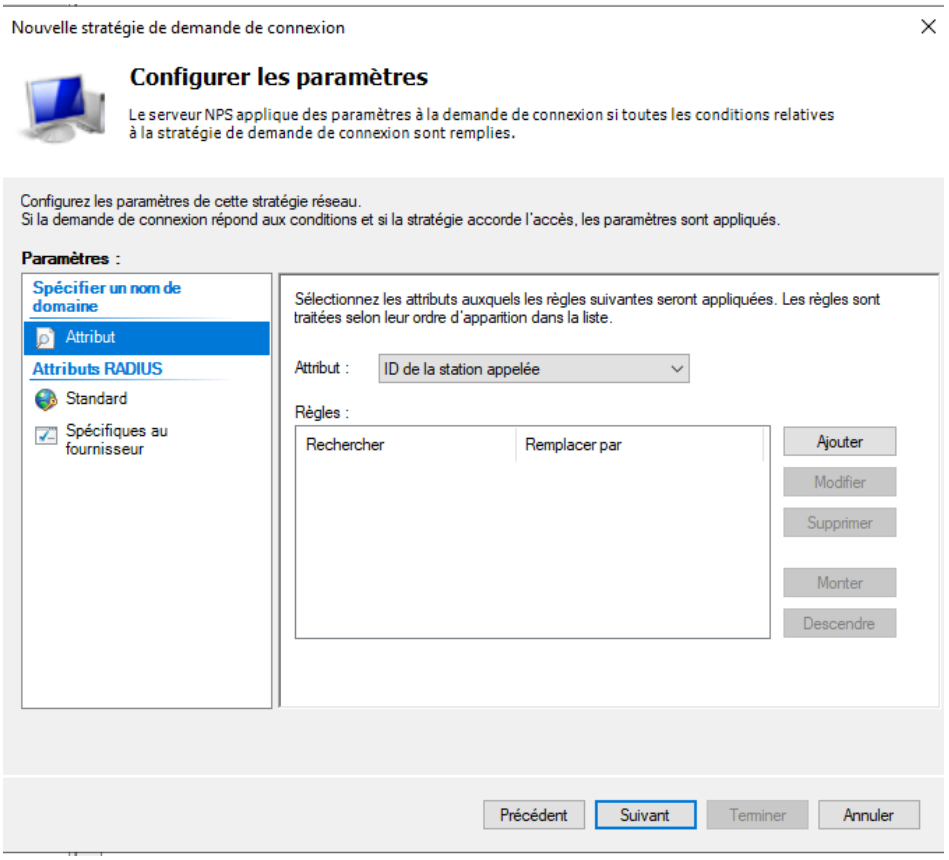

- Nous gardons le choix par défaut dans l'écran suivant.



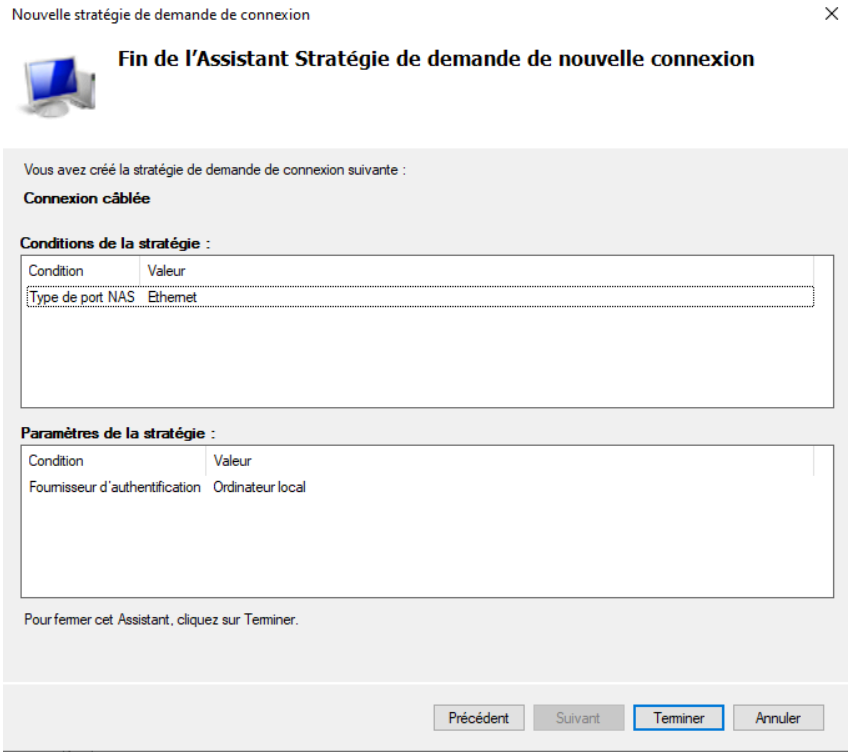
- Nous devenons laisser tel que cela est. On clique de nouveau sur suivant

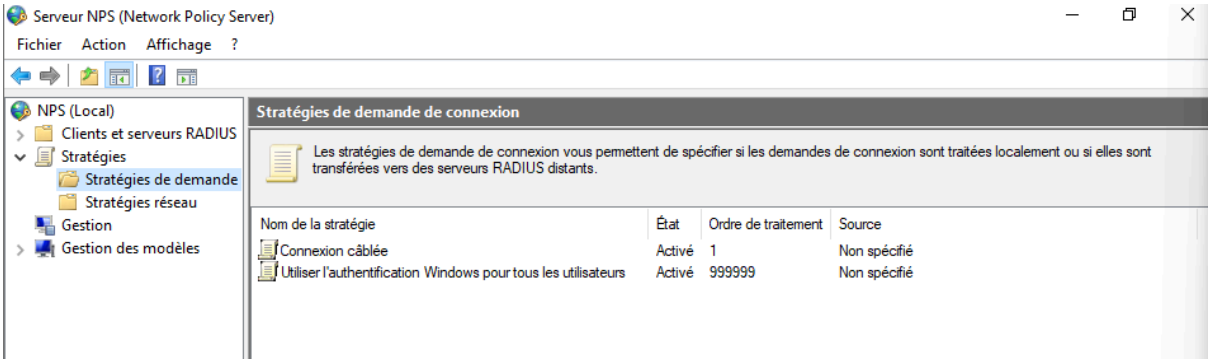



- Suivant



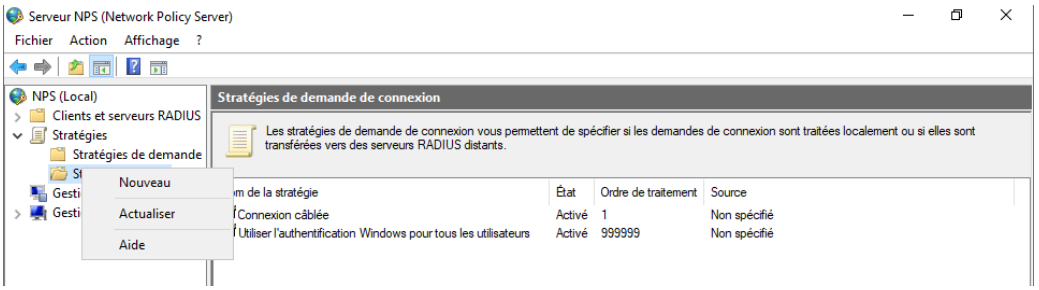
- Nous cliquons sur terminer



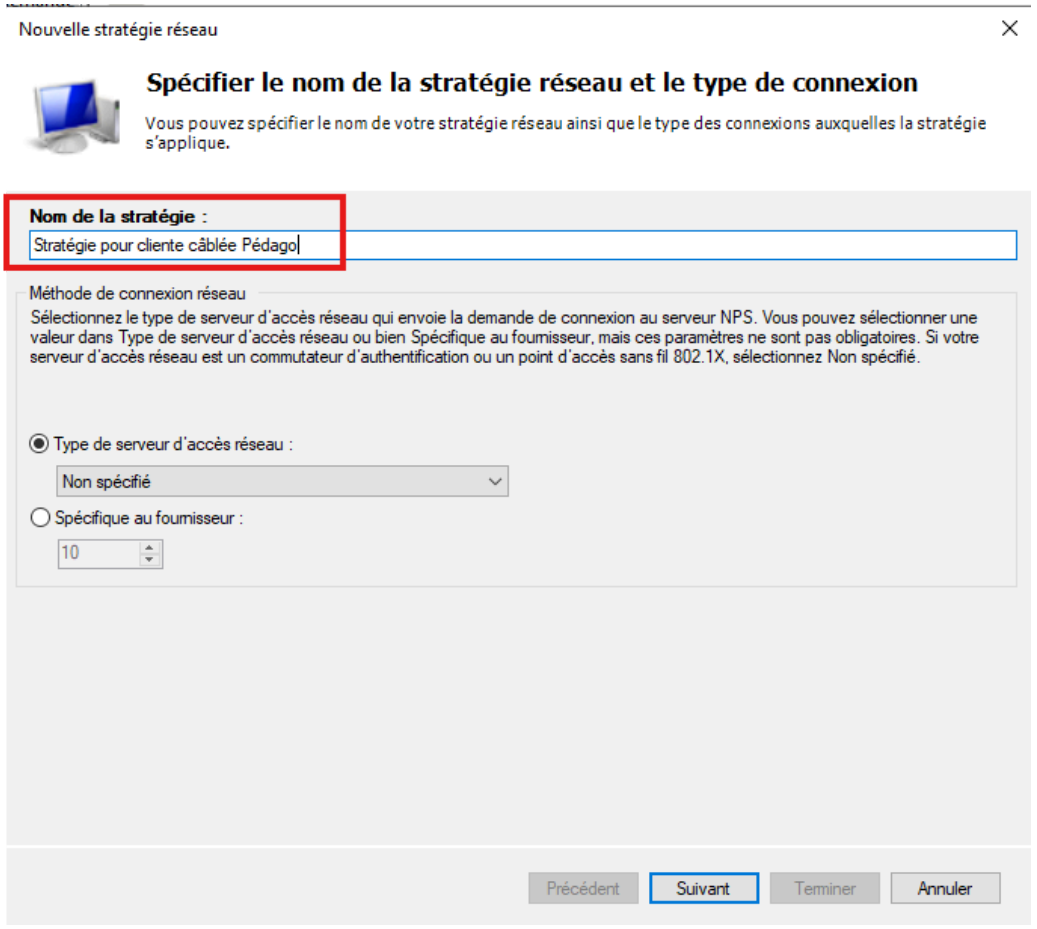



## 2.4.3 Déclaration d'une stratégie d'accès au réseau

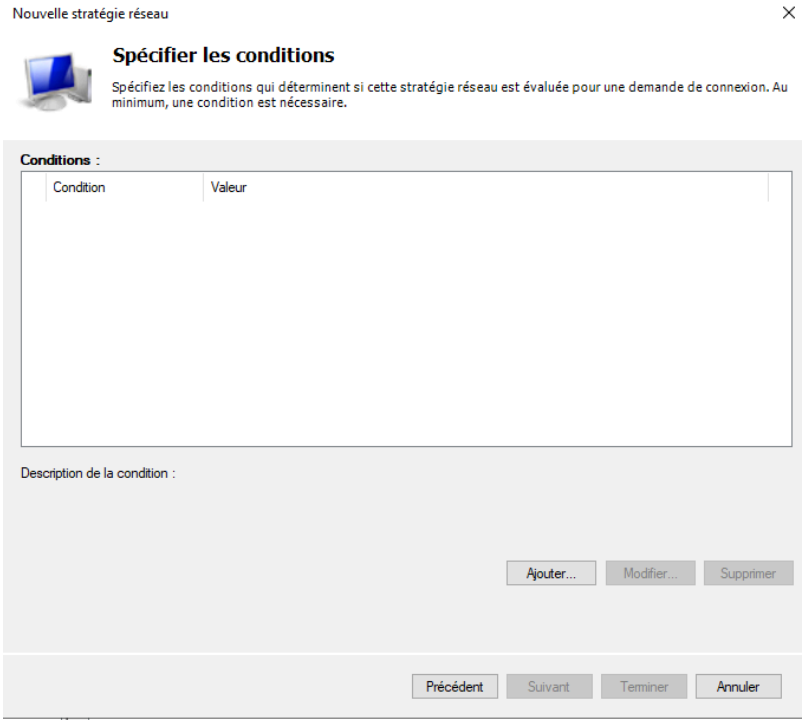
▪ Nous cliquons droit sur l'entrée Stratégie Réseau et nous sélectionnons Nouveau



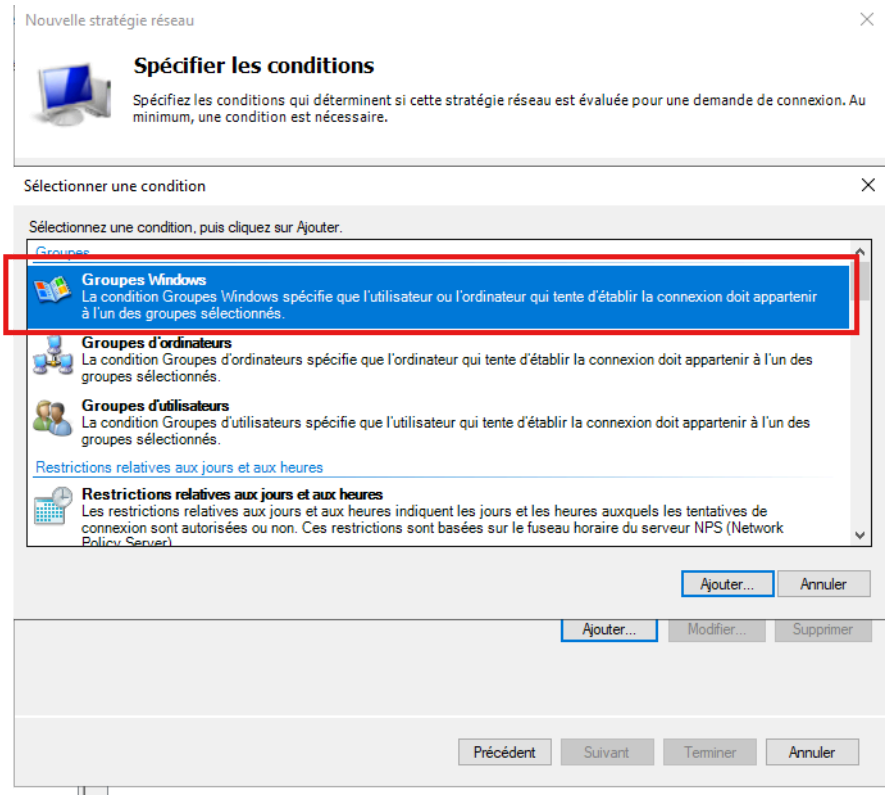

▪ Nous spécifions le nom de la stratégie, en l'occurrence, ici (Pédagogie).



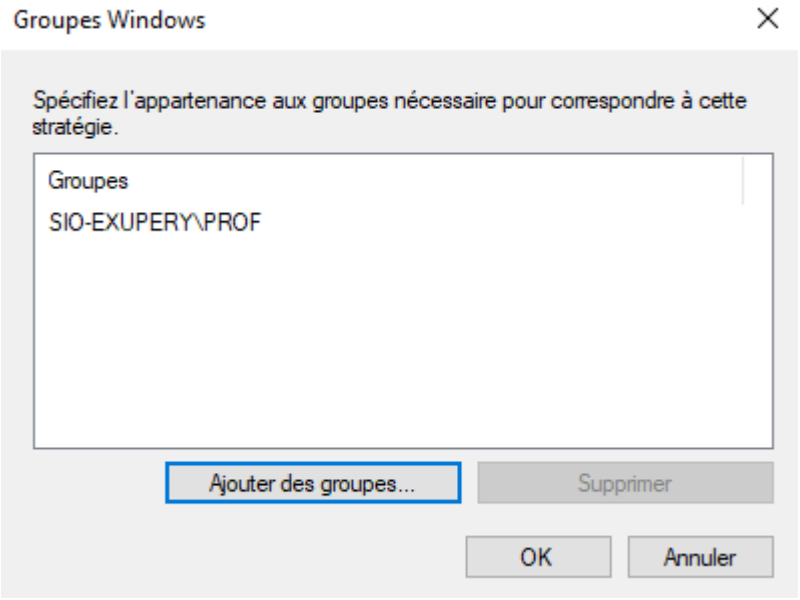
- Nous cliquons sur ajouter afin de spécifier une condition :



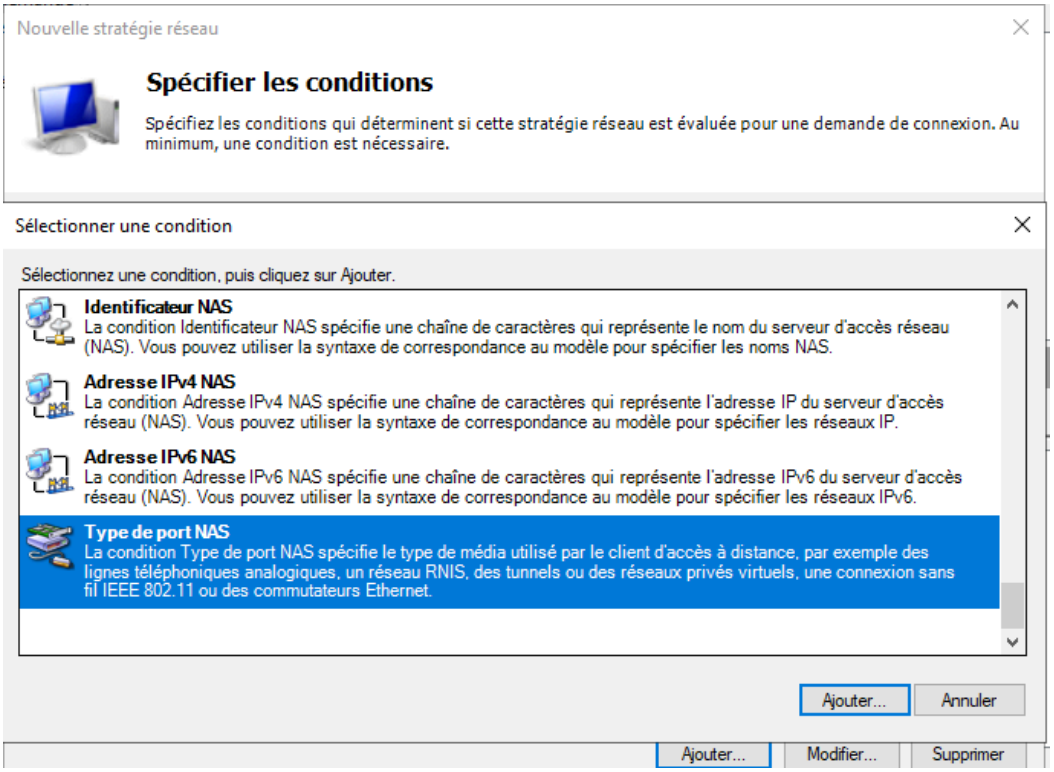

- Nous sélectionnons pour les groupes Windows



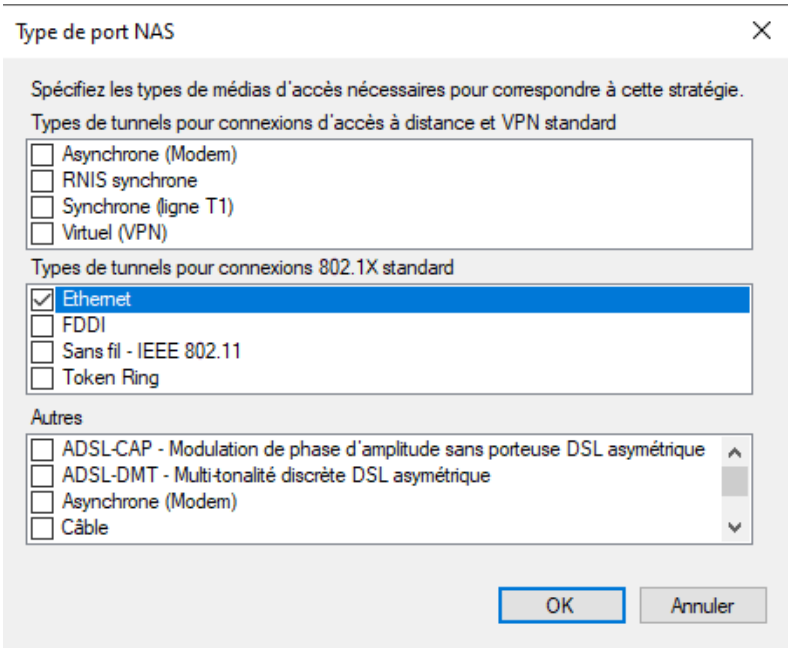
▪ Nous y ajoutons le groupe “Prof”



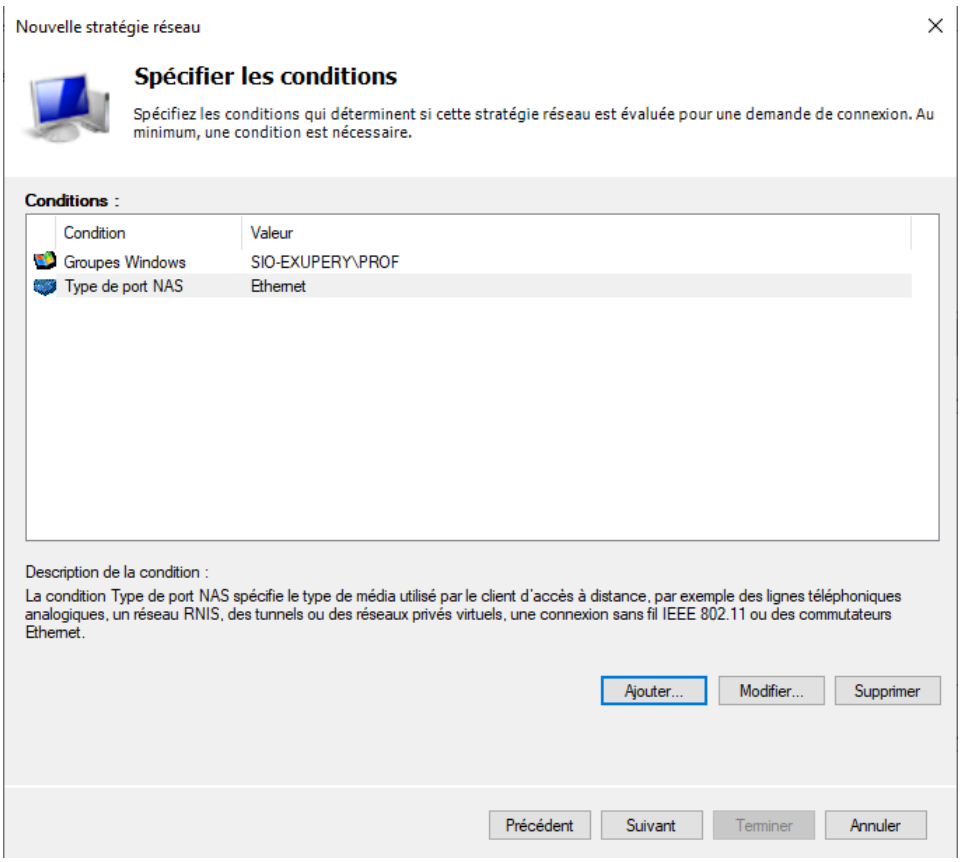

▪ Nous ajoutons une deuxième condition en y spécifiant le port NAS



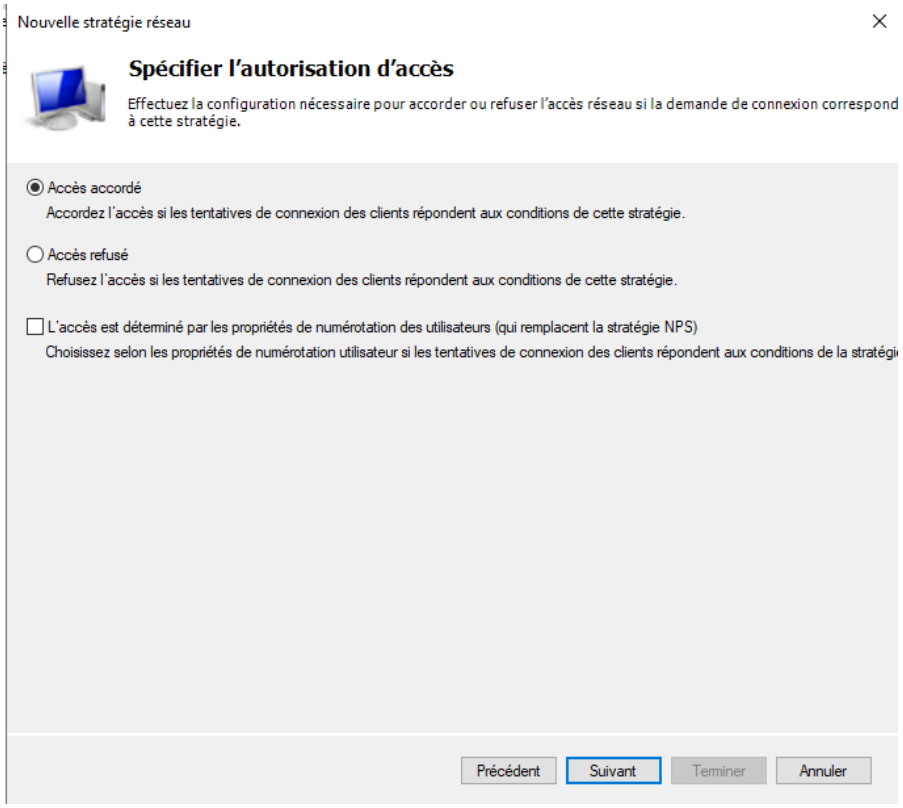
- Nous cochons Ethernet.



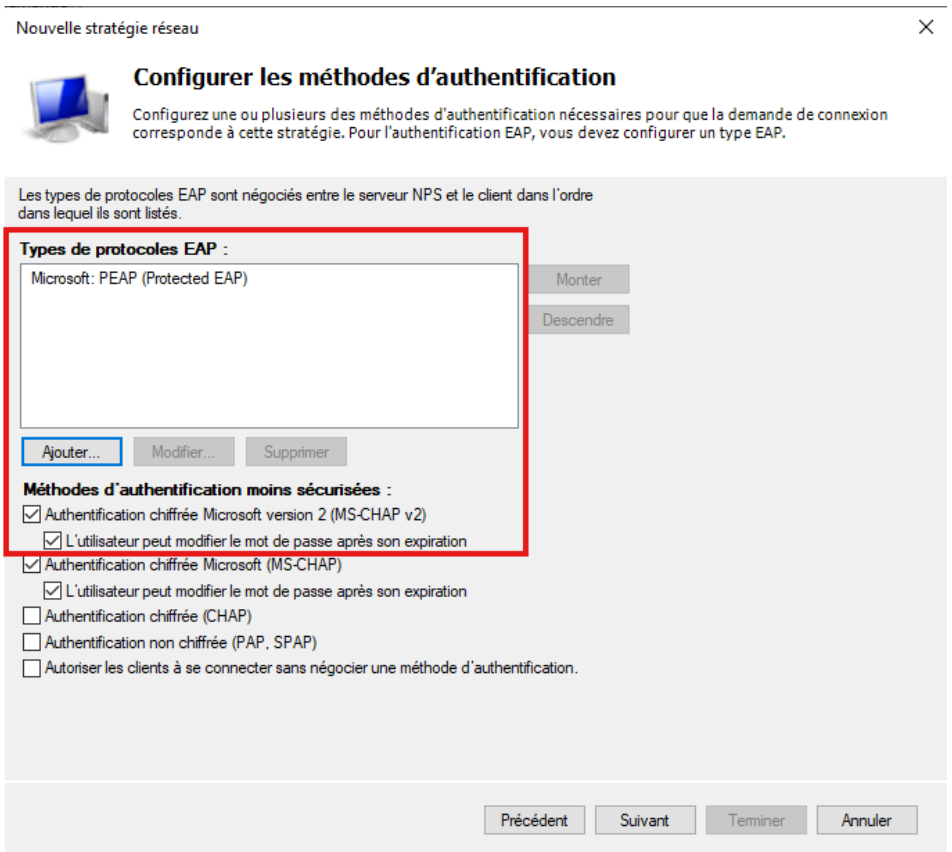

- Nous cliquons sur Suivant



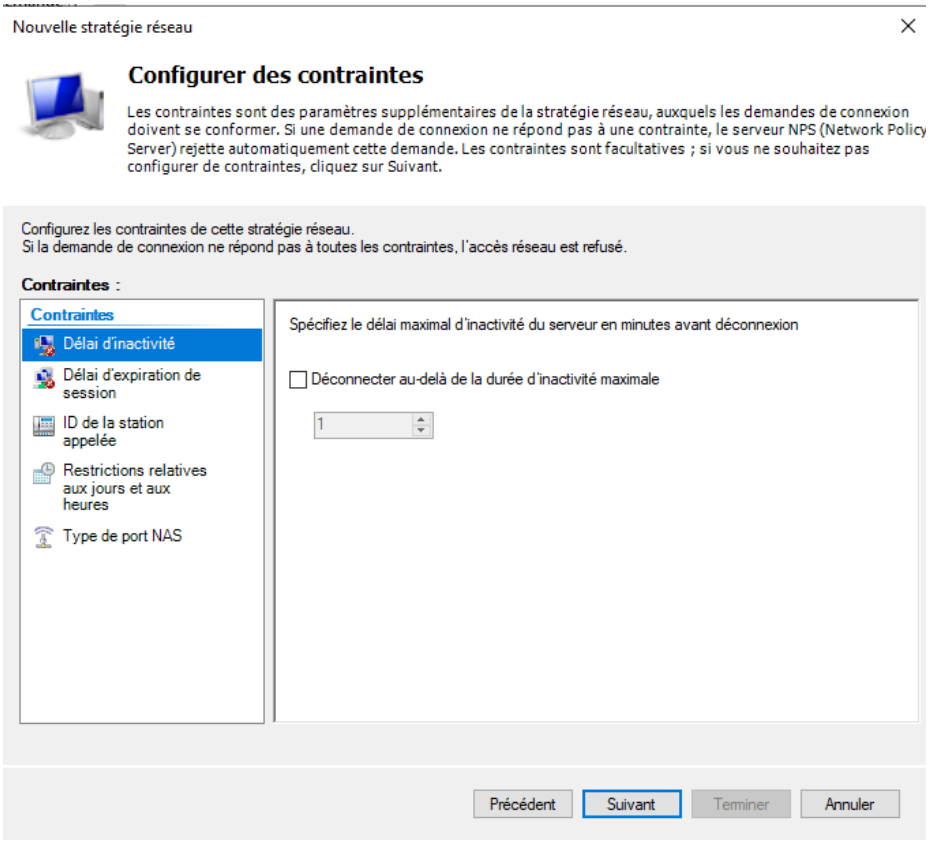
▪ Nous accordons l'accès pour les membres de ce groupe.



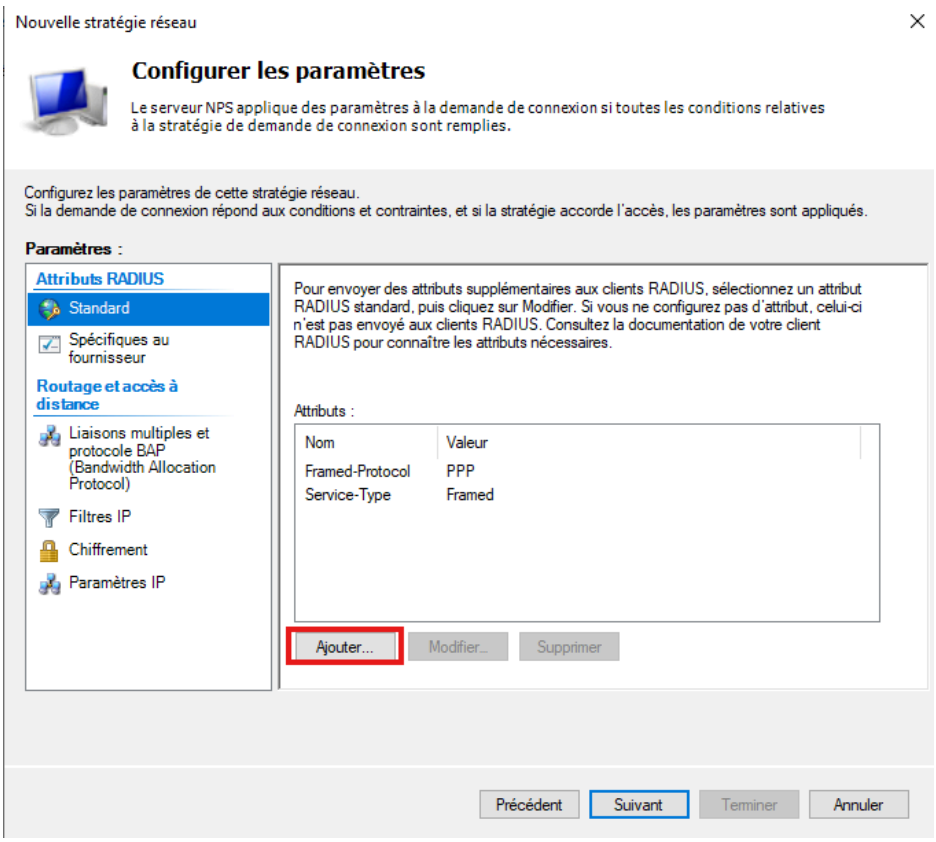

▪ Dans l'écran Configurer les méthodes d'authentification, nous y déclarons le type de protocoles EAP (PEAP) en cliquant sur Ajouter.



▪ Nous cliquons sur suivant :

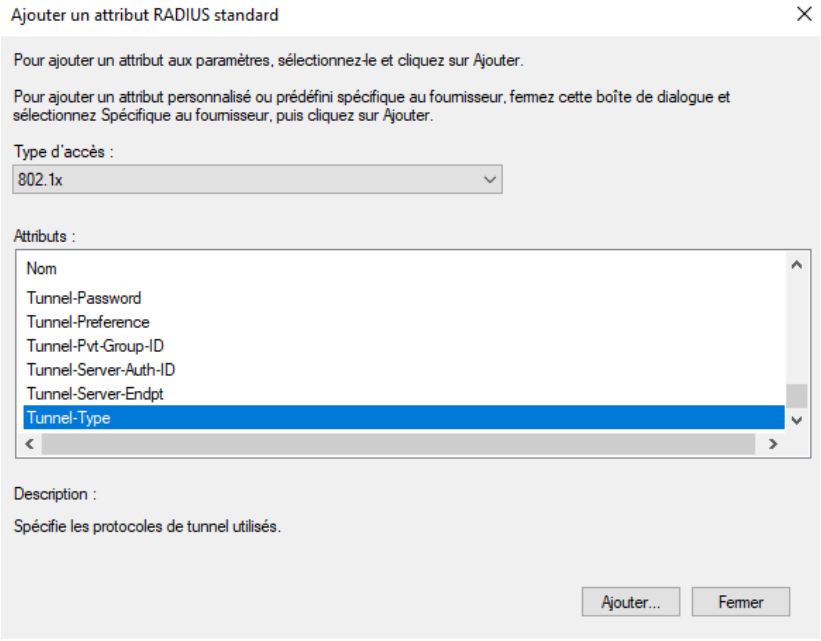



▪ Dans l'écran Configurer les paramètres, nous cliquons sur Ajouter afin d'envoyer des attributs au client RADIUS.

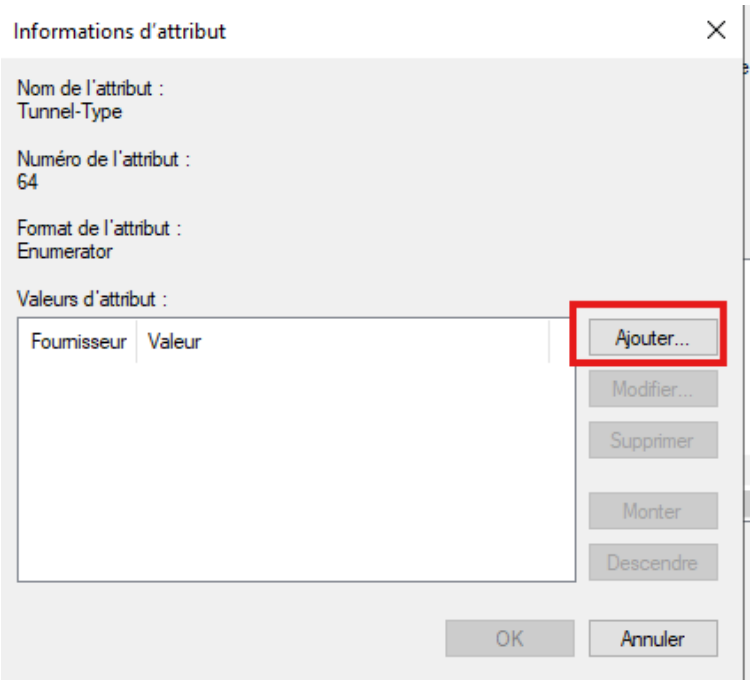


▪ Nous sélectionnons 802.1x dans Type d'accès puis nous sélectionnons l'attribut Tunnel-Type :

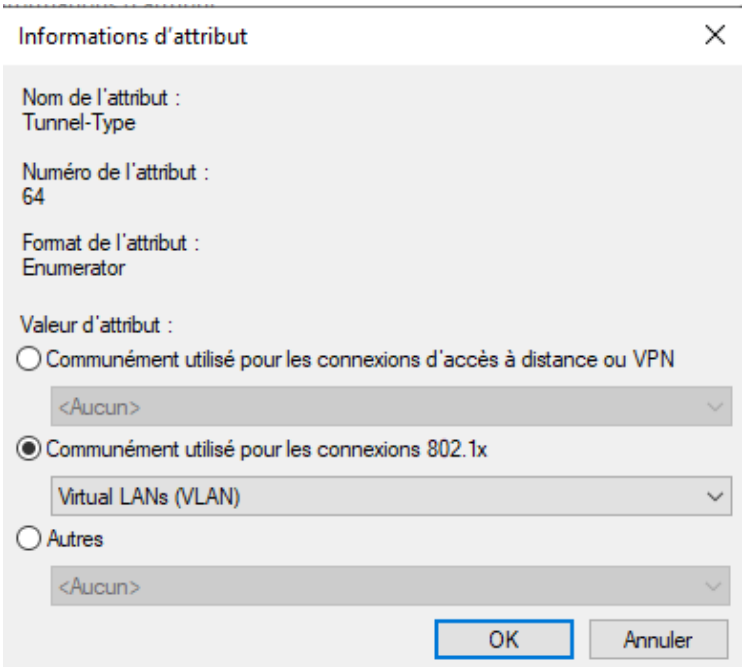
- Nous cliquons sur Ajouter.



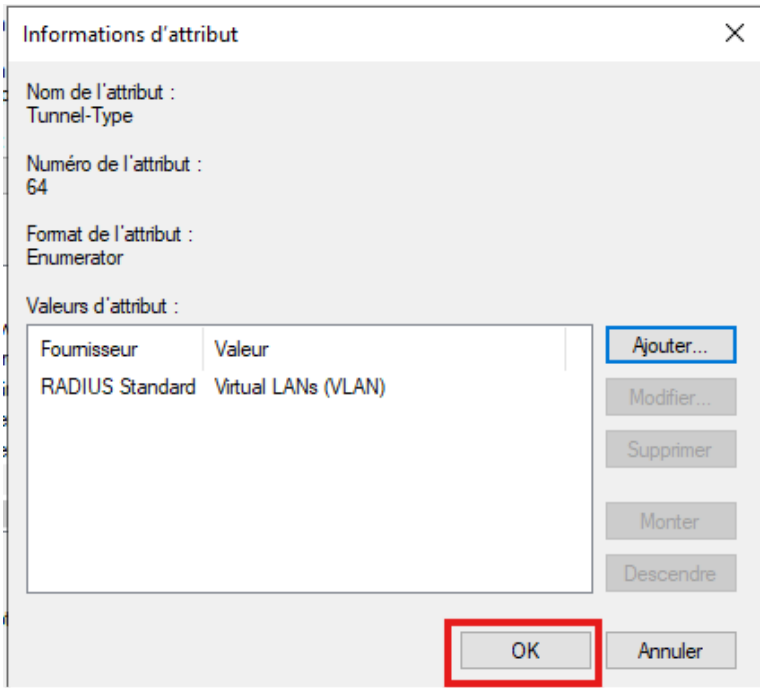

▪ On clique sur Ajouter.



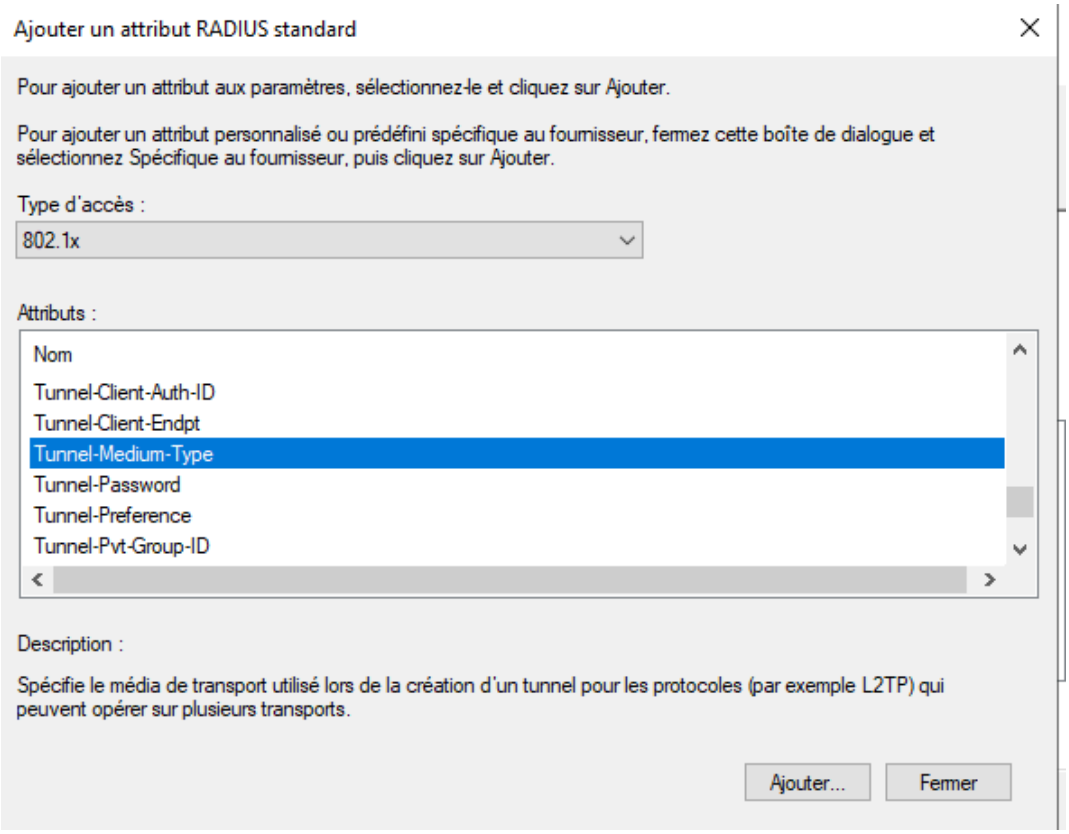
▪ On sélectionne Virtual LANs (VLAN) dans Communément utilisé pour les connexions 802.1x.



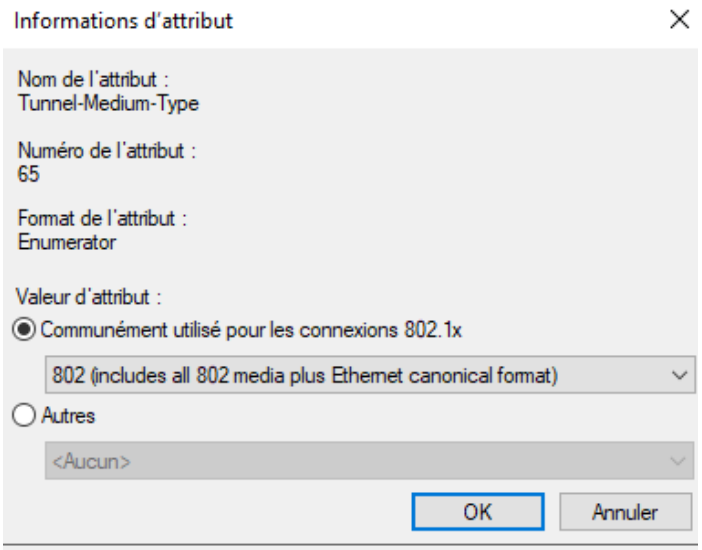

▪ On clique sur OK.



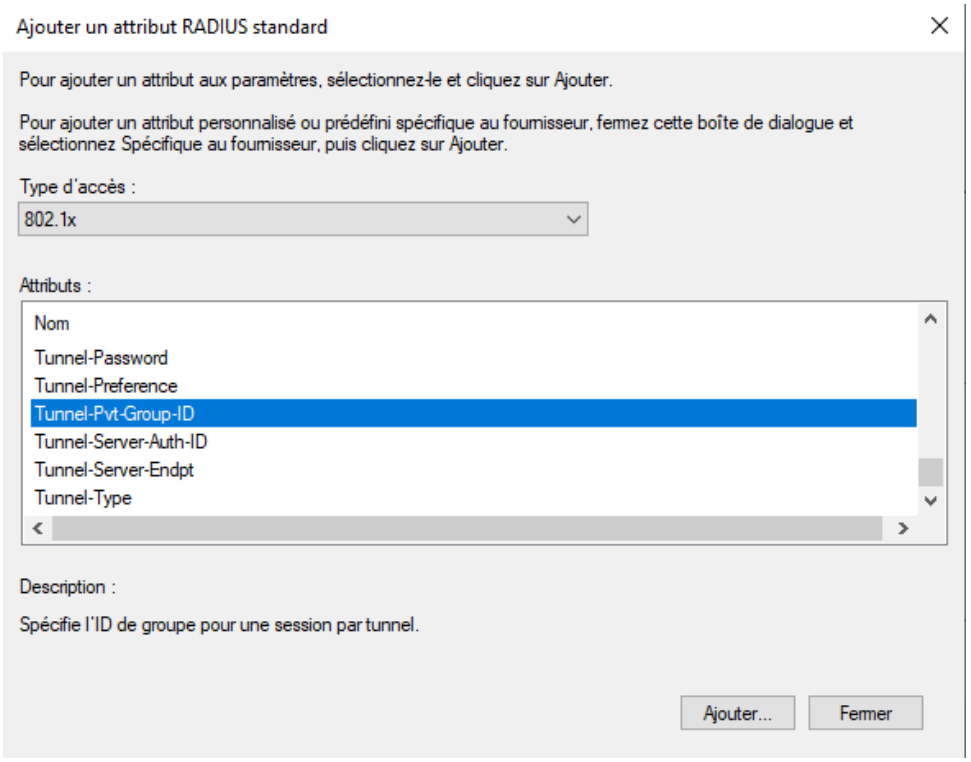
- Nous procédons de la même façon pour ajouter l'attribut Tunnel-Medium-Type.



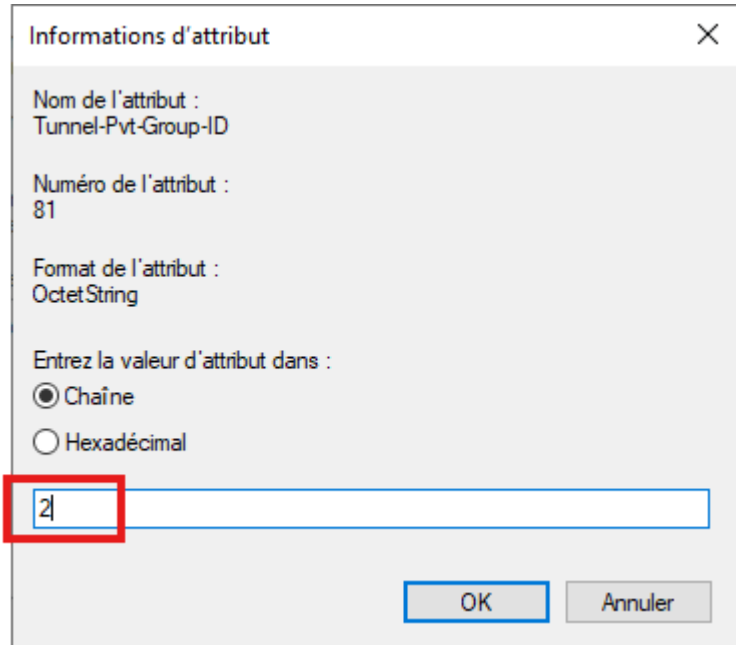

- On sélectionne 802 (includes...).



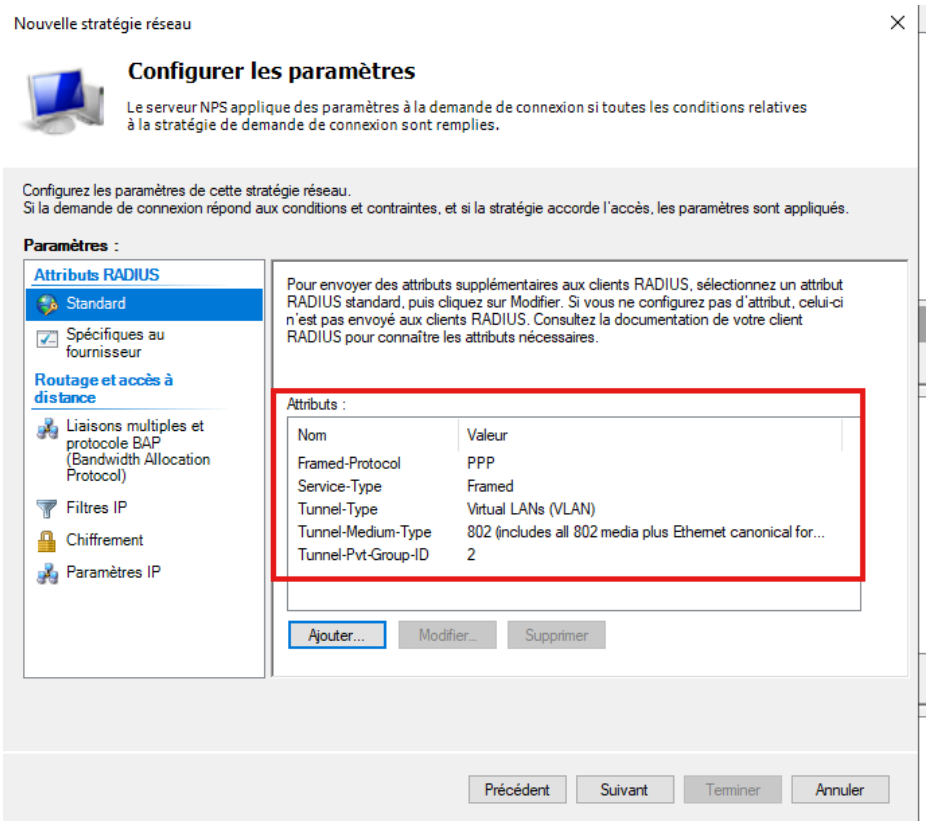
▪ Nous ajoutons l'attribut Tunnel-Pvt-Group-ID.



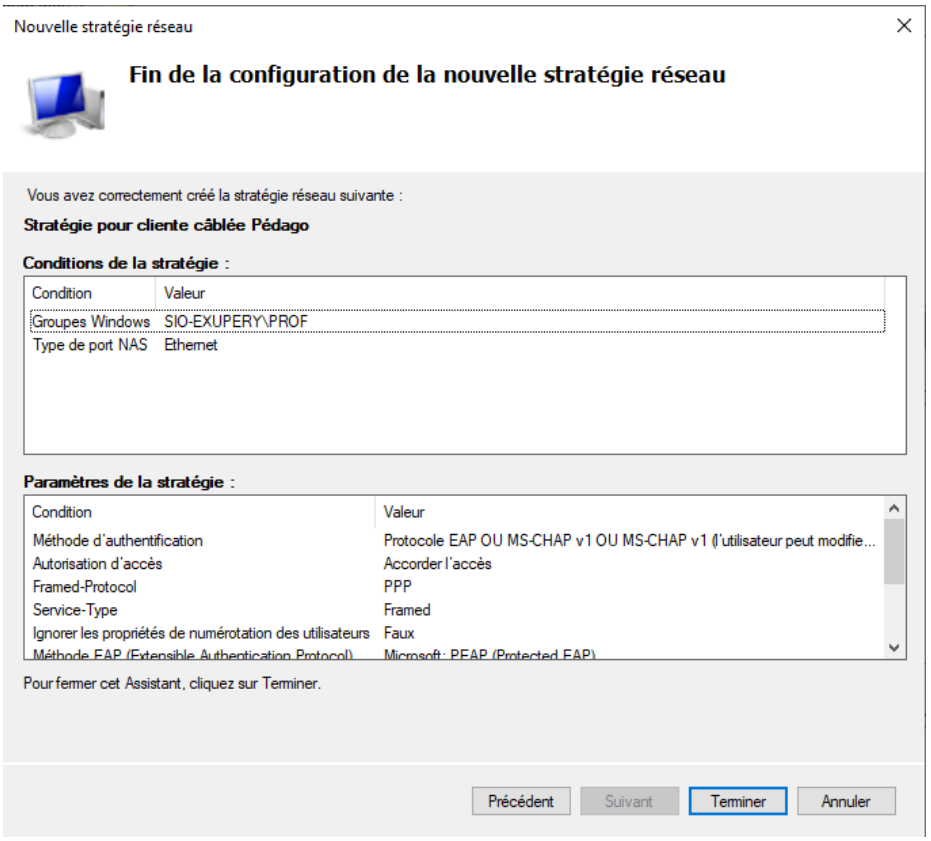

▪ Nous y spécifions le numéro de VLAN dans lequel on veut positionner les membres du groupe Prof.



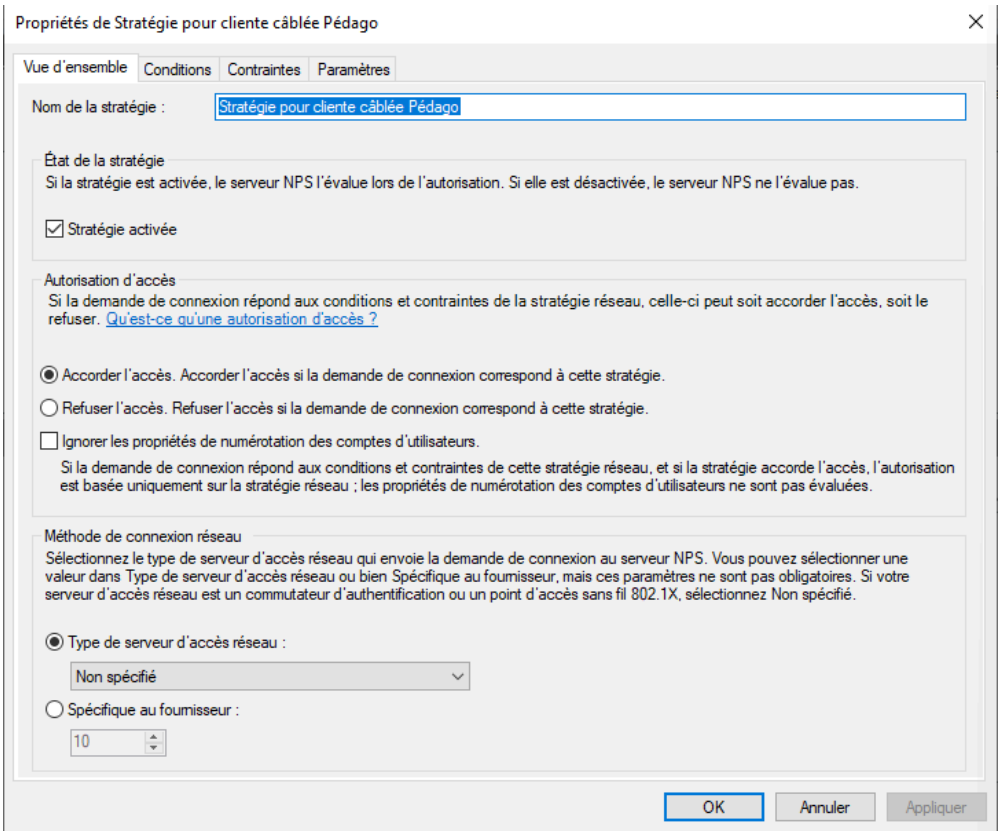
- Nous cliquons sur suivant :

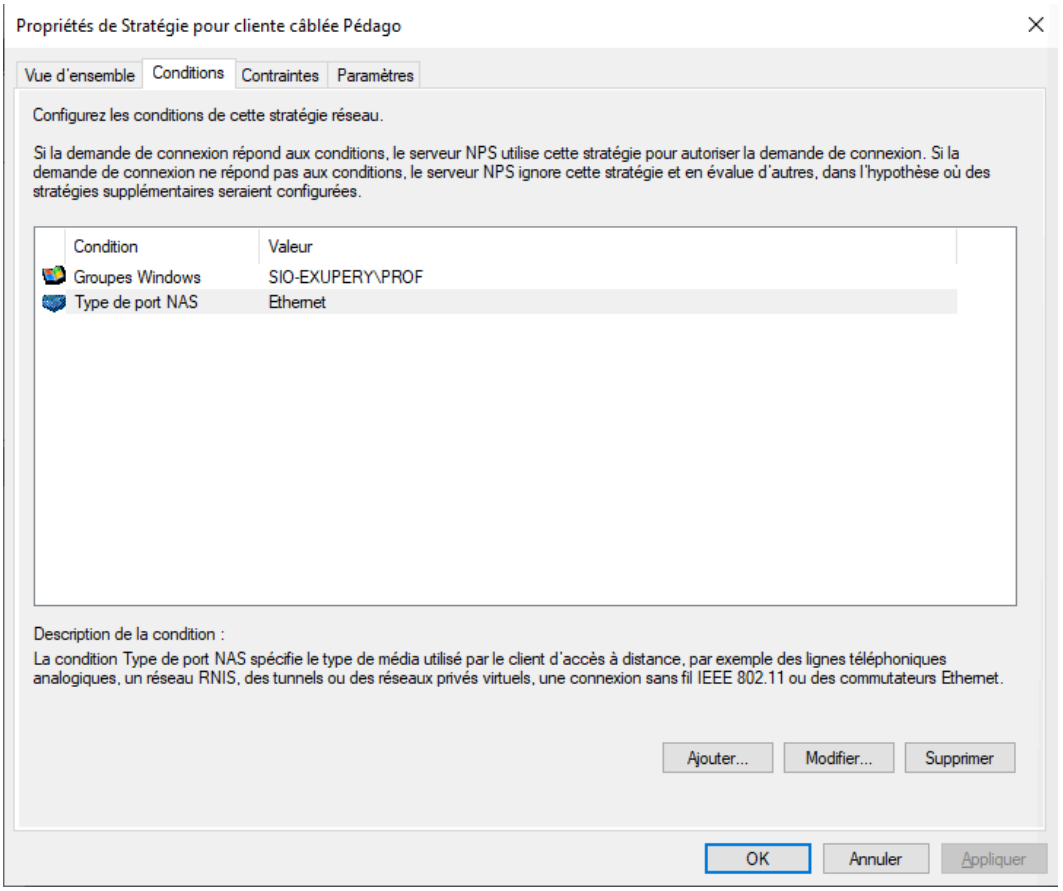


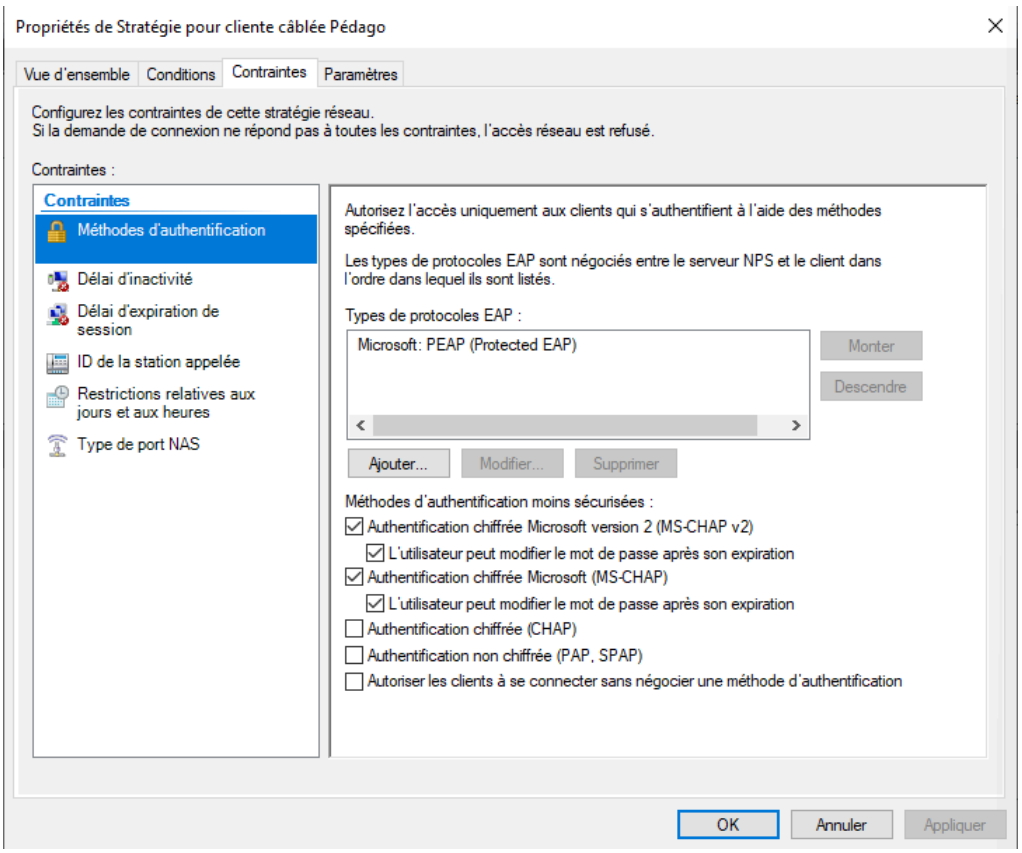

- On clique sur Terminer.

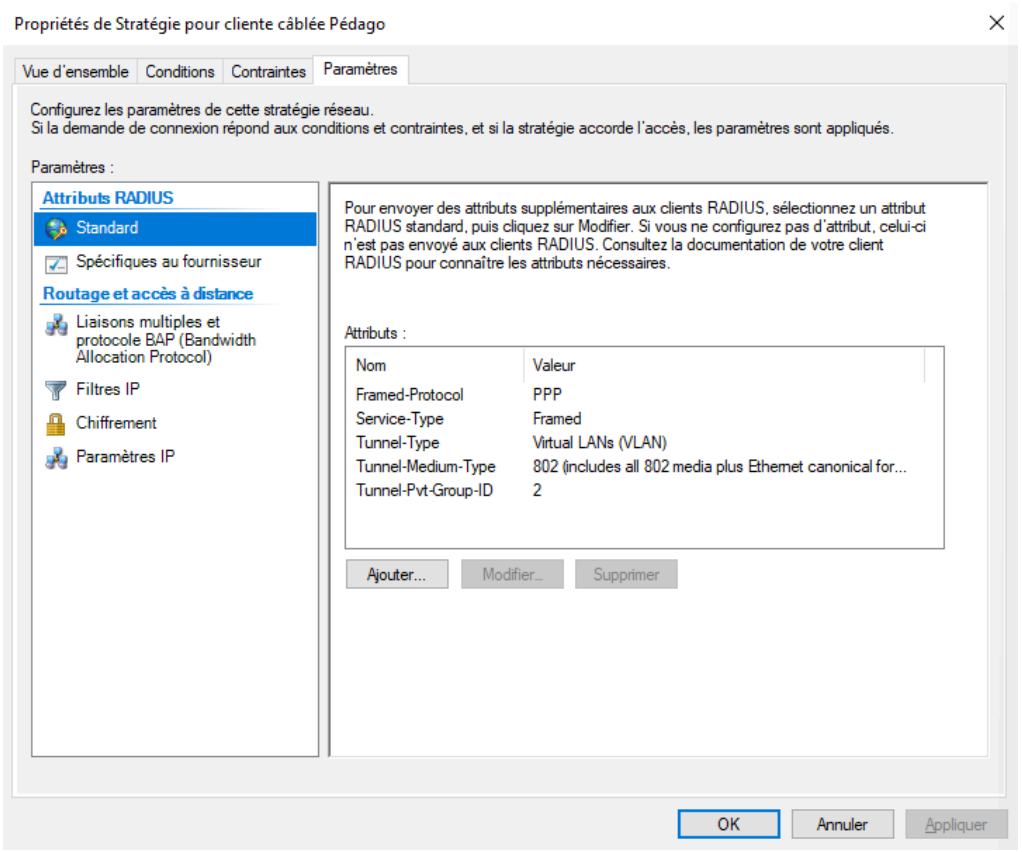


- Une vue d'ensemble afin de résumer tout ce que l'on a sélectionné pour la stratégie :

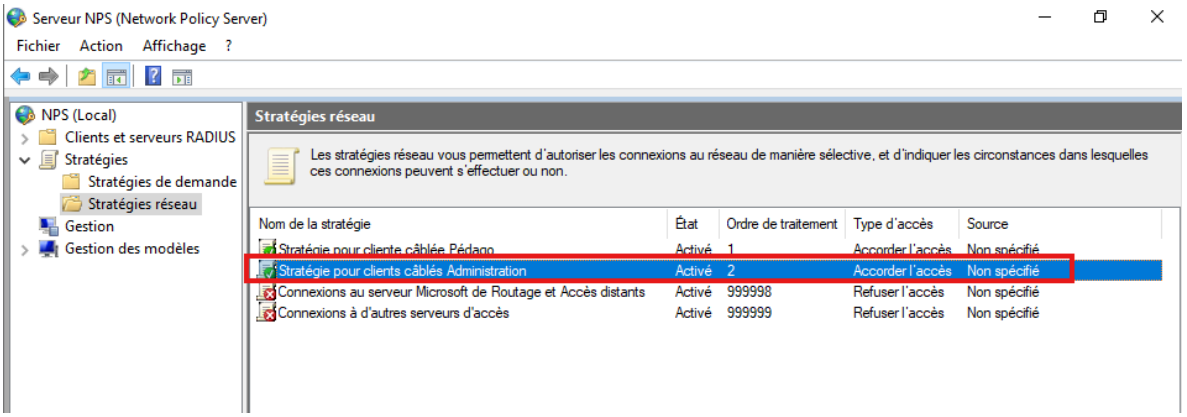


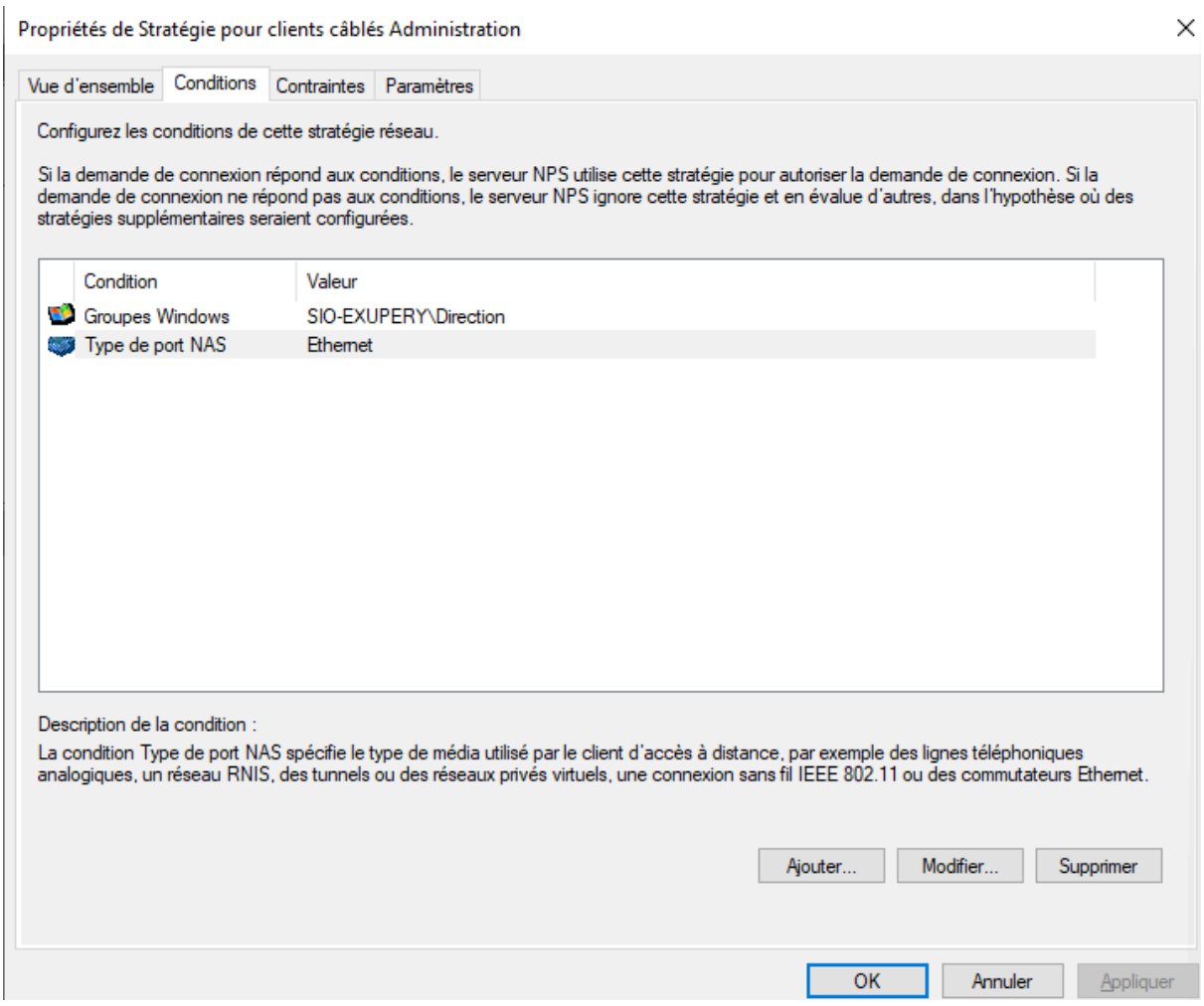



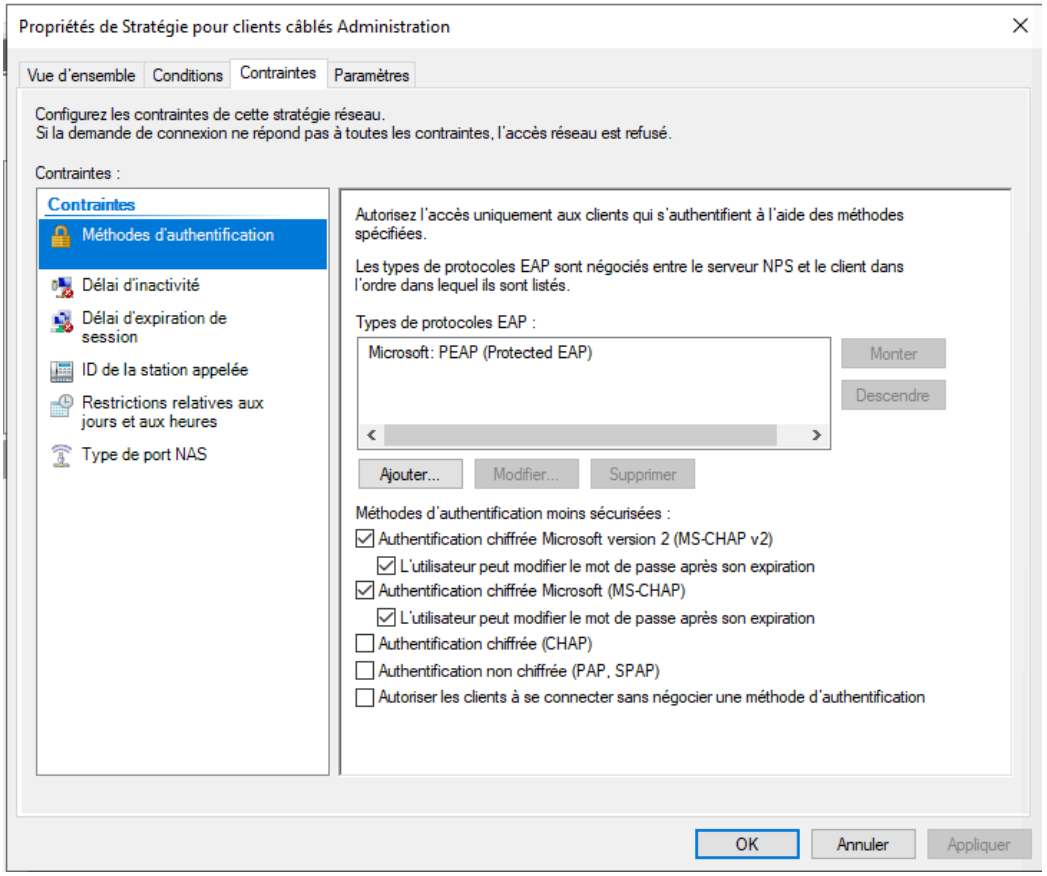

Propriétés de Stratégie pour cliente câblée Pédago
Vue d'ensemble
Conditions
Contraintes
Paramètres
Configurez les contraintes de cette stratégie réseau.
Si la demande de connexion ne répond pas à toutes les contraintes, l'accès réseau est refusé.
Contraintes :
Contraintes
Méthodes d'authentification
Délai d'inactivité
Délai d'expiration de session
ID de la station appelée
Restrictions relatives aux jours et aux heures
Type de port NAS
Autorisez l'accès uniquement aux clients qui s'authentifient à l'aide des méthodes spécifiées.
Les types de protocoles EAP sont négociés entre le serveur NPS et le client dans l'ordre dans lequel ils sont listés.
Types de protocoles EAP :
Microsoft: PEAP (Protected EAP)
Monter
Descendre
Ajouter...
Modifier...
Supprimer
Méthodes d'authentification moins sécurisées :
Authentification chiffrée Microsoft version 2 (MS-CHAP v2)
L'utilisateur peut modifier le mot de passe après son expiration
Authentification chiffrée Microsoft (MS-CHAP)
L'utilisateur peut modifier le mot de passe après son expiration
Authentification chiffrée (CHAP)
Authentification non chiffrée (PAP, SPAP)
Autoriser les clients à se connecter sans négocier une méthode d'authentification
OK
Annuler
Appliquer

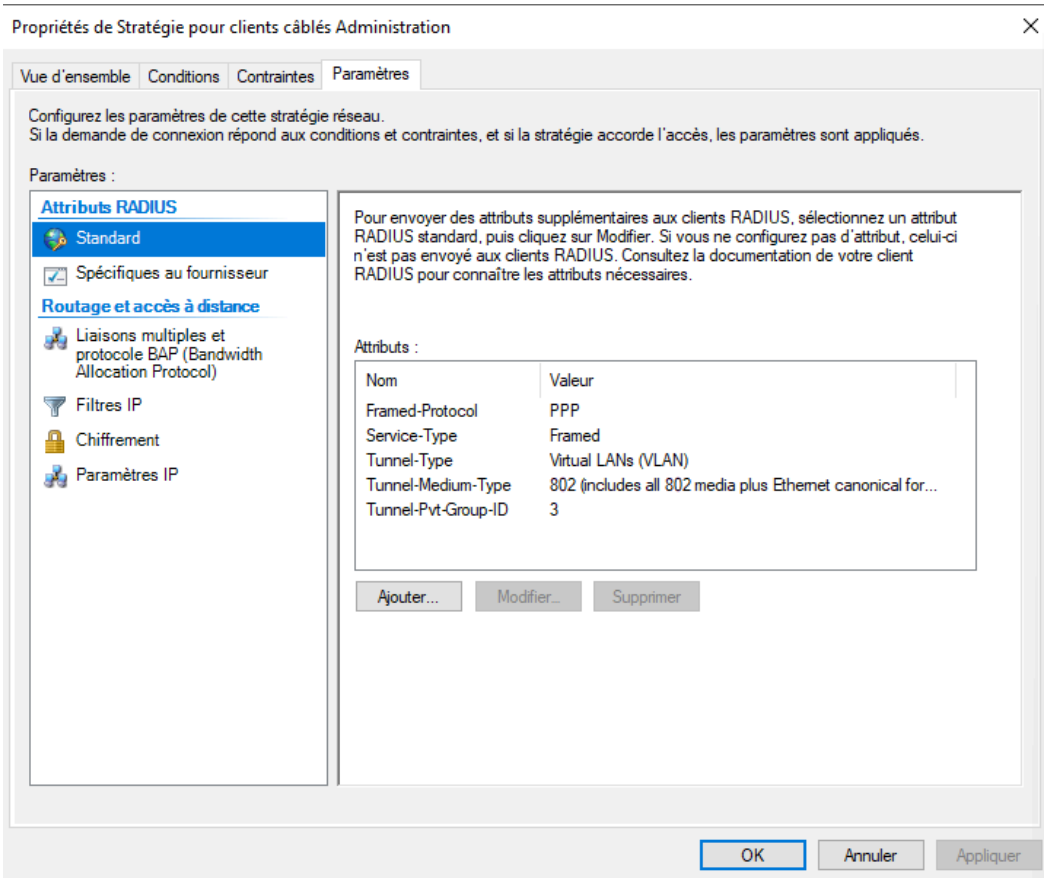

Propriétés de Stratégie pour cliente câblée Pédago
Vue d'ensemble
Conditions
Contraintes
Paramètres
Configurez les paramètres de cette stratégie réseau.
Si la demande de connexion répond aux conditions et contraintes, et si la stratégie accorde l'accès, les paramètres sont appliqués.
Paramètres :
Attributs RADIUS
Standard
Spécifiques au fournisseur
Routage et accès à distance
Liaisons multiples et protocole BAP (Bandwidth Allocation Protocol)
Filtres IP
Chiffrement
Paramètres IP
Pour envoyer des attributs supplémentaires aux clients RADIUS, sélectionnez un attribut RADIUS standard, puis cliquez sur Modifier. Si vous ne configurez pas d'attribut, celui-ci n'est pas envoyé aux clients RADIUS. Consultez la documentation de votre client RADIUS pour connaître les attributs nécessaires.
Attributs :
Nom
Valeur
Framed-Protocol
PPP
Service-Type
Framed
Tunnel-Type
Virtual LANs (VLAN)
Tunnel-Medium-Type
802 (includes all 802 media plus Ethernet canonical for...
Tunnel-Pvt-Group-ID
2
Ajouter...
Modifier...
Supprimer
OK
Annuler
Appliquer

▪ Nous définissons de manière analogue une stratégie d'accès réseau plaçant dans le VLAN3 les membres authentifiés comme faisant partie du groupe Direction :



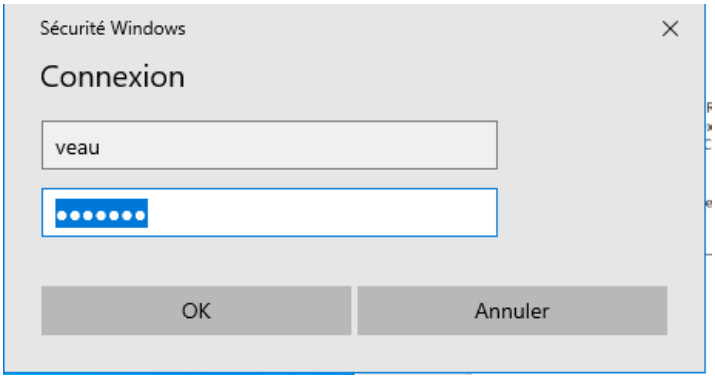



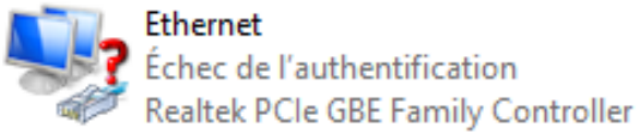

Propriétés de Stratégie pour clients câblés Administration
Vue d'ensemble
Conditions
Contraintes
Paramètres
Configurez les contraintes de cette stratégie réseau.
Si la demande de connexion ne répond pas à toutes les contraintes, l'accès réseau est refusé.
Contraintes :
Contraintes
Méthodes d'authentification
Délai d'inactivité
Délai d'expiration de session
ID de la station appelée
Restrictions relatives aux jours et aux heures
Type de port NAS
Autorisez l'accès uniquement aux clients qui s'authentifient à l'aide des méthodes spécifiées.
Les types de protocoles EAP sont négociés entre le serveur NPS et le client dans l'ordre dans lequel ils sont listés.
Types de protocoles EAP :
Microsoft: PEAP (Protected EAP)
Monter
Descendre
Ajouter...
Modifier...
Supprimer
Méthodes d'authentification moins sécurisées :
Authentification chiffrée Microsoft version 2 (MS-CHAP v2)
L'utilisateur peut modifier le mot de passe après son expiration
Authentification chiffrée Microsoft (MS-CHAP)
L'utilisateur peut modifier le mot de passe après son expiration
Authentification chiffrée (CHAP)
Authentification non chiffrée (PAP, SPAP)
Autoriser les clients à se connecter sans négocier une méthode d'authentification
OK
Annuler
Appliquer


Propriétés de Stratégie pour clients câblés Administration
Vue d'ensemble
Conditions
Contraintes
Paramètres
Configurez les paramètres de cette stratégie réseau.
Si la demande de connexion répond aux conditions et contraintes, et si la stratégie accorde l'accès, les paramètres sont appliqués.
Paramètres :
Attributs RADIUS
Standard
Spécifiques au fournisseur
Routage et accès à distance
Liaisons multiples et protocole BAP (Bandwidth Allocation Protocol)
Filtres IP
Chiffrement
Paramètres IP
Pour envoyer des attributs supplémentaires aux clients RADIUS, sélectionnez un attribut RADIUS standard, puis cliquez sur Modifier. Si vous ne configurez pas d'attribut, celui-ci n'est pas envoyé aux clients RADIUS. Consultez la documentation de votre client RADIUS pour connaître les attributs nécessaires.
Attributs :
Nom
Valeur
Framed-Protocol
PPP
Service-Type
Framed
Tunnel-Type
Virtual LANs (VLAN)
Tunnel-Medium-Type
802 (includes all 802 media plus Ethernet canonical for...
Tunnel-Pvt-Group-ID
3
Ajouter...
Modifier...
Supprimer
OK
Annuler
Appliquer

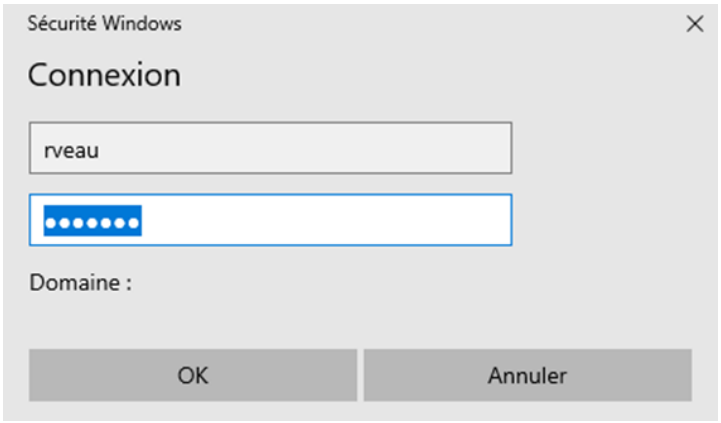
# Annexe 3 : Demande de connexion des utilisateurs rveau et cgeley

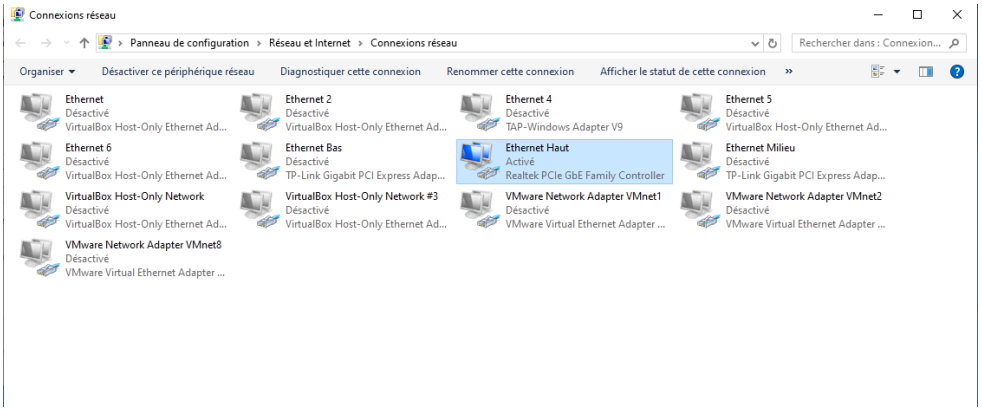
▪ Sur le second poste, nous essayons une authentification avec un compte de la Pédagogie, nous simulons une erreur :



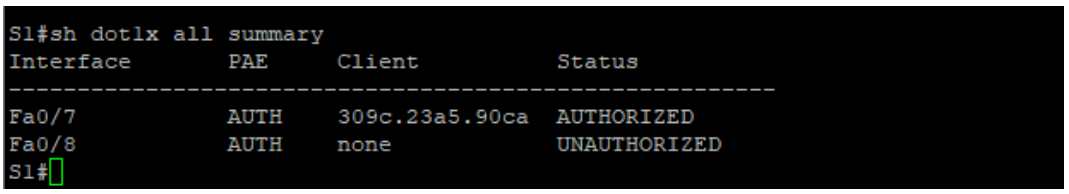

▪ Cette fois-ci nous allons réellement tenter la connexion au compte :

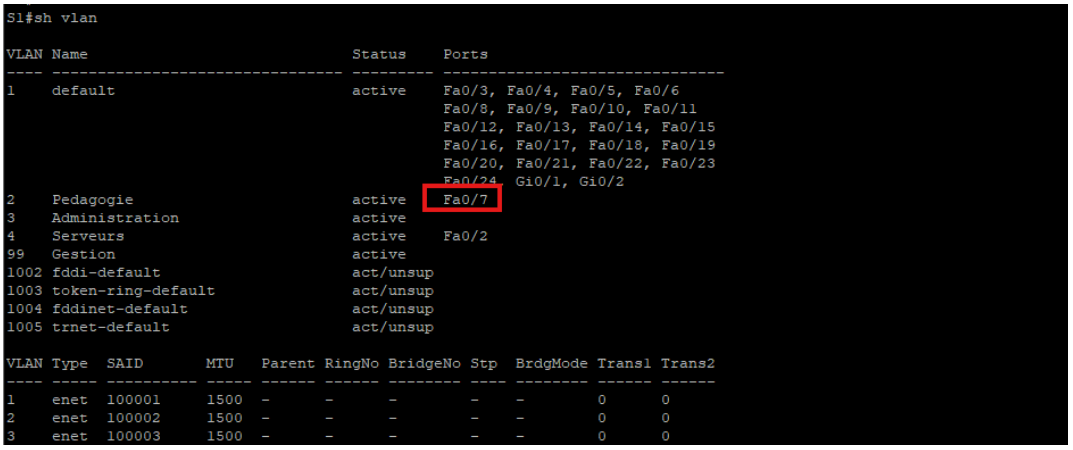


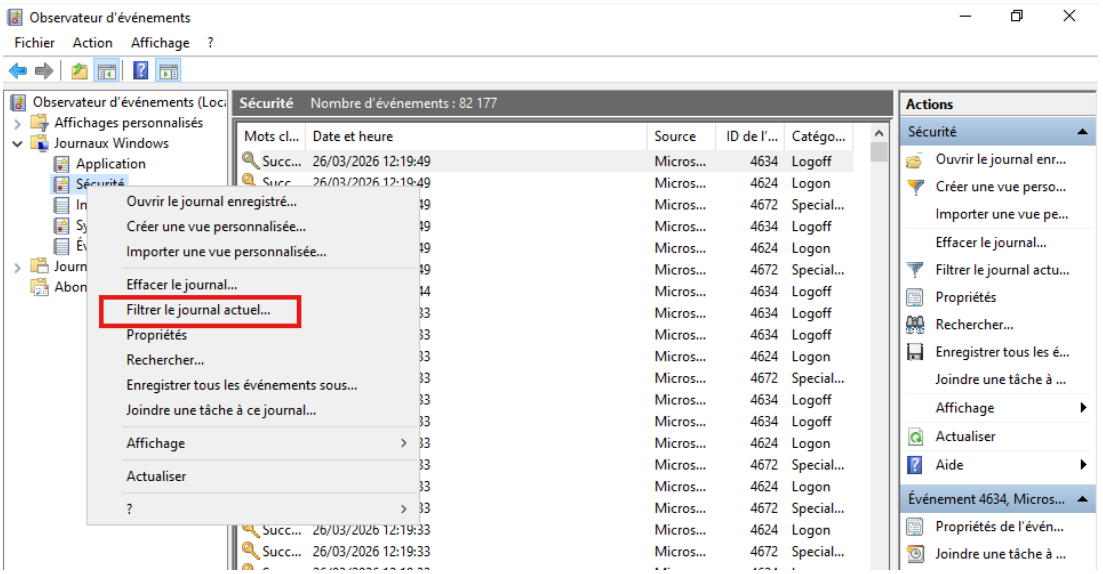
▪ Nous vérifions qu'il ait reçu une IP ainsi que le reste des informations nécessaires :

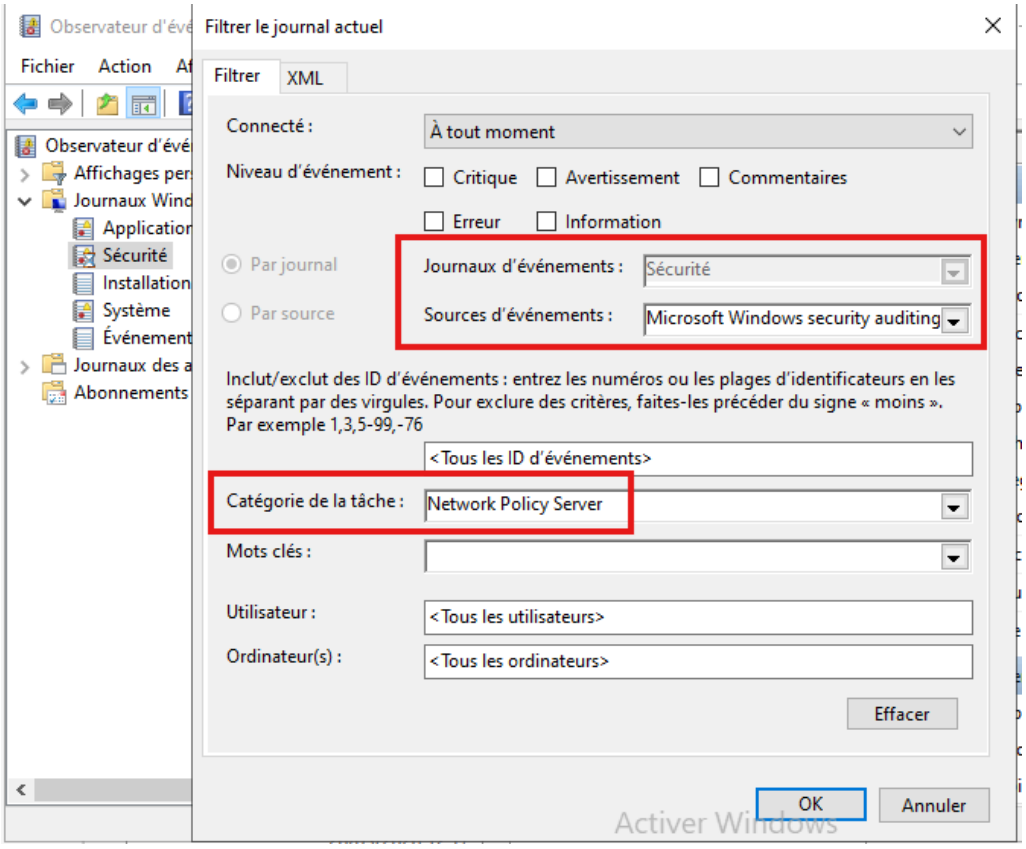

▪ Nous vérifions sur le commutateur radius :



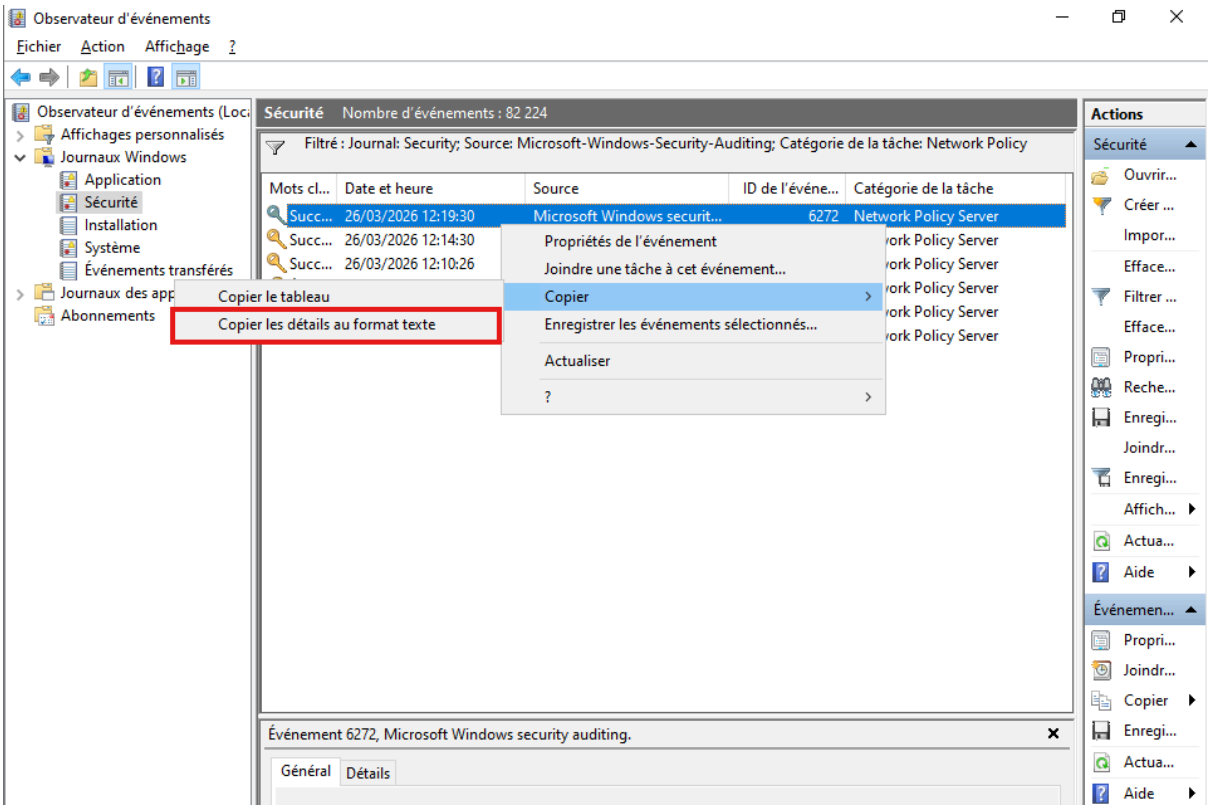



▪ Nous allons exporter un xml depuis l'observateur. Pour cela, nous allons dans l'observateur d'événements, nous effectuons un clic droit sur l'onglet Sécurité, puis nous cliquons sur Filtrer le journal actuel :



▪ Nous copions les informations au format texte :



Nom du journal :Security
Source : Microsoft-Windows-Security-Auditing
Date : 26/03/2026 12:19:30
ID de l'événement :6272
Catégorie de la tâche :Network Policy Server
Niveau : Information
Mots clés : Succès de l'audit
Utilisateur : N/A
Ordinateur : AD.sio-exupery.local
Description :
Le serveur NPS a accordé l'accès à un utilisateur.

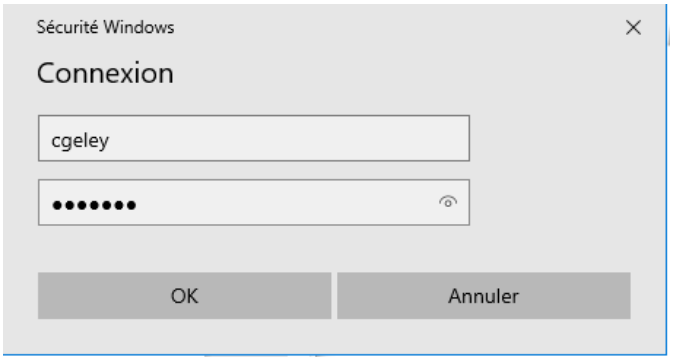
Utilisateur :
ID de sécurité : SIO-EXUPERY\rveau
Nom de compte : rveau
Domaine de compte : SIO-EXUPERY
Nom de compte complet : sio-exupery.local/Pédagogie/PROF/Régis VEAU

Ordinateur client :
ID de sécurité : NULL SID
Nom de compte : -
Nom de compte complet : -
Identificateur de la station appelée : 00-08-2F-45-CD-87
Identificateur de la station appelante : 30-9C-23-A5-90-CA

Serveur NAS :
Adresse IPv4 du serveur NAS : 192.168.0.2
Adresse IPv6 du serveur NAS : -
Identificateur du serveur NAS : -
Type de port du serveur NAS : Ethernet
Port du serveur NAS : 50107

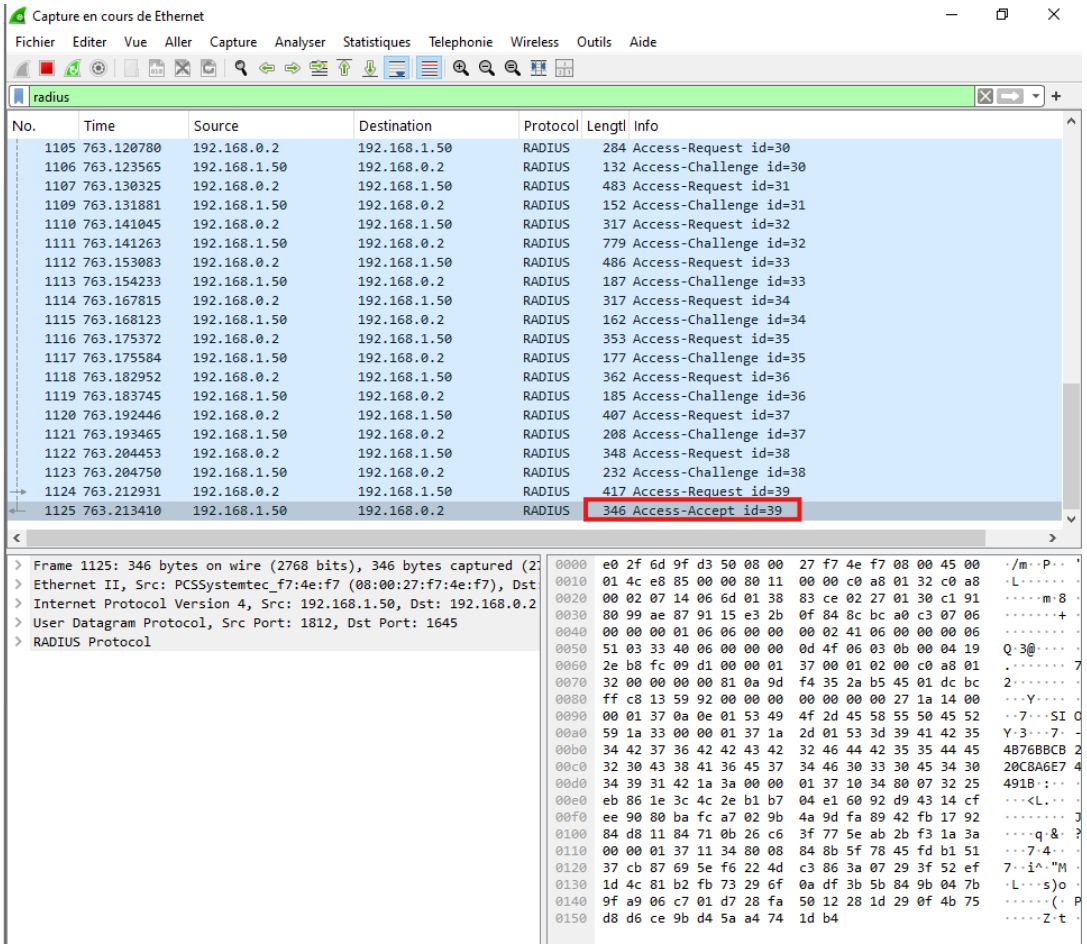
Client RADIUS :
Nom convivial du client : Client-Cisco-2960
Adresse IP du client : 192.168.0.2

Informations détaillées sur l'authentification :
Nom de stratégie de demande de connexion : Connexion câblée
Nom de stratégie réseau : Stratégie pour cliente câblés Pédago
Fournisseur d'authentification : Windows
Serveur d'authentification : AD.sio-exupery.local
Type d'authentification : PEAP
Type EAP : Microsoft: Mot de passe sécurisé (EAP-MSCHAP version 2)
Identificateur de la session du compte : -
Résultats de la journalisation : Les informations de suivi ont été inscrites dans le fichier journal local.


Sécurité Windows
Connexion
cgeley
OK
Annuler

# Annexe 4 : Capture de trames : messages RADIUS

▪ Après avoir installé WireShark sur le serveur RADIUS, nous effectuons une capture des trames RADIUS entre le client RADIUS et le serveur RADIUS.



▪ Nous développons la section RADIUS Protocol, comme ci-dessous, et nous constatons l'encapsulation RADIUS :

- lorsque le client RADIUS reçoit un paquet EAP du client final, il encapsule dans un attribut EAP-Message, lui-même encapsulé dans un message Access-Request.
- Il en est de-même pour un message Access-Challenge provenant du serveur RADIUS.