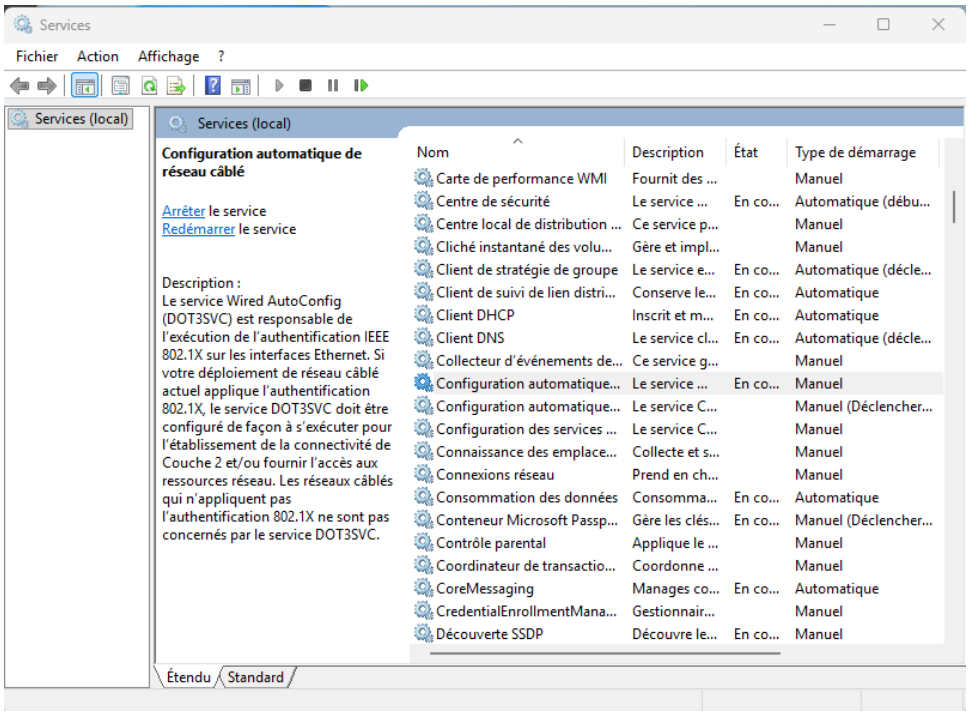
TP1 : Radius

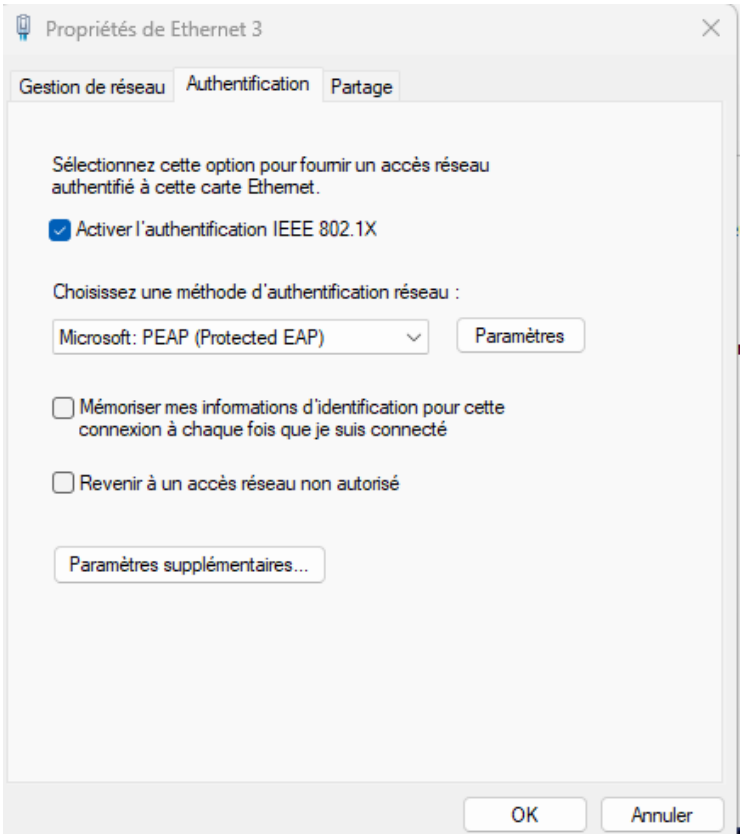
Sommaire

1 – Préparation client

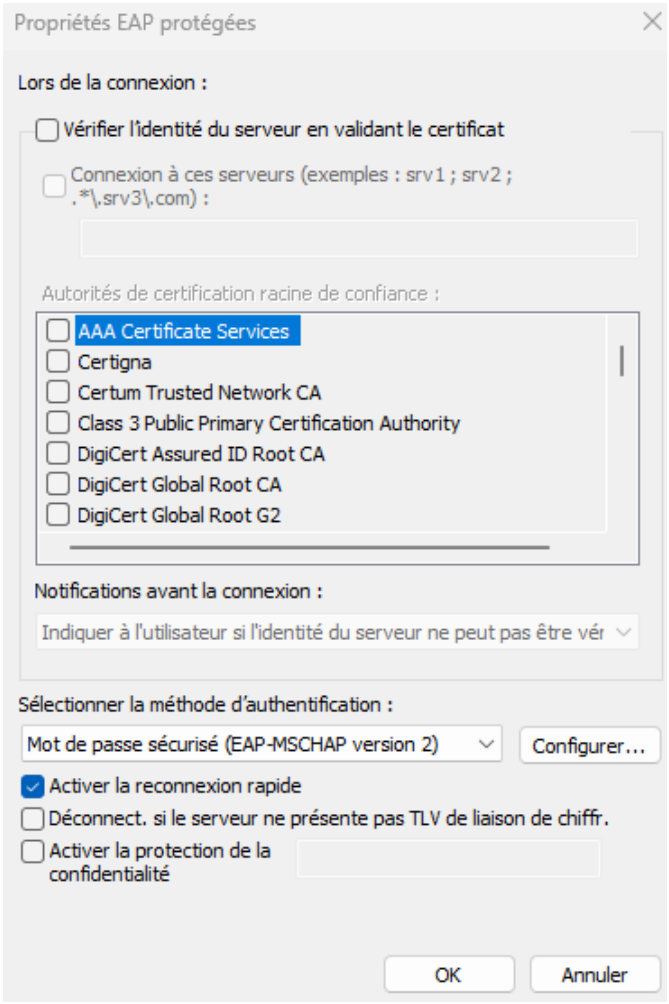
- Dans Windows, pour activer cette couche logicielle, il faut lancer le service Configuration automatique de réseau câblé :



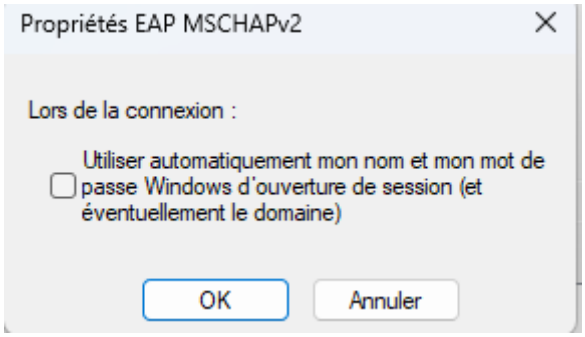
- La mise en route du service provoque l'apparition de l'onglet Authentification dans les propriétés de la carte réseau.



- J’ouvre l'écran Propriétés EAP protégées en cliquant sur Paramètres à côté du choix Microsoft PEAP (Protected EAP) :



- Le bouton Configurer de l'écran ci-dessus permet d’indiquer si on veut utiliser ou non le nom et le mot de passe d'ouverture de session Windows dans le dialogue 802.1x :



2 – Annexe 1 : Commutateur et Routeur

- Création des VLAN
- Paramétrage général 802.1x - déclaration du serveur RADIUS
- Paramétrage des ports contrôlés 802.1x
- Paramétrage des ports utiles non contrôlés

```
Current configuration : 3416 bytes
!
! Last configuration change at 21:49:34 UTC Tue Mar 2 1993
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Switch
!
boot-start-marker
boot-end-marker
!
!
aaa new-model
!
!
aaa authentication dot1x default group radius
aaa authorization network default group radius
!
!
!
!
!
!
aaa session-id common
system mtu routing 1500
!
!
!
!
crypto pki trustpoint TP-self-signed-226913920
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-226913920
 revocation-check none
 rsakeypair TP-self-signed-226913920
!
```

```
dot1x system-auth-control
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
!
!
!
interface FastEthernet0/1
 switchport trunk allowed vlan 1-4,99
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 4
 switchport mode access
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
 switchport mode access
 authentication port-control auto
 dot1x pae authenticator
!
interface FastEthernet0/8
 switchport mode access
 authentication port-control auto
 dot1x pae authenticator
!
```

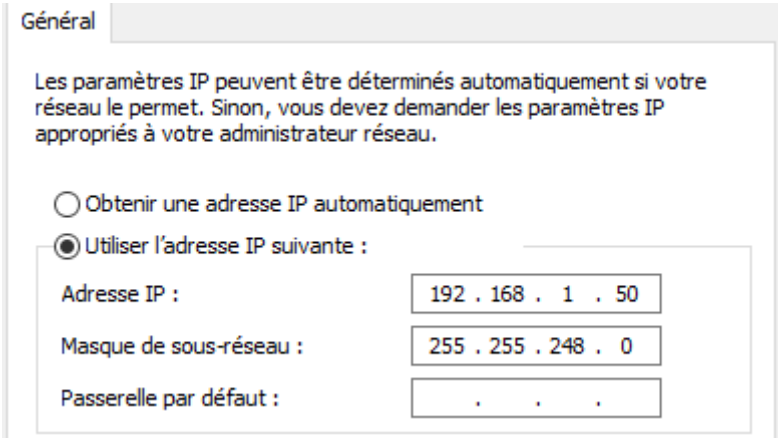
```
interface Vlan1
 ip address 192.168.0.2 255.255.255.248
!
ip http server
ip http secure-server
radius-server host 192.168.1.50 auth-port 1812 acct-port 1813 key sio1234567
!
!
!
!
line con 0
line vty 5 15
!
end
```

- Je paramètre le routeur :
    - Mise en place du routage inter-VLANs
    - Mise en place du service DHCP

```
ip dhcp excluded-address 192.168.1.1
ip dhcp excluded-address 192.168.1.17
!
ip dhcp pool vlan2
 network 192.168.1.0 255.255.255.240
!
ip dhcp pool vlan3
 network 192.168.1.16 255.255.255.240
 default-router 192.168.1.17
 dns-server 192.168.1.50
!
ip dhcp pool vlan 2
 default-router 192.168.1.1
 dns-server 192.168.1.50
!
!
multilink bundle-name authenticated
!
!
crypto pki token default removal timeout 0
!
!
license udi pid CISCO2901/K9 sn FCZ1648C1E
!
!
!
!
!
!
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 192.168.0.1 255.255.255.248
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.2
 encapsulation dot1Q 2
 ip address 192.168.1.1 255.255.255.240
!
interface GigabitEthernet0/0.3
 encapsulation dot1Q 3
 ip address 192.168.1.17 255.255.255.240
!
interface GigabitEthernet0/0.4
 encapsulation dot1Q 4
 ip address 192.168.1.49 255.255.255.248
!
```

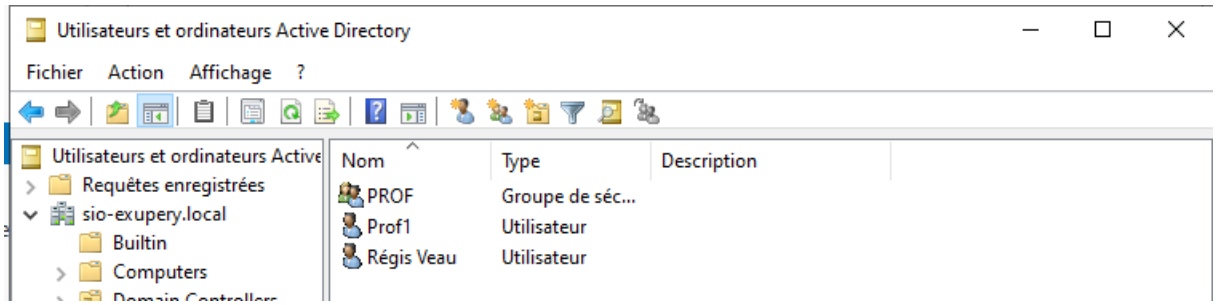
3 – Annexe 2 : Mise en place du serveur RADIUS (service NPS)

- J'applique une configuration IP au serveur AD :



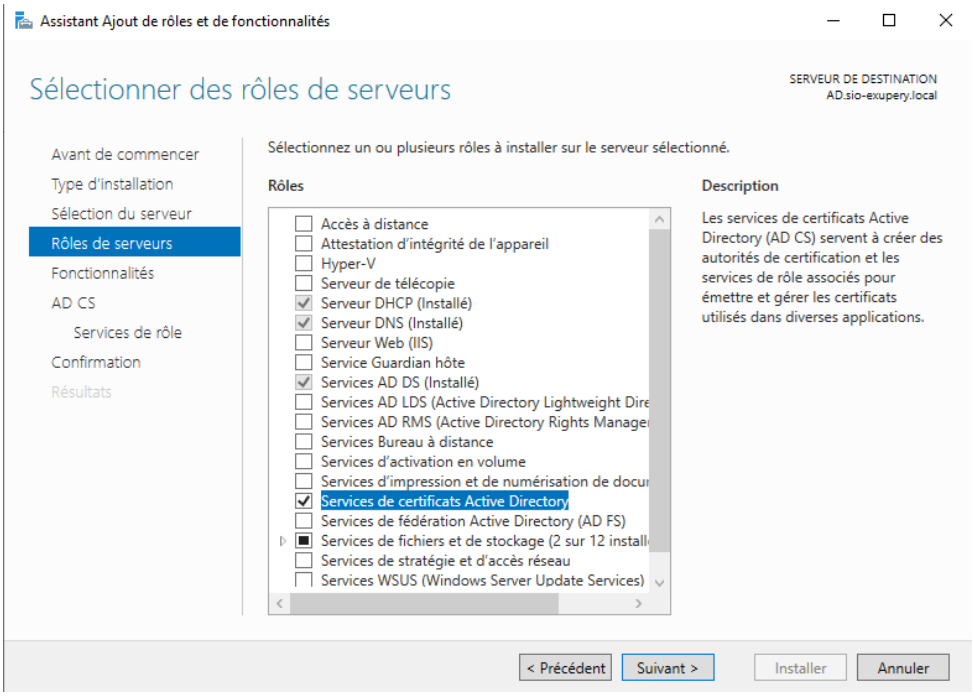
- Je désactive le serveur DHCP :

- Je crée deux UO :

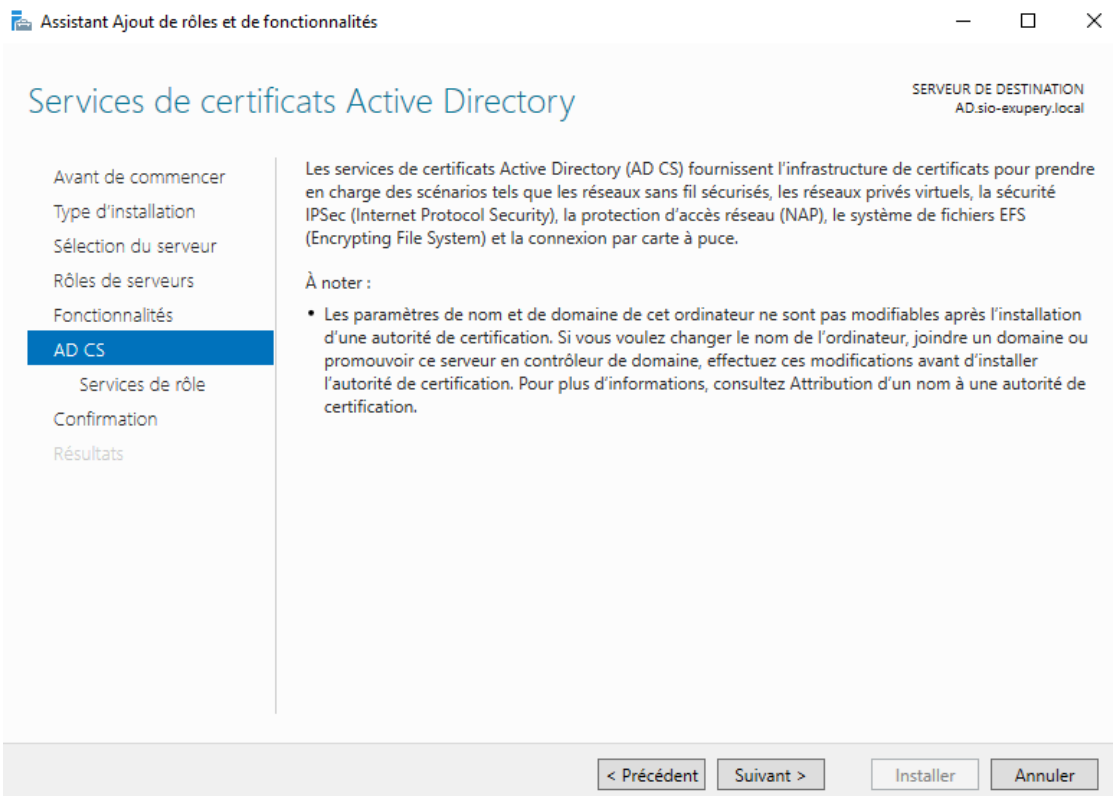


3.2- Ajout du rôle Services de certificats Active Directory

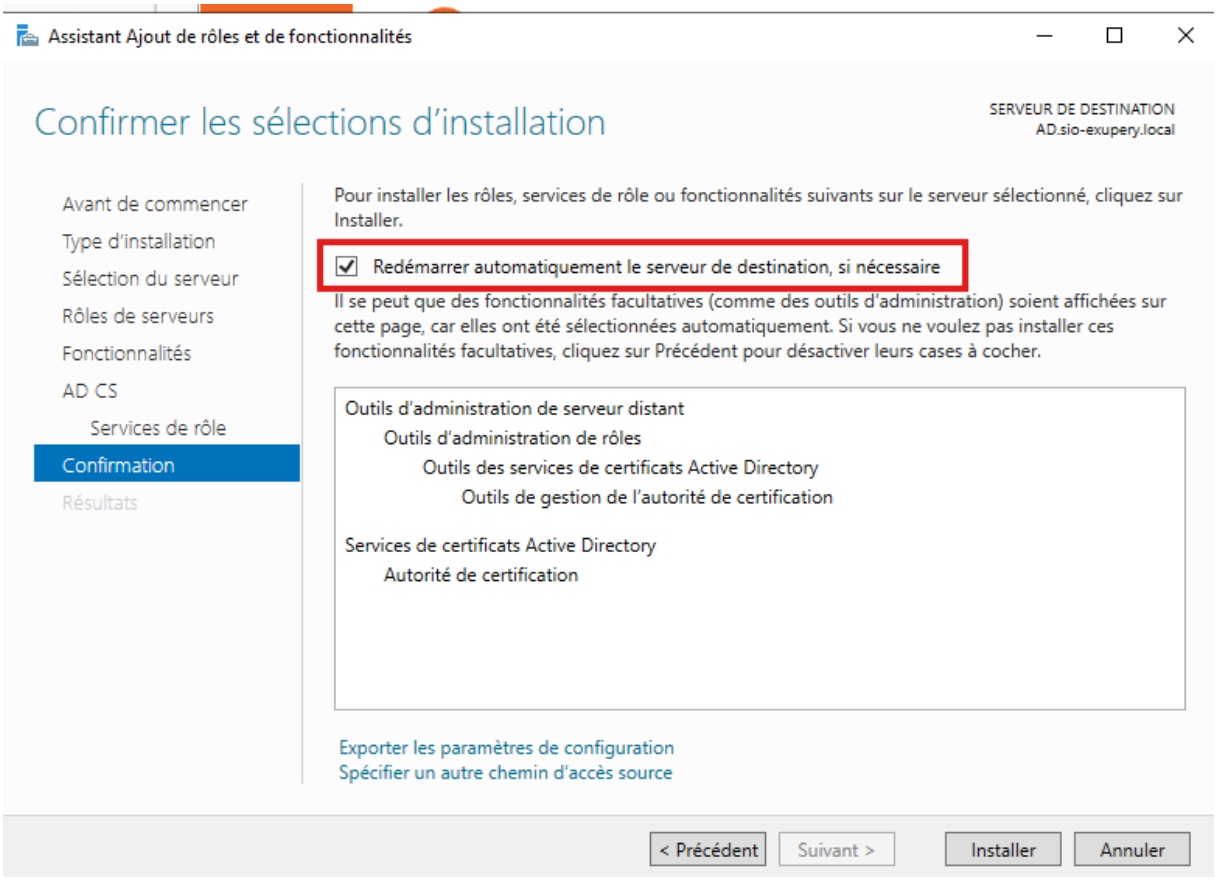
- J'ajoute le rôle Service de certificats Active Directory :



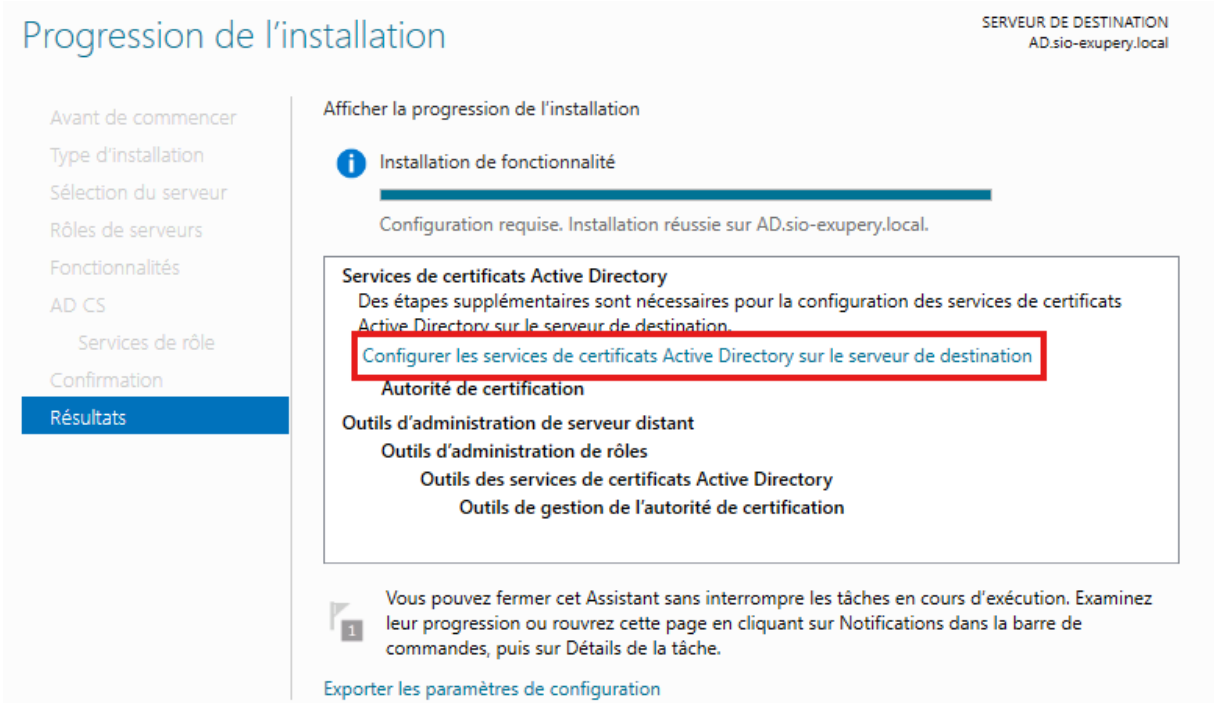
- Je prends connaissance des informations la page d'information AD CS et je clique sur le bouton Suivant :



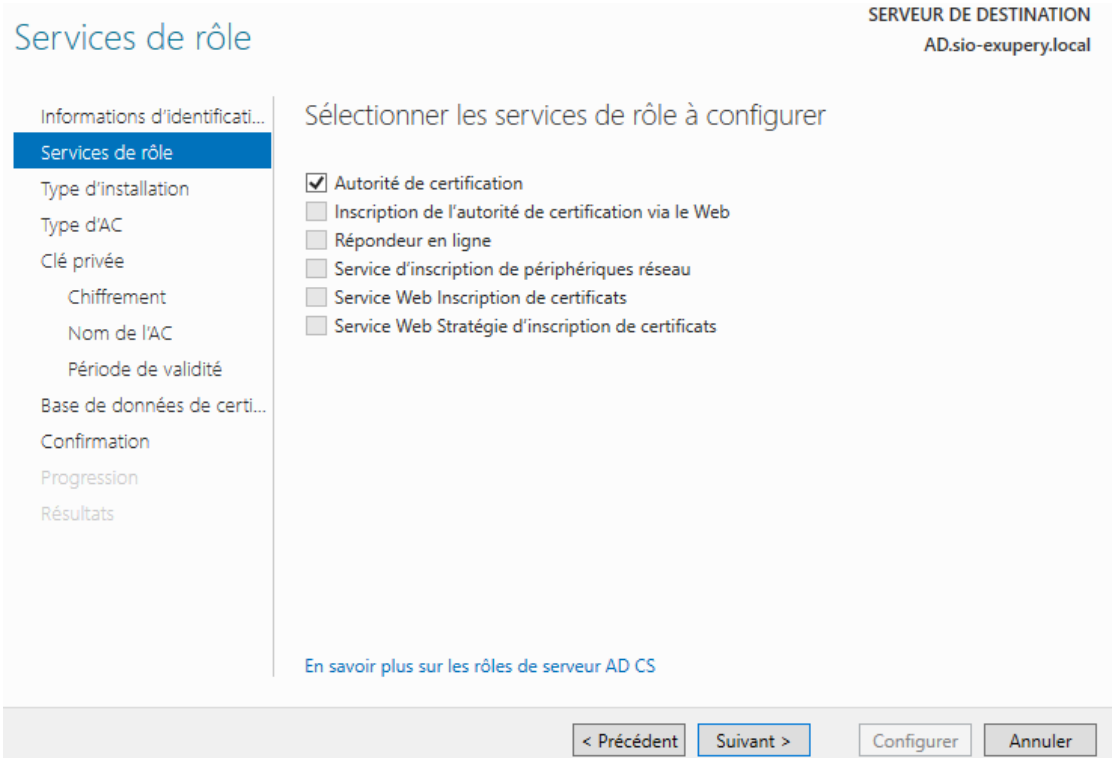
- Je coche la case Redémarrer automatiquement... et je clique sur Installer :



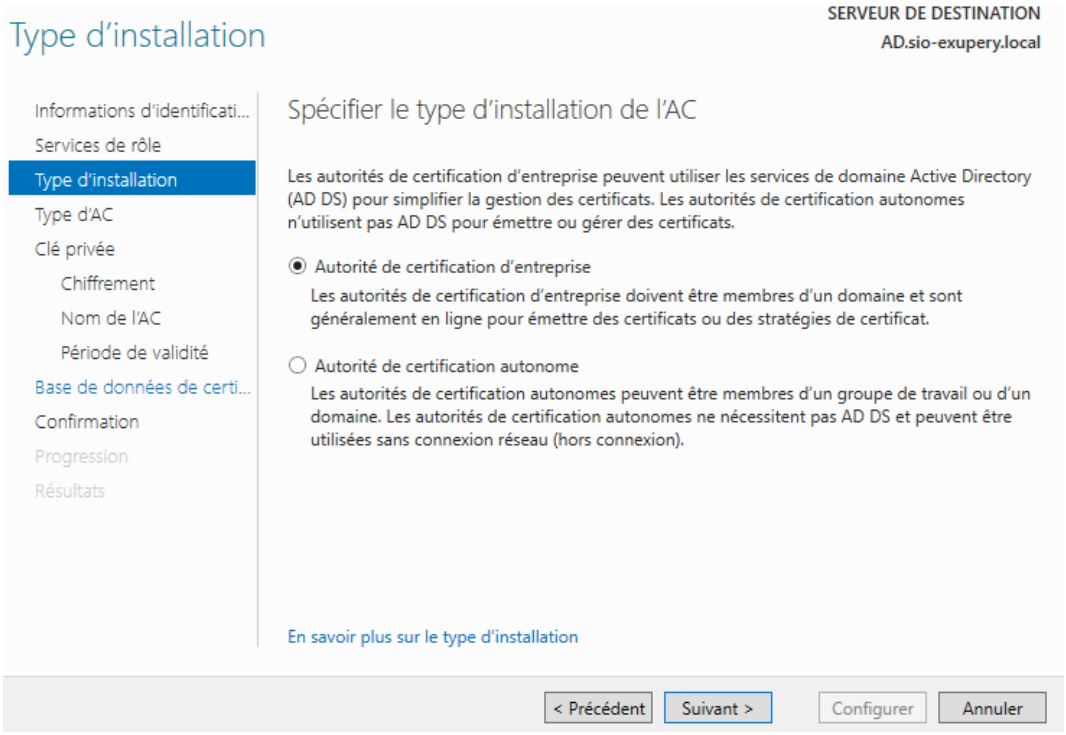
- Une fois l'installation terminée, je clique sur le lien Configurer les services de certificats Active Directory sur le serveur de destination :



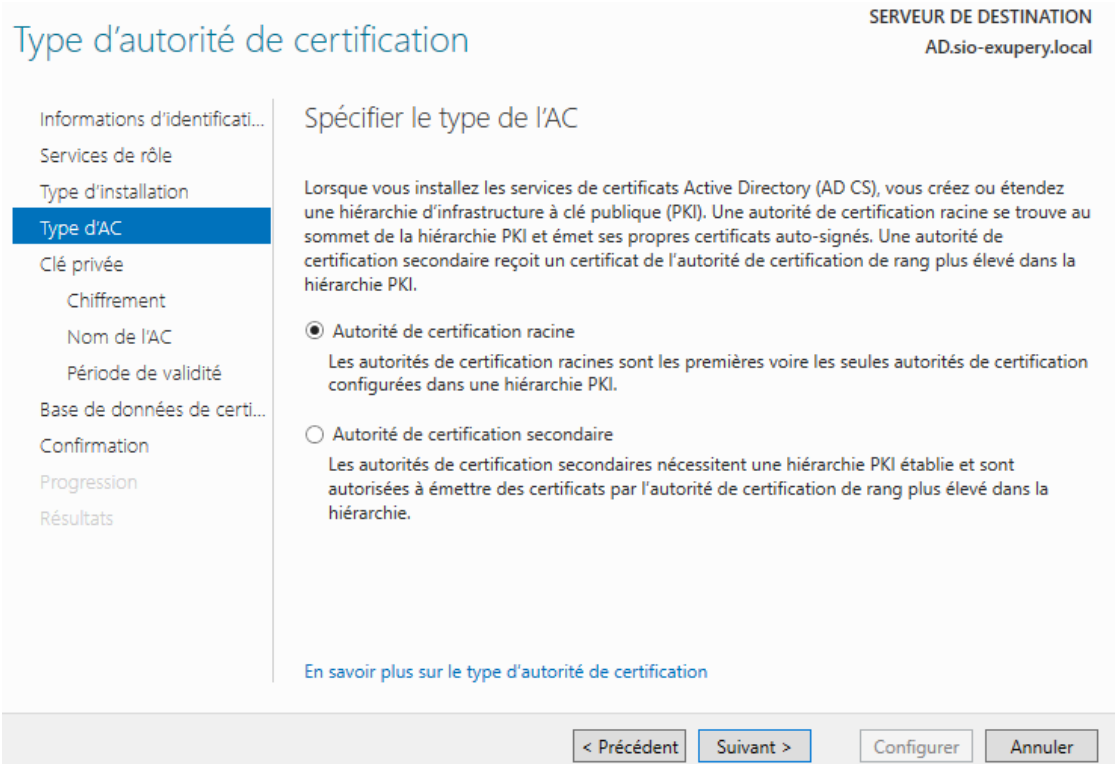
- Je coche la case Autorité de certification pour configurer ce rôle :



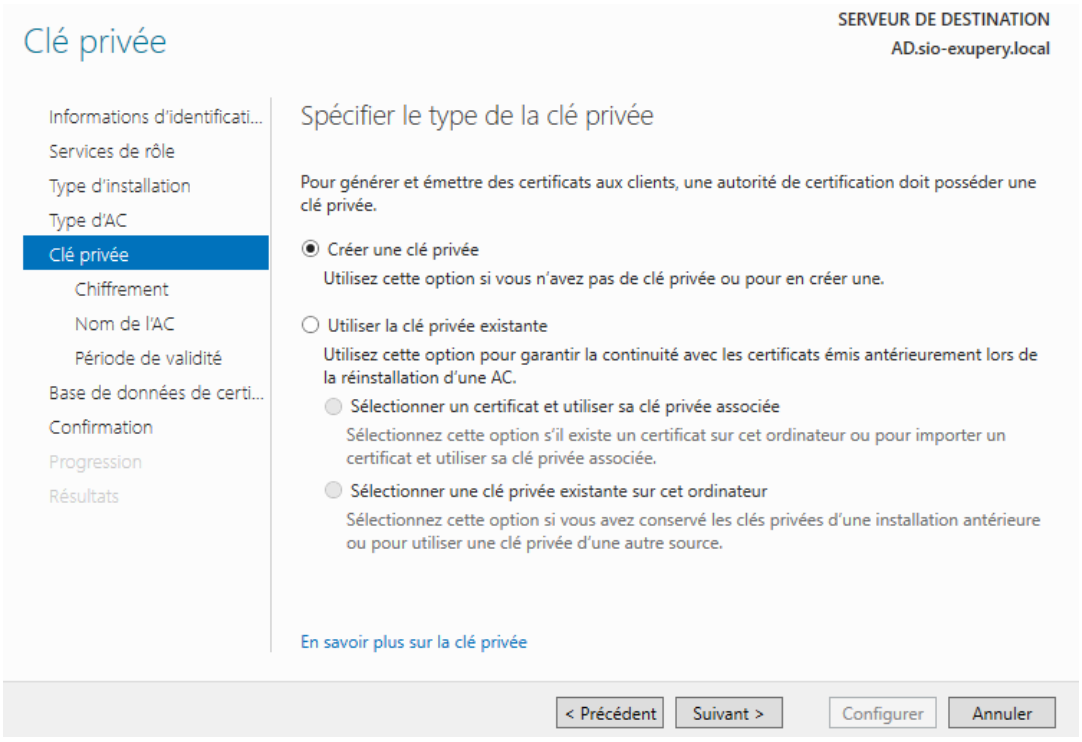
- Je sélectionne Autorité de certification d'entreprise.



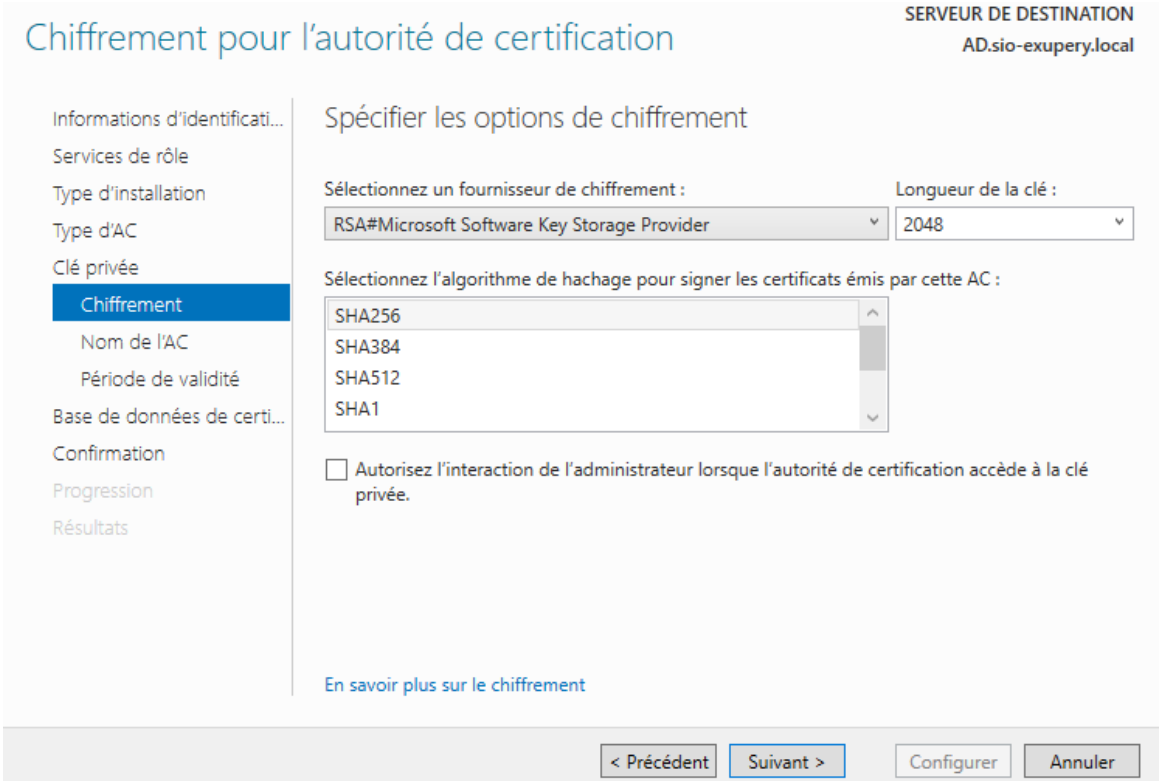
- Je sélectionne Autorité de certification racine car notre autorité ne sera pas dépendante d'une autre.



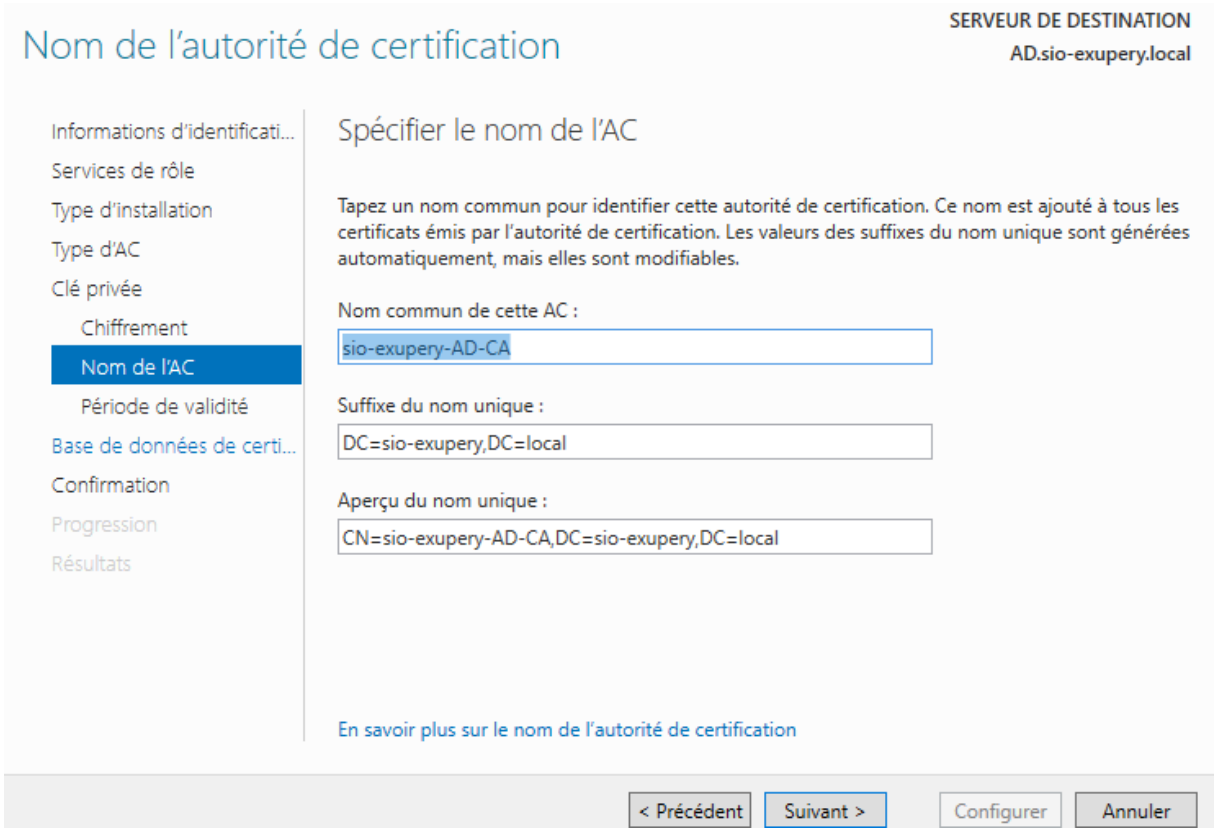
- Je sélectionne Créer une nouvelle clé privée :



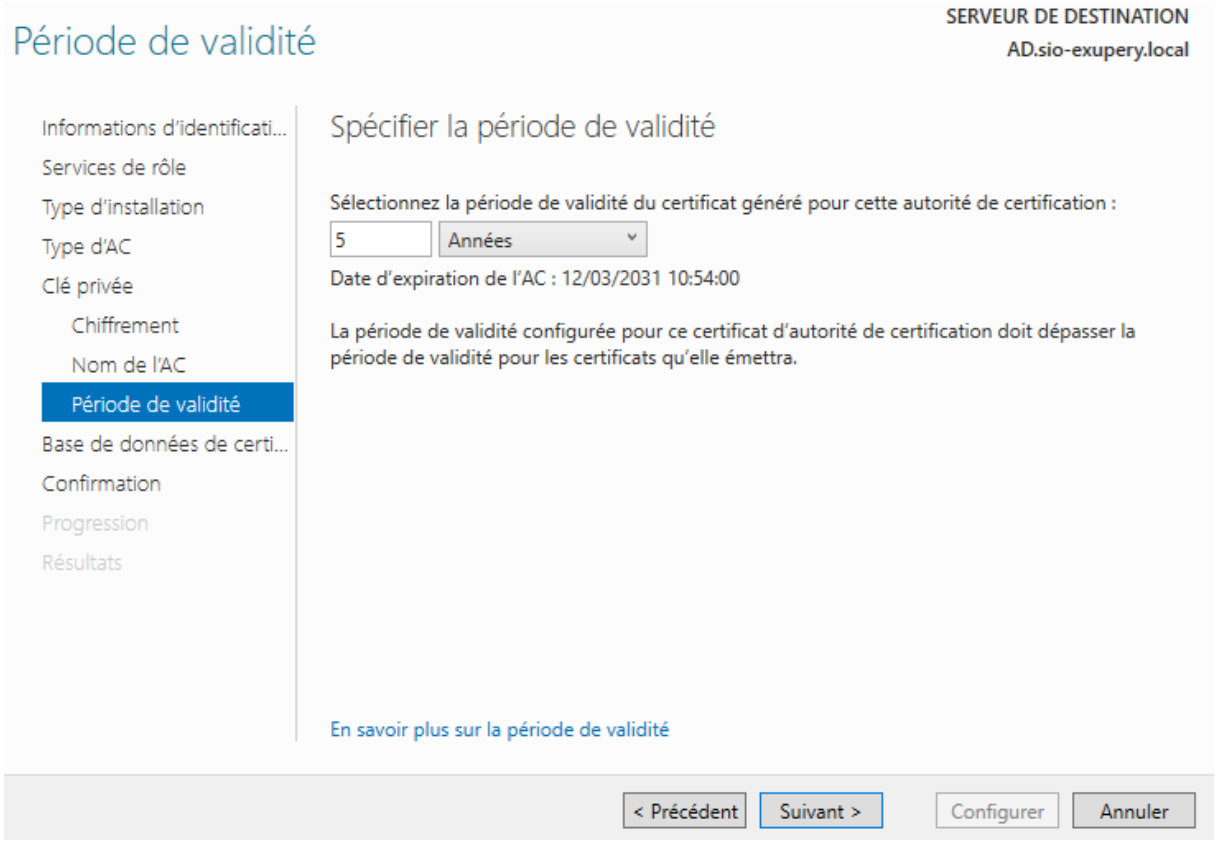
- Je choisi l'algorithme de chiffrement ainsi que de hachage par défaut :



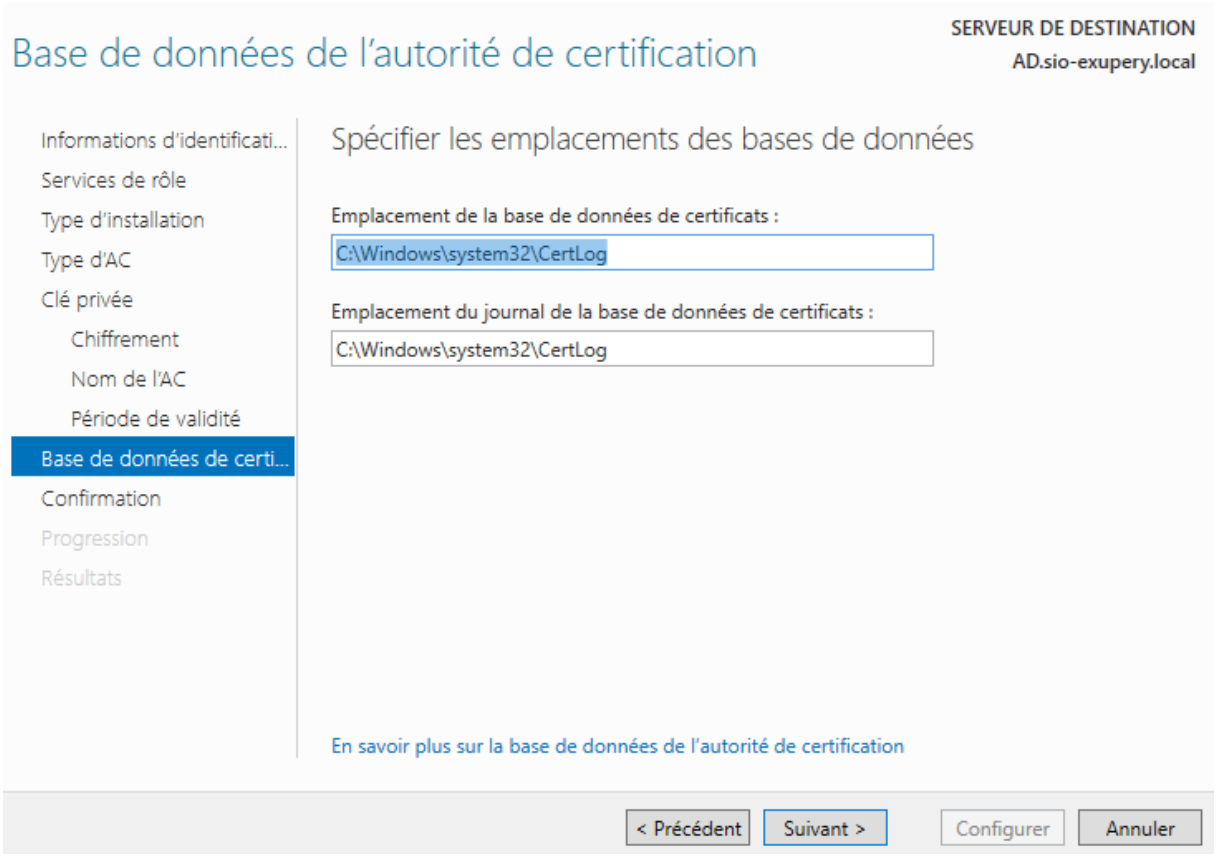
- Par défaut, l'assistant nomme l'autorité de certification avec le nom de domaine suivi du nom de machine : sio-exupery-AD-CA :



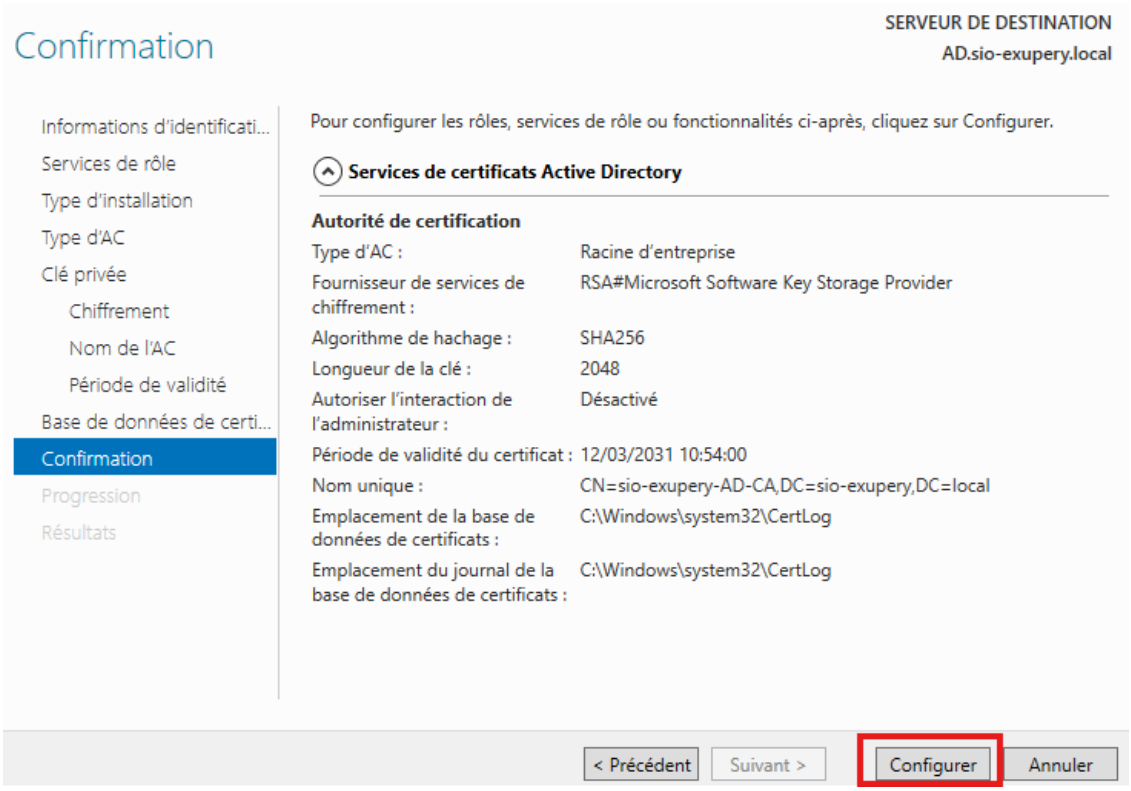
- Je laisse la période de validité par défaut :



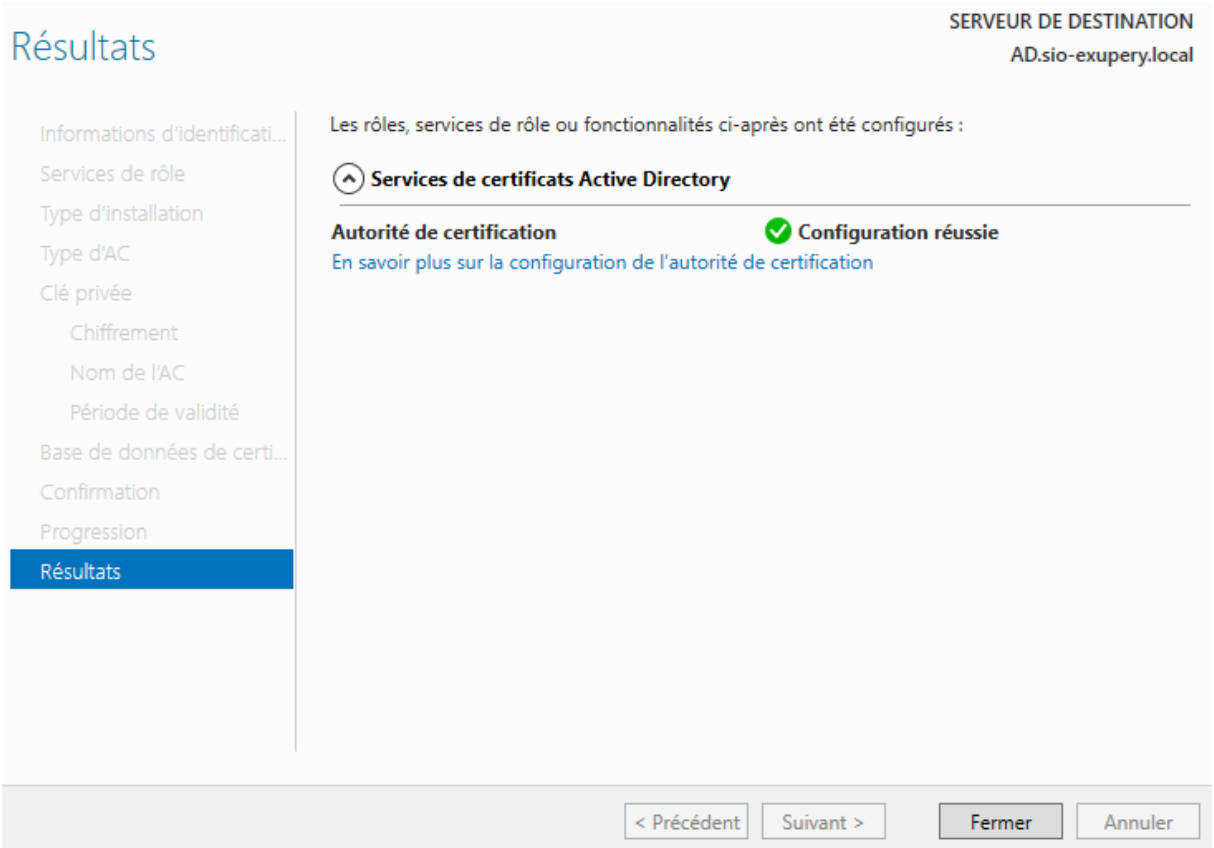
- Je laisse les dossiers des bases de données, par défaut :



- L'assistant affiche un résumé de la configuration. Je clique sur Configurer :

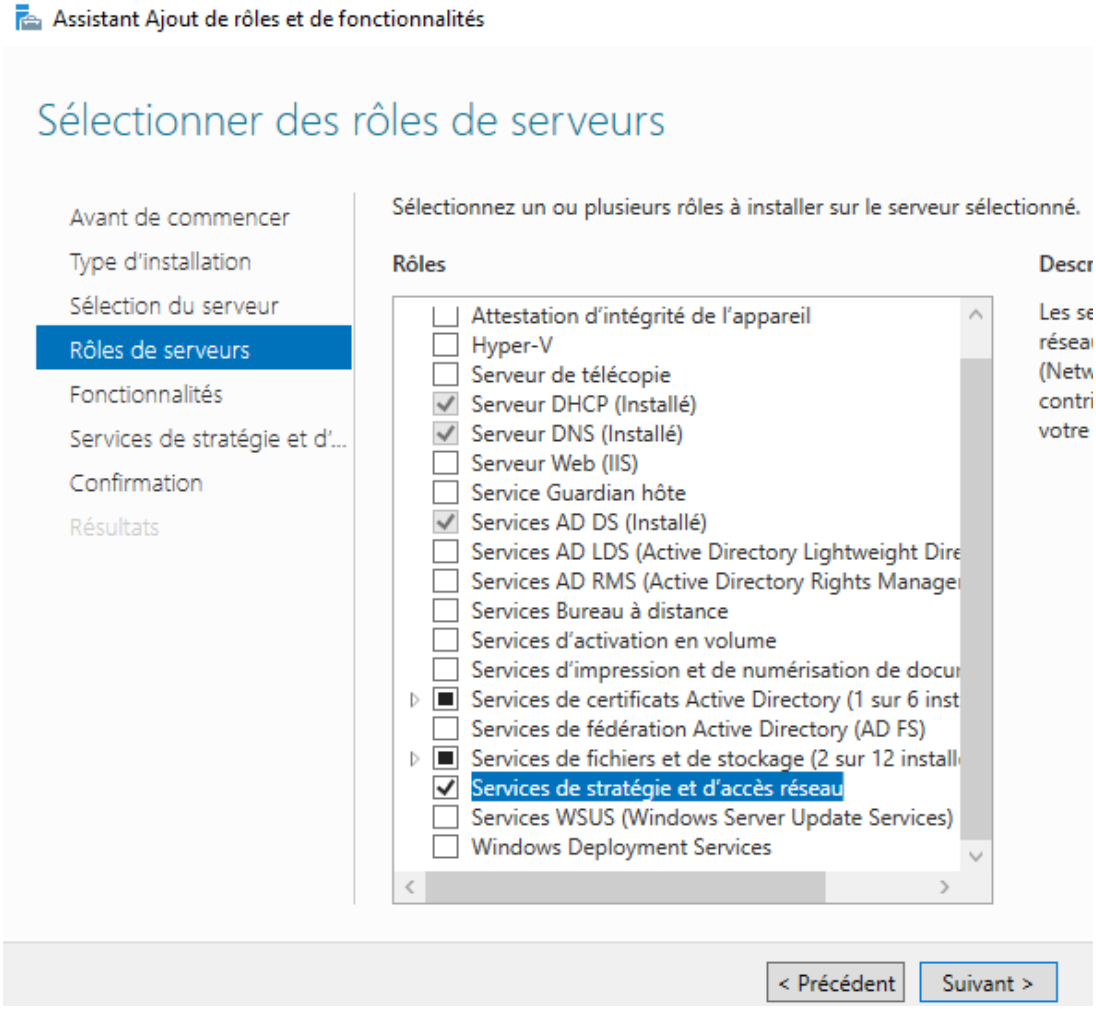


- L'autorité de certification est maintenant installée et configurée. Je clique sur Fermer :

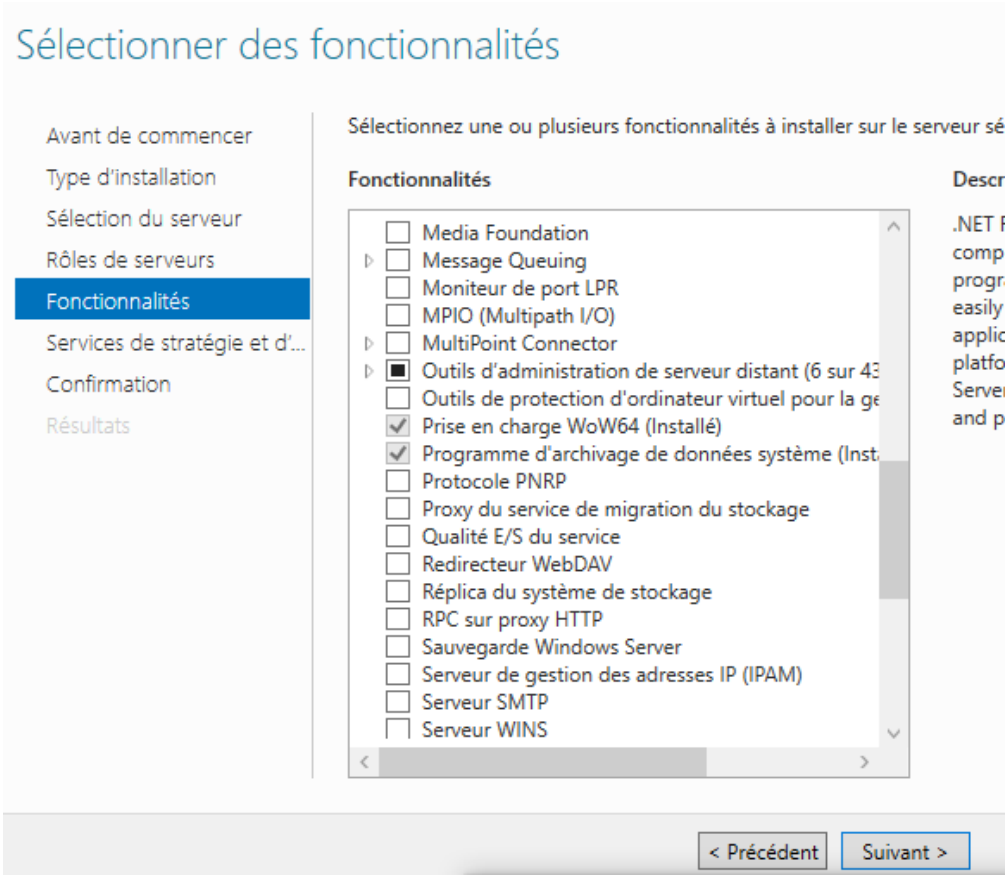


3-3- Installation du service NPS :

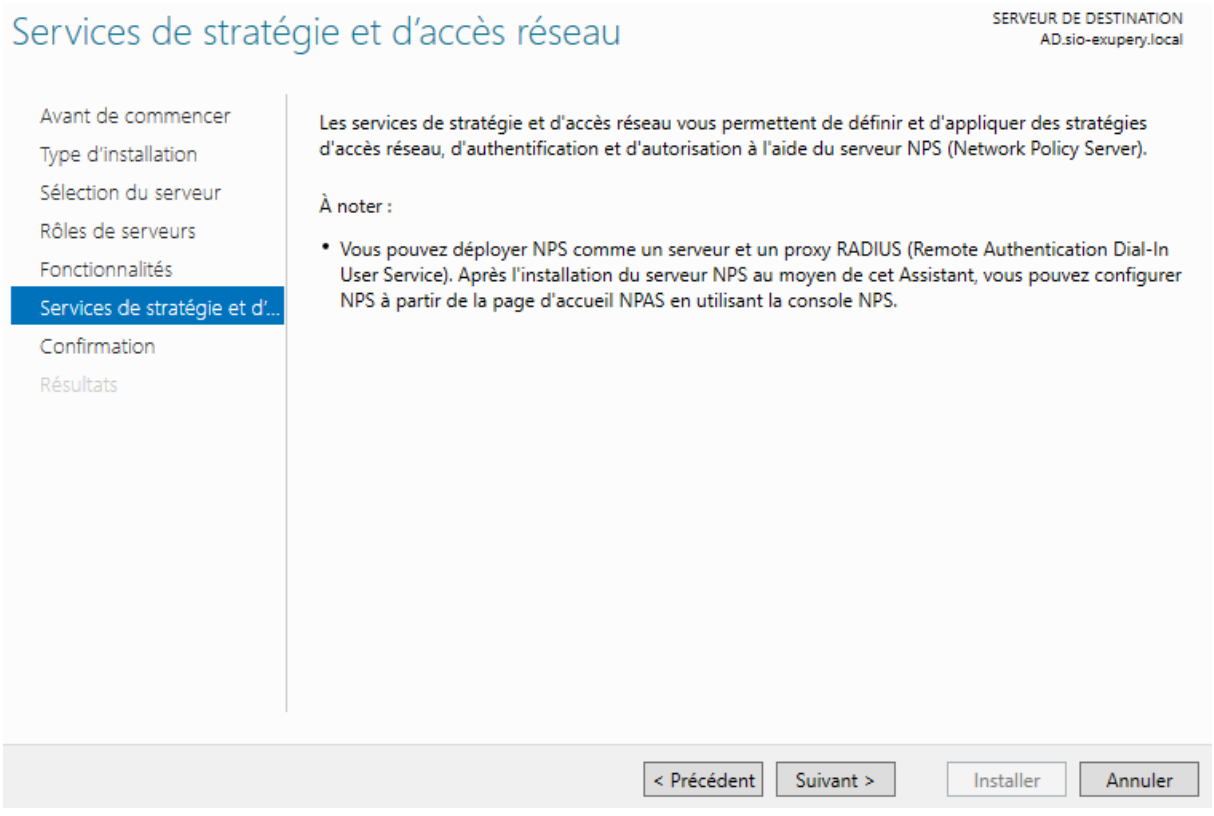
- J’ajoute le rôle Services de stratégie et d'accès réseau :



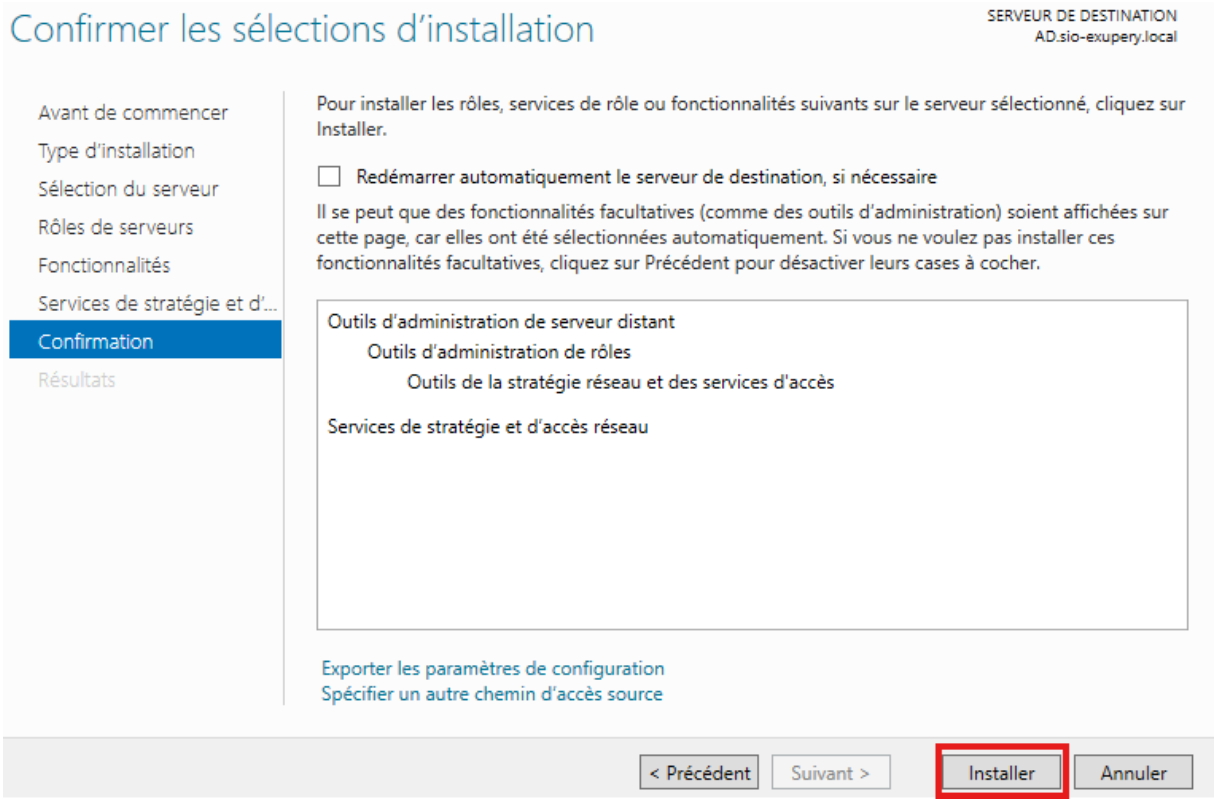
- Je clique sur le bouton Ajouter des fonctionnalités puis sur suivant :



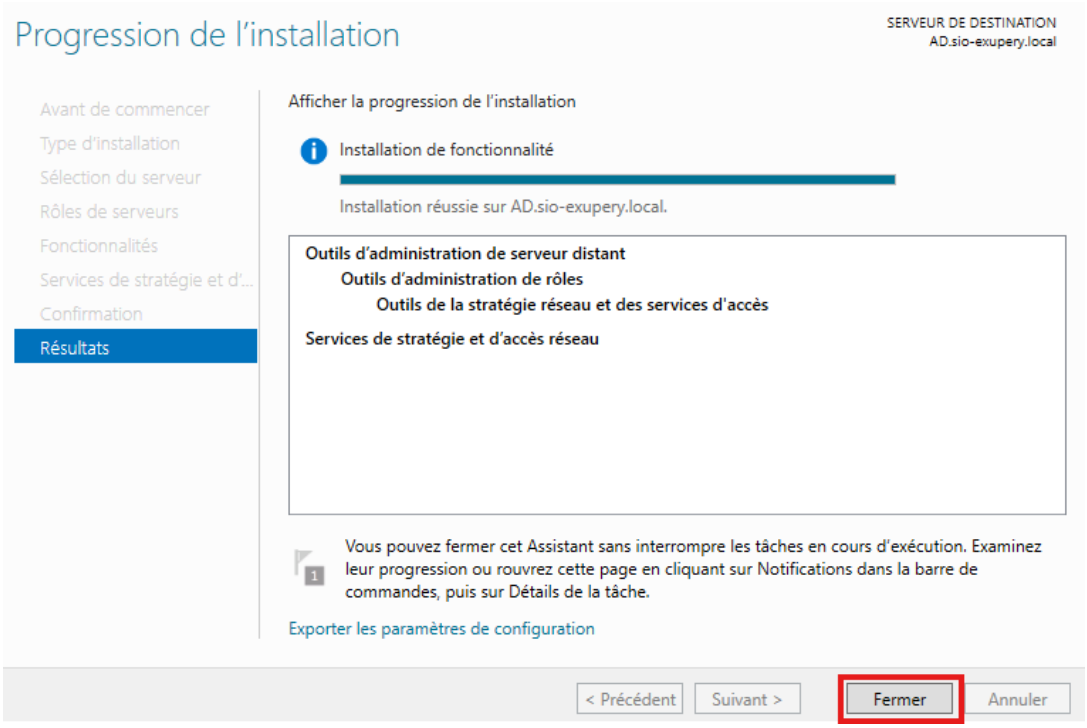
- L'écran d'information Services de stratégie et d'accès réseau s'affiche. Je clique sur le bouton Suivant :



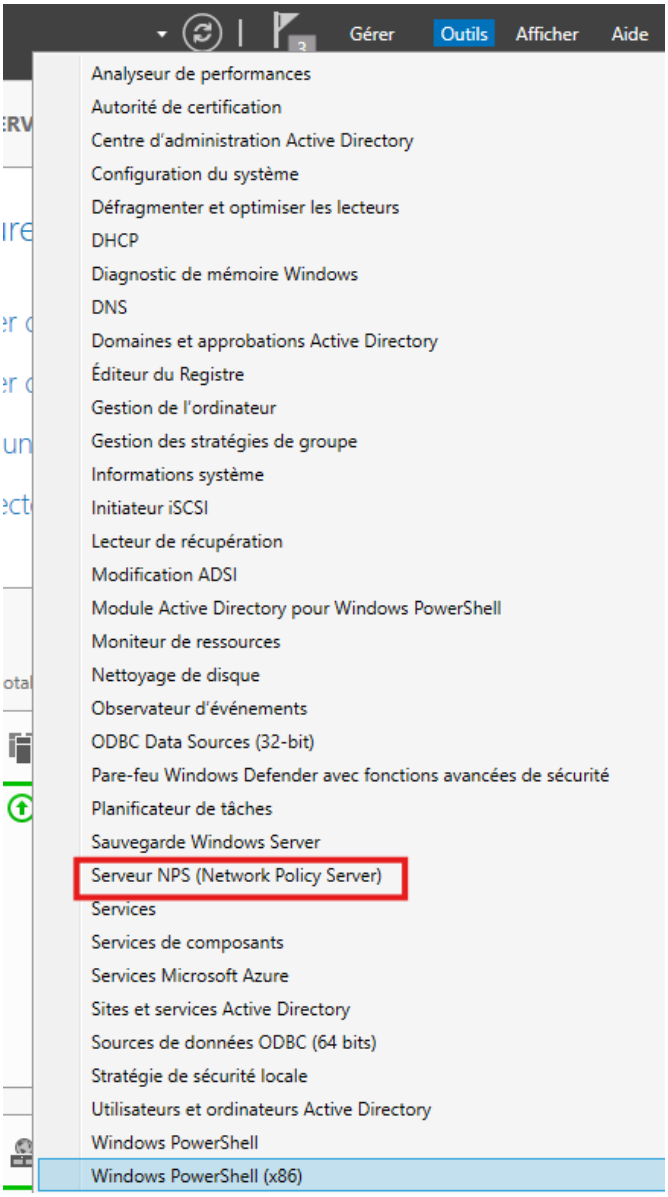
- Je clique sur le bouton Installer :



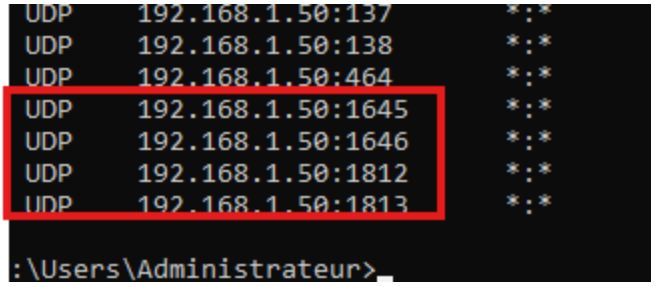
- Je clique sur le bouton Fermer :



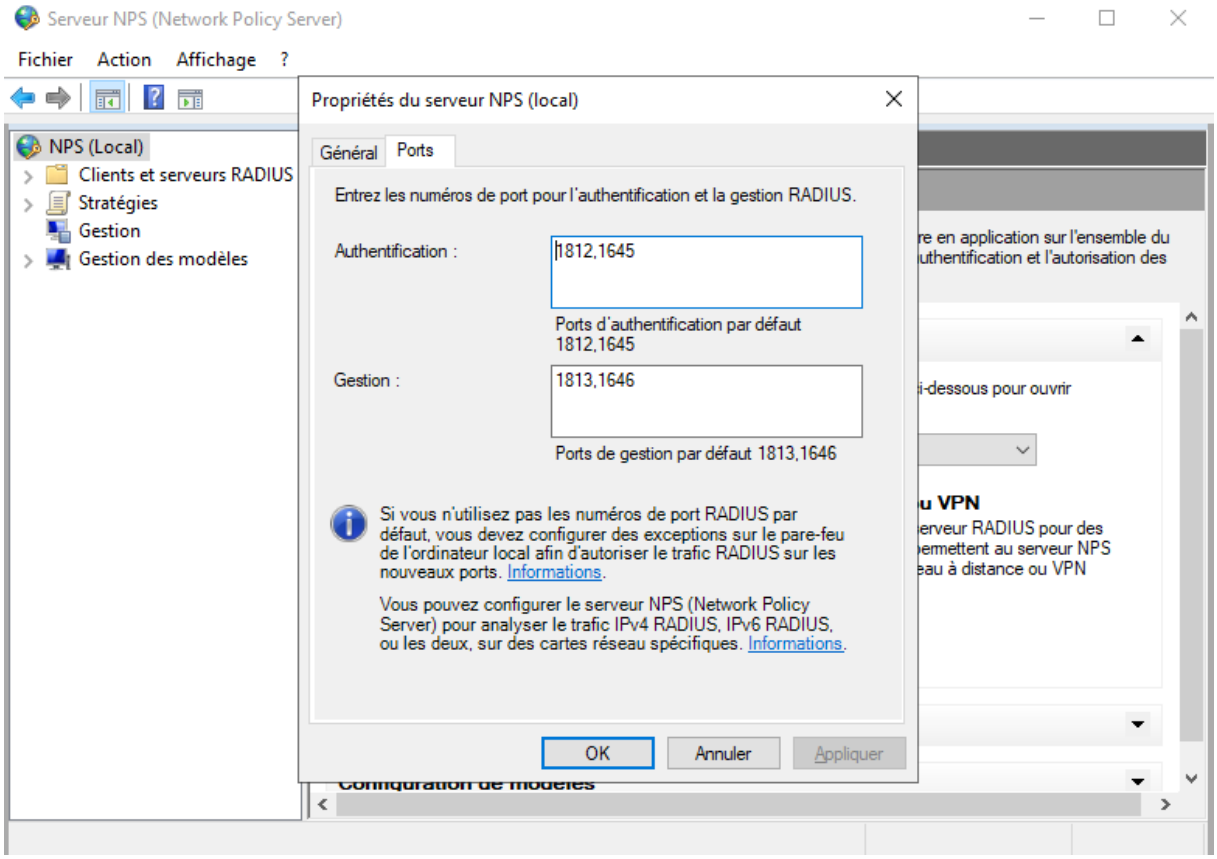
- Je constate la présence de la console Serveur NPS :



- Pour vérifier le bon fonctionnement du service NPS sur le serveur, j'affiche les ports en écoute sur celui-ci avec la commande netstat -a -p udp :

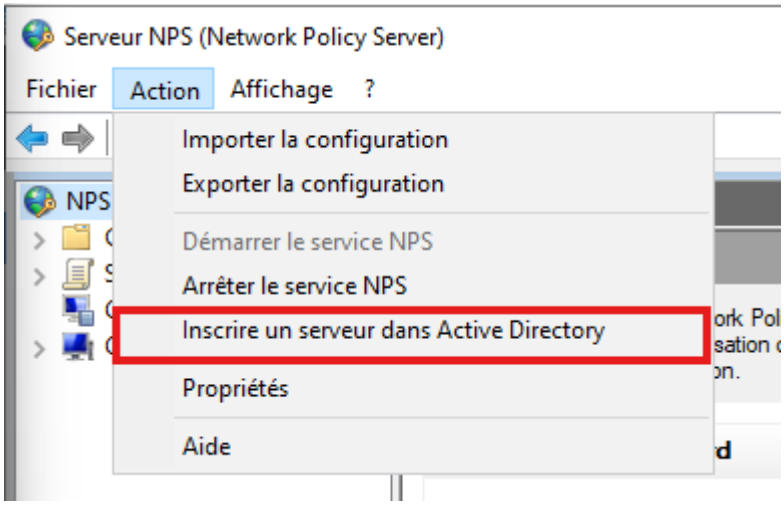


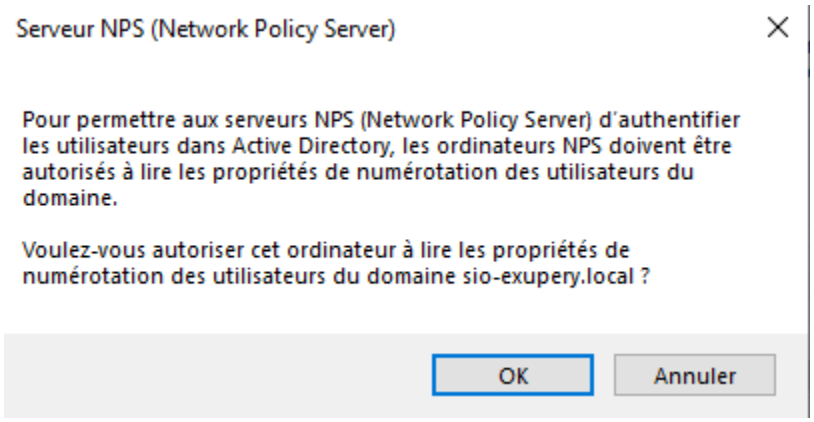
- J’ouvre la console Serveur NPS (Network Policy Server) et je retrouve ces ports dans les propriétés du serveur NPS :

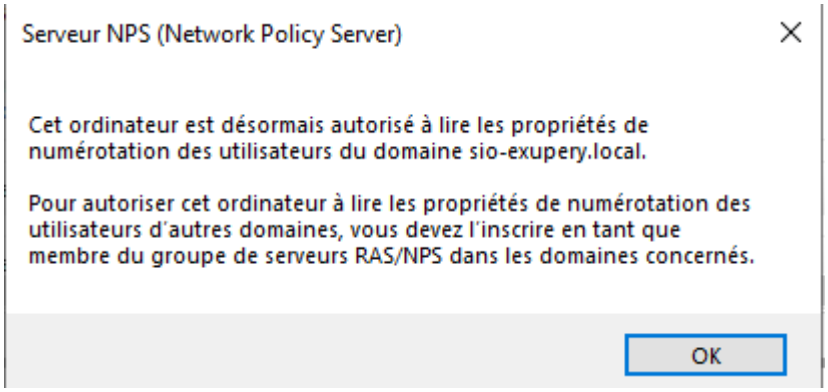


3.4- Configuration du serveur RADIUS NPS :

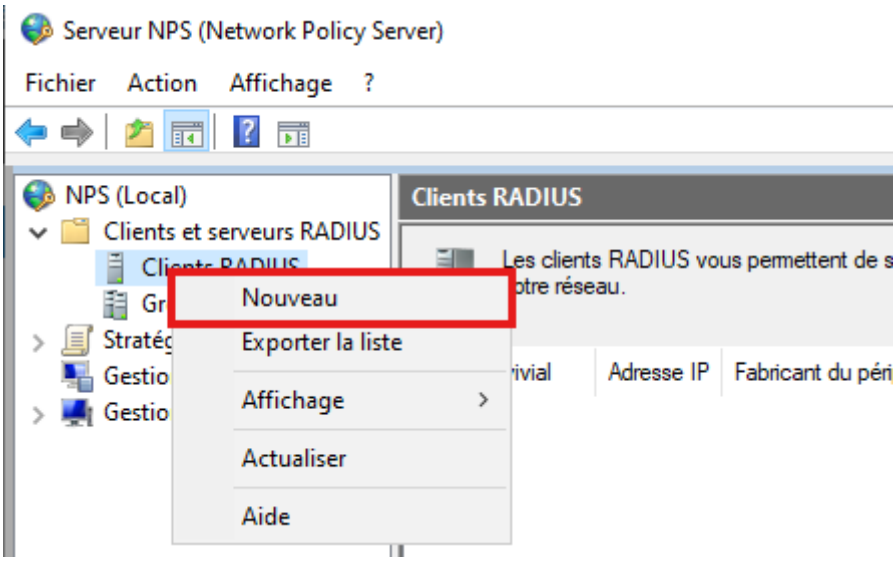
- Afin d’inscrire NPS dans Active Directory pour lui permettre d'interroger la base des utilisateurs, je clique depuis le menu Action sur Inscrire un serveur dans Active Directory :



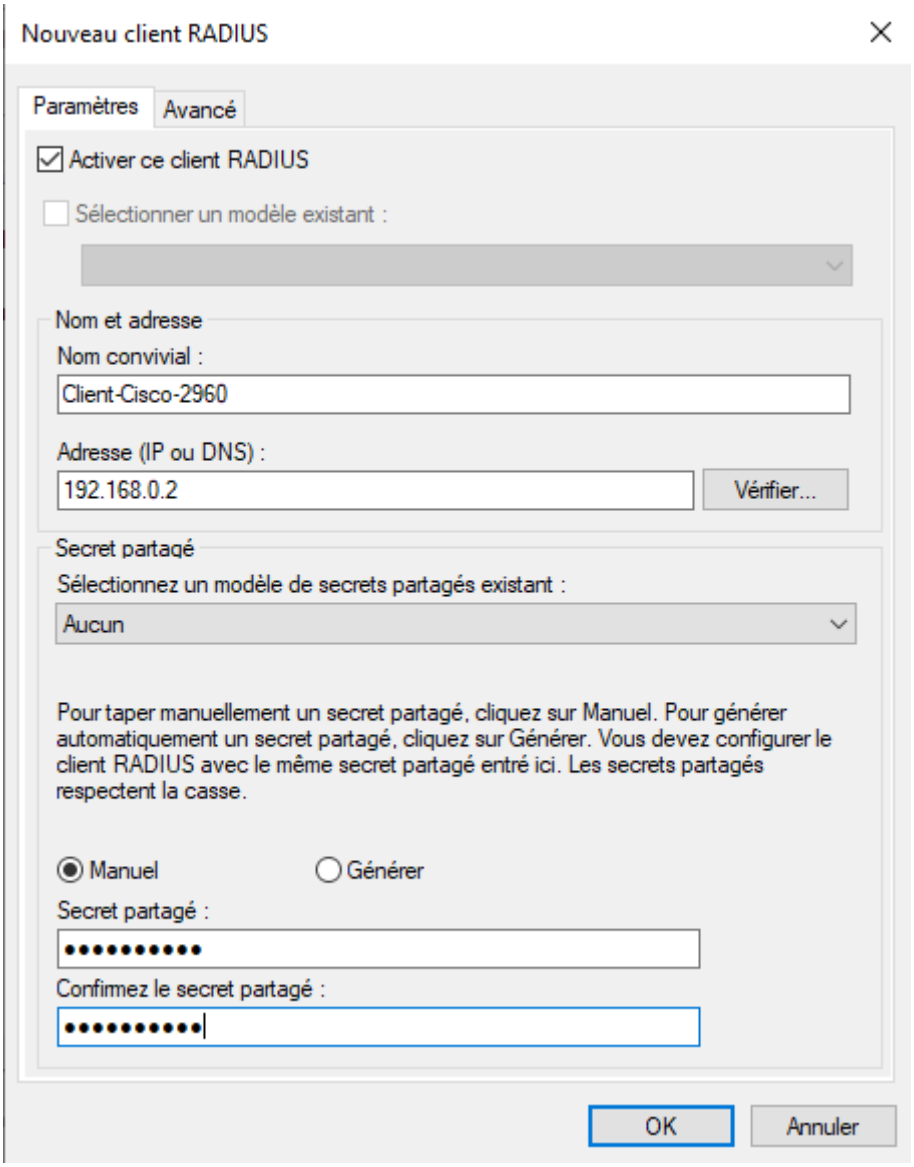




- Je clic droit sur l'entrée Clients RADIUS puis sélectionne Nouveau :

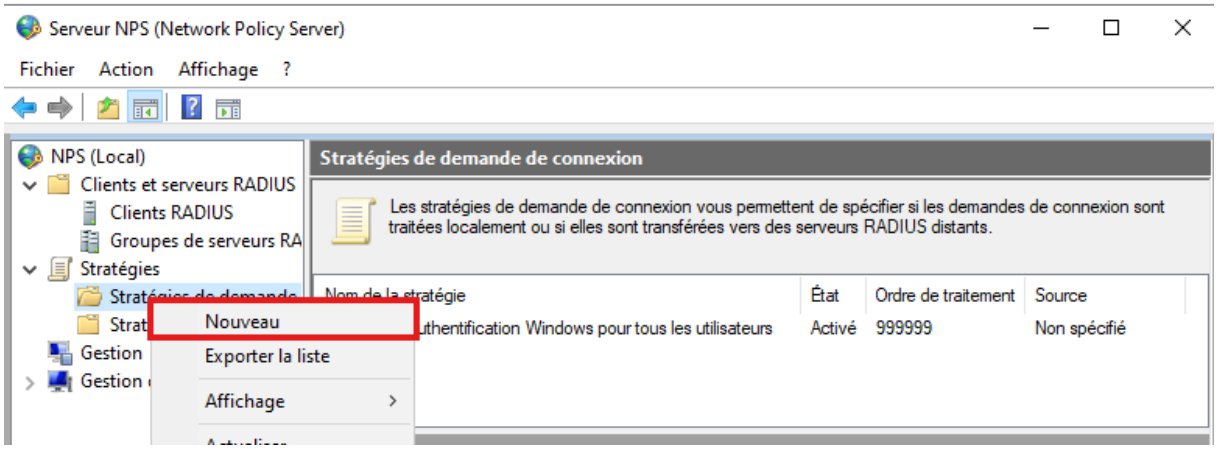


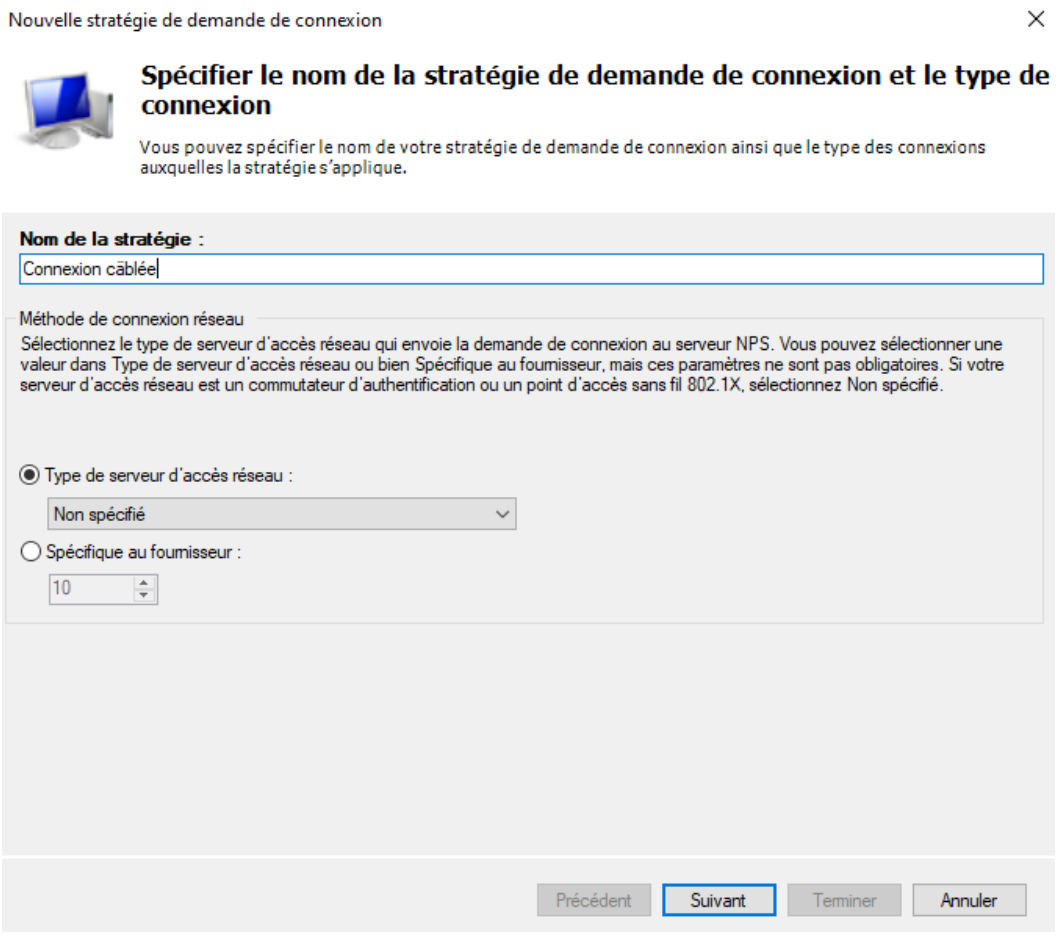
- Je rentre les informations nécessaires pour ajouter le nouveau client RADIUS :



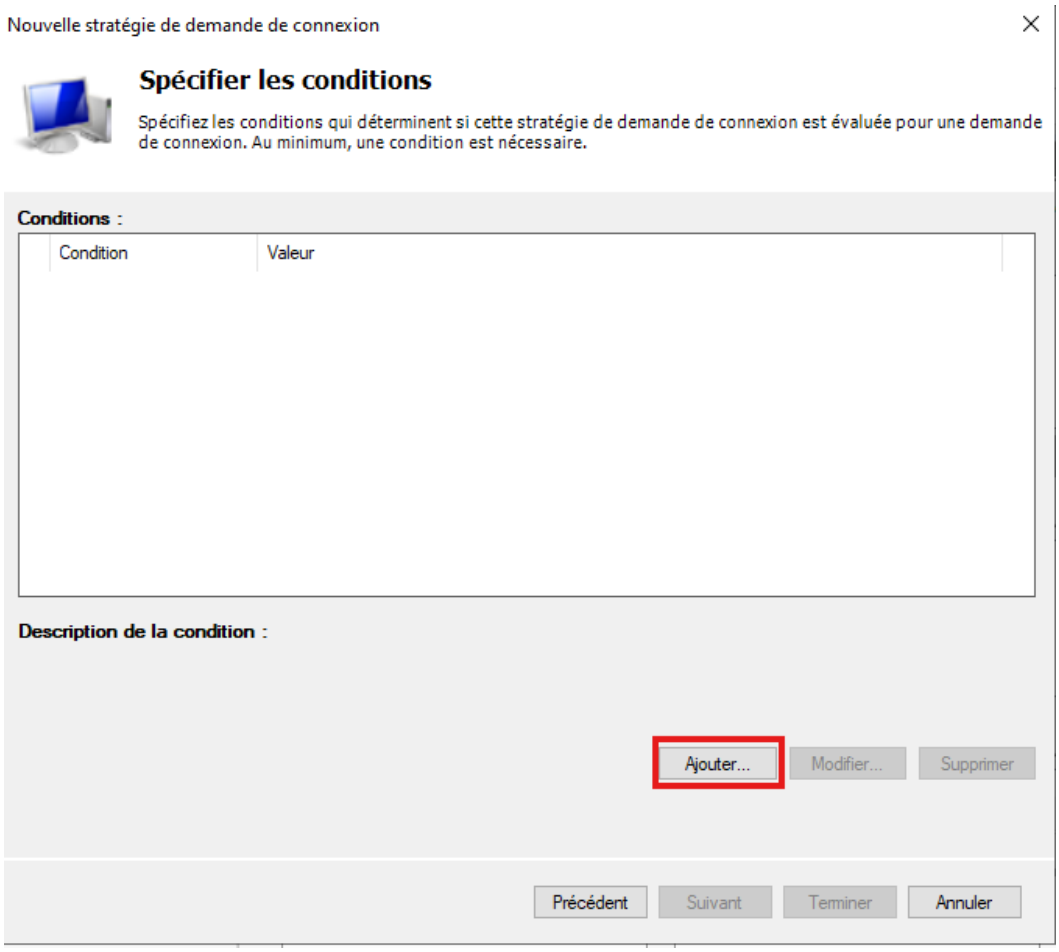
Déclaration d'une stratégie de demande de connexion :

- Je clic droit sur l'entrée Stratégies de demande de connexion et je sélectionne Nouveau. Je déclare une stratégie de demande de connexion pour Ethernet. Je spécifie un nom de stratégie (Connexion câblée). Je laisse le type de serveur d'accès réseau sur Unspecified car j'utilise un commutateur en tant que client Radius :

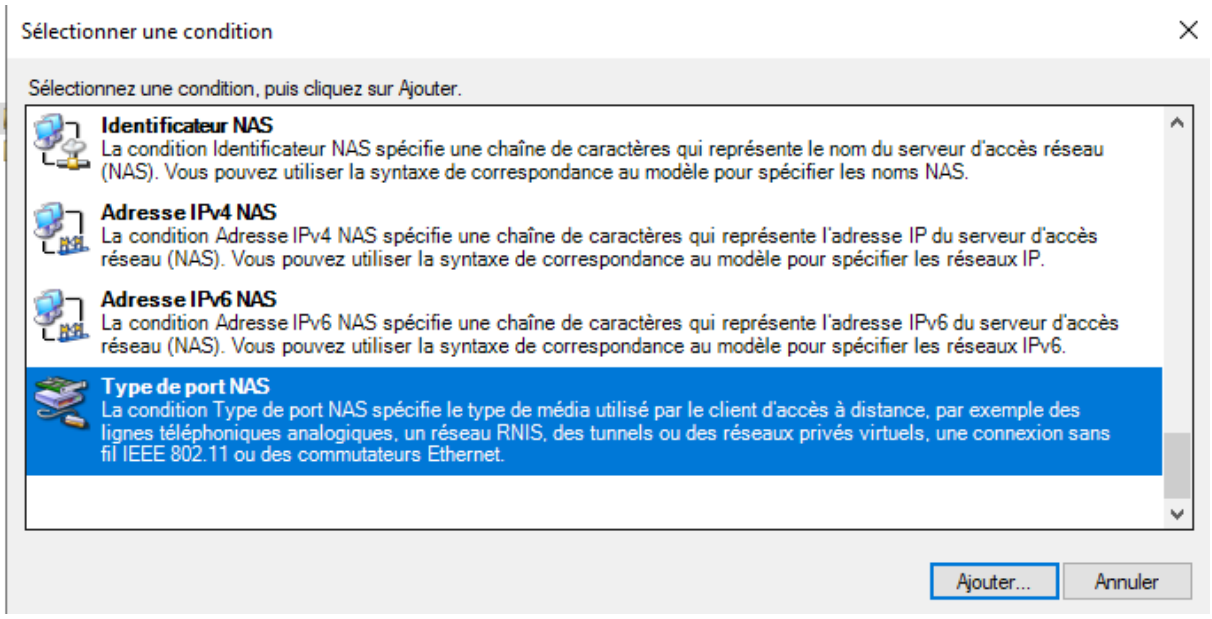




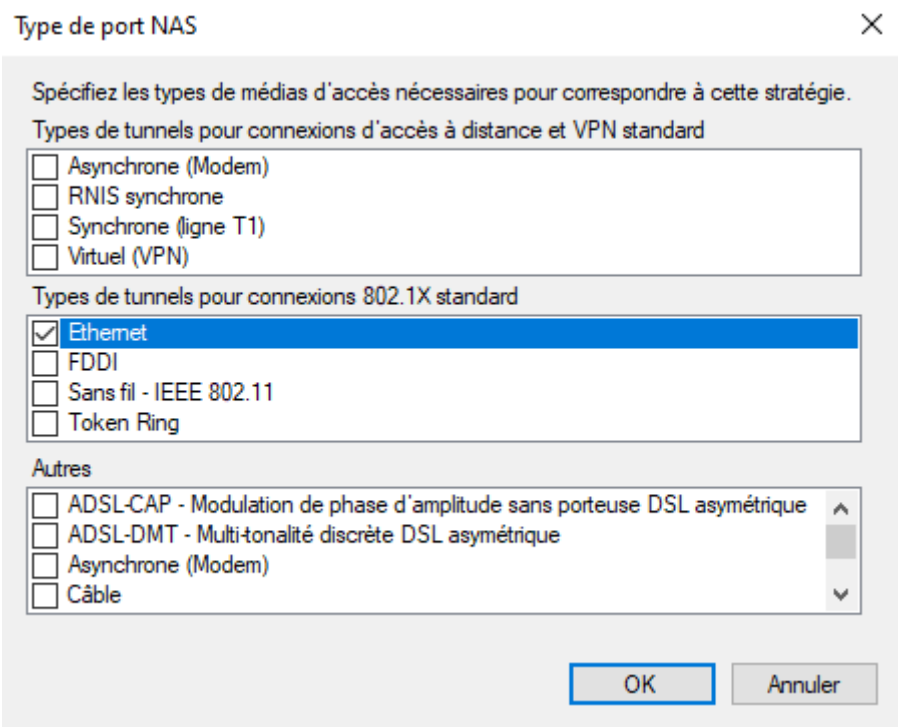
- Je clique sur le bouton Ajouter :



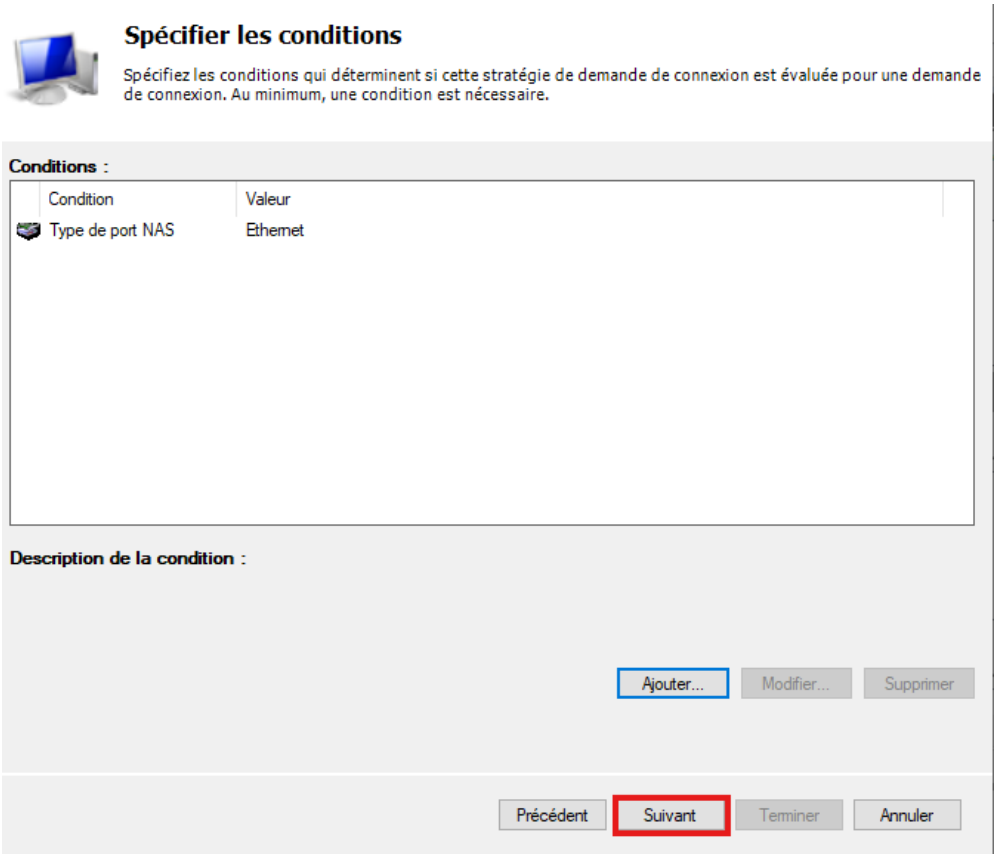
- J'indique le type de média utilisé par le client d'accès à distance. Je sélectionne pour cela Type de port NAS puis cliquez sur le bouton Ajouter :



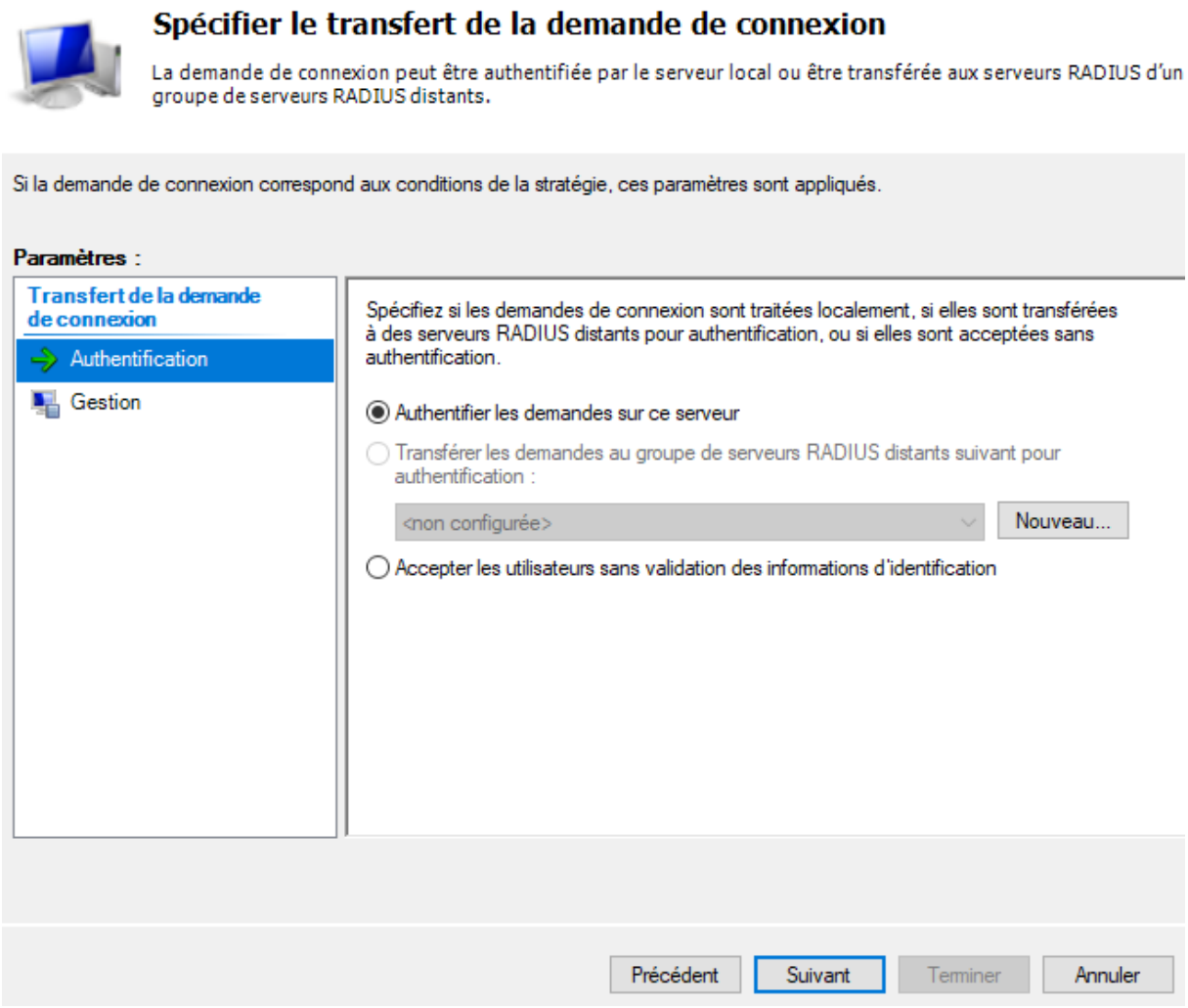
- Je coche Ethernet dans l'écran Type de port NAS :



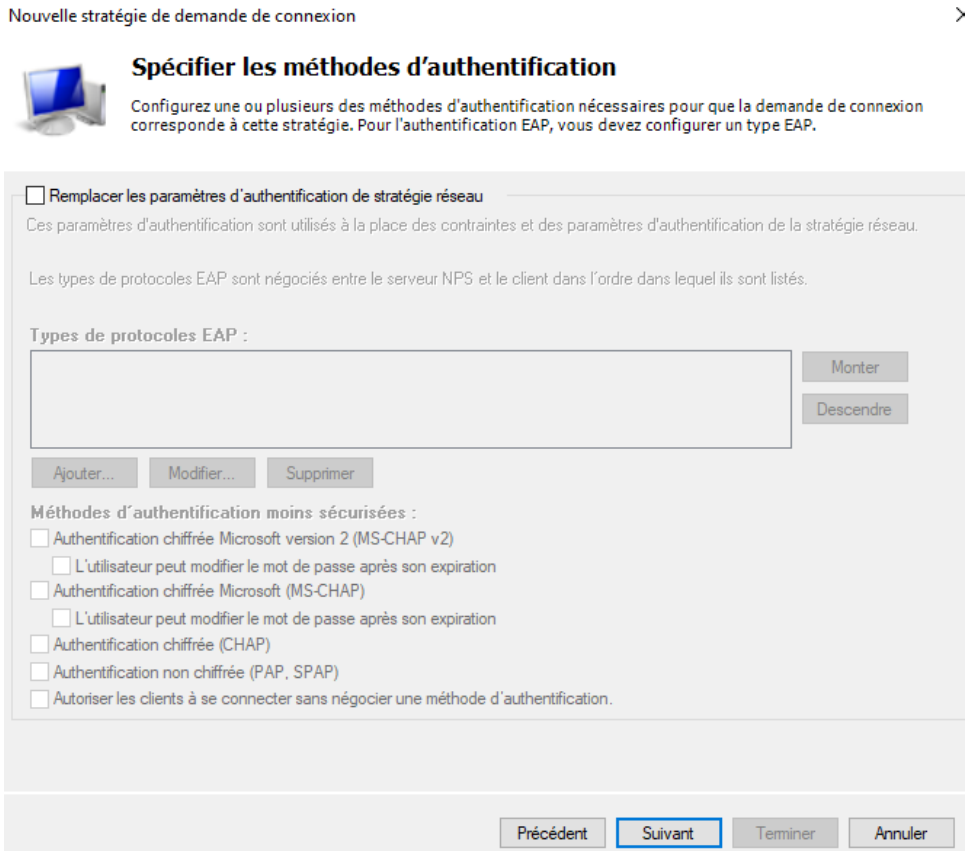
- Je clique sur le bouton Suivant :



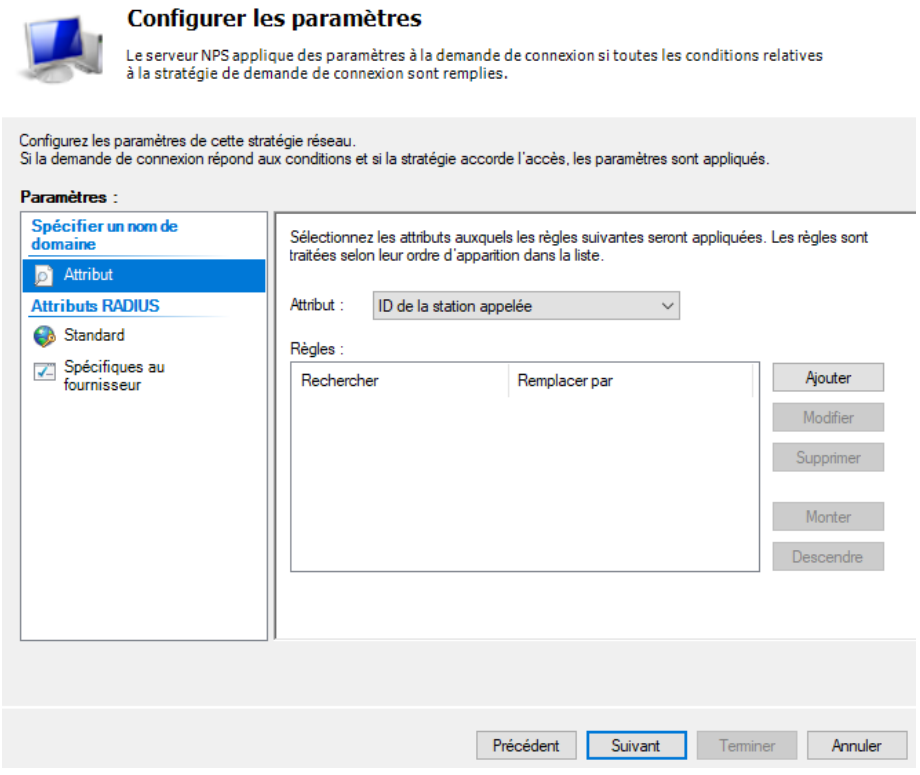
- Je garde le choix par défaut dans l'écran suivant. Les demandes seront traitées sur ce serveur et non sur un autre. Ce qui veut dire que ce NPS pourrait jouer un rôle de PROXY NPS s'il relayait les demandes à un autre serveur :



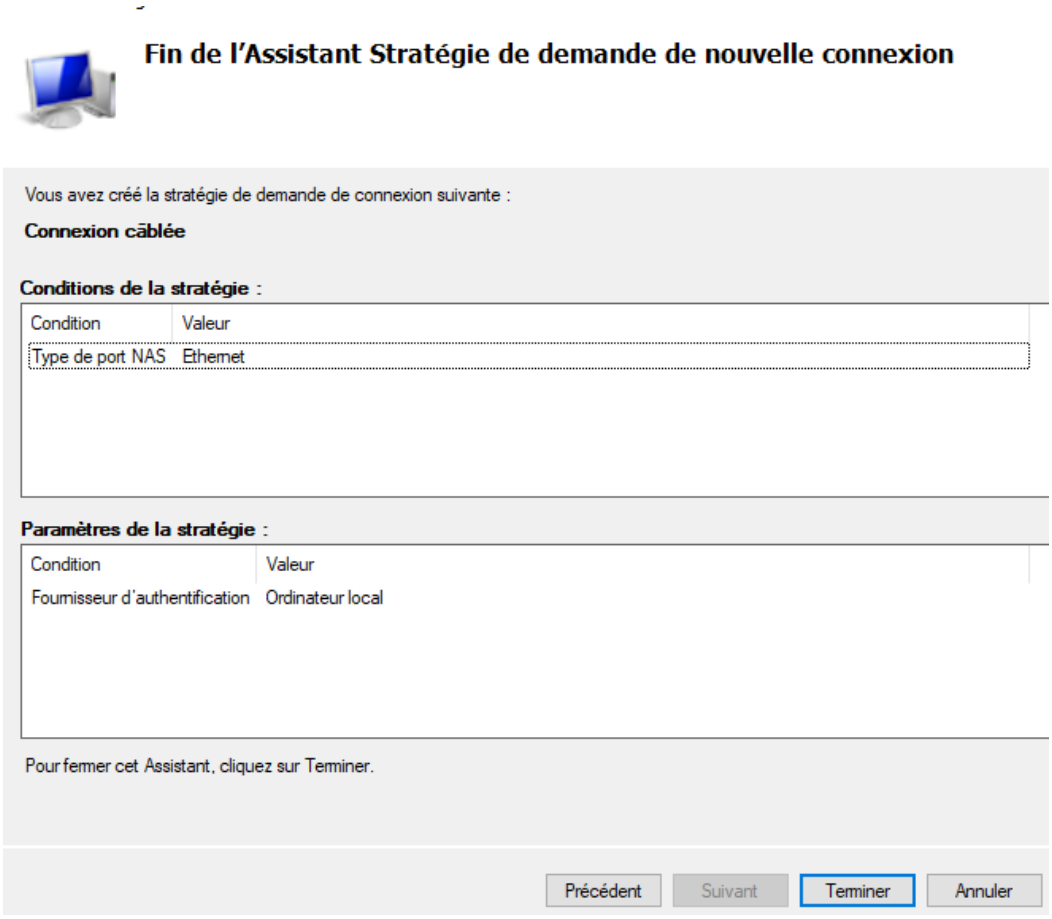
- Je laisse tel quel l'écran Je spécifie les méthodes d'authentification. C'est la stratégie d'accès réseau qui sera déclarée au paragraphe suivant qui va primer :

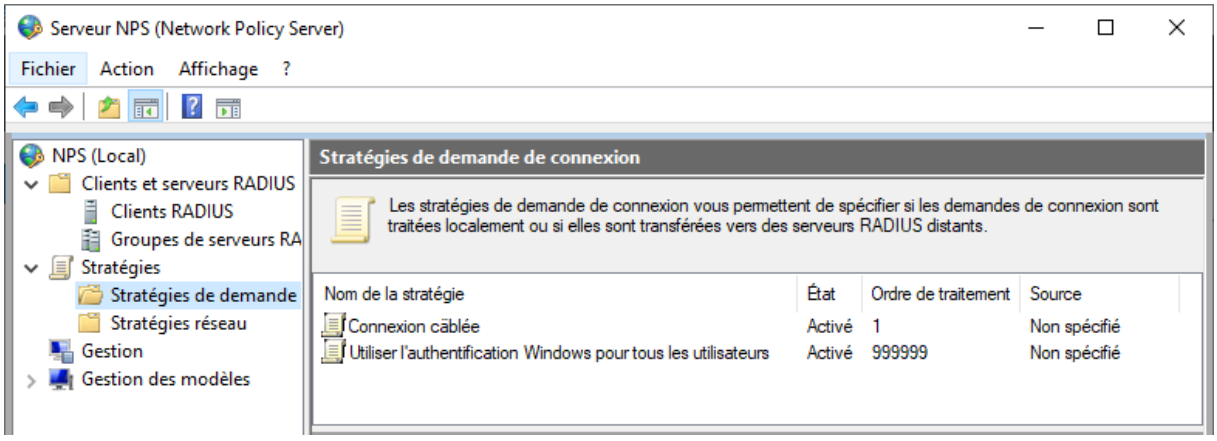


- Je clique de nouveau sur le bouton Suivant :



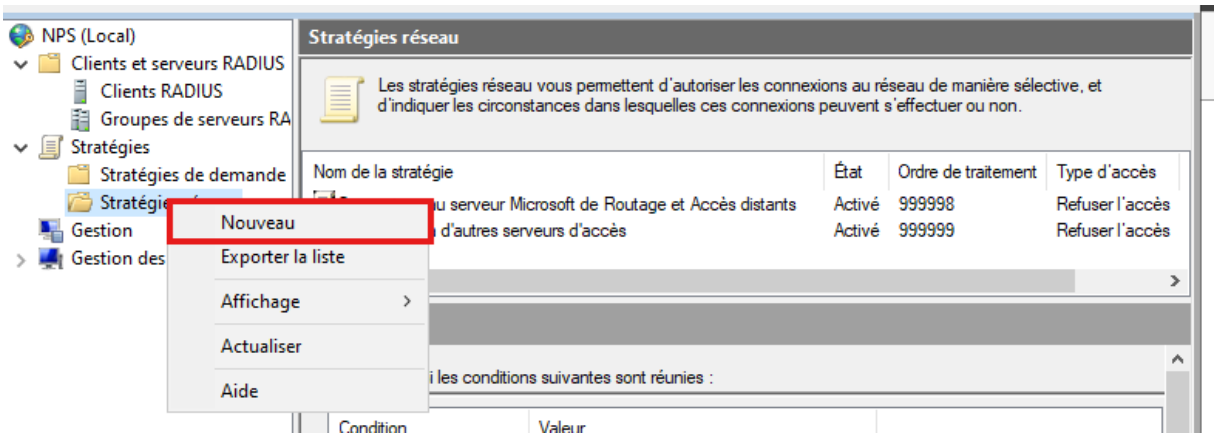
- Je clique sur le bouton Terminer dans l'écran récapitulatif de la stratégie de demande de connexion :

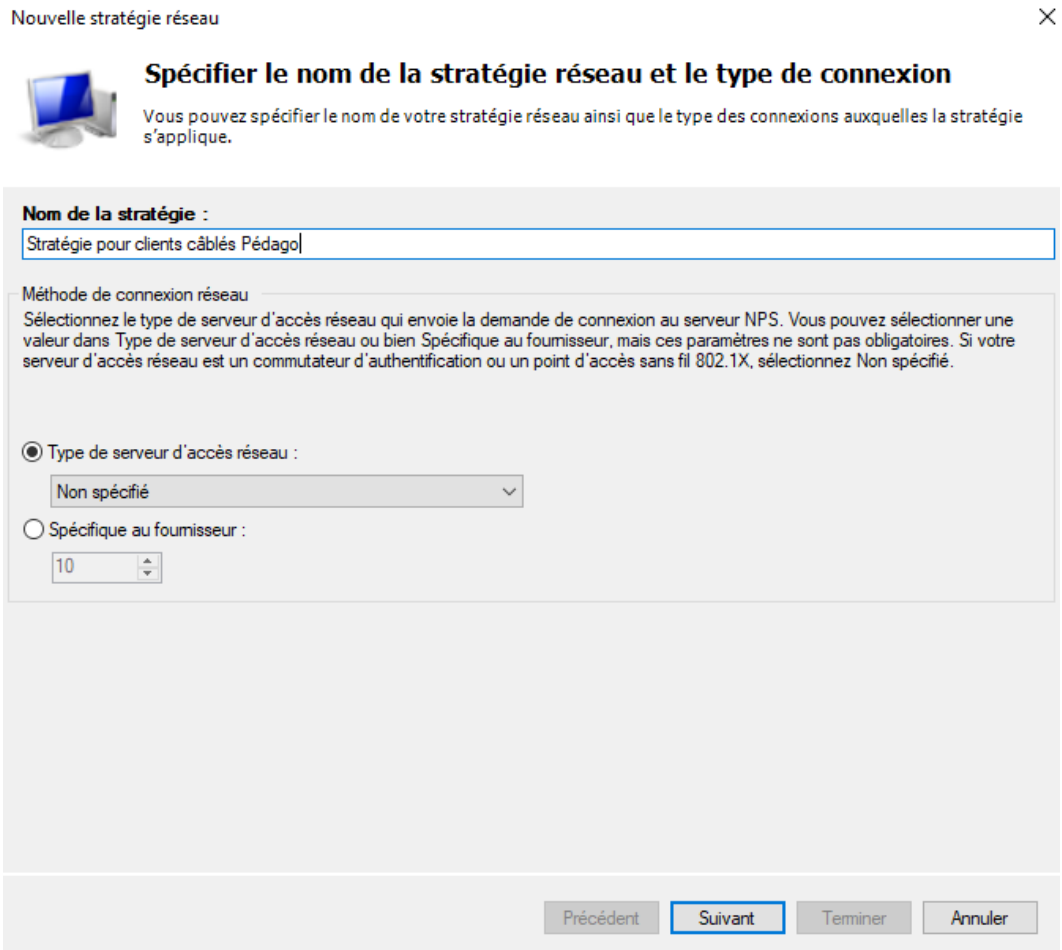




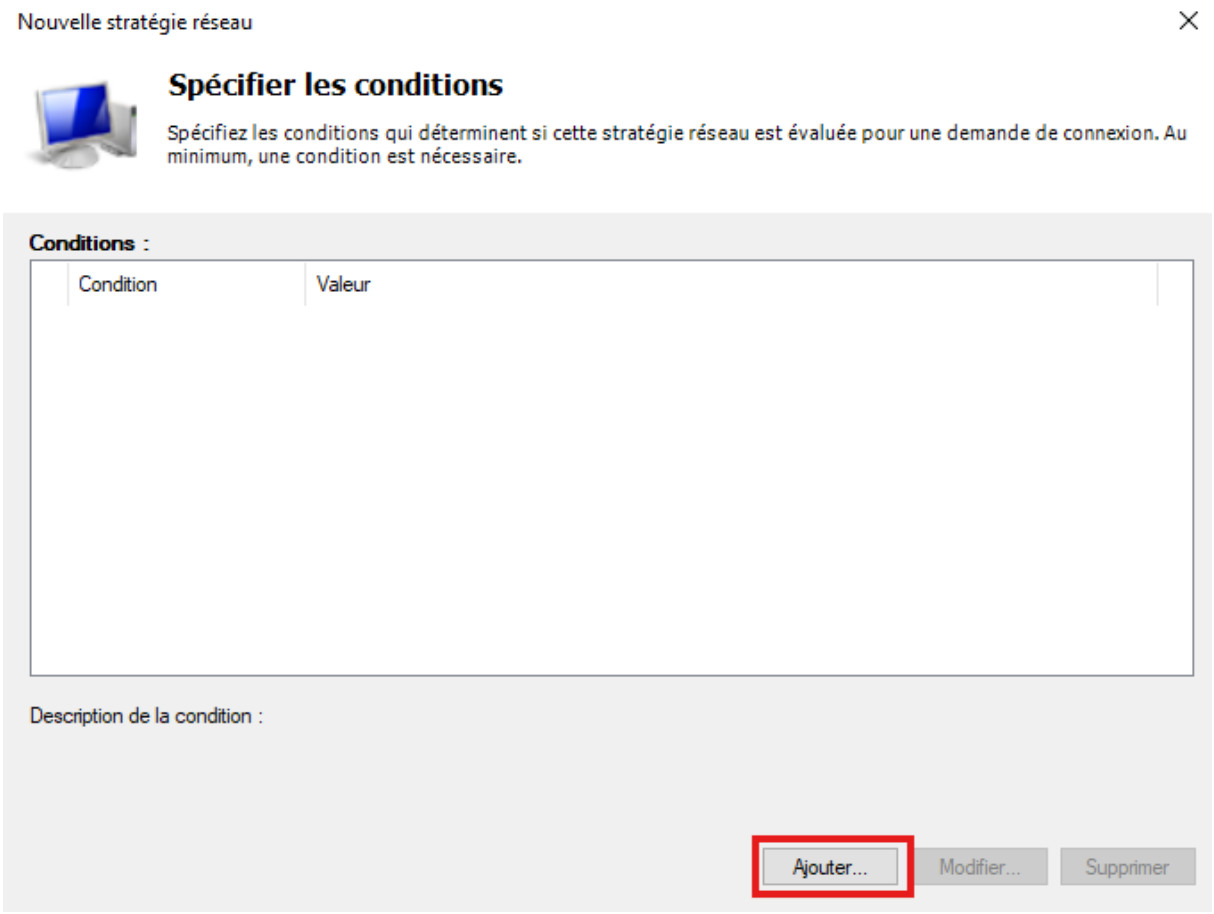
Déclaration d'une stratégie d'accès au réseau :

- Je clic droit sur l'entrée Stratégie Réseau et Je sélectionne Nouveau. Je spécifie le nom de la stratégie (celle pour les membres du groupe Prof). Je reste sur un type de serveur d'accès réseau non spécifié car s'agit d'une authentification via un commutateur 802.1x :

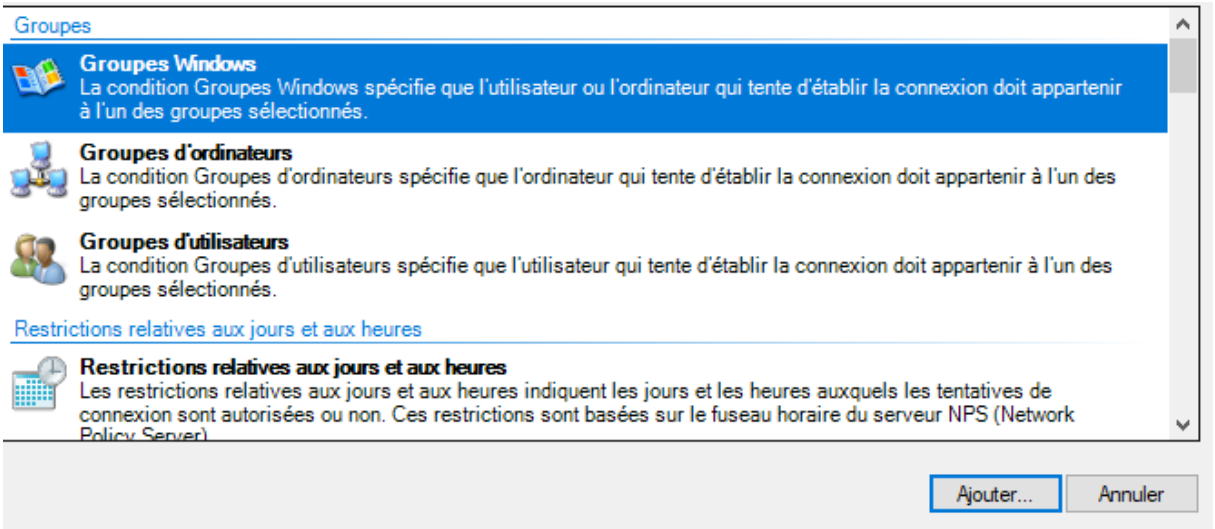




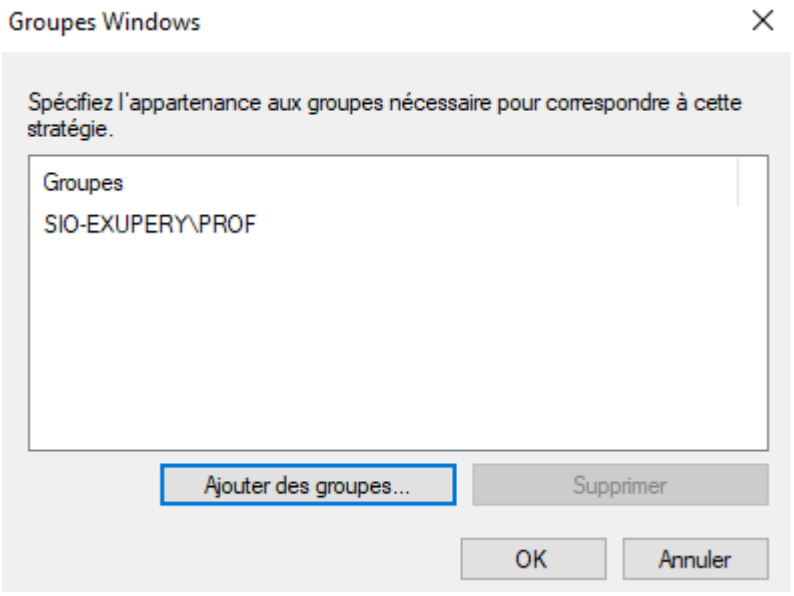
- Je clique sur Ajouter pour spécifier une condition :



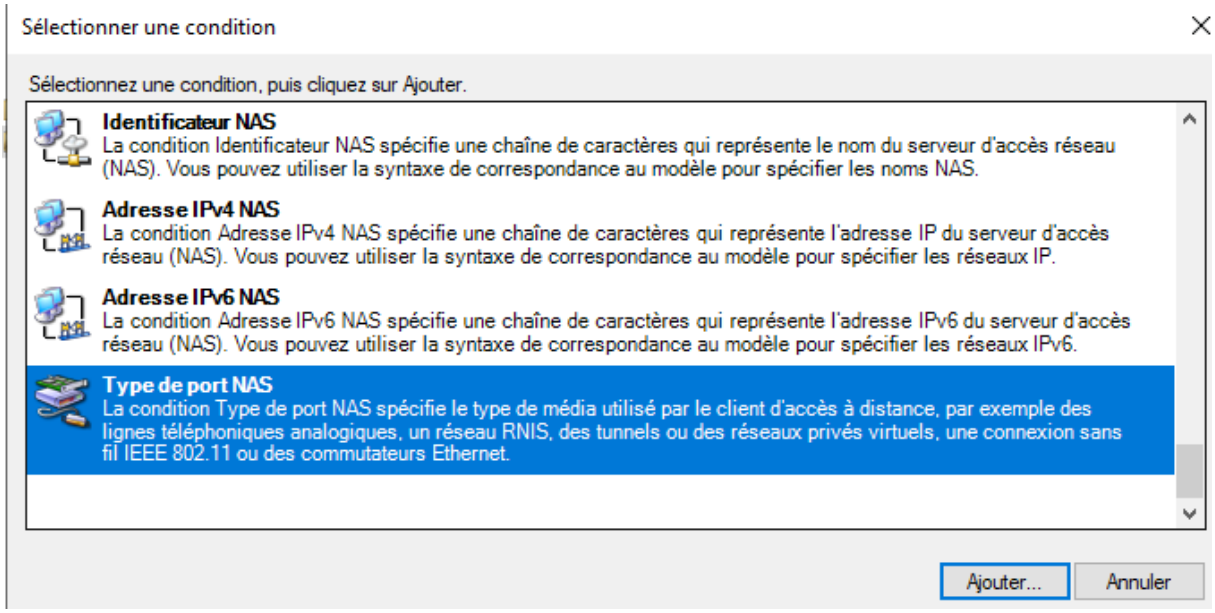
- Dans l'écran Sélectionner une condition, je choisi Groupe Windows et je clique sur Ajouter :



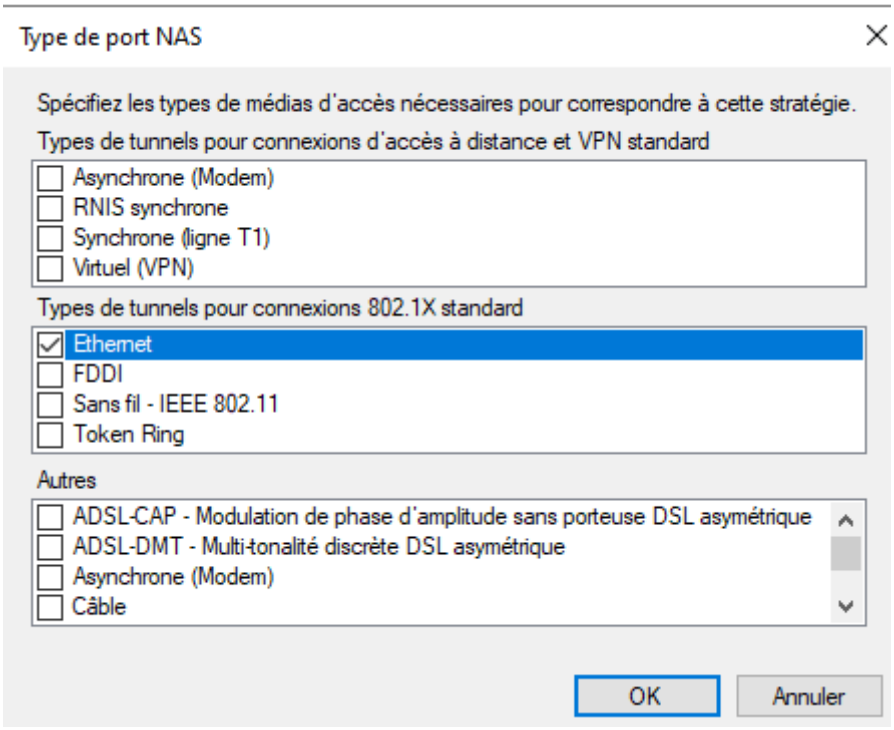
- J’ajoute le groupe Prof :



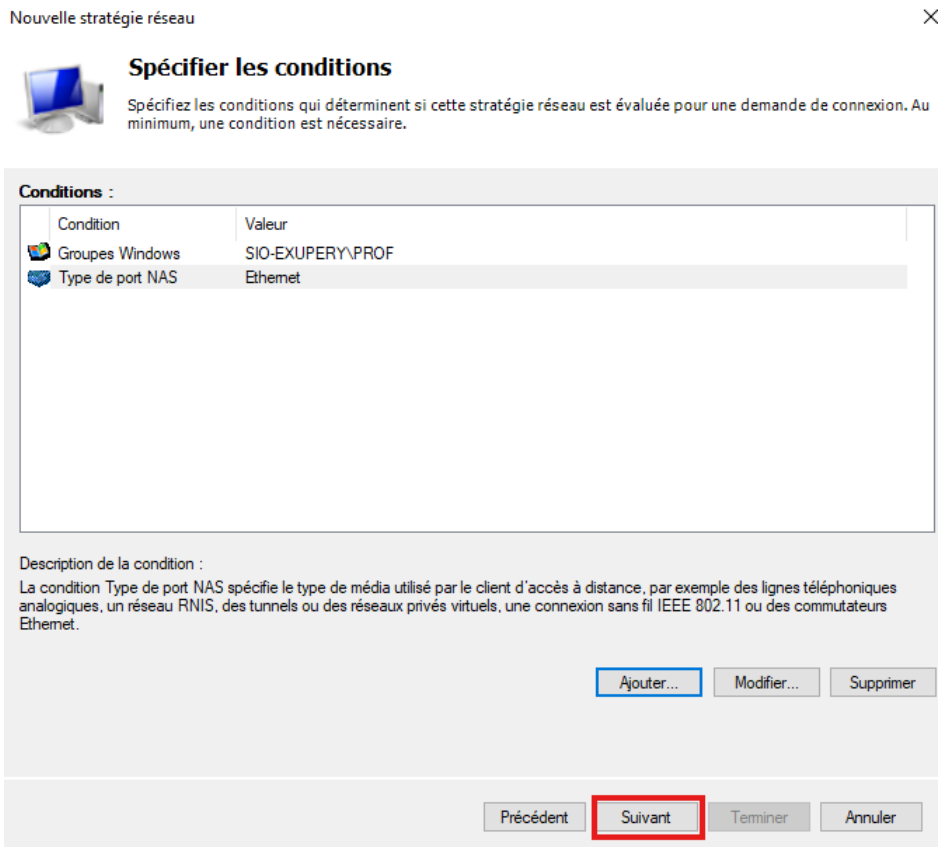
- J’ajoute une deuxième condition pour spécifier le type de port NAS :



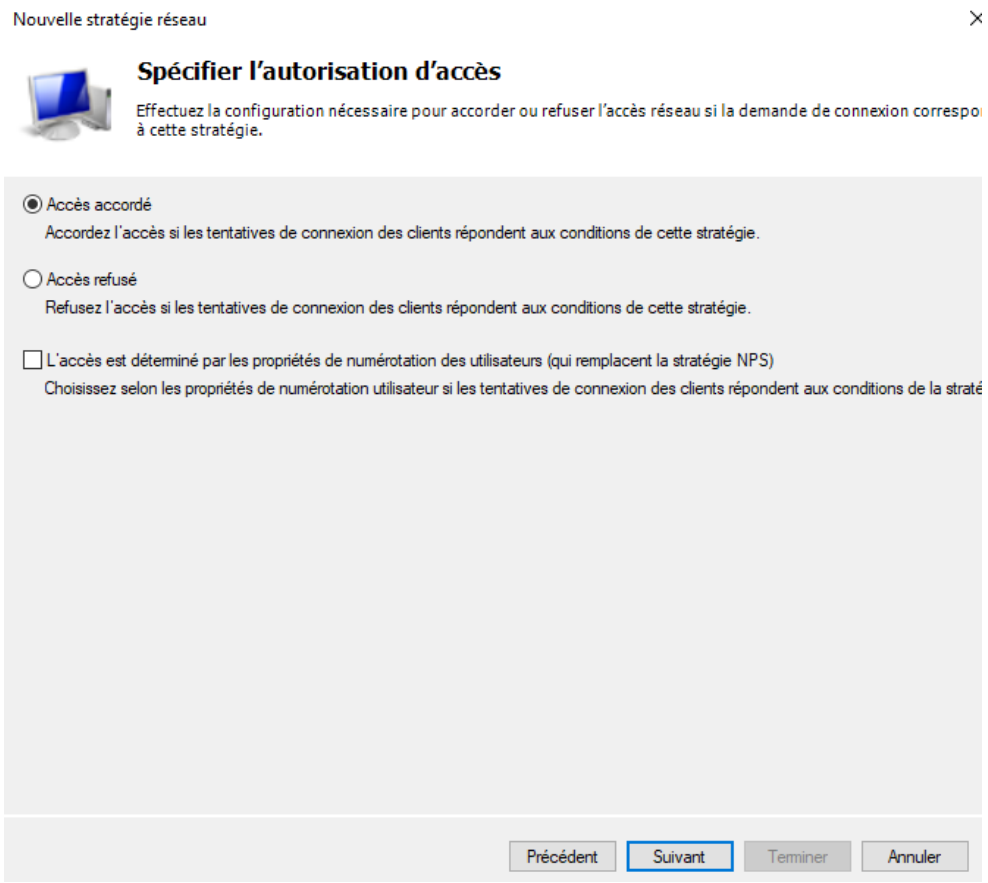
- Je coche Ethernet :



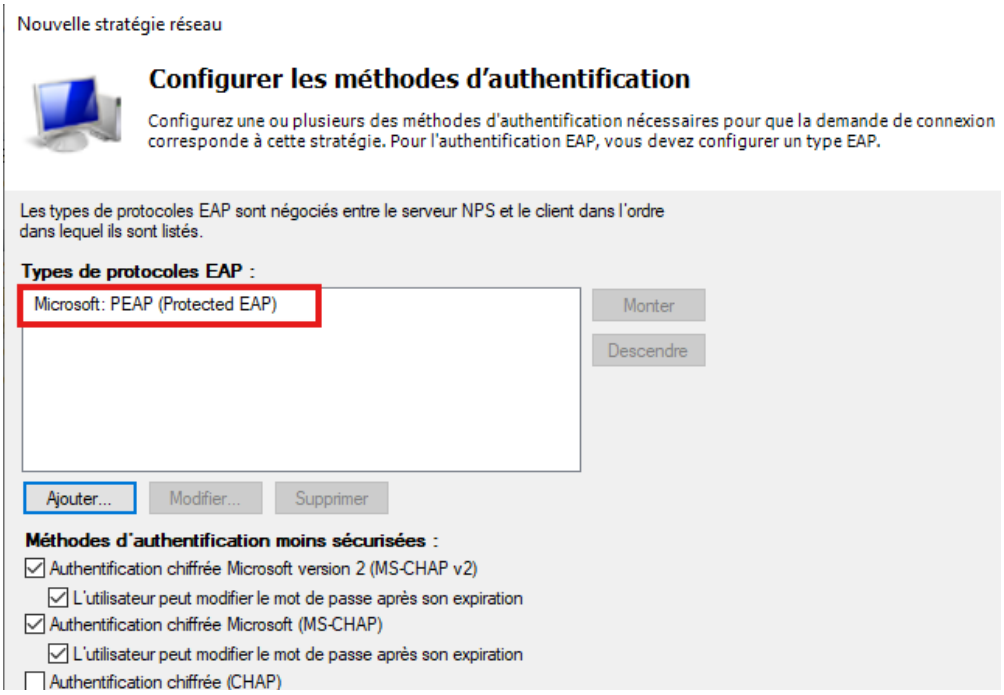
- Je clique sur Suivant :



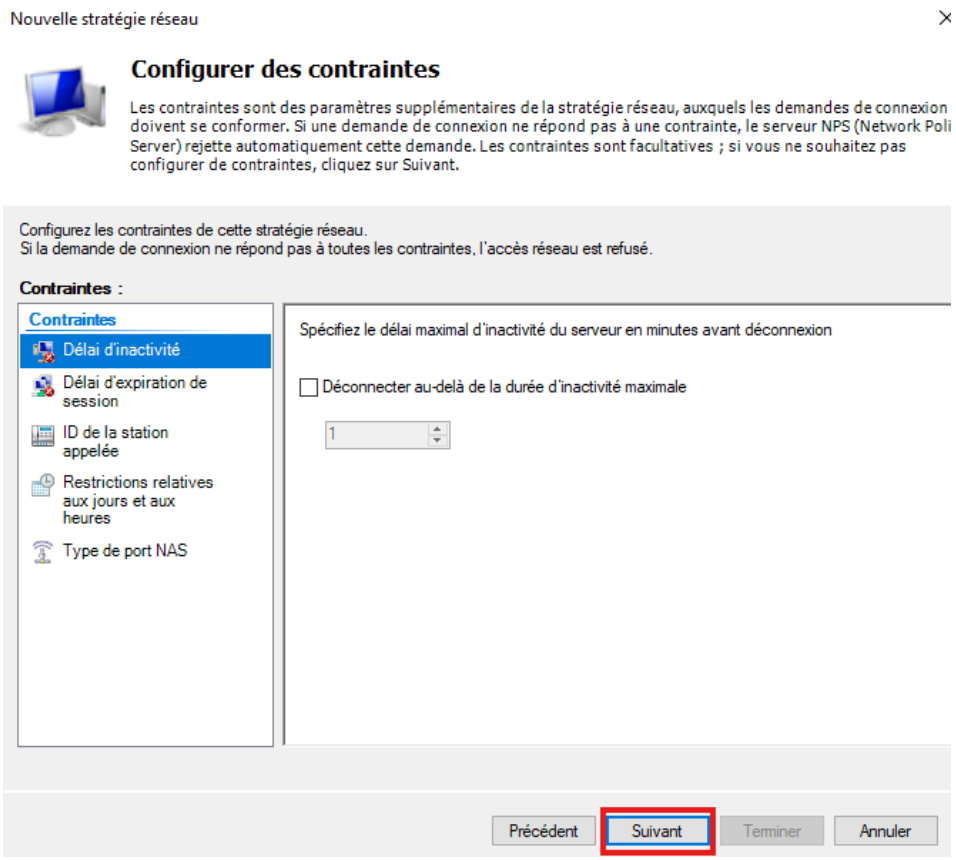
- J’accorde l’accès pour les membres de ce groupe :



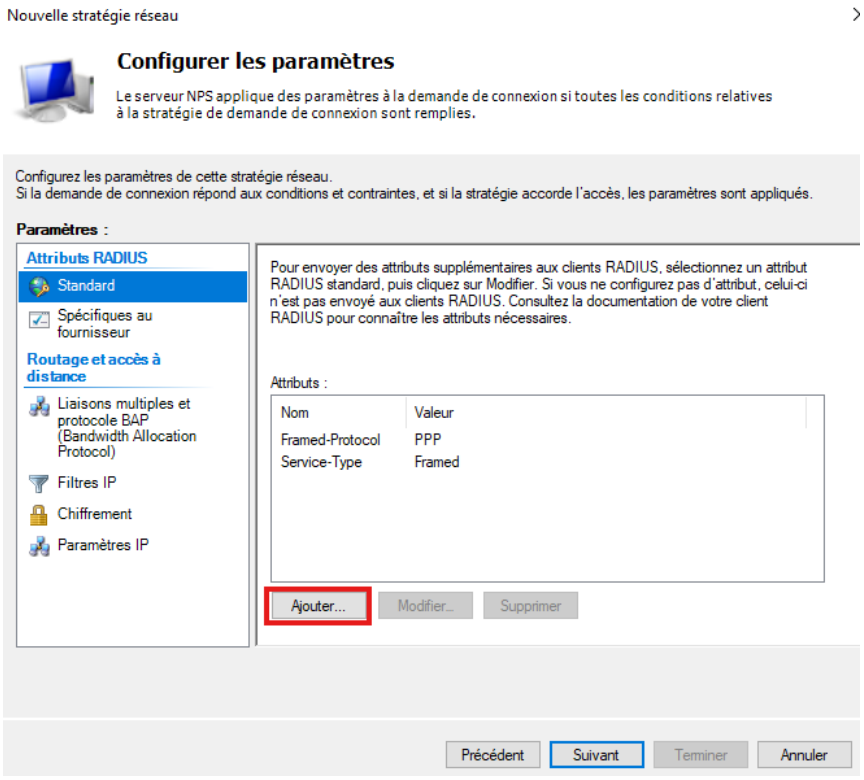
- Dans l’écran Configurer les méthodes d’authentification, Je déclare le type de protocoles EAP (PEAP) en cliquant sur Ajouter :



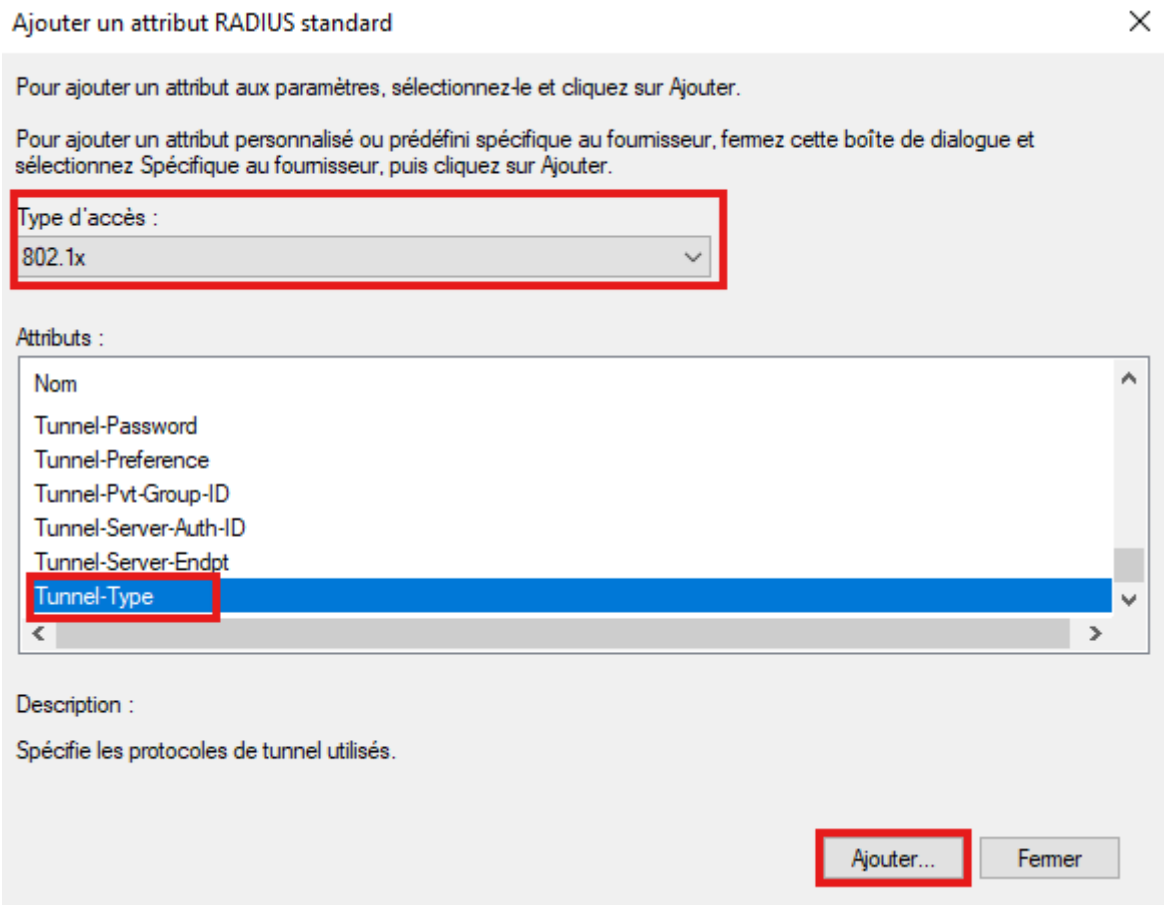
- Dans l'écran Configurer des contraintes, je clique sur Suivant :



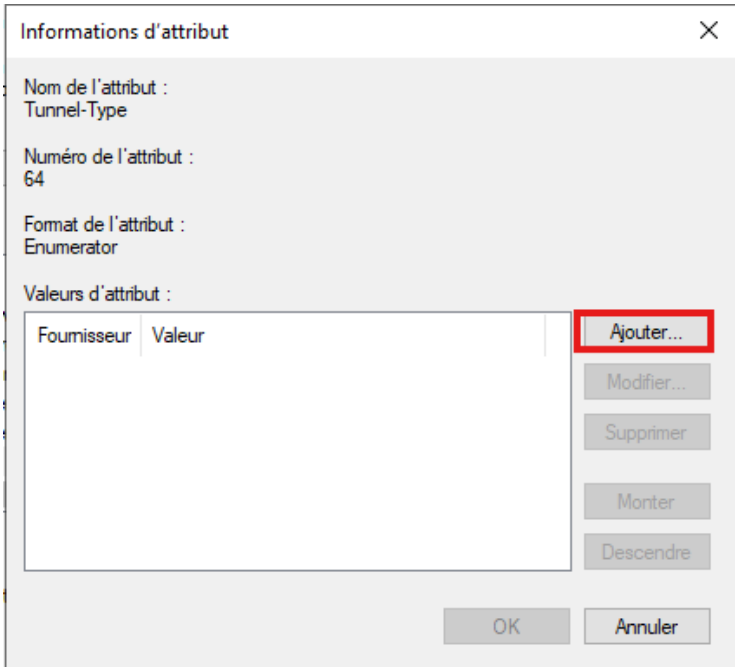
- Dans l'écran Configurer les paramètres, je clique sur Ajouter pour envoyer des attributs au client RADIUS :



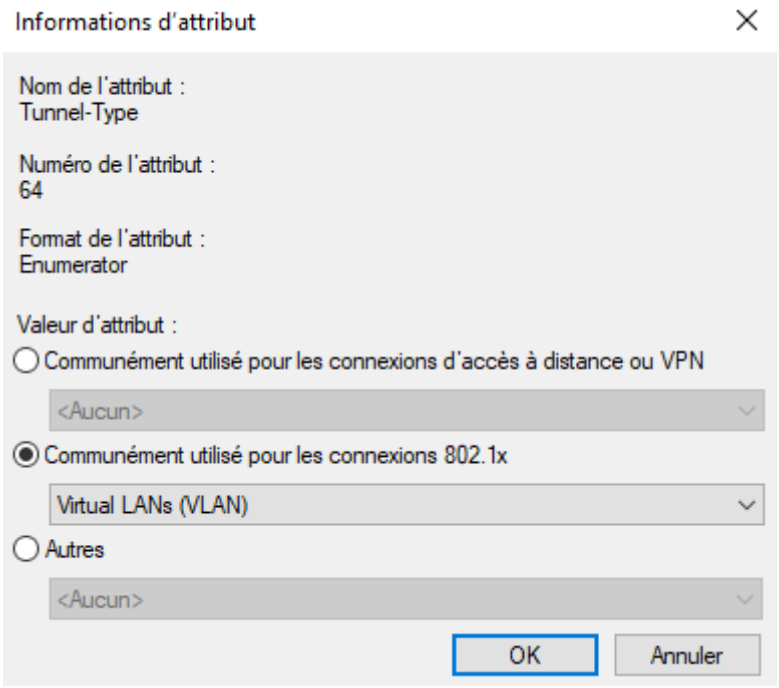
- Je sélectionne 802.1x dans Type d'accès puis je sélectionne l'attribut Tunnel-Type et je clique sur Ajouter :



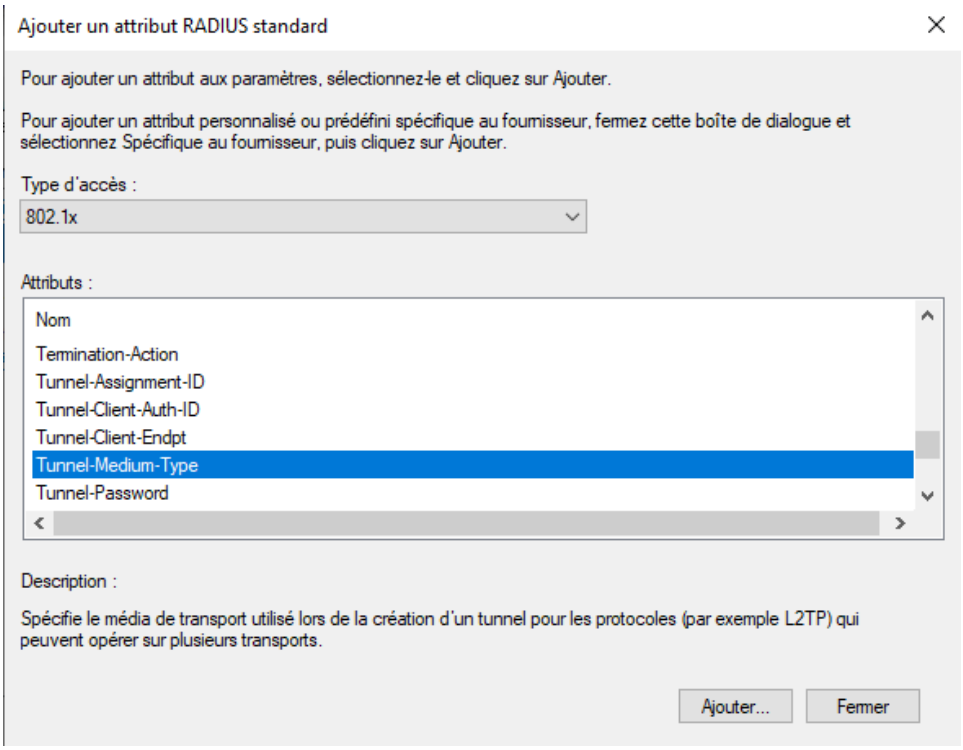
- Je clique sur Ajouter :



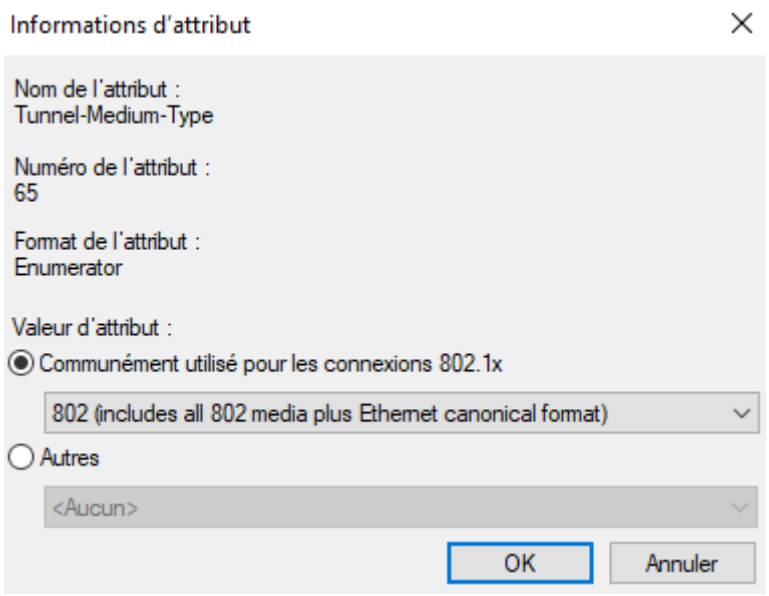
- Je sélectionne Virtual LANs (VLAN) dans Communément utilisé pour les connexions 802.1x :



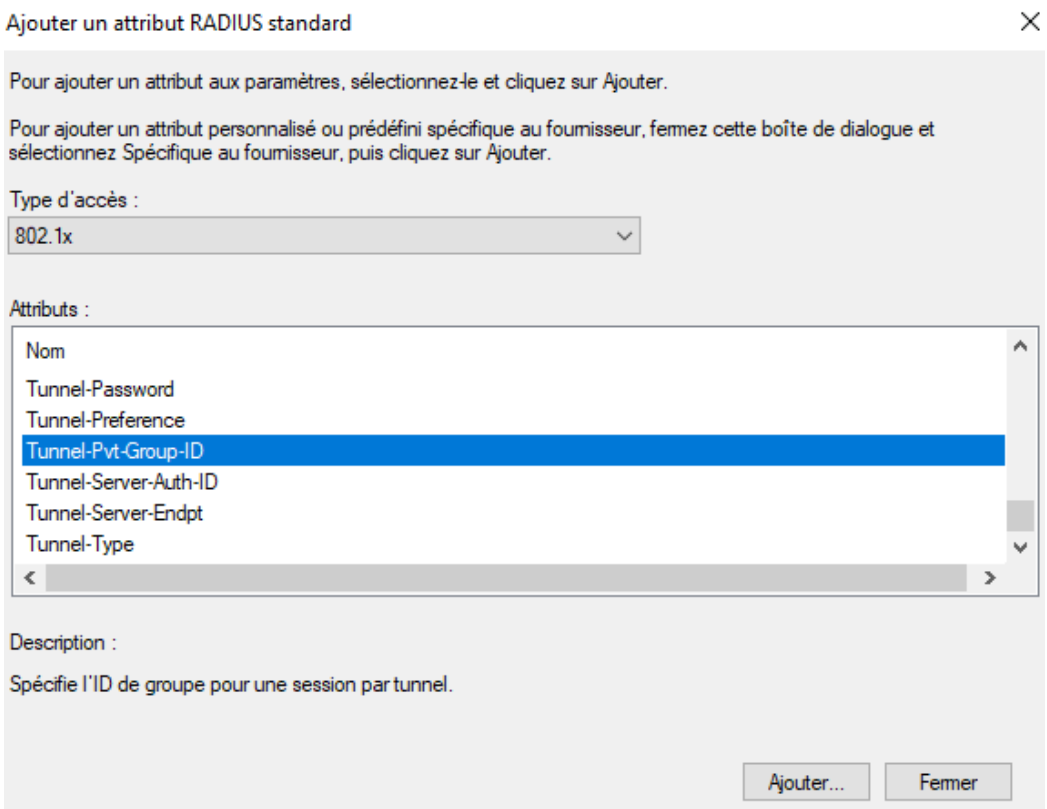
- Je procède de la même façon pour ajouter l'attribut Tunnel-Medium-Type :



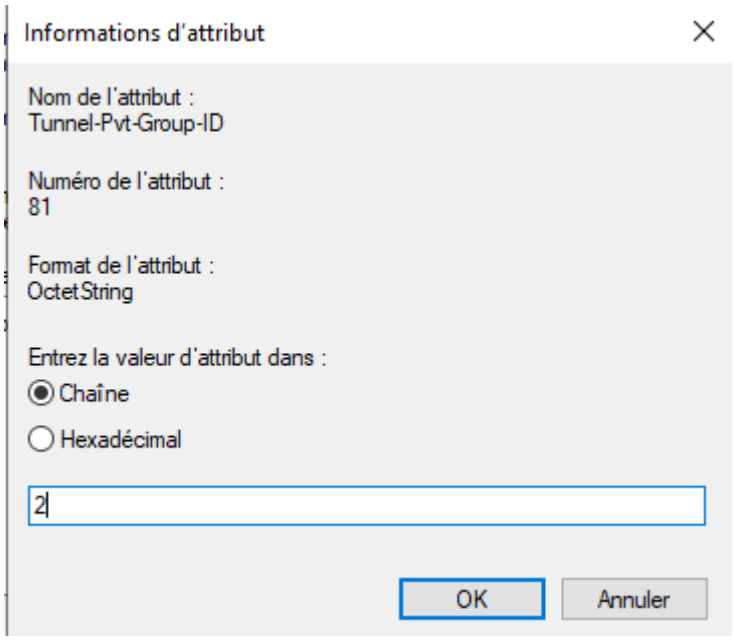
- Je sélectionne 802 (includes…) :



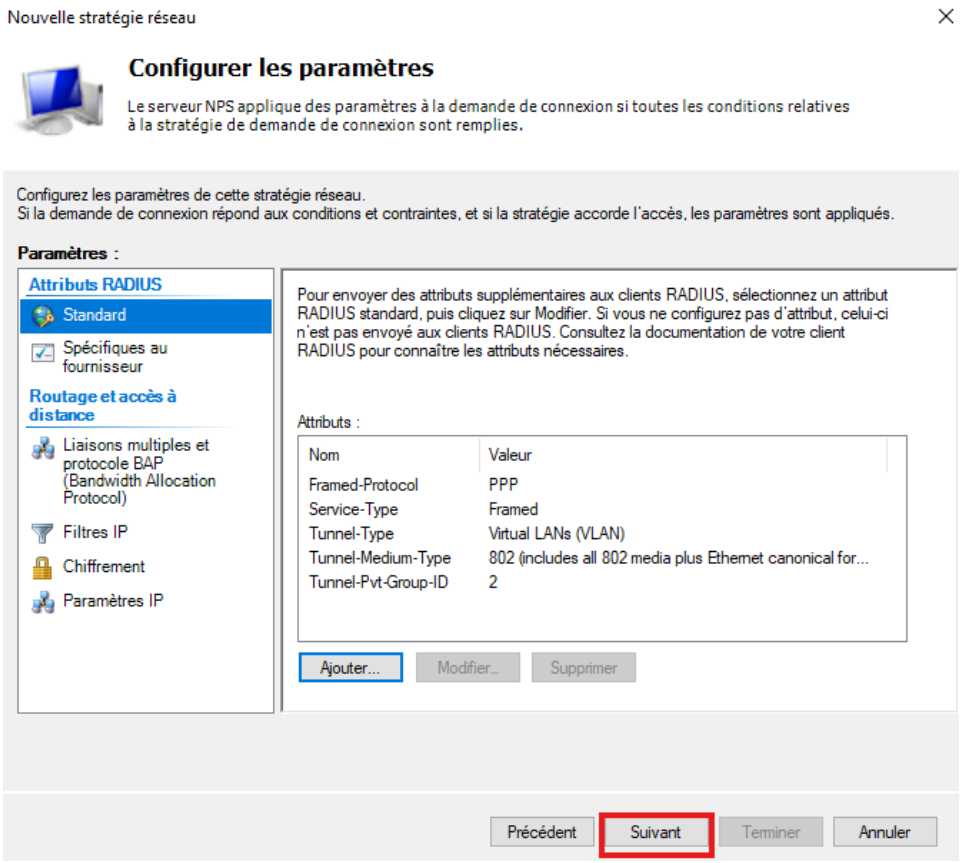
- Enfin, j'ajoute l'attribut Tunnel-Pvt-Group-ID :



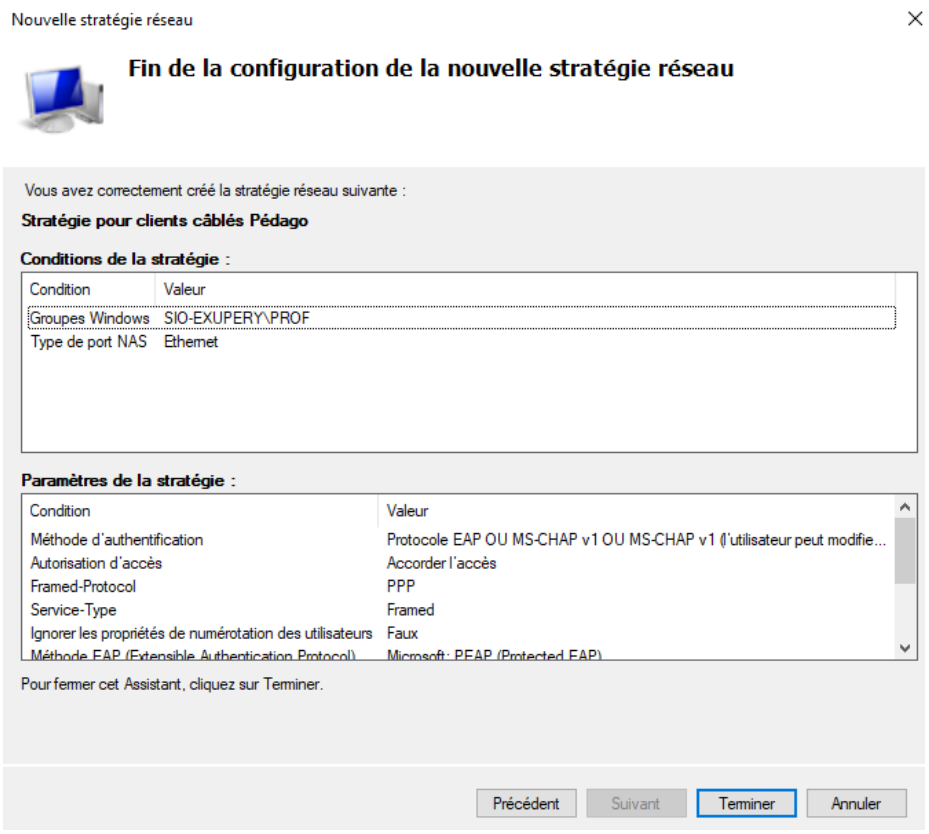
- Je spécifie le numéro de VLAN dans lequel on veut positionner les membres du groupe Prof :



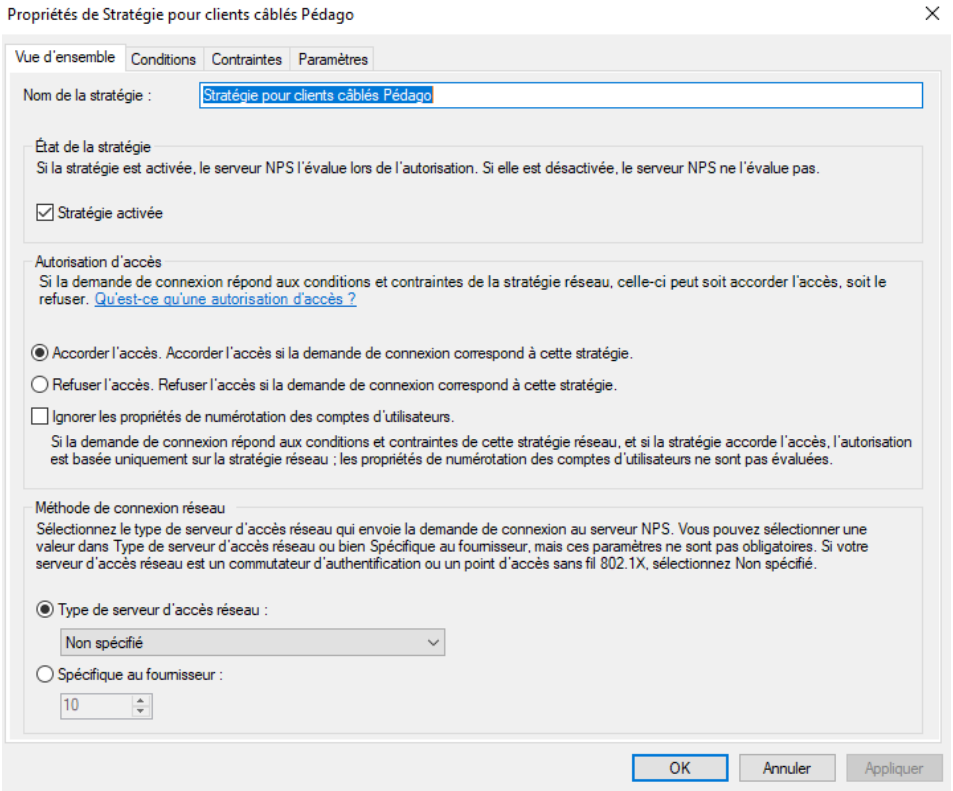
- Je clique sur Fermer dans l'écran Ajouter un attribut RADIUS standard puis sur Suivant dans l'écran récapitulatif des attributs :

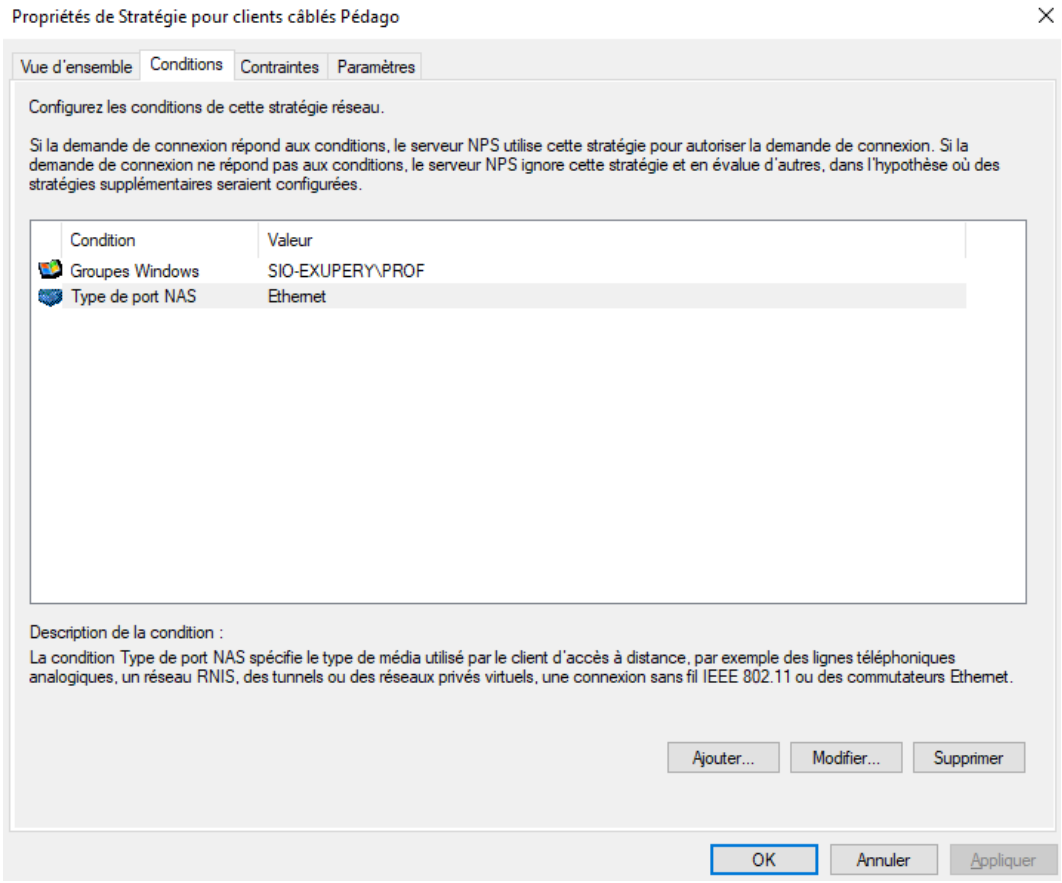


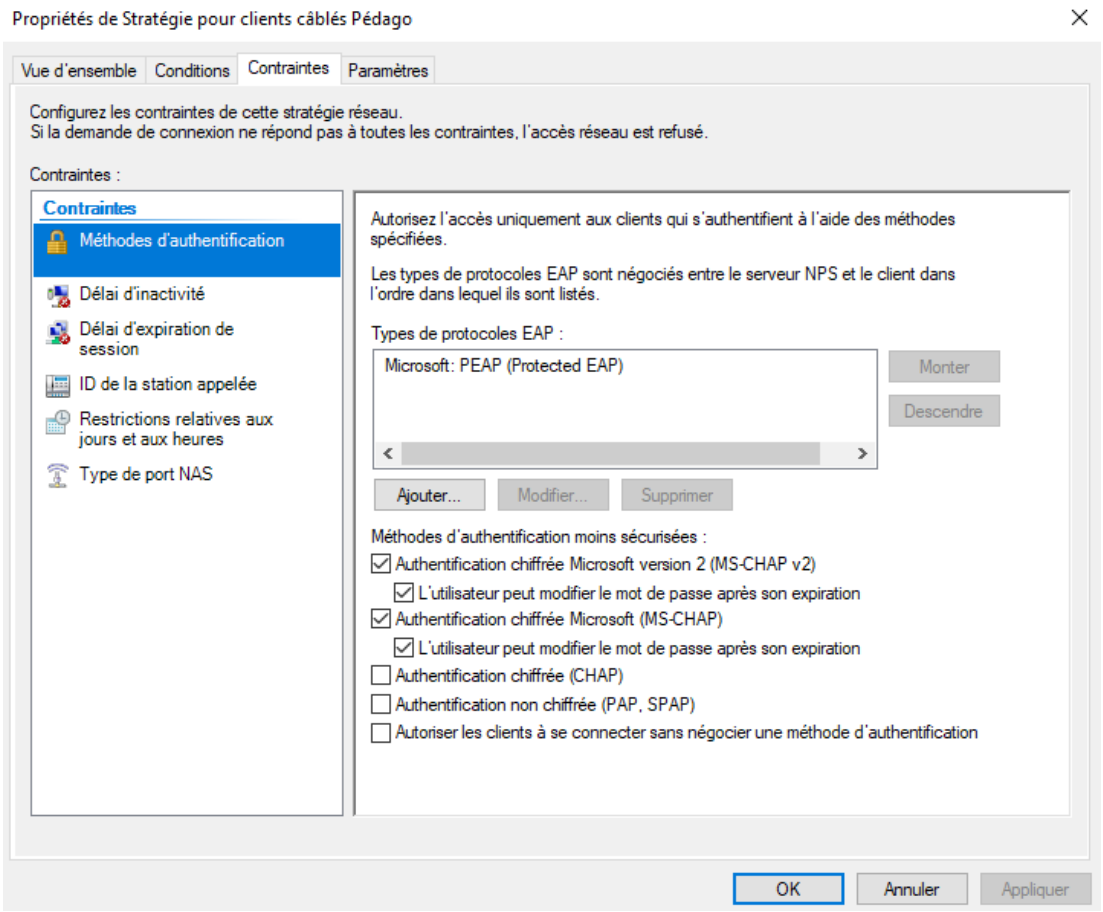
- Je clique sur Terminer dans l'écran Fin de la configuration de la nouvelle stratégie réseau :

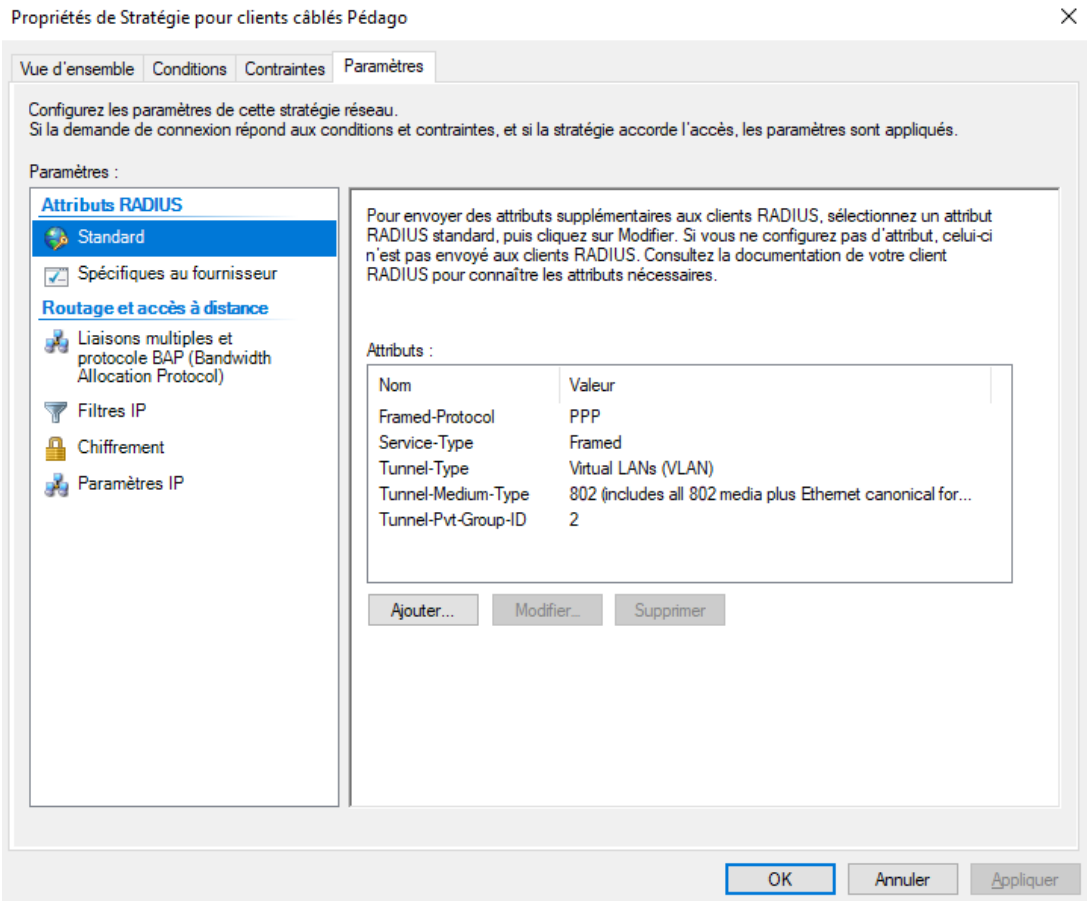


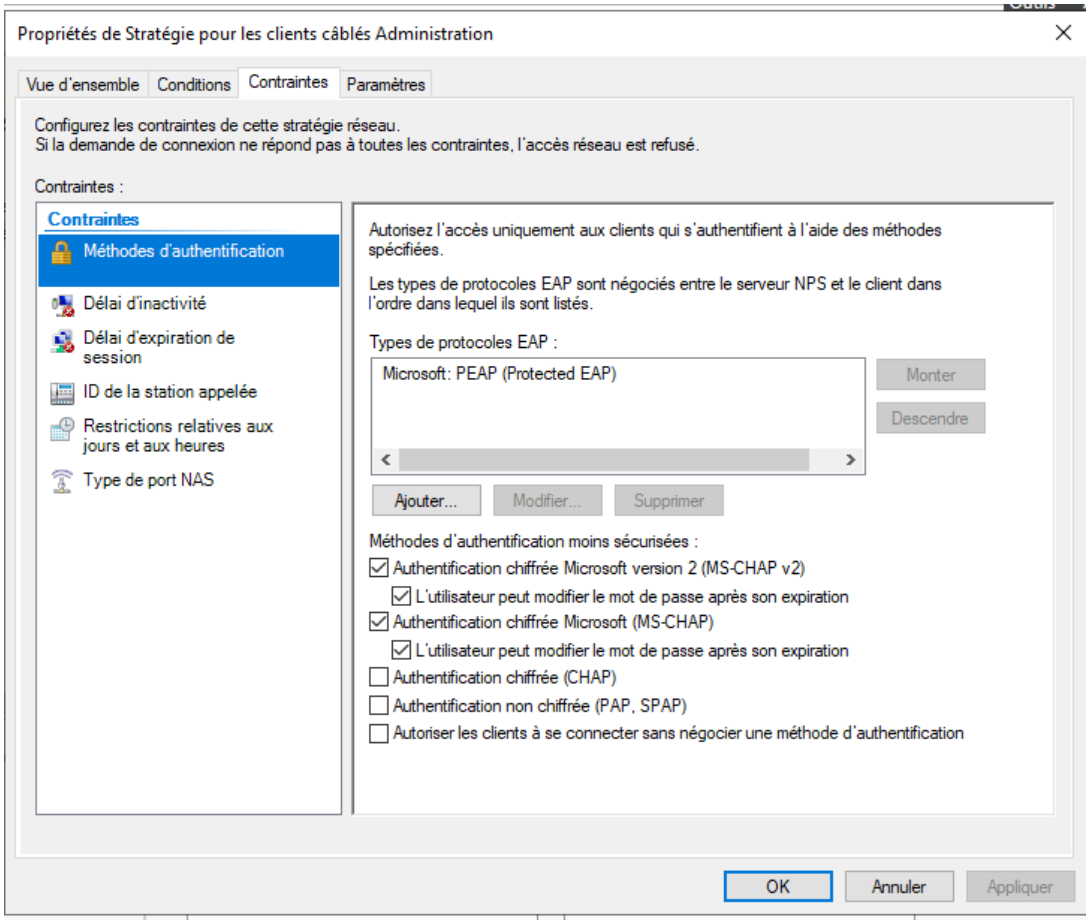
- Je peux cliquer droit sur la stratégie réseau et revoir ou modifier ses propriétés au travers des 4 onglets :



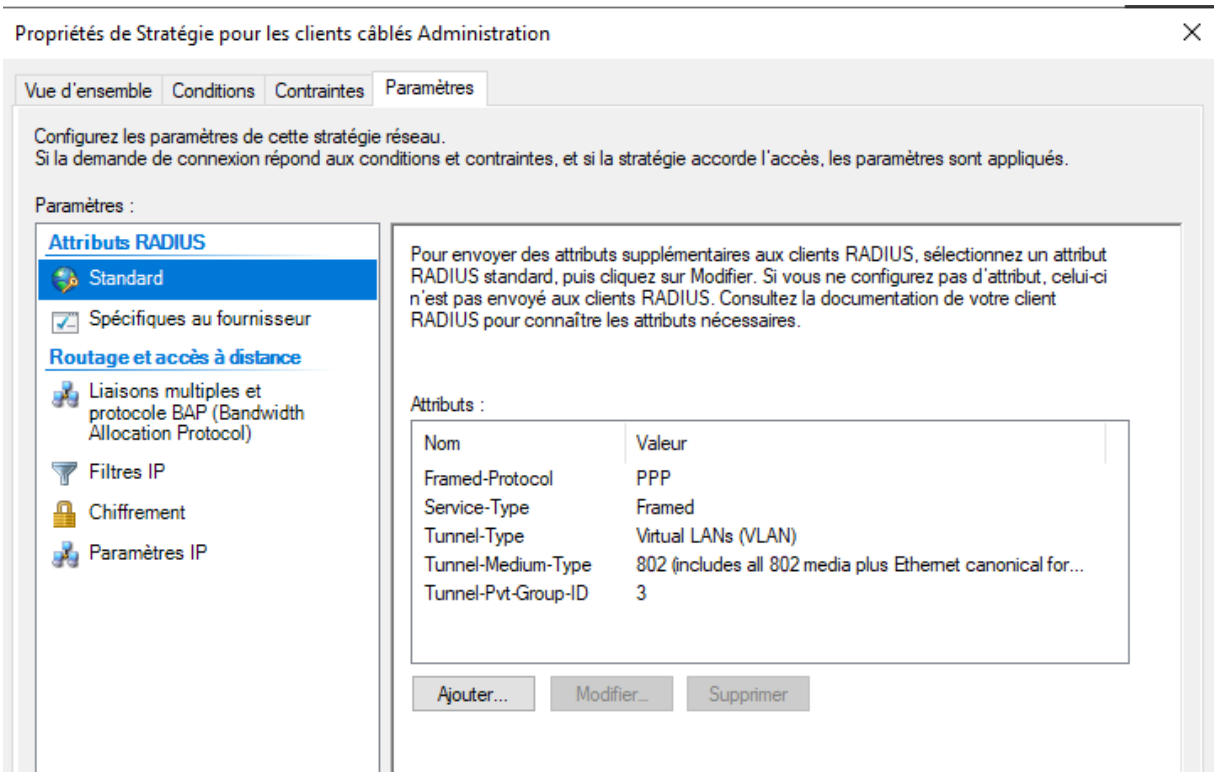

Propriétés de Stratégie pour clients câblés Pédago
Vue d'ensemble
Conditions
Contraintes
Paramètres
Configurez les conditions de cette stratégie réseau.
Si la demande de connexion répond aux conditions, le serveur NPS utilise cette stratégie pour autoriser la demande de connexion. Si la demande de connexion ne répond pas aux conditions, le serveur NPS ignore cette stratégie et en évalue d'autres, dans l'hypothèse où des stratégies supplémentaires seraient configurées.
Condition
Valeur
Groupes Windows
SIO-EXUPERY\PROF
Type de port NAS
Ethernet
Description de la condition :
La condition Type de port NAS spécifie le type de média utilisé par le client d'accès à distance, par exemple des lignes téléphoniques analogiques, un réseau RNIS, des tunnels ou des réseaux privés virtuels, une connexion sans fil IEEE 802.11 ou des commutateurs Ethernet.
Ajouter...
Modifier...
Supprimer
OK
Annuler
Appliquer


Propriétés de Stratégie pour clients câblés 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 clients câblés 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

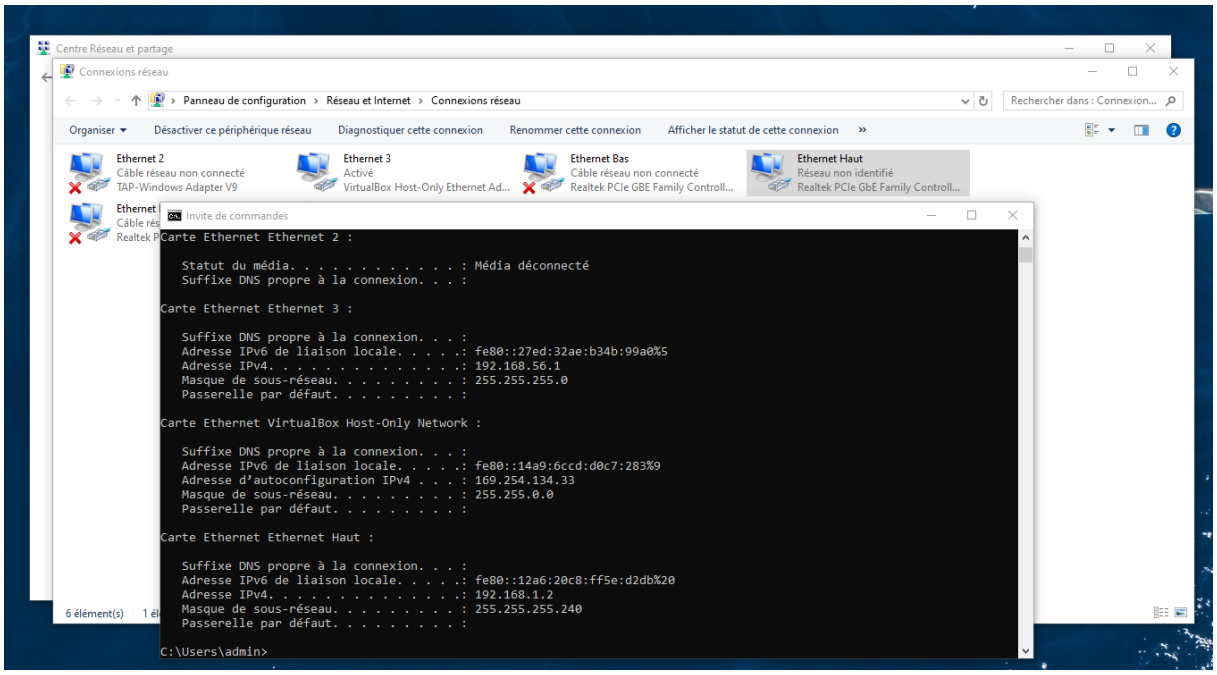

Propriétés de Stratégie pour les clients câblés Administration
Vue d'ensemble
Conditions
Contraintes
Paramètres
Configurez les contraintes de cette stratégie réseau.
Si la demande de connexion ne répond pas à toutes les contraintes, l'accès réseau est refusé.
Contraintes :
Contraintes
Méthodes d'authentification
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

- Je défini de manière analogue une stratégie d'accès réseau plaçant dans le VLAN3 les membres authentifiés comme faisant partie du groupe Direction :

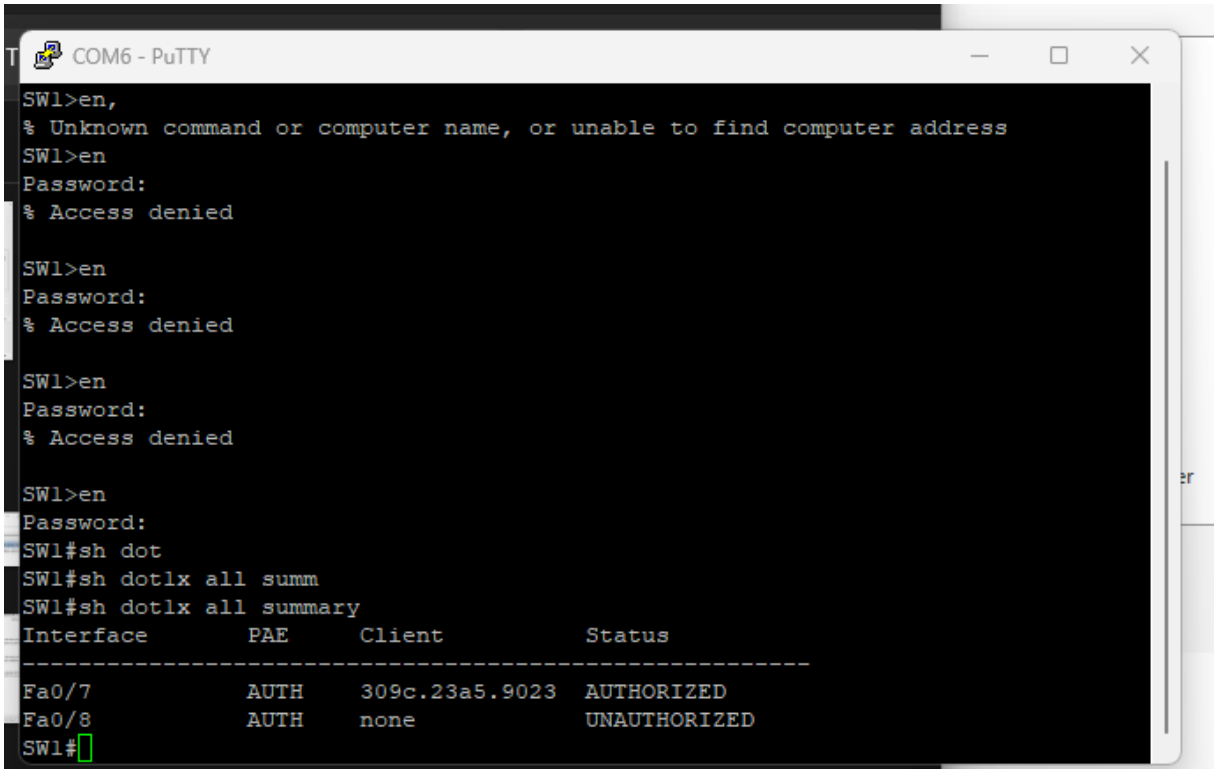


4- Annexe 3 : Demande de connexion des utilisateurs rveau et cgeley :

- PC2 poste hors domaine avec 802.1x activé branché sur le port fa0/7



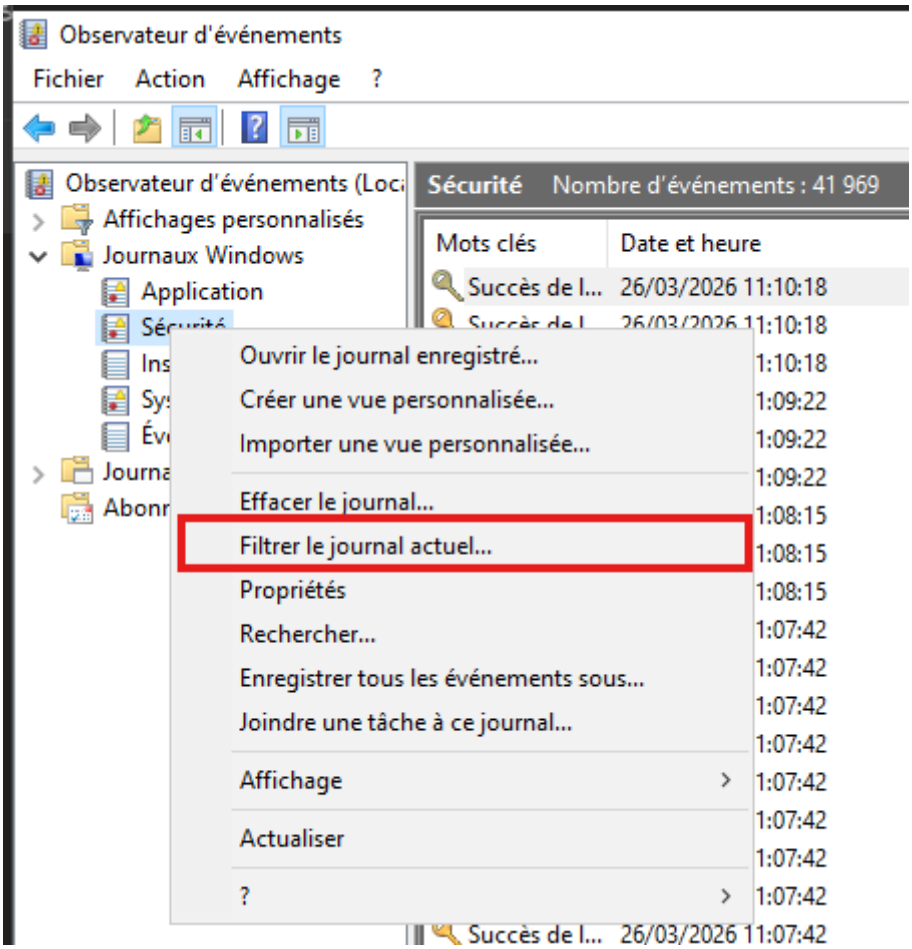
- Commutateur client Radius :

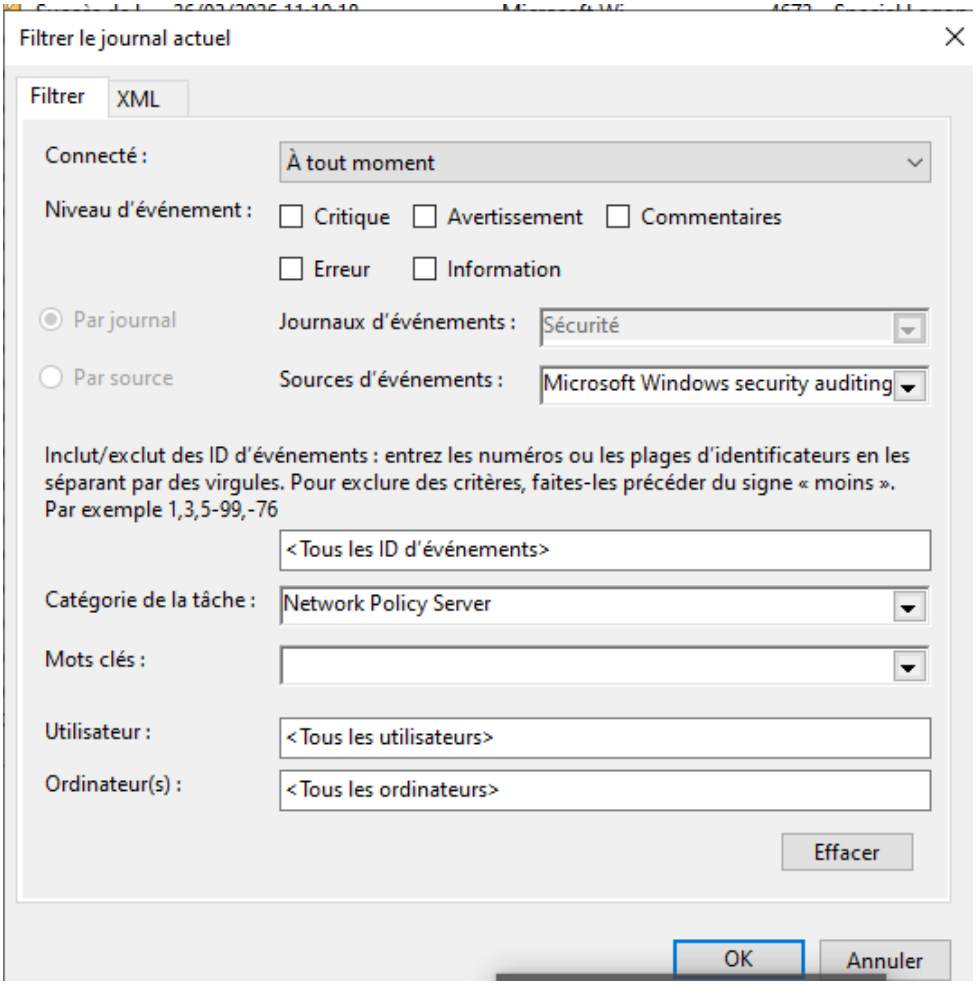


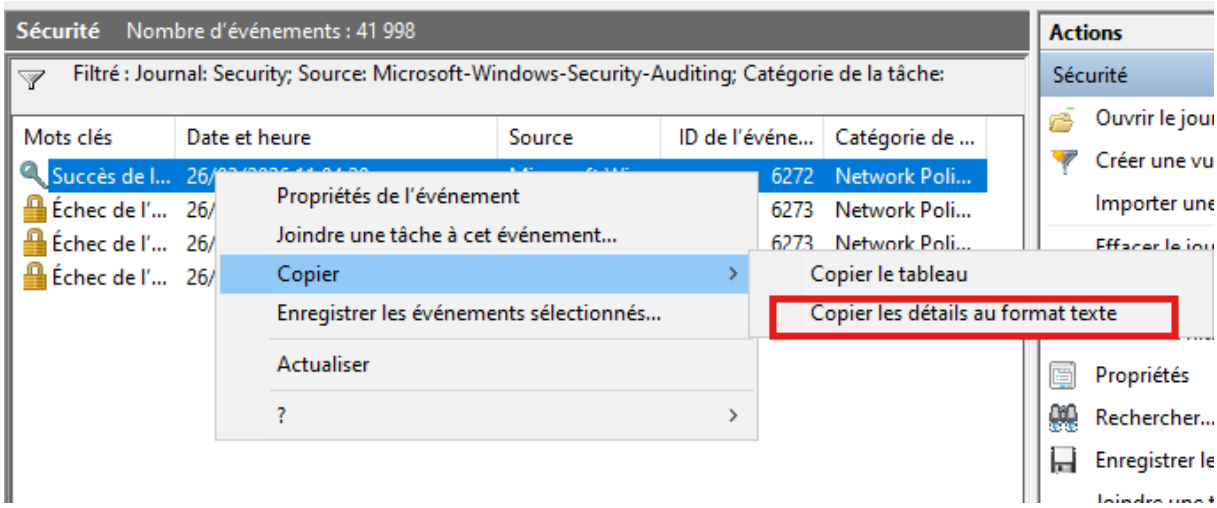
```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                 Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                 Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                 Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                 Fa0/24, Gi0/1, Gi0/2
2    Pedagogie                         active    Fa0/7
3    Administration                    active
4    Serveurs                          active    Fa0/2
99   Guest                             active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
```

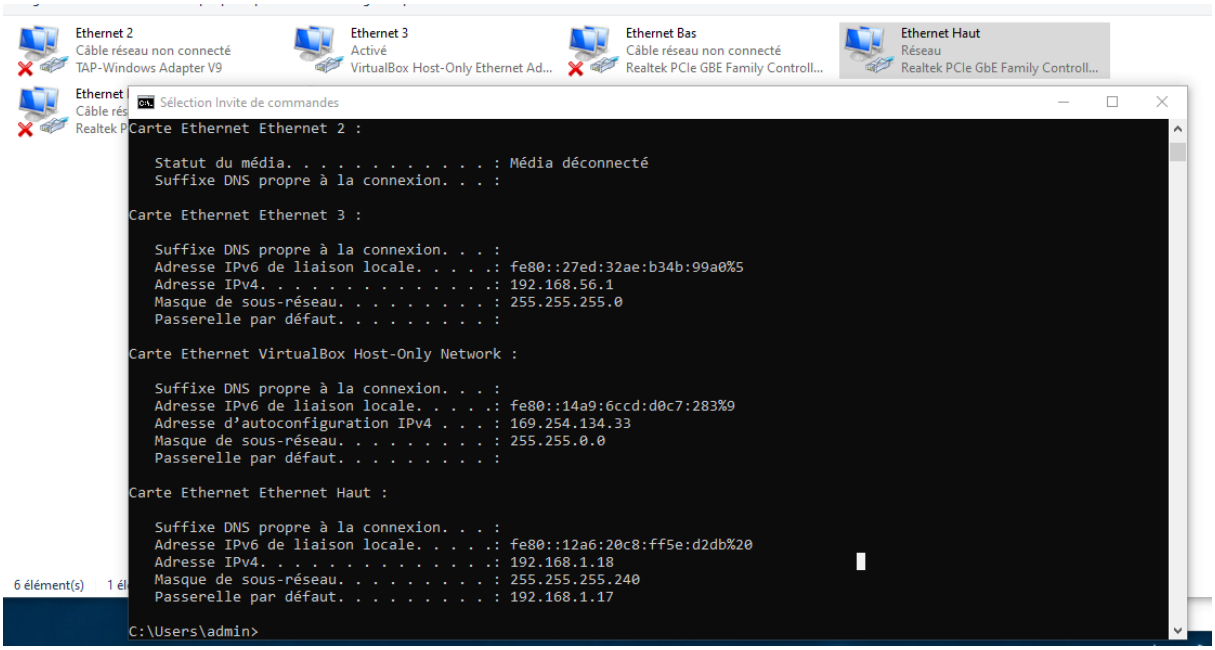
- Exportation XML depuis l'observateur des évènements de Windows 2022 Server :




Filtrer le journal actuel
Filtrer
XML
Connecté :
À tout moment
Niveau d'événement :
Critique
Avertissement
Commentaires
Erreur
Information
Par journal
Journaux d'événements :
Sécurité
Par source
Sources d'événements :
Microsoft Windows security auditing
Inclut/exclut des ID d'événements : entrez les numéros ou les plages d'identificateurs en les séparant par des virgules. Pour exclure des critères, faites-les précéder du signe « moins ». Par exemple 1,3,5-99,-76
<Tous les ID d'événements>
Catégorie de la tâche :
Network Policy Server
Mots clés :
Utilisateur :
<Tous les utilisateurs>
Ordinateur(s) :
<Tous les ordinateurs>
Effacer
OK
Annuler

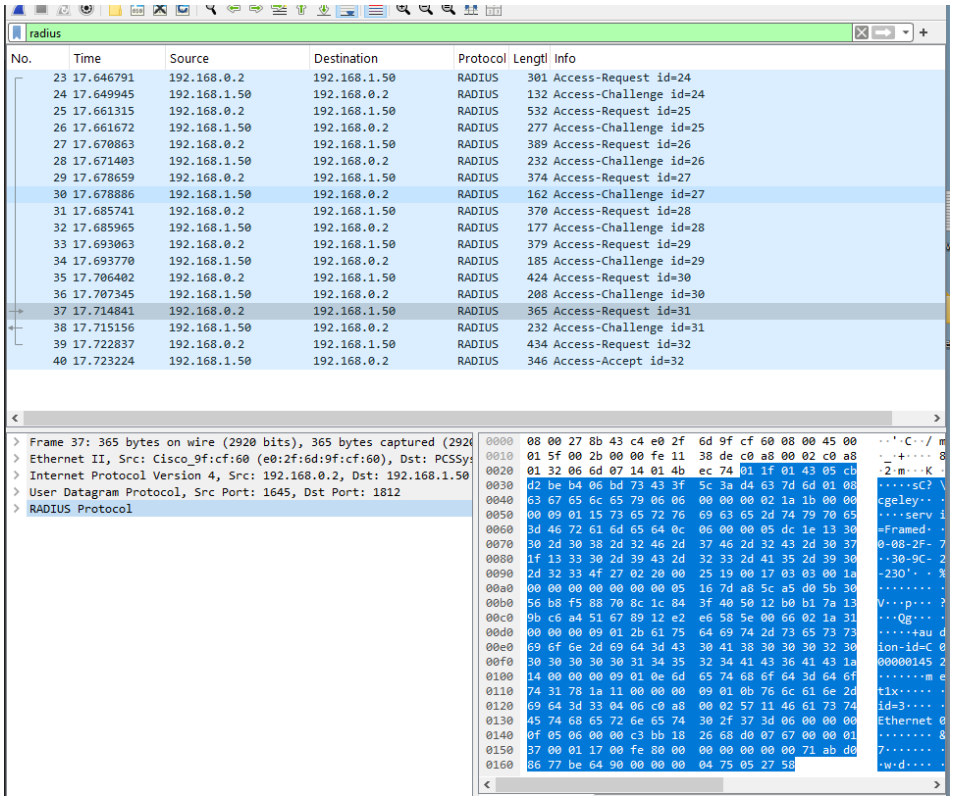

Sécurité
Nombre d'événements : 41 998
Filtré : Journal: Security; Source: Microsoft-Windows-Security-Auditing; Catégorie de la tâche:
Mots clés
Date et heure
Source
ID de l'événe...
Catégorie de ...
Succès de l...
Échec de l'...
6272
6273
Network Poli...
Propriétés de l'événement
Joindre une tâche à cet événement...
Copier
Enregistrer les événements sélectionnés...
Actualiser
?
Copier le tableau
Copier les détails au format texte
Actions
Sécurité
Ouvrir le jou
Créer une vu
Importer une
Propriétés
Rechercher...
Enregistrer le

- PC2 et demande de connexion de l'utilisateur cgeley :



5- Annexe 4 : Capture de trames : messages RADIUS :

- J'installe Wireshark sur le serveur RADIUS et j'effectue une capture des trames RADIUS entre le client RADIUS et le serveur RADIUS :



- Je développe la section RADIUS Protocol, comme ci-dessous, et je constate l'encapsulation RADIUS : lorsque le client RADIUS reçoit un paquet EAP du client final, il l'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 :