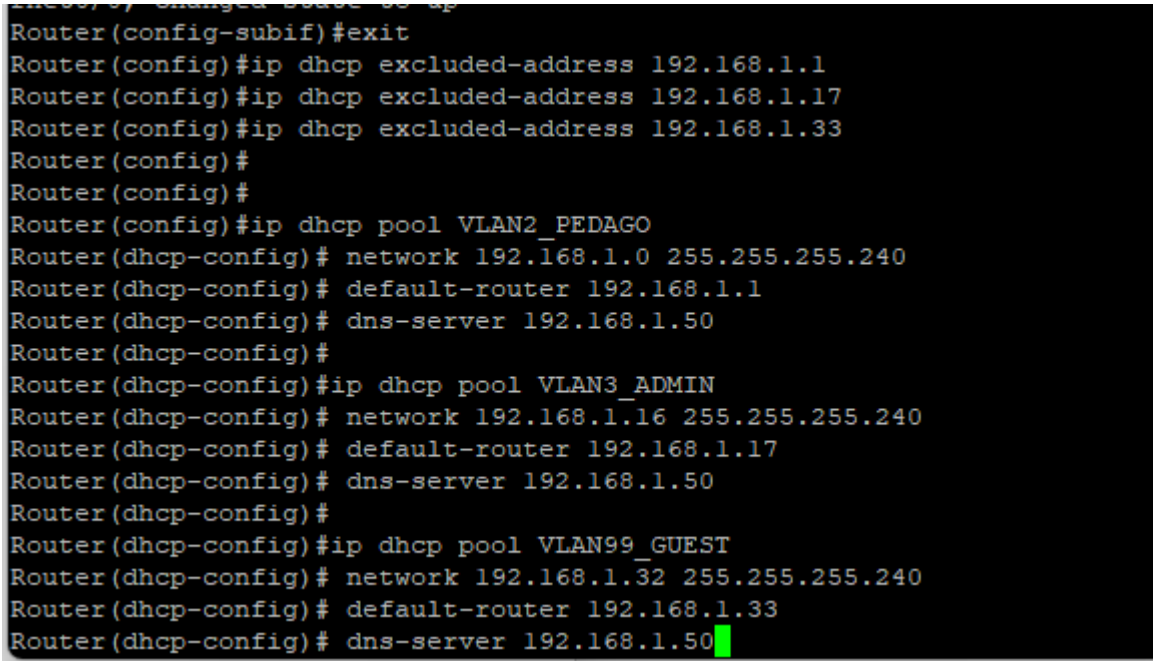
TP1 – Mise en oeuvre d’une infrastructure 802.1x : connexions câblées

Table des matières

Configuration du routeur :

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface G0/0
Router(config-if)# no shutdown
Router(config-if)#
Router(config-if)#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 G0/0.99
Router(config-subif)# encapsulation dot1Q 99
Router(config-subif)# ip address 192.168.1.33 255.255.255.240
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
Mar  5 09:56:05.427: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed sta
 to down
Mar  5 09:56:08.727: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed sta
 to up
Mar  5 09:56:09.727: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEt
rnet0/0, changed state to up
```

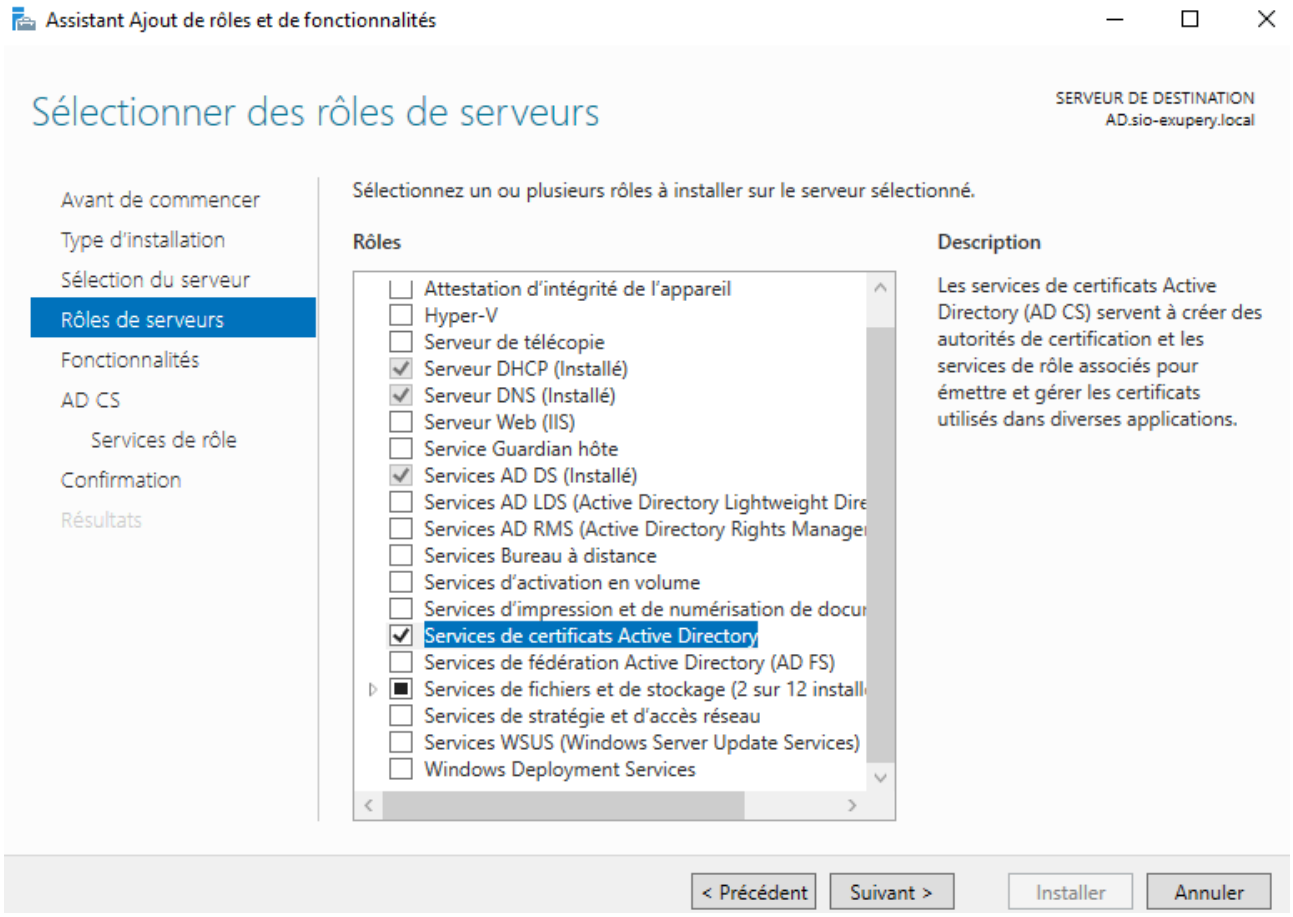


Configuration de base du switch

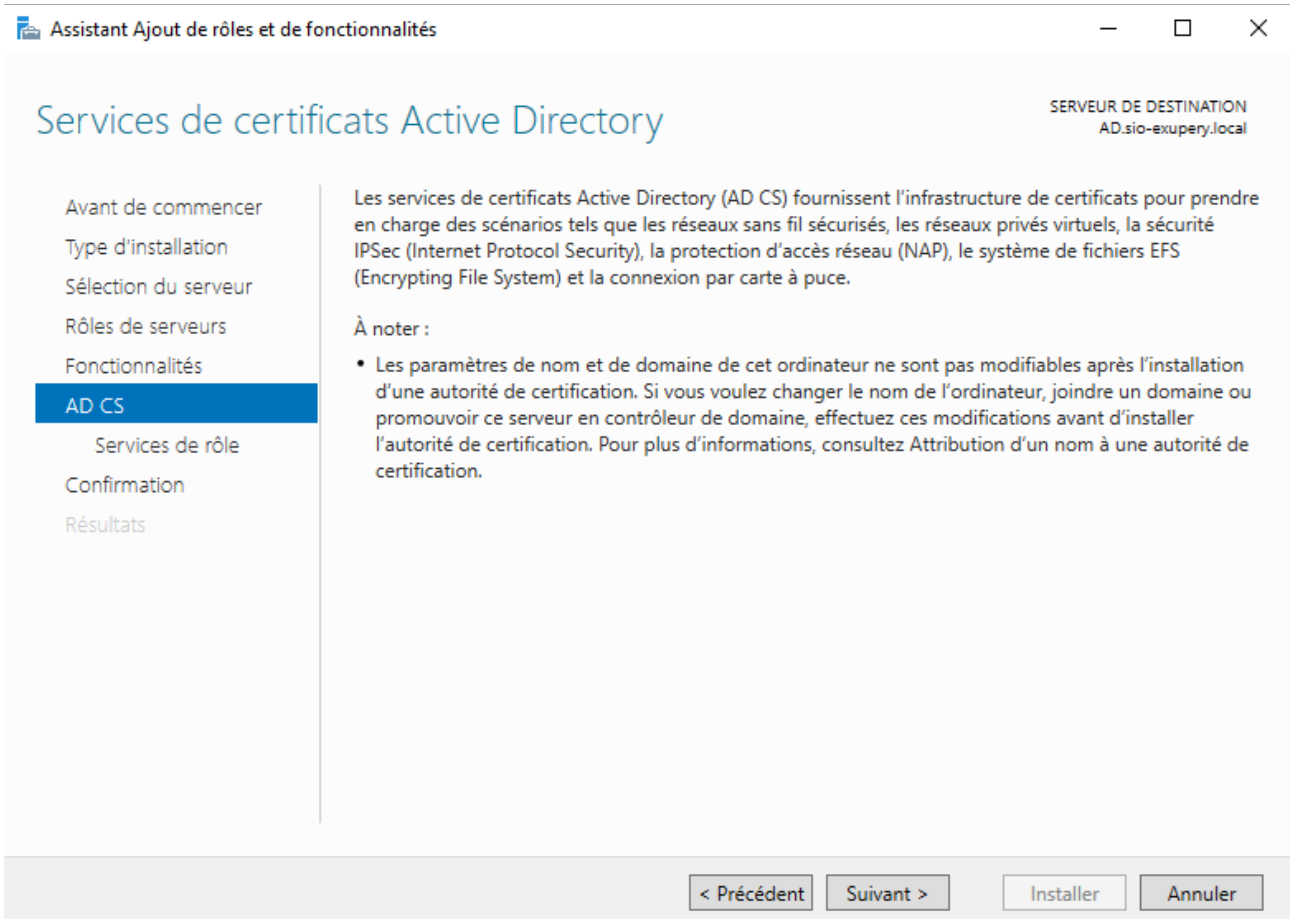
```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 2
Switch(config-vlan)# name Pedagogie
Switch(config-vlan)#vlan 3
Switch(config-vlan)# name Administration
Switch(config-vlan)#vlan 4
Switch(config-vlan)# name Serveurs
Switch(config-vlan)#vlan 99
Switch(config-vlan)# name Gestion
Switch(config-vlan)#
Switch(config-vlan)#
Switch(config-vlan)#interface Fa0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 1,2,3,4,99
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#interface vlan 1
Switch(config-if)# ip address 192.168.0.2 255.255.255.248
Switch(config-if)# no shutdown
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#interface Fa0/2
Switch(config-if)# switchport access vlan 4
Switch(config-if)# switchport mode access
Switch(config-if)#
Switch(config-if)#interface Fa0/19
Switch(config-if)# switchport mode trunk
Switch(config-if)#exit
Switch(config)#exit
Switch#copy run s
*Mar  1 00:25:30.895: %SYS-5-CONFIG_I: Configured from console by consoletart
Destination filename [startup-config]?
Building configuration...
[OK]
Switch#
```

2.2 Ajout du rôle Services de certificats Active Directory

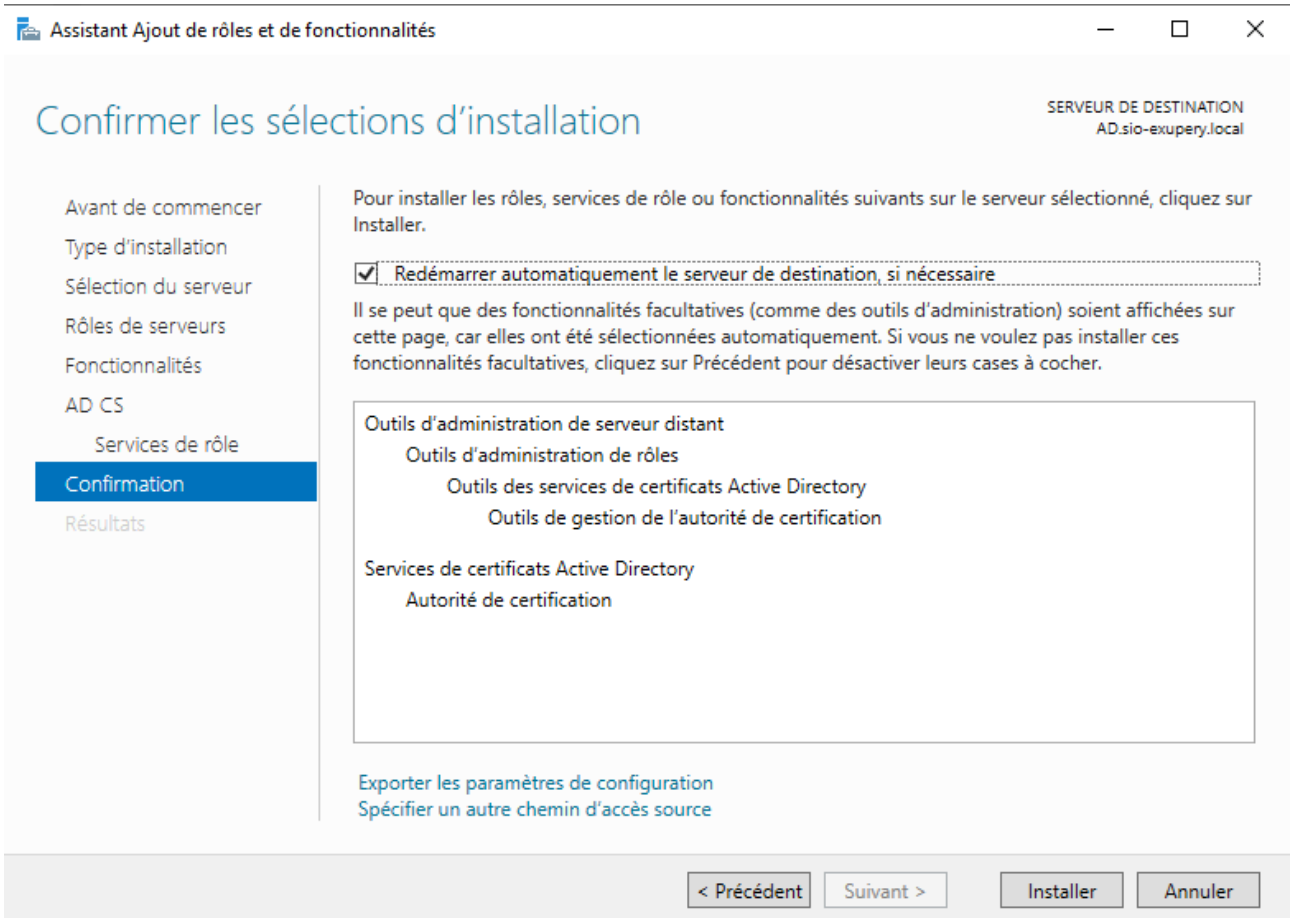
Ajoutez le rôle Service de certificats Active Directory.
Remarque : il est possible d'installer Network Policy Server (NPS) sans service de certificats mais ce rôle est nécessaire pour l'utilisation de PEAP dans une stratégie d'accès réseau.



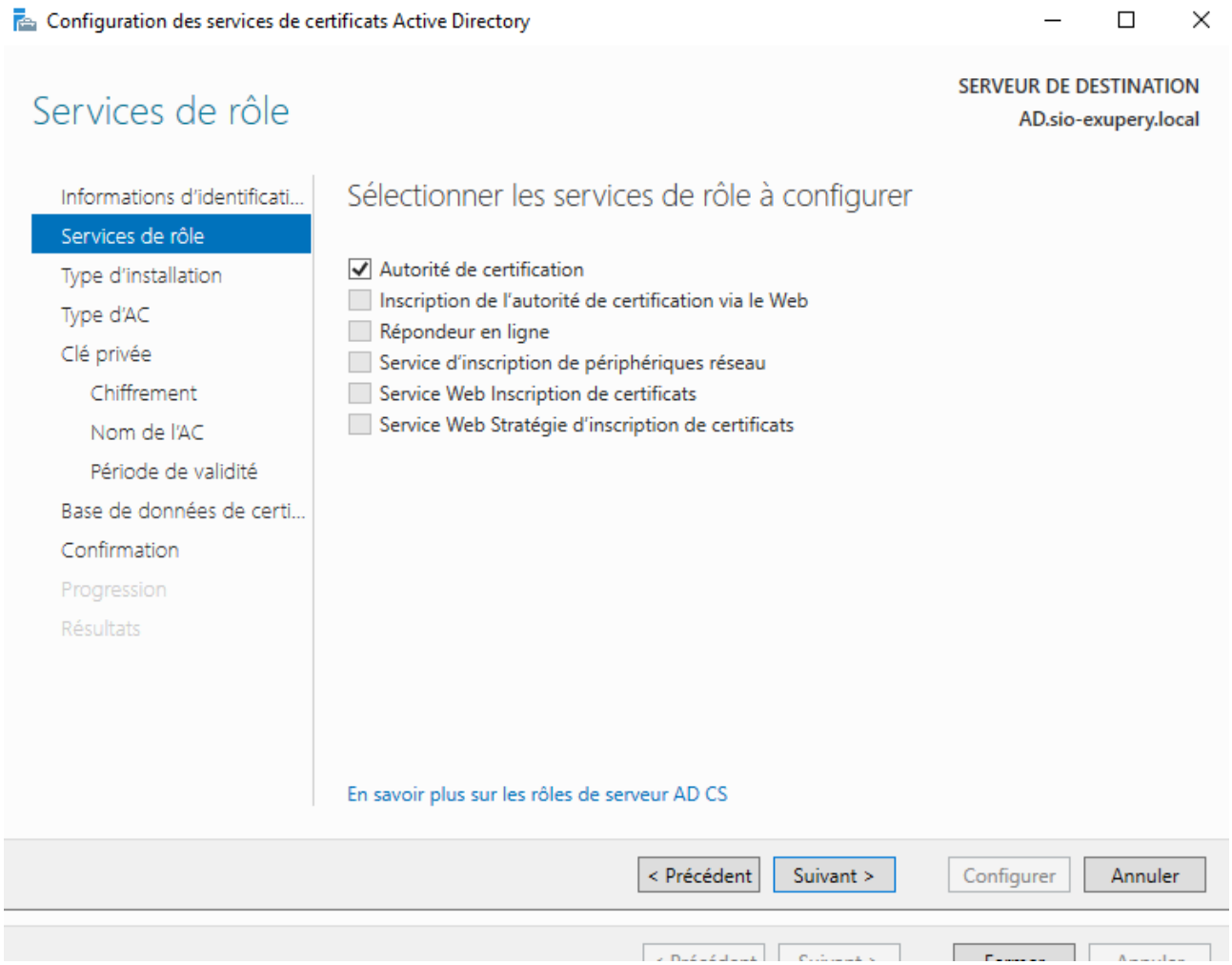
Prenez connaissance des informations la page d'information AD CS et cliquez sur le bouton Suivant.



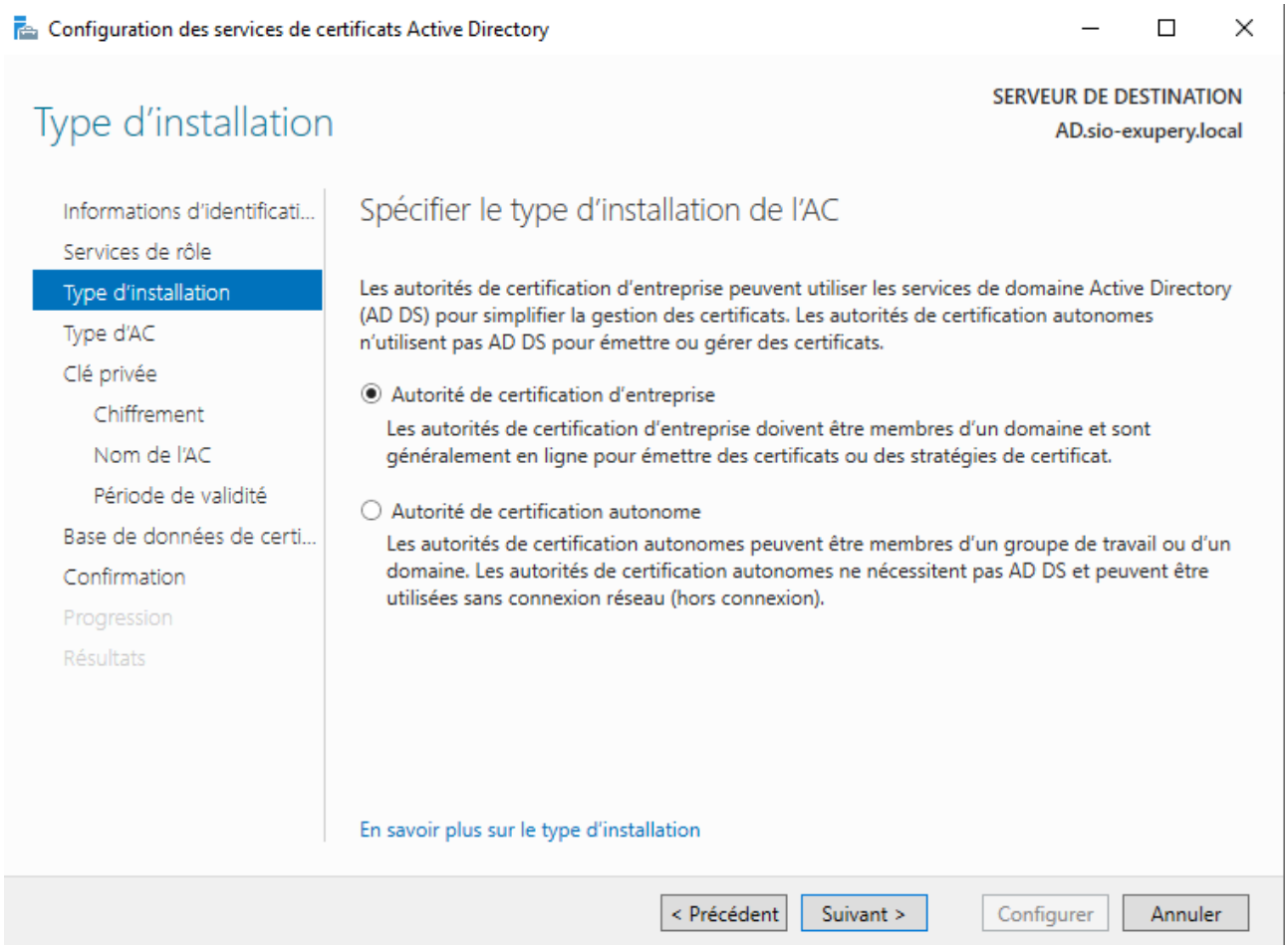
Cochez la case Redémarrer automatiquement... et cliquez sur Installer.



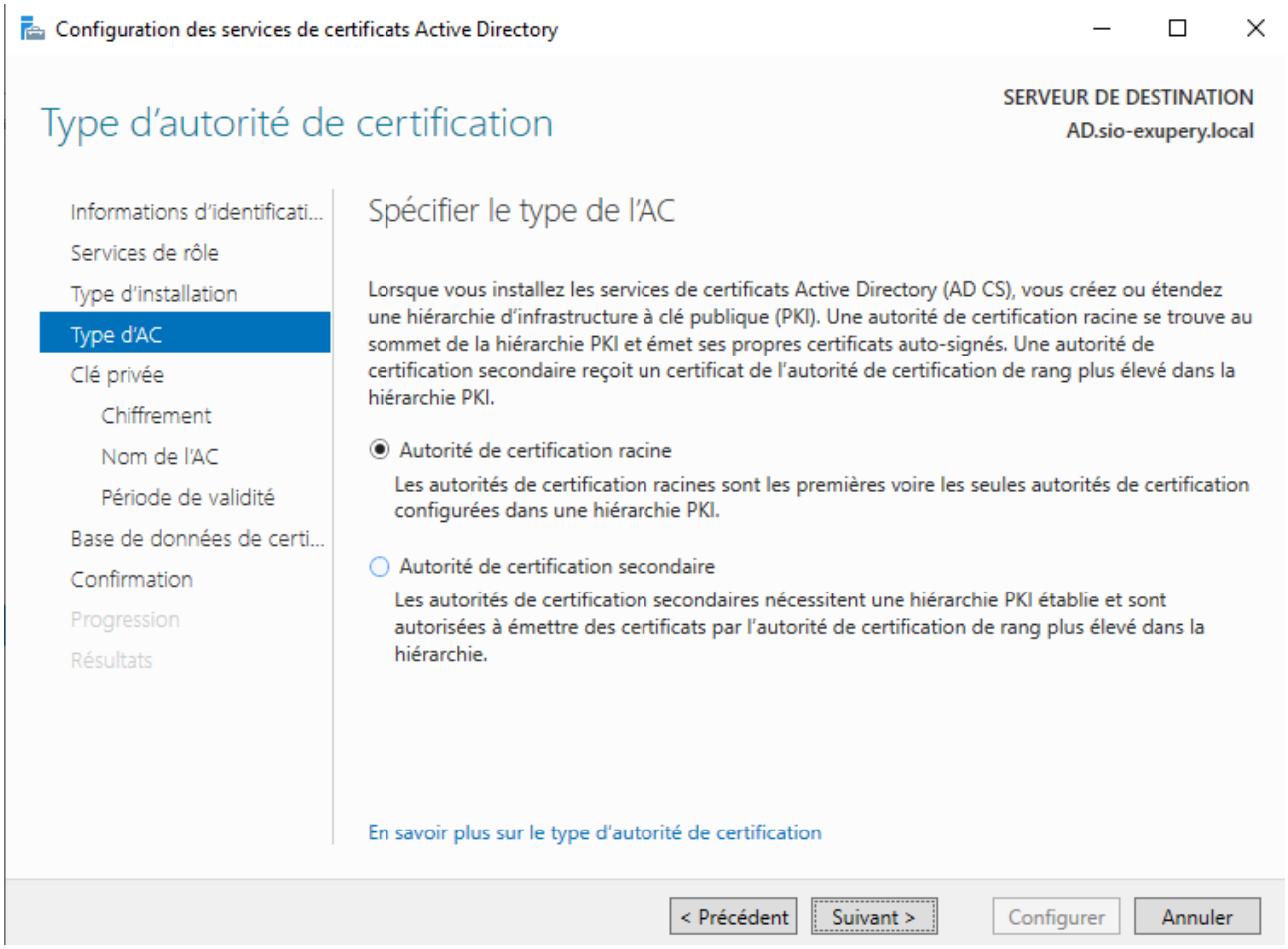
Je coche la case Autorité de certification pour configurer ce rôle



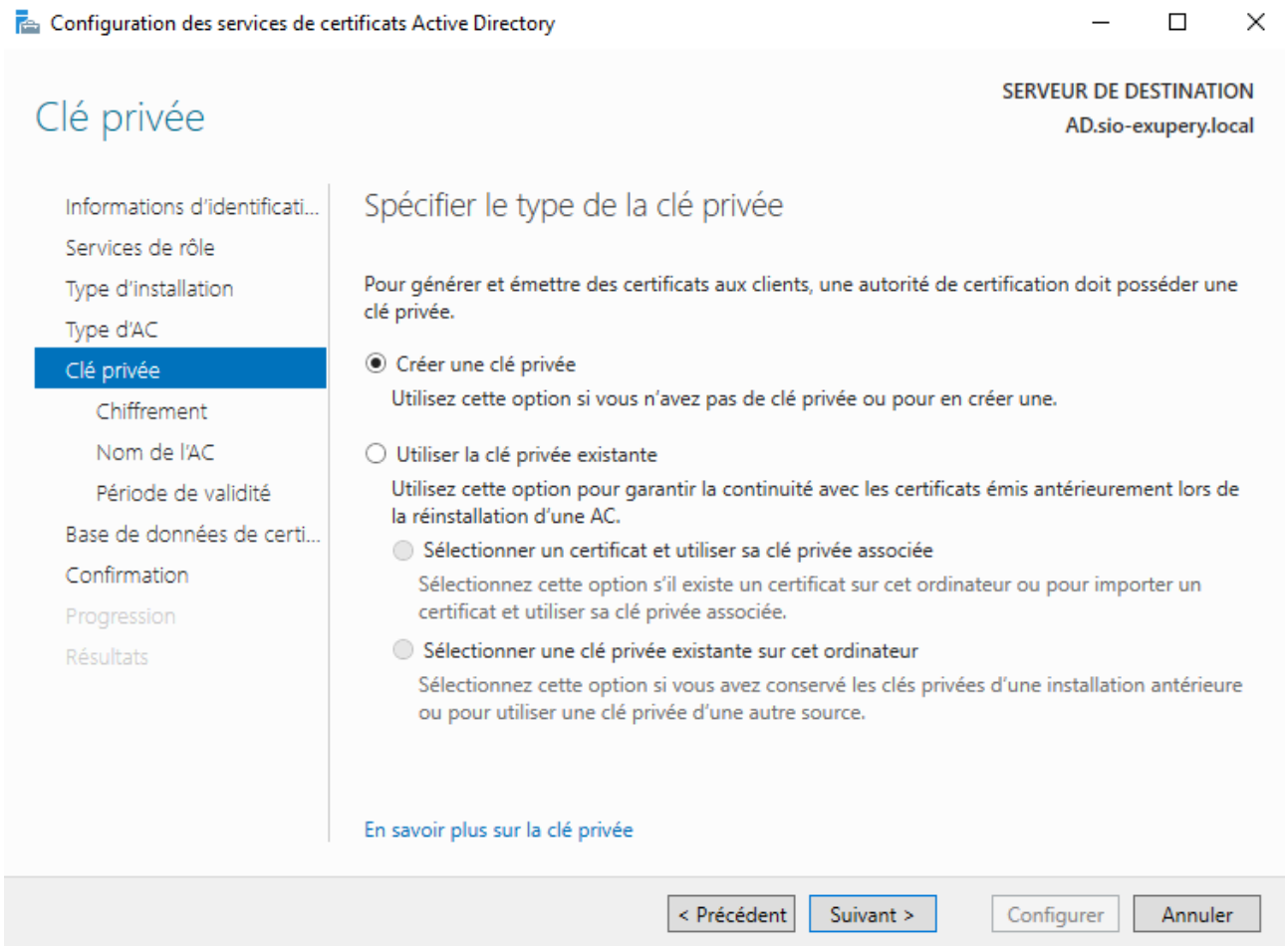
Je sélectionne l’authorité de certification d’entreprise



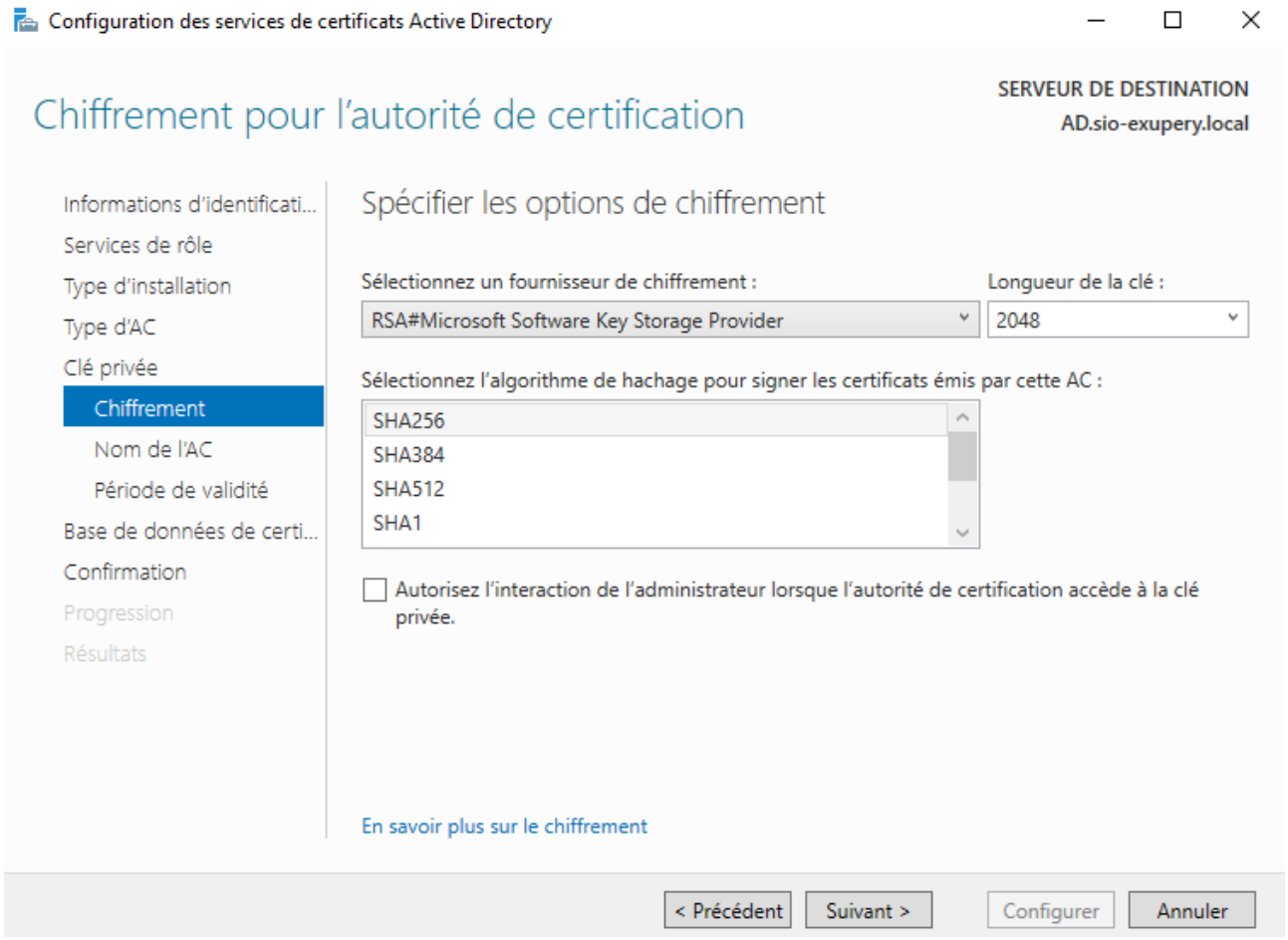
Je selectionne l’autorité de certification racine



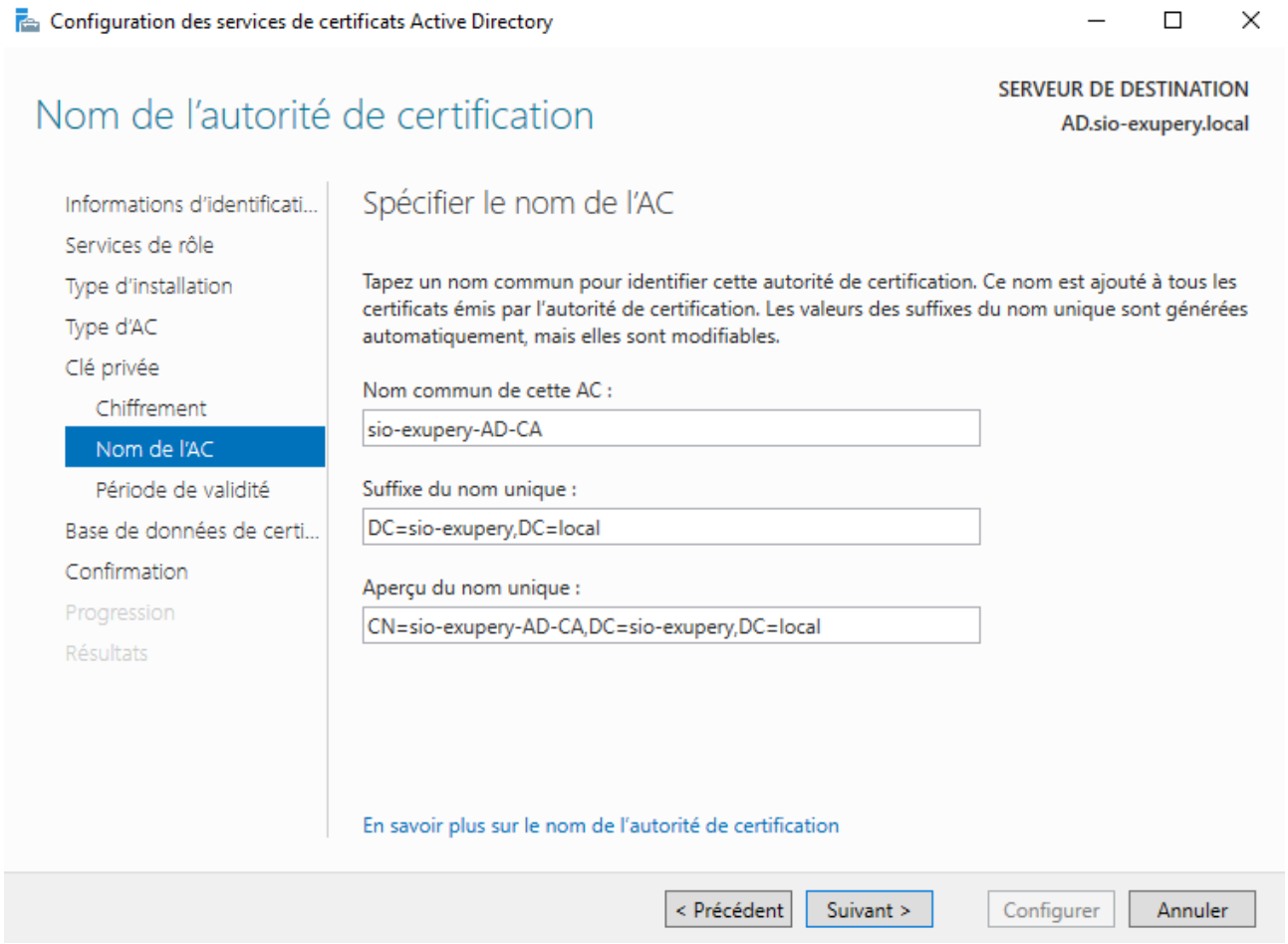
Je sélectionne Créer une nouvelle clé privée



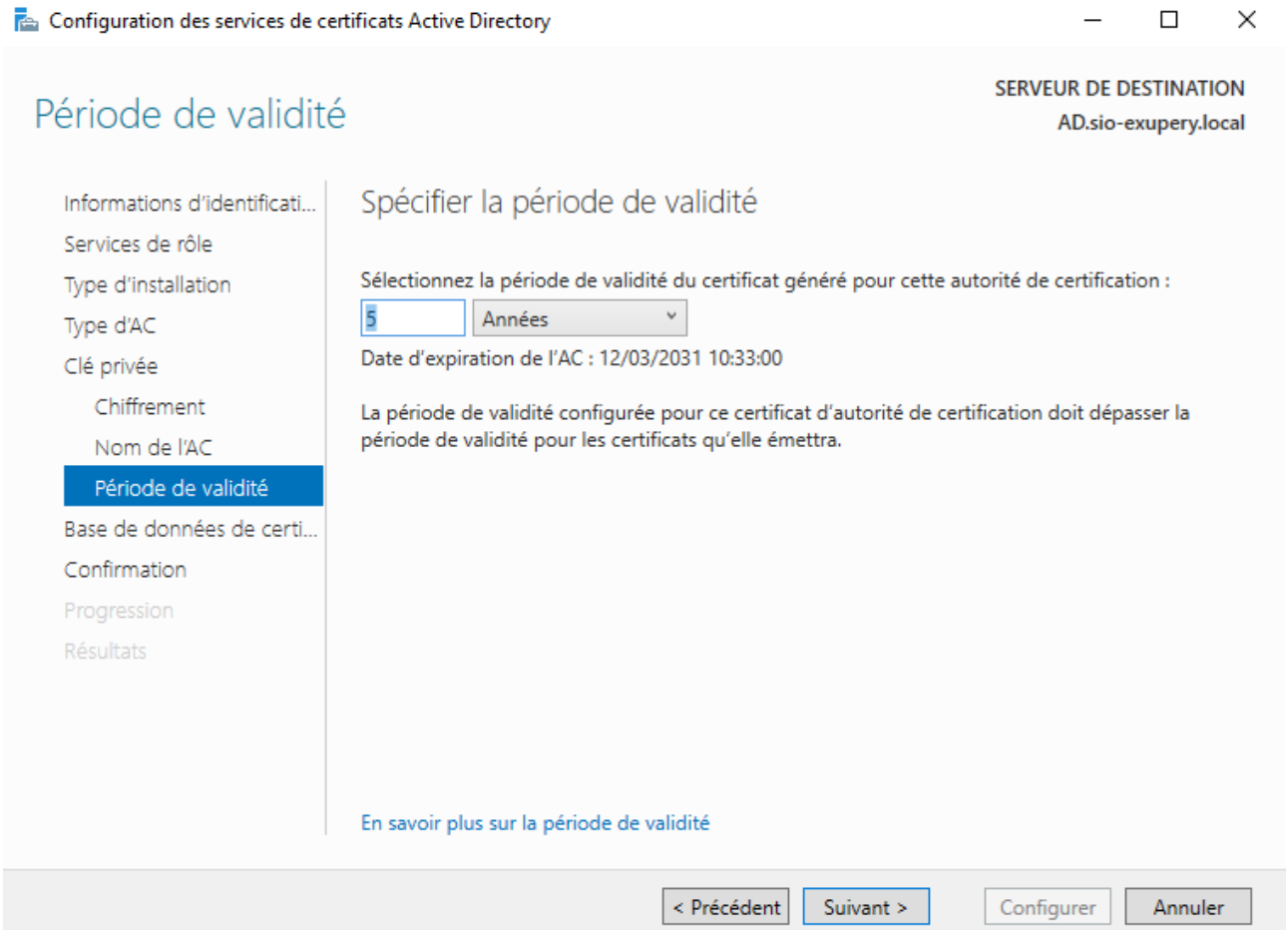
Je choisis l'algorithme de chiffrement ainsi que le hachage par défaut



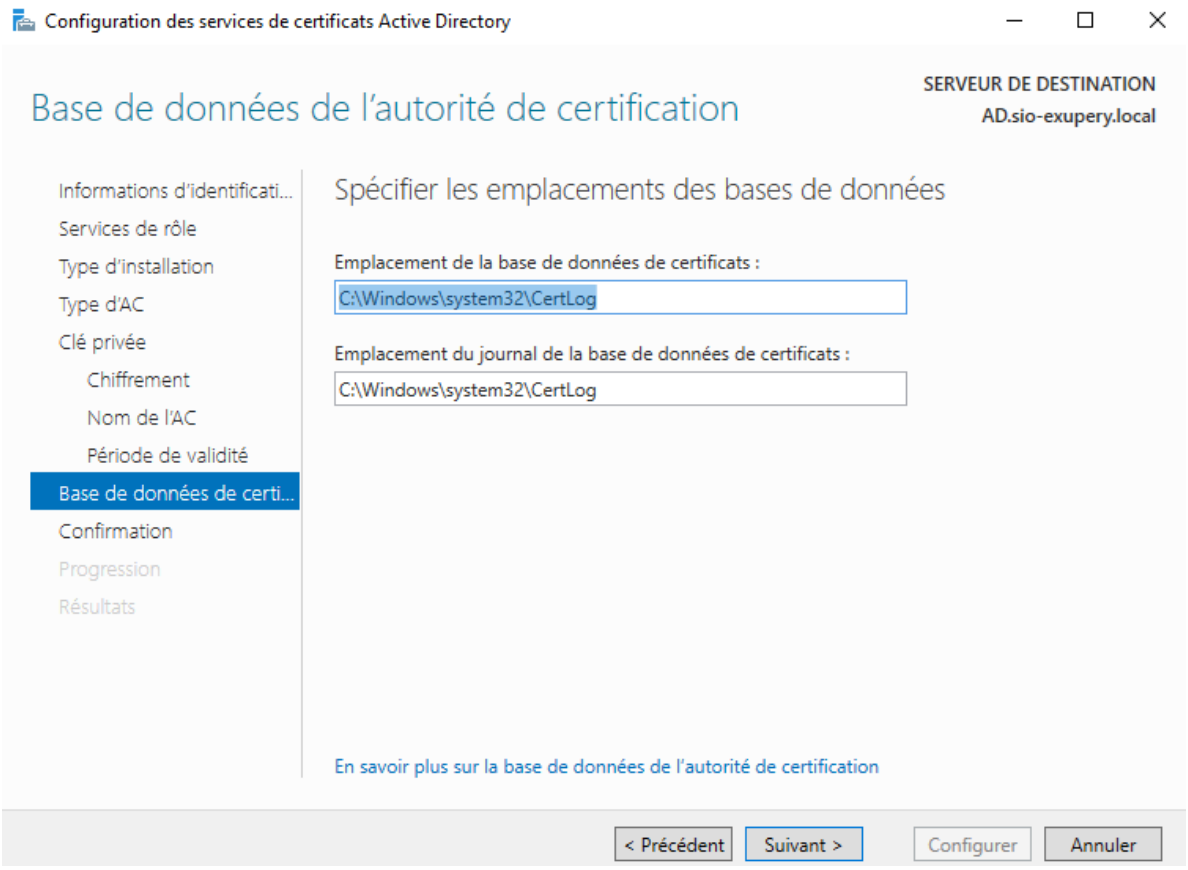
Par défaut, l'assistant nomme l'autorité de certification avec le nom de domaine suivi du nom de machine : sio-exupery-AD-CA.



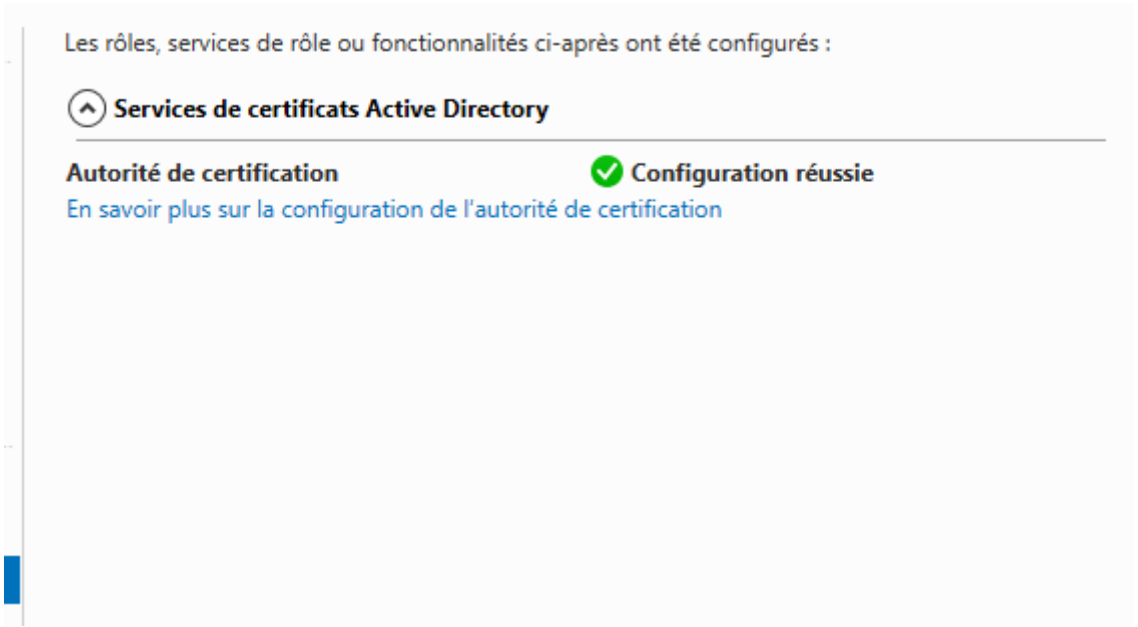
Je laisse la validité par défaut



Laissez les dossiers des bases de données, par défaut

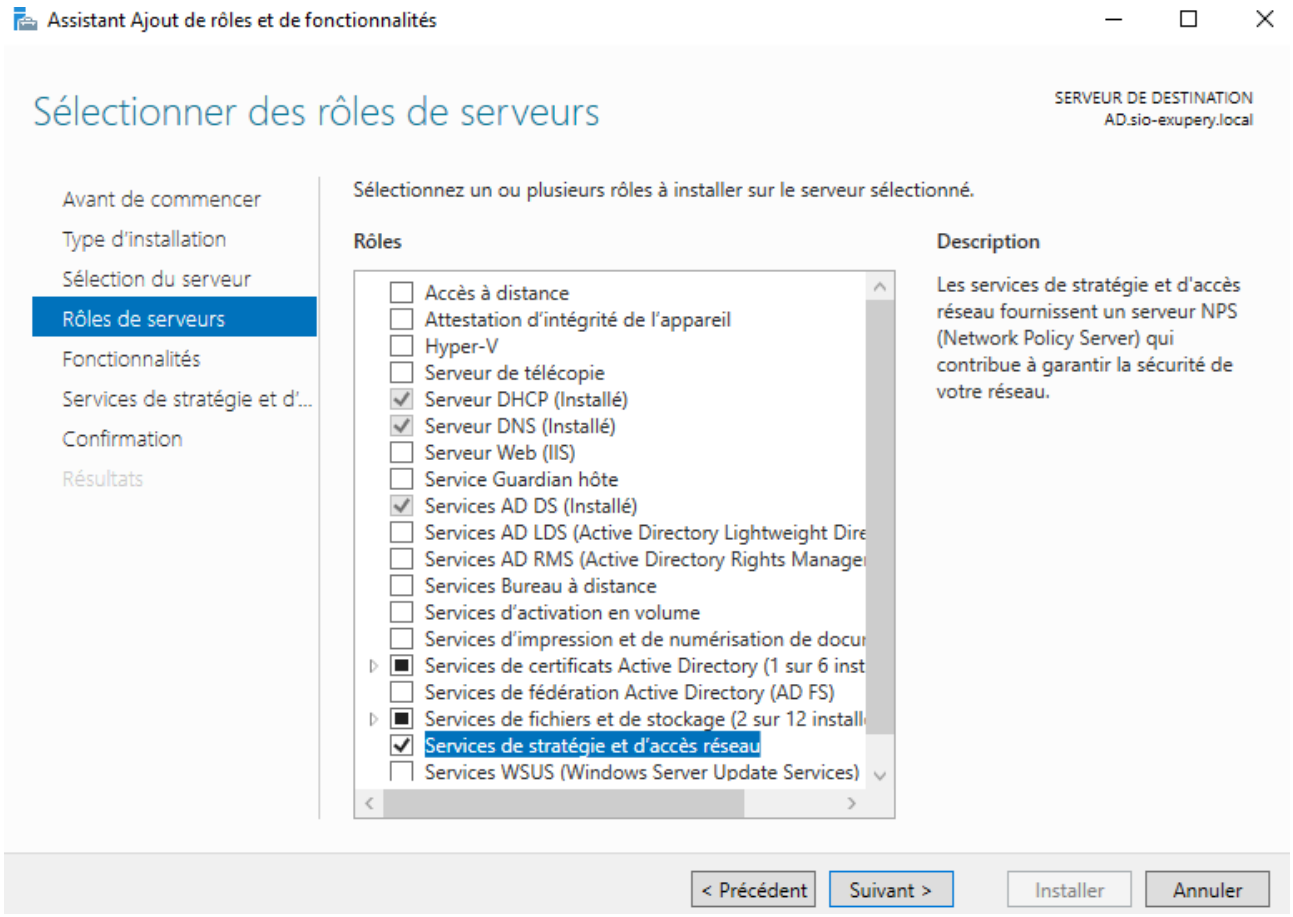


Votre autorité de certification est maintenant installée et configurée. Cliquez sur Fermer

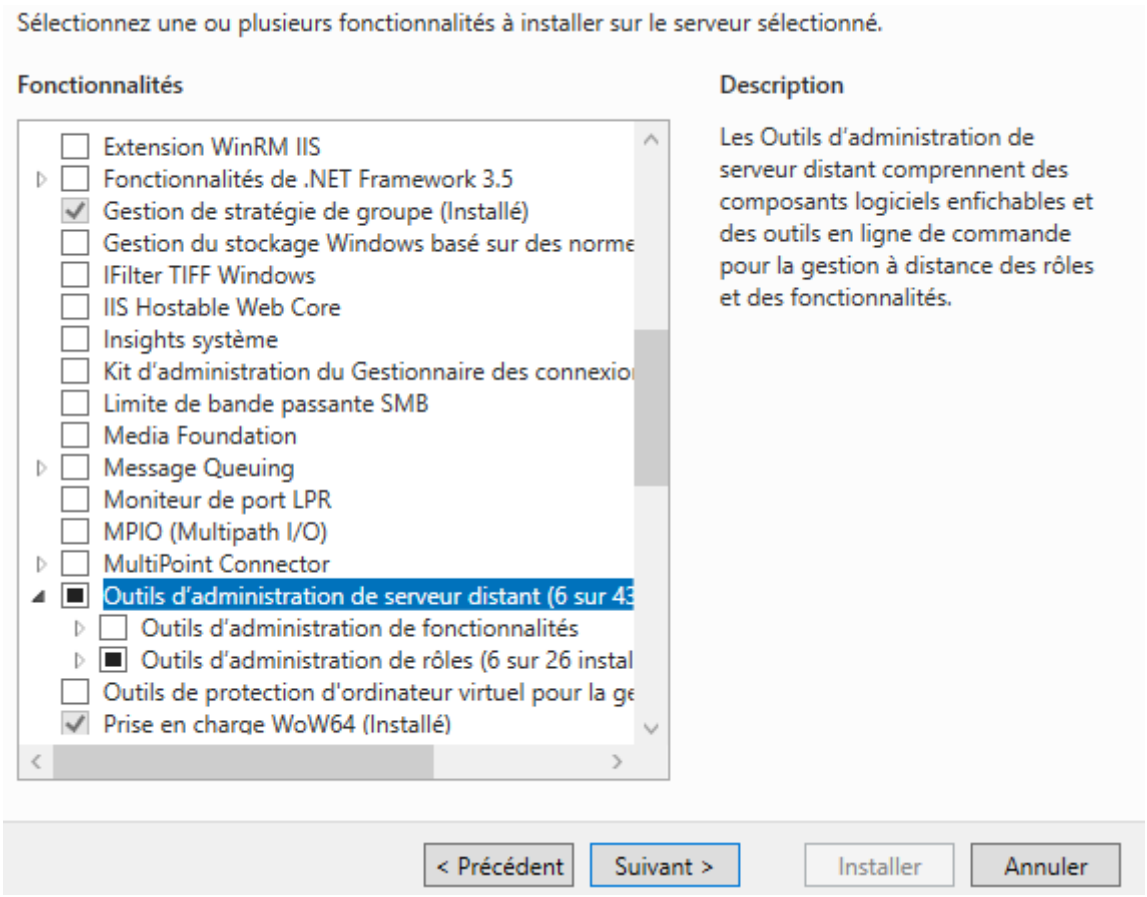


2.3 Installation du service NPS

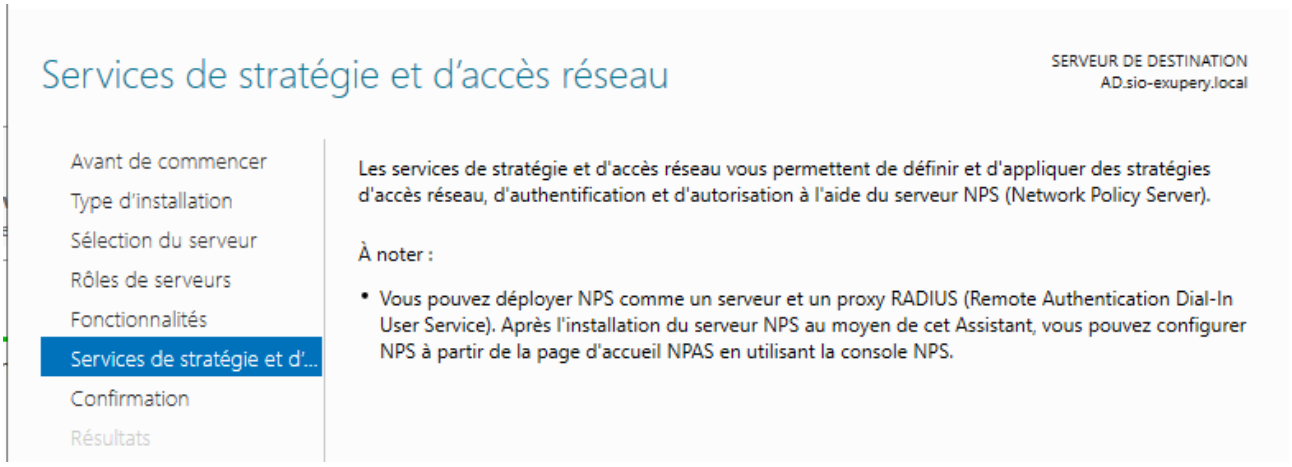
J’ajoute la fonctionnalité Services de stratégie et d’accès réseaux



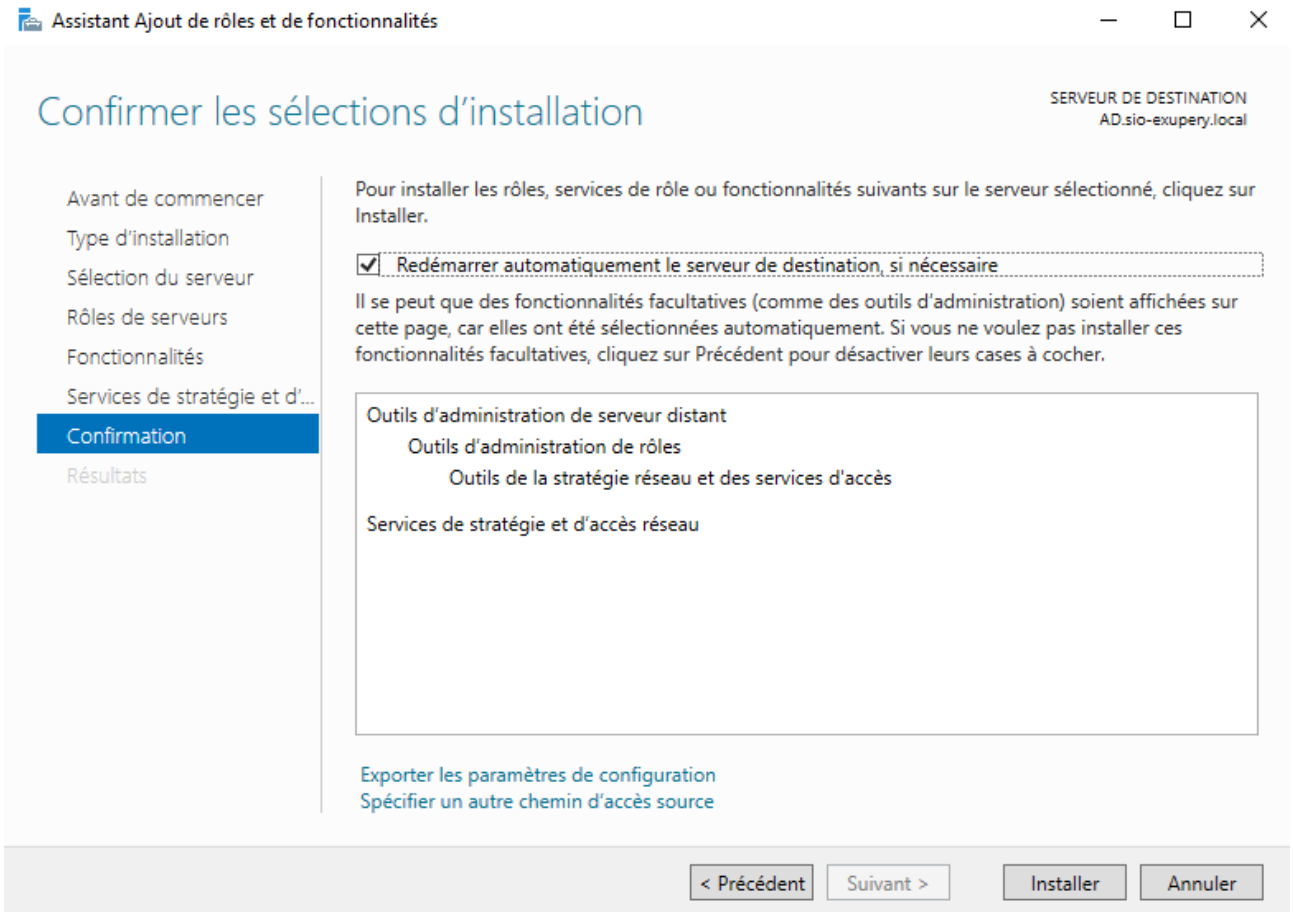
Je clique sur suivant



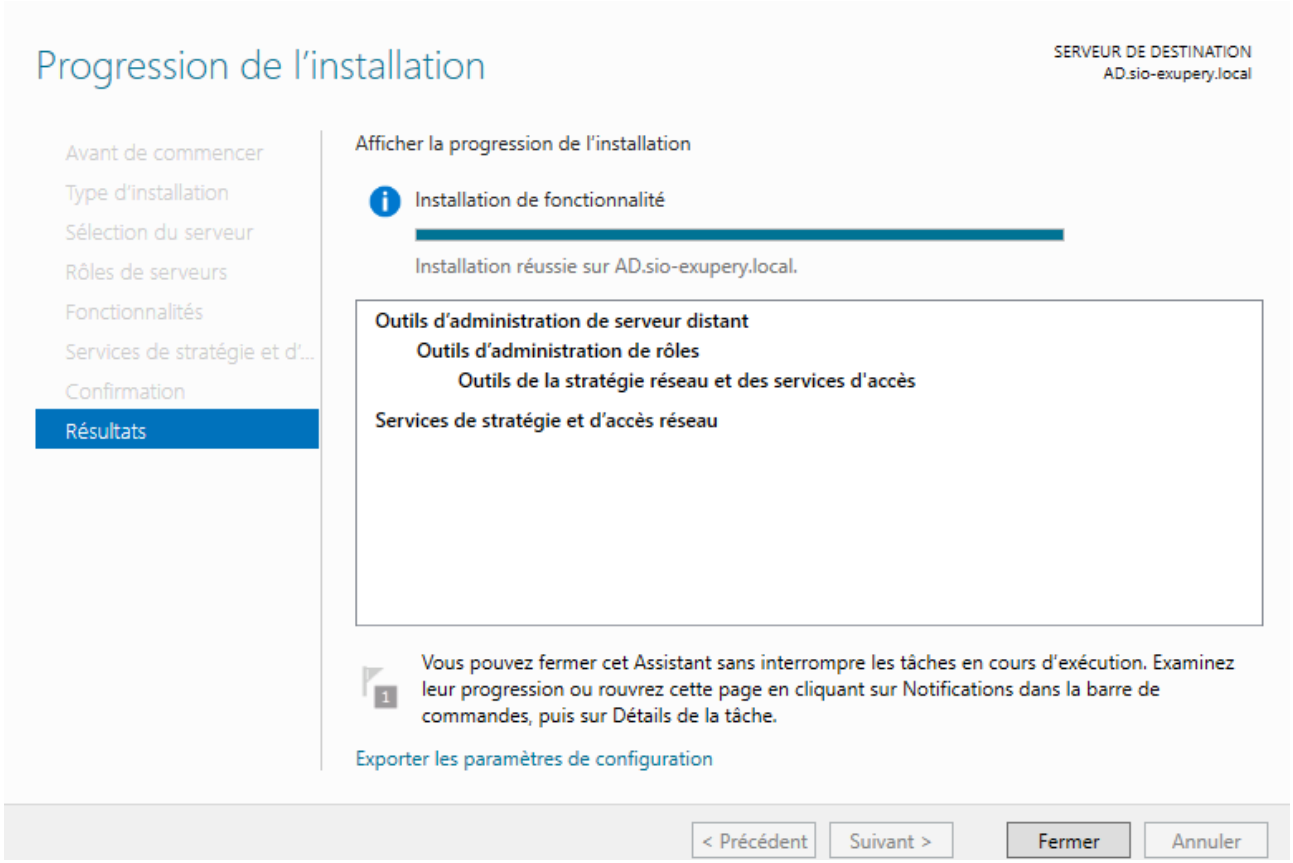
Je clique sur suivant



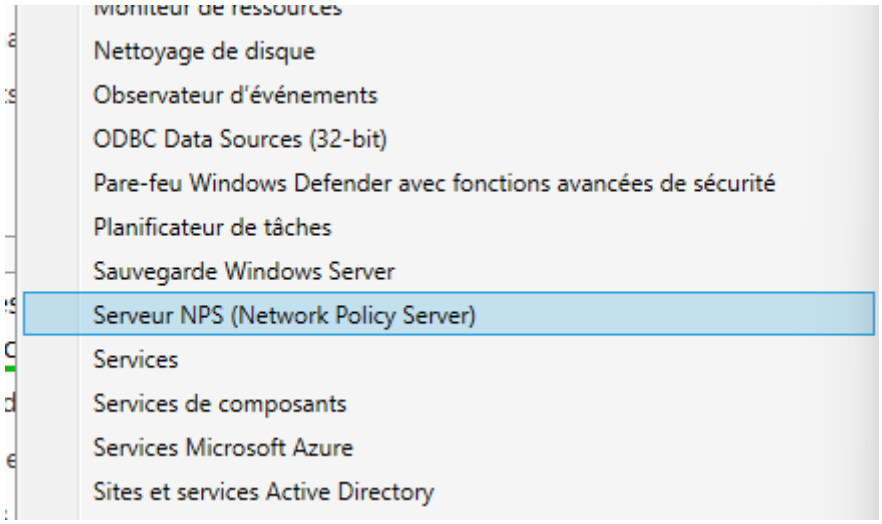
Je coche le redémarrage automatique du serveur



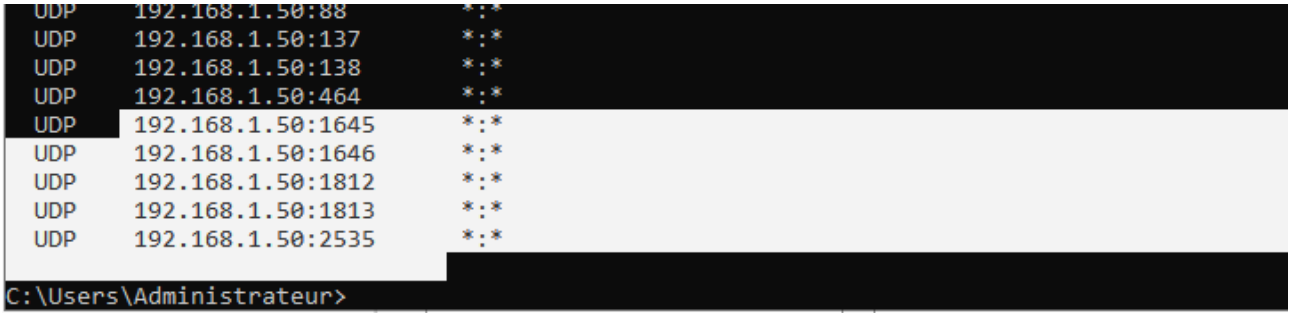
Puis j'installe et je ferme



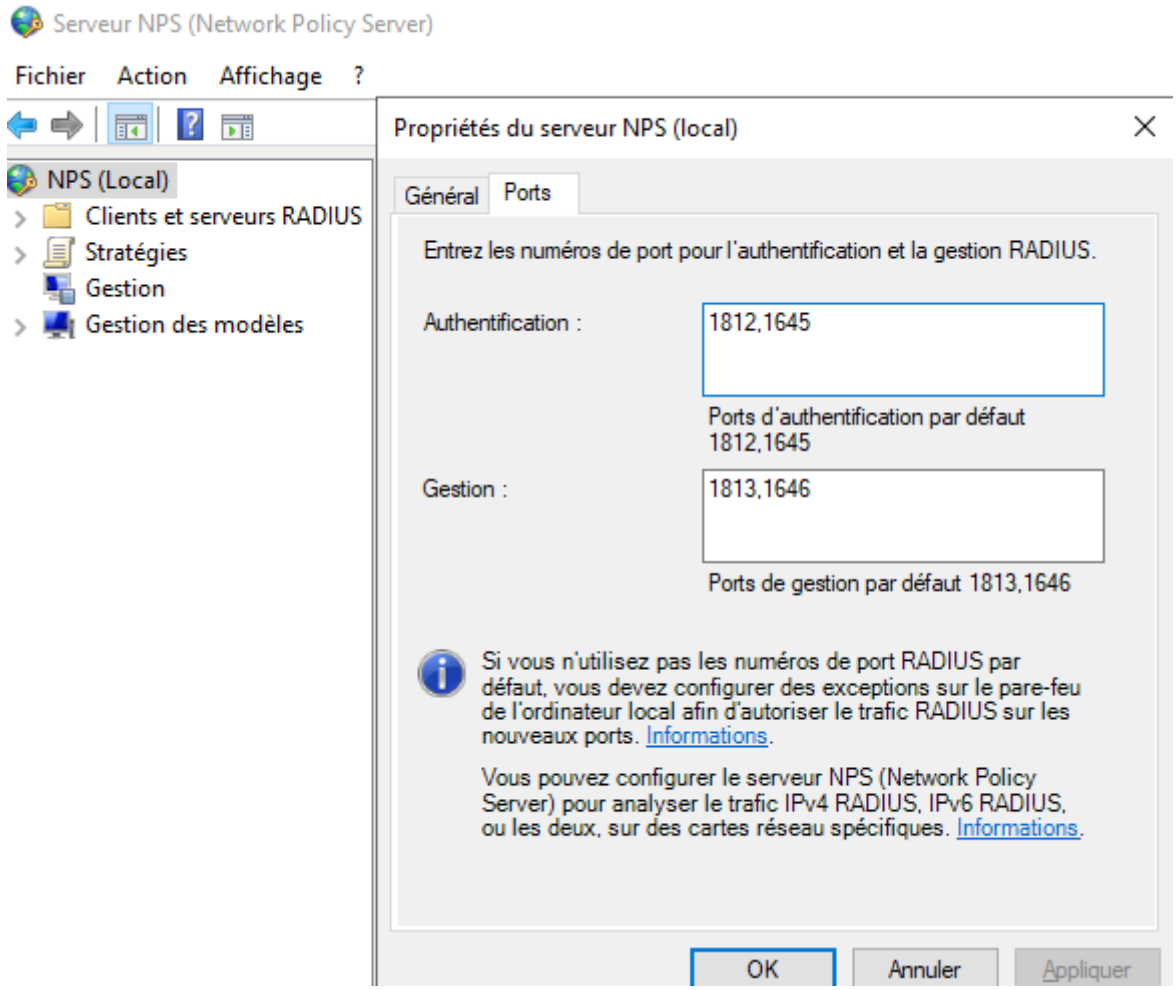
Constatez la présence de la console Serveur NPS



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

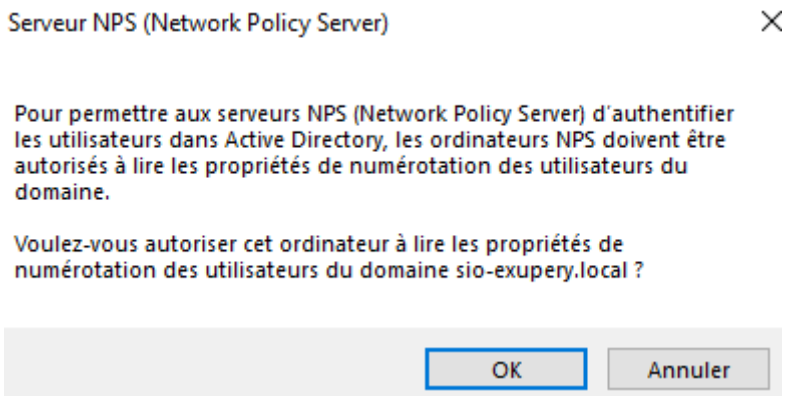


Ouvrez la console Serveur NPS (Network Policy Server) et retrouvez ces ports dans les propriétés du serveur NPS



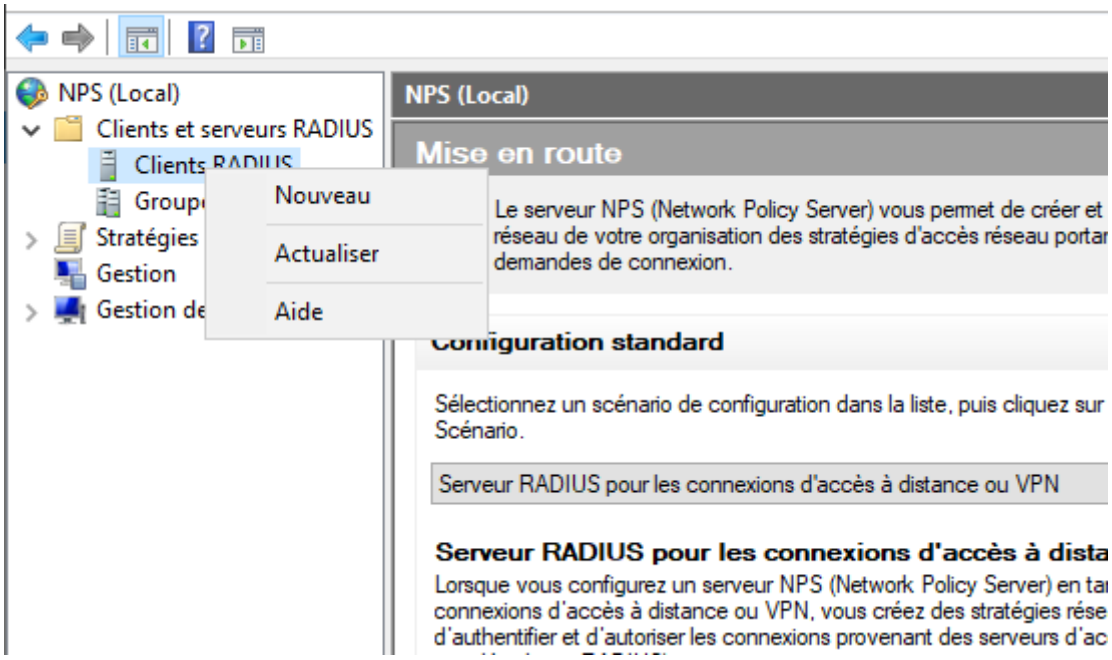
2.4 Configuration du serveur RADIUS NPS

Afin d’inscrire NPS dans Active Directory pour lui permettre d'interroger la base des utilisateurs, cliquez depuis le menu Action sur Inscrire un serveur dans Active Directory puis OK

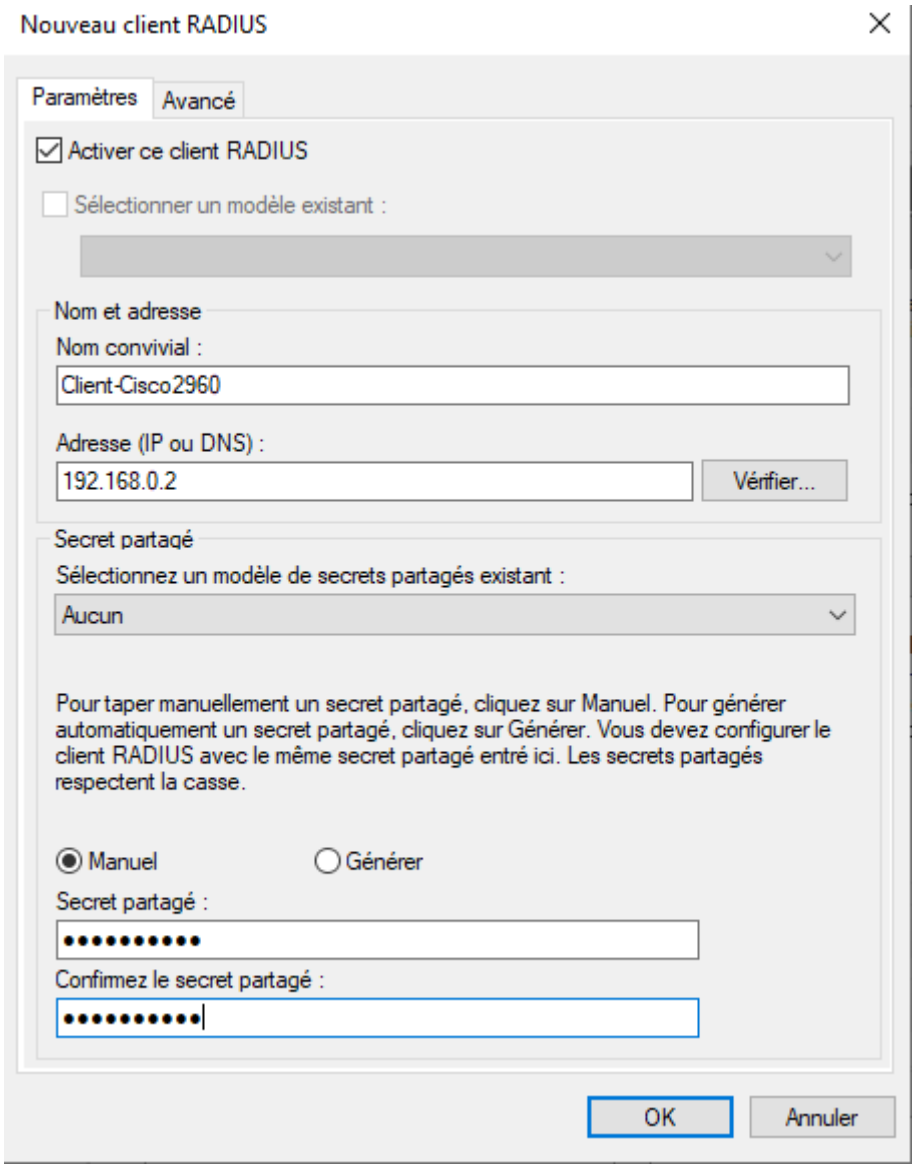


Un agent s’est mis en route

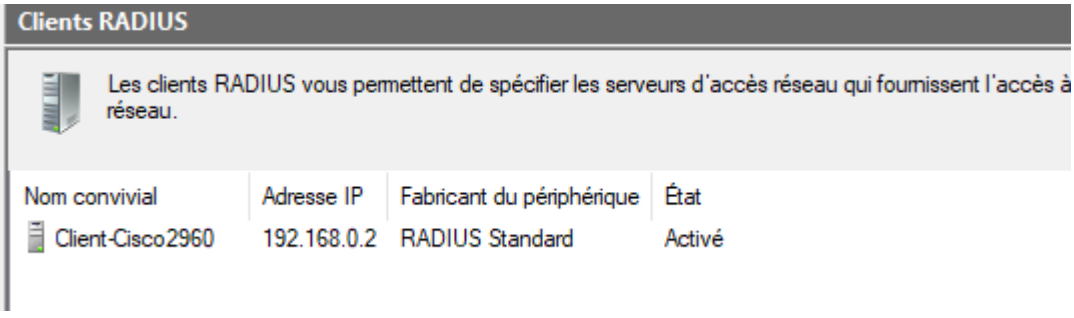
Ensuite clic droit sur client radius puis nouveau



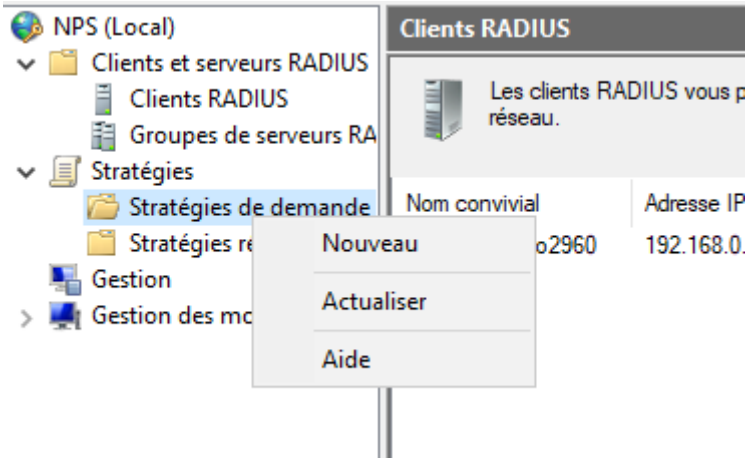
Ensuite je rentre les infos le mot de passe son est sio1234567



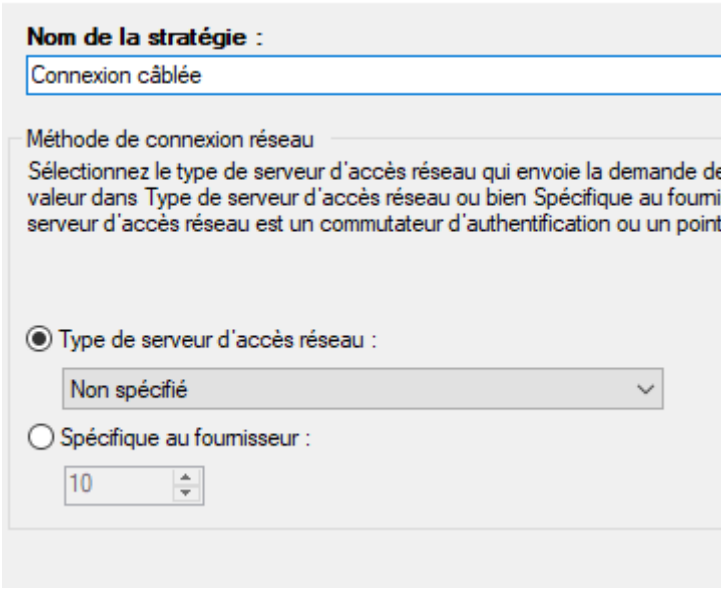
Le client est bien ajouté

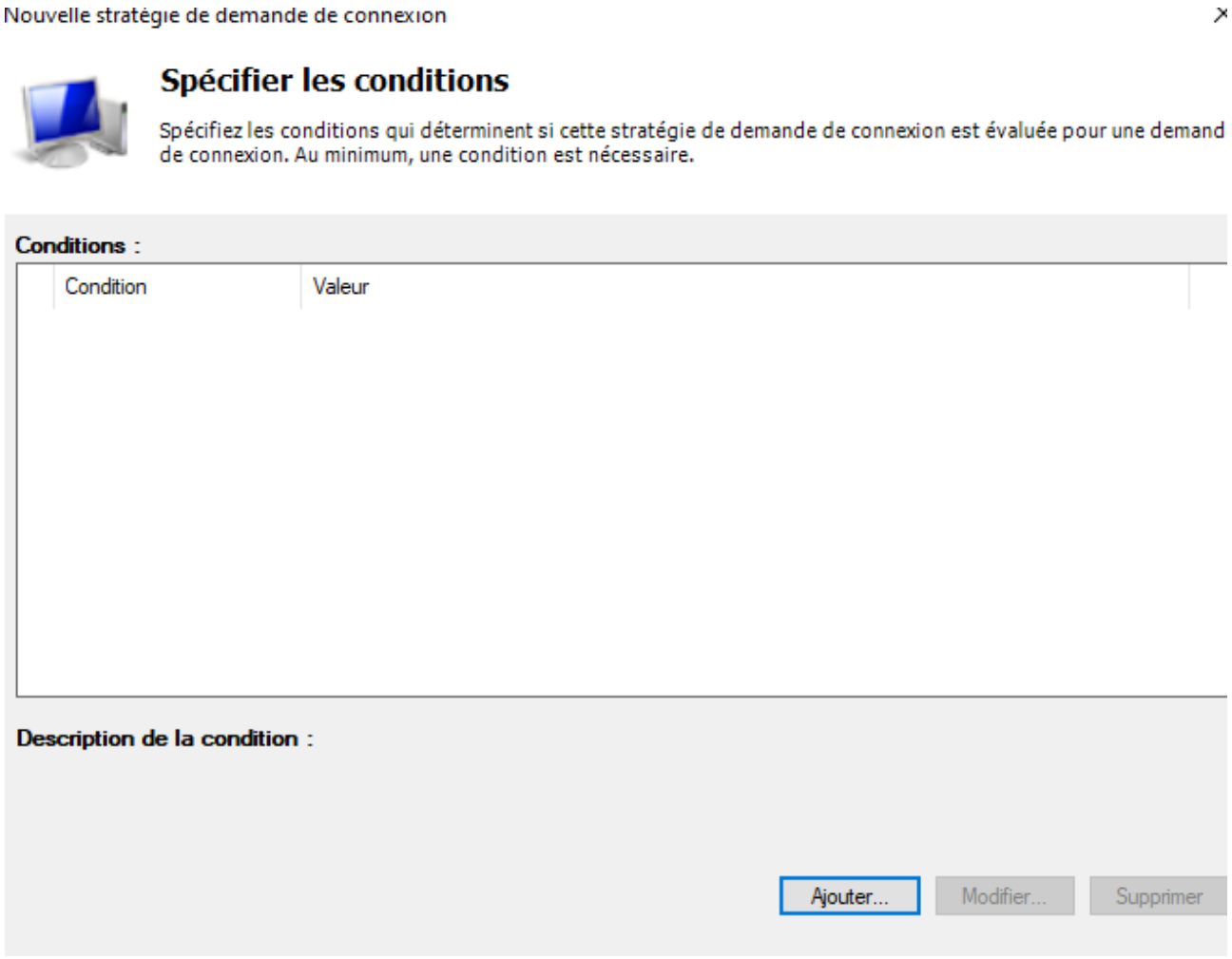


Je clique droit sur l’entrée Stratégies de demande de connexion et sélectionne Nouveau

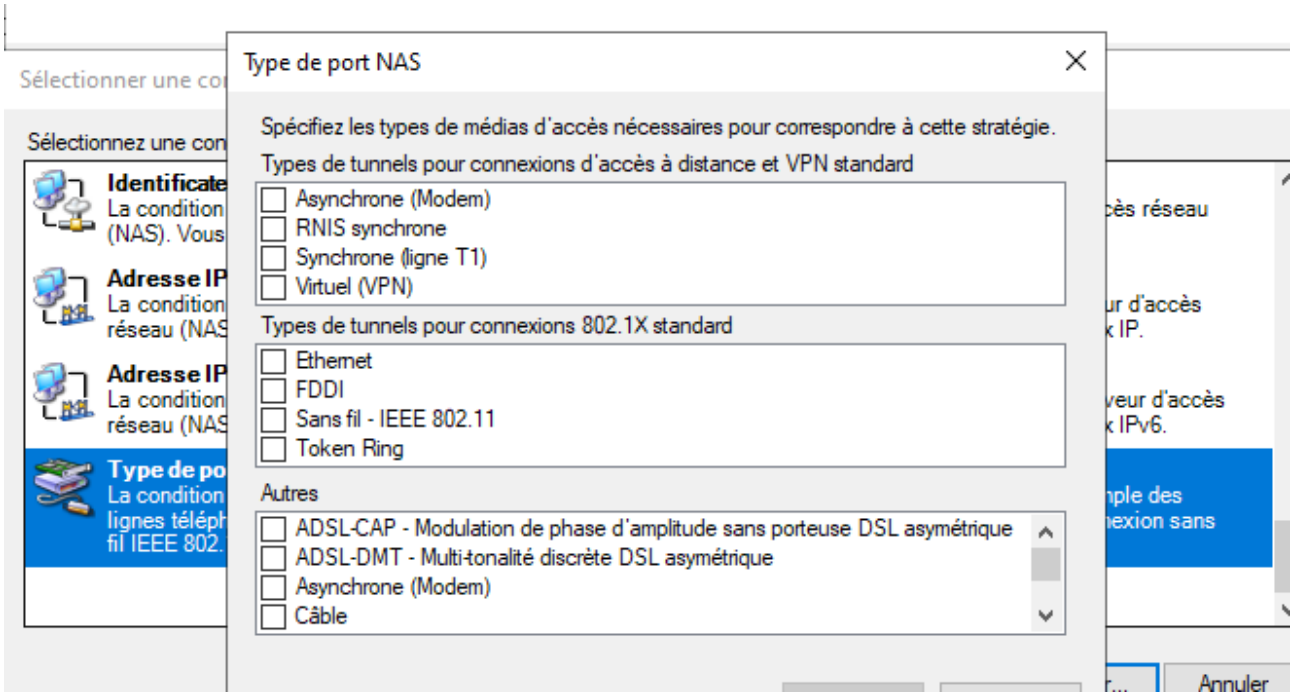


Je la nomme :

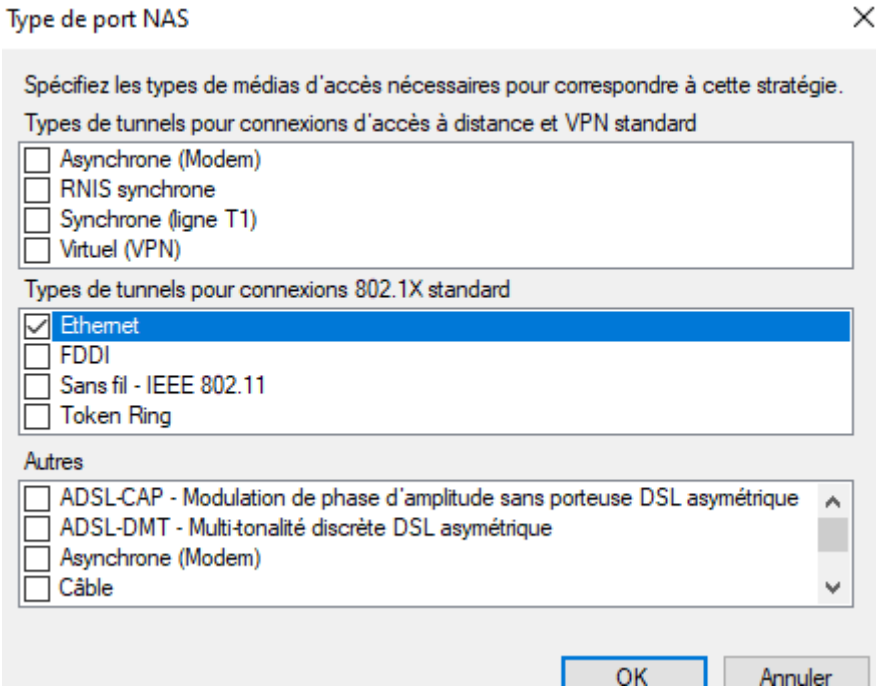




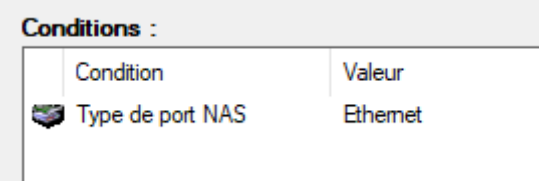
Ensuite je clique sur ajouter puis type de port NAS



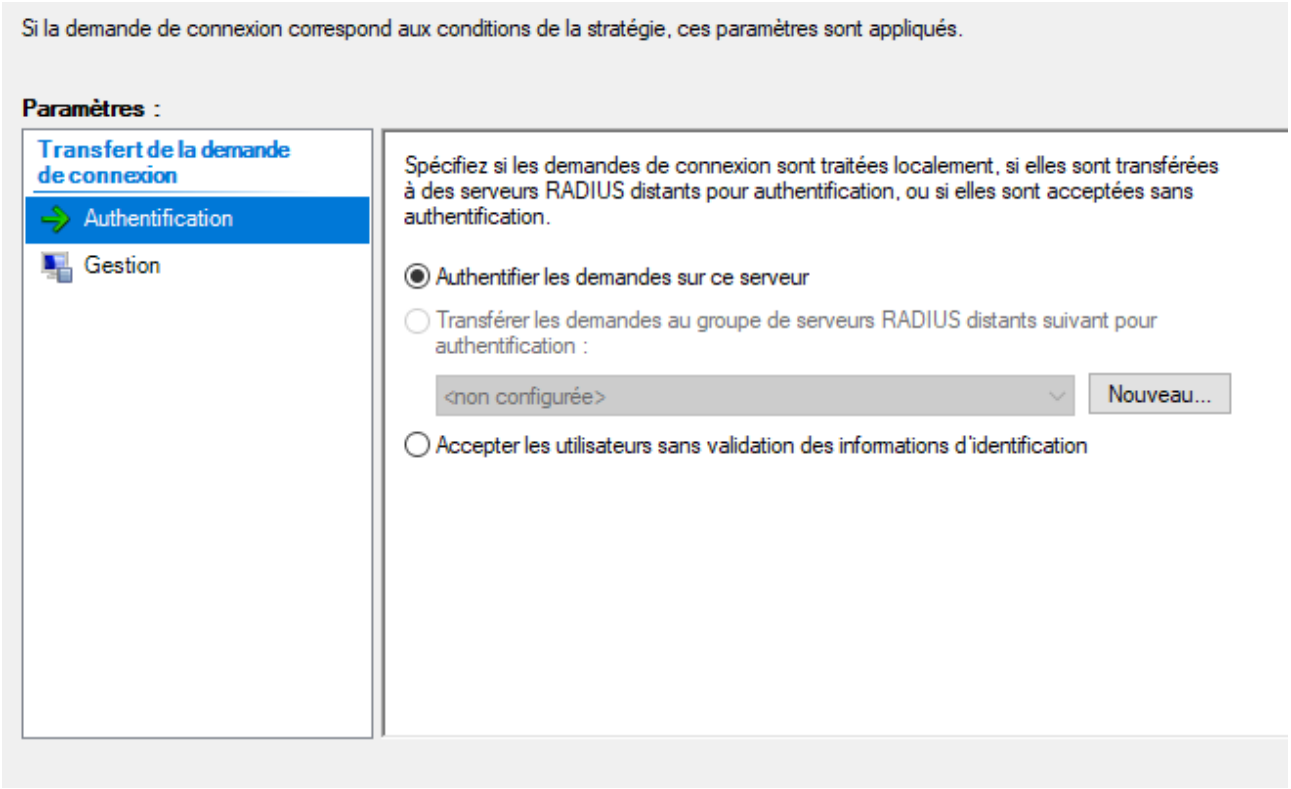
Je coche ethernet



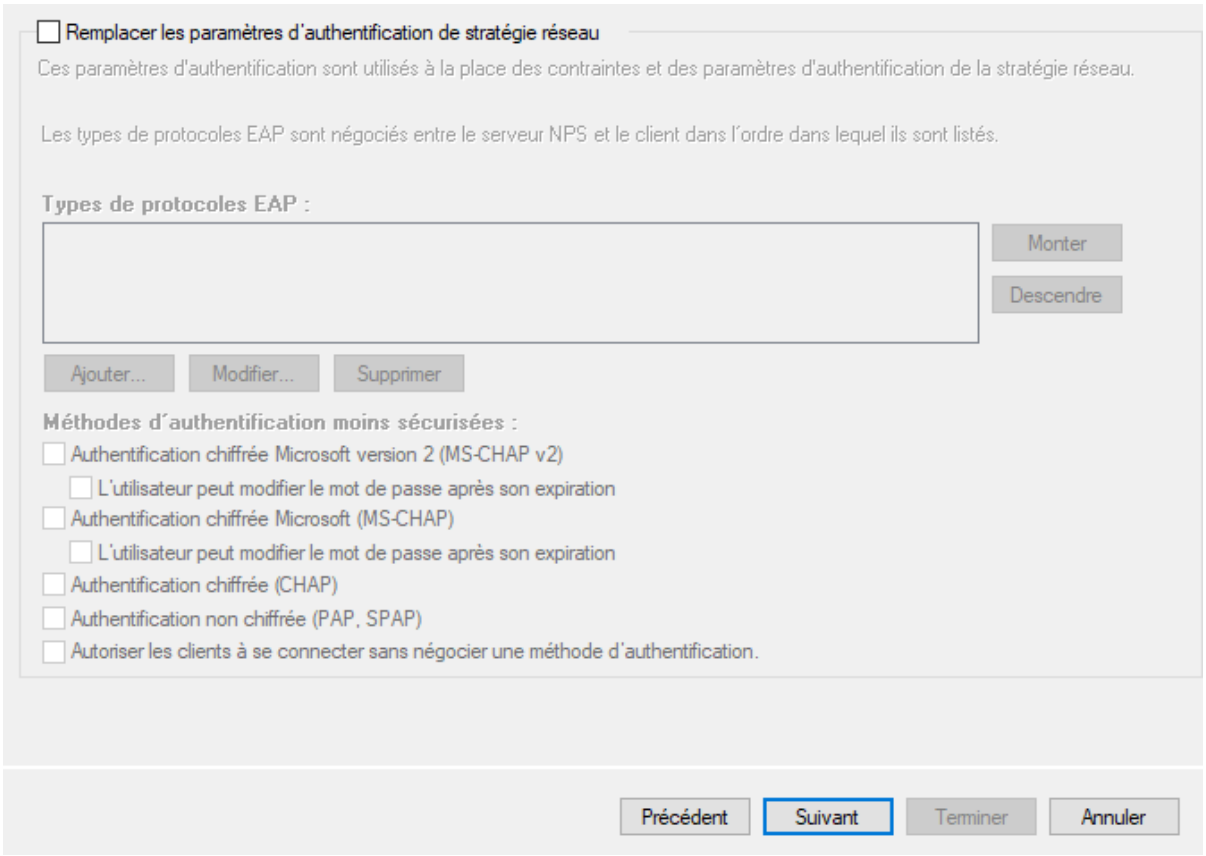
Puis je valide et il apparaît dans les conditions

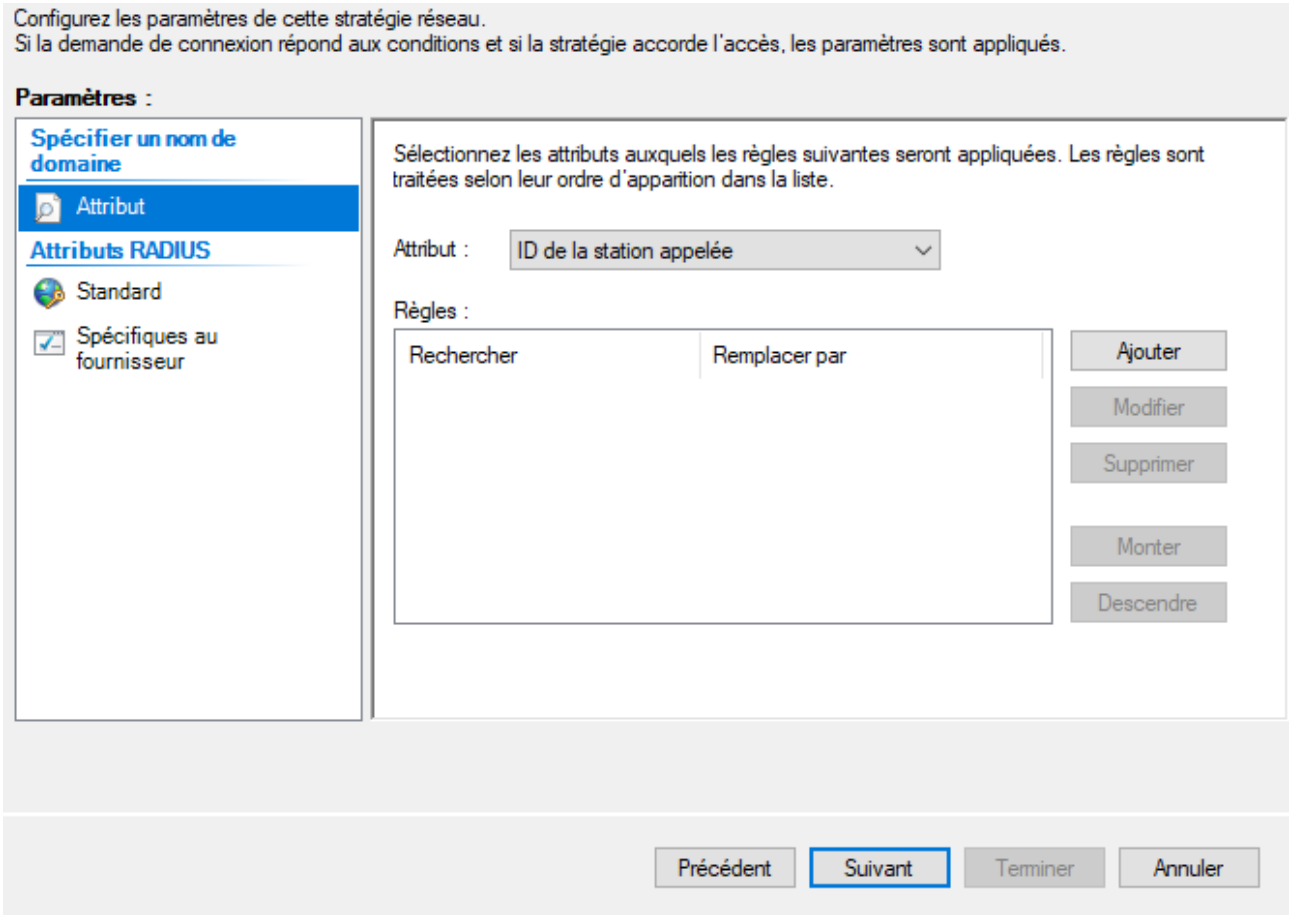


Je clique sur suivant

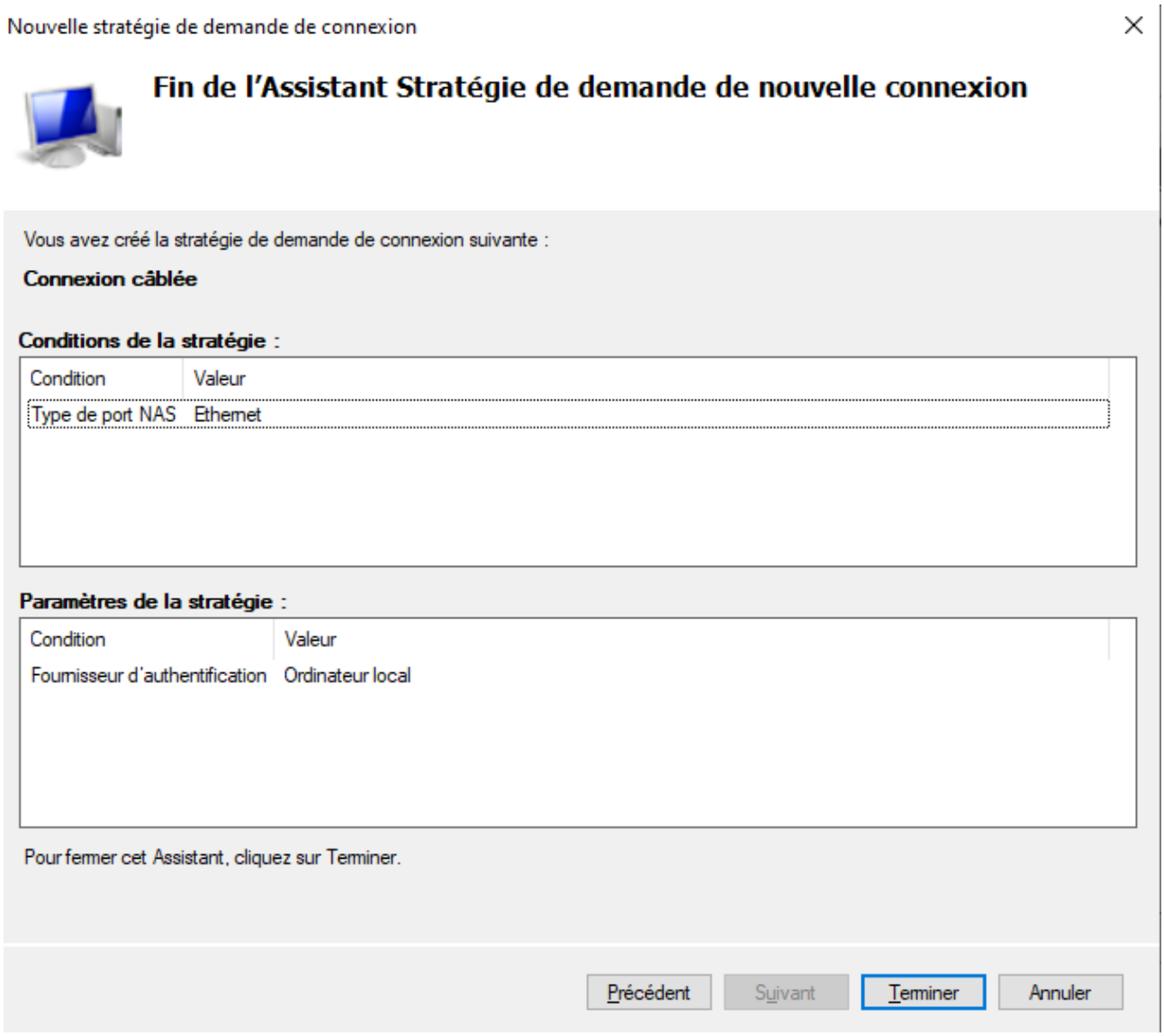


et encore sur suivant J’apparait sur cet page et on clique encore sur suivant

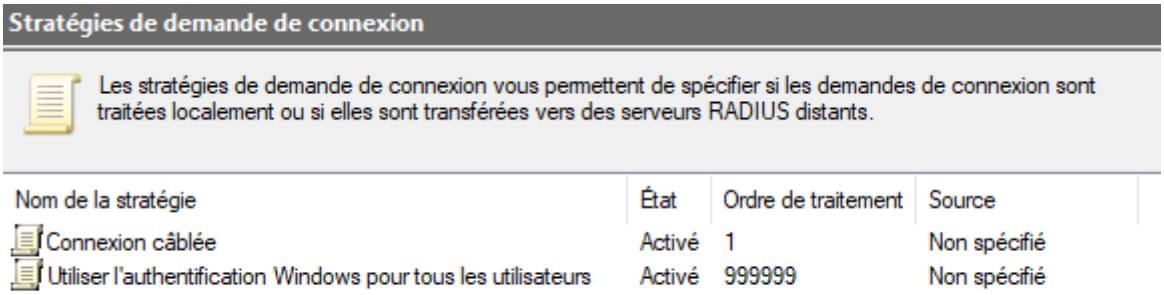




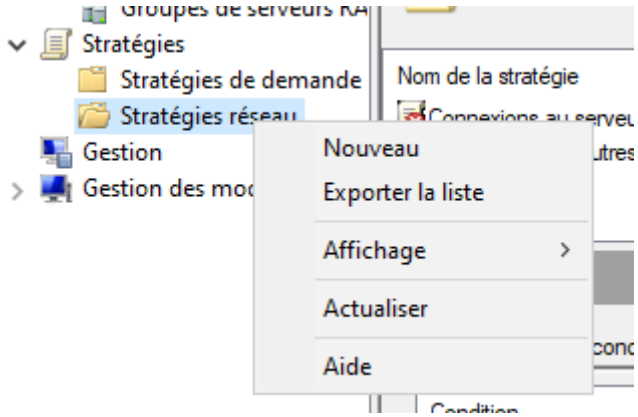
On clique mainteant sur valider

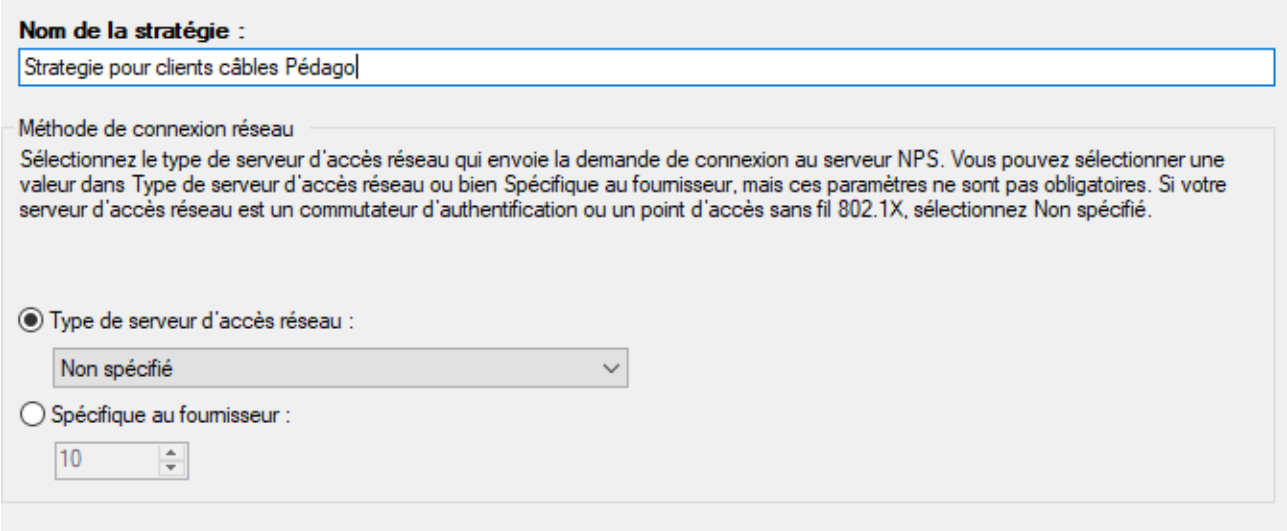


La stratégie a été rajouter

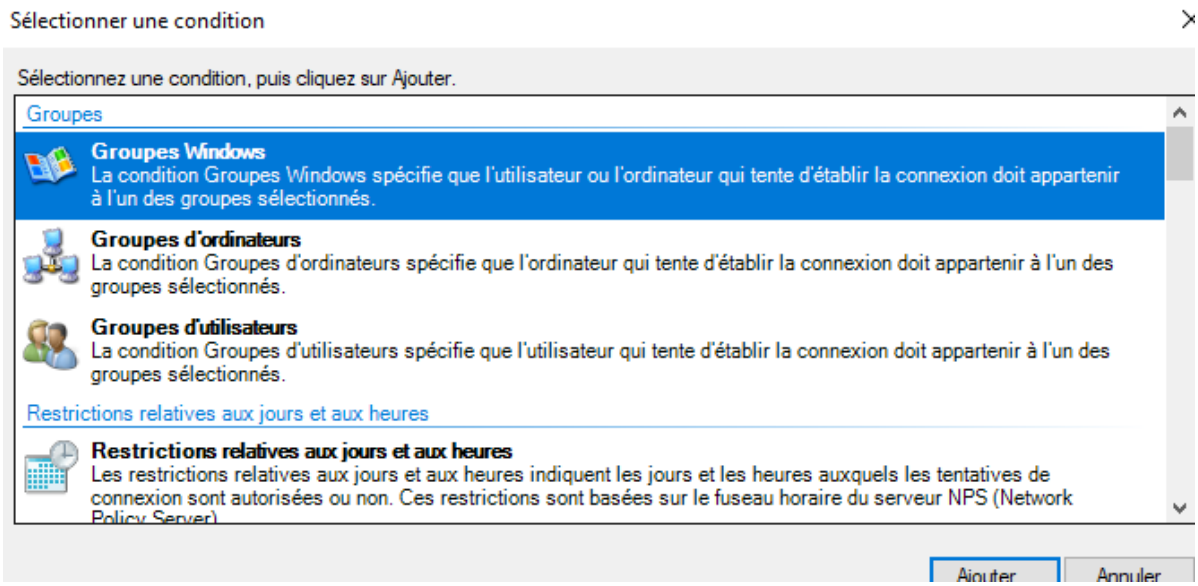


Je fais un clique droit sur l'entrée Stratégie Réseau et je sélectionne Nouveau. Je spécifie le nom de la stratégie (celle pour les membres du groupe Prof). On reste sur un type de serveur d’accès réseau non spécifié car s'agit d'une authentification via un commutateur 802.1x

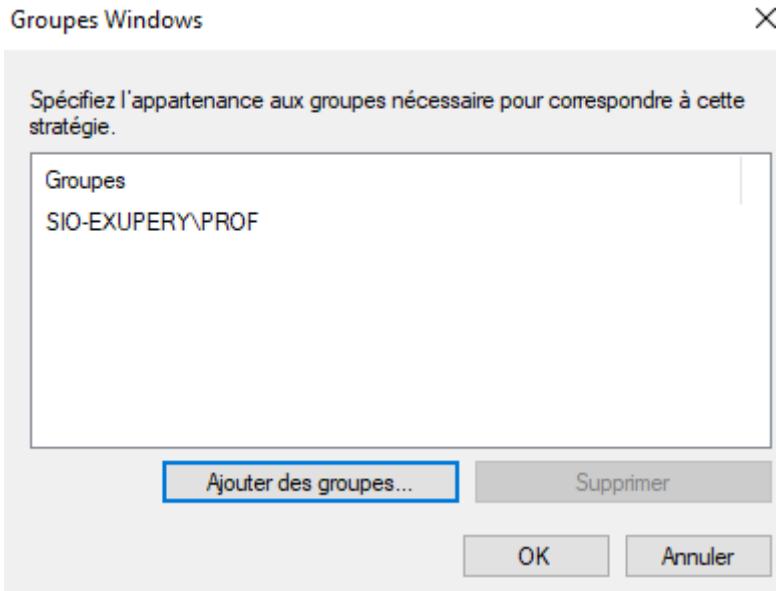




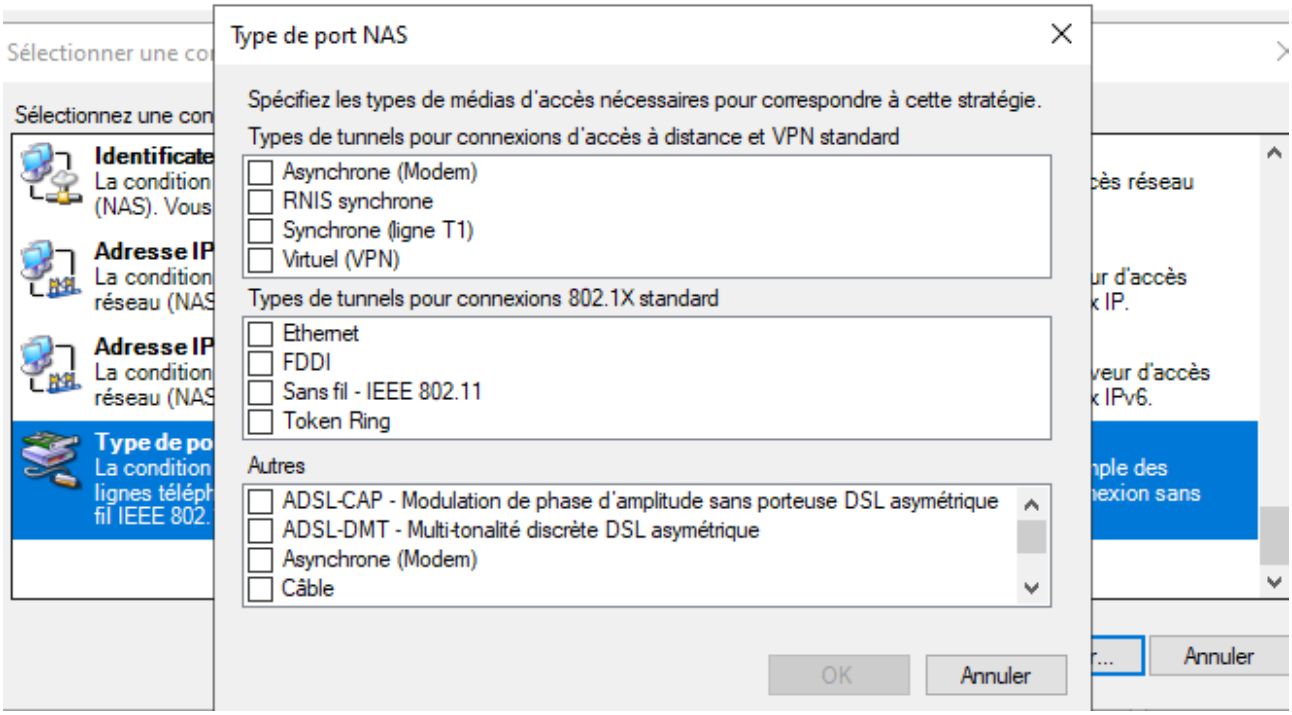
Je clique sur suivant puis je rajoute une condition et on sélectionne groupe Windows



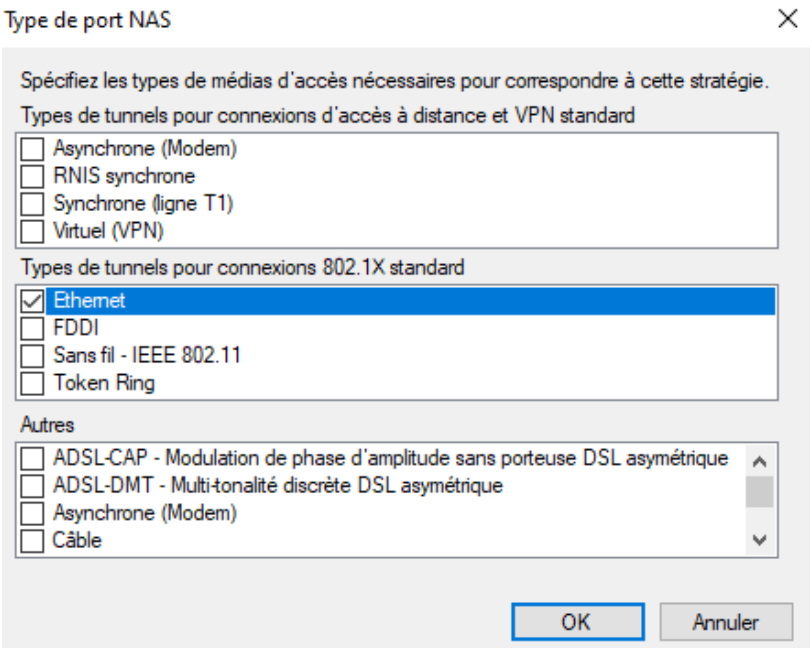
J’ajoute le groupe prof



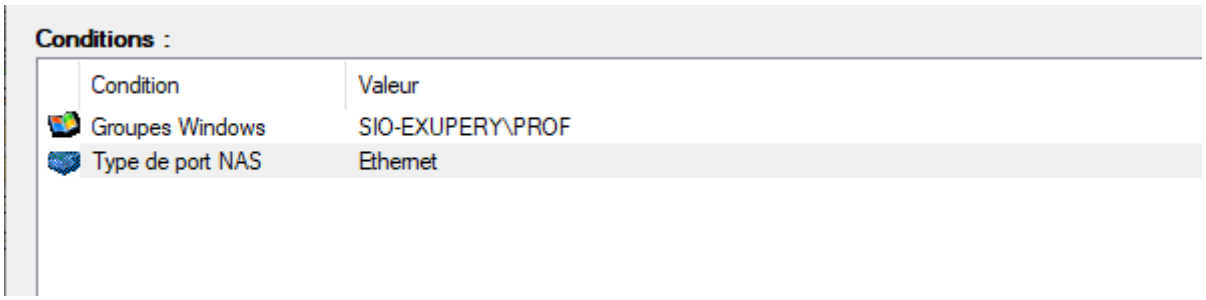
J’ajoute une deuxième condition pour spécifier le type de port NAS.



Je coche ethernet

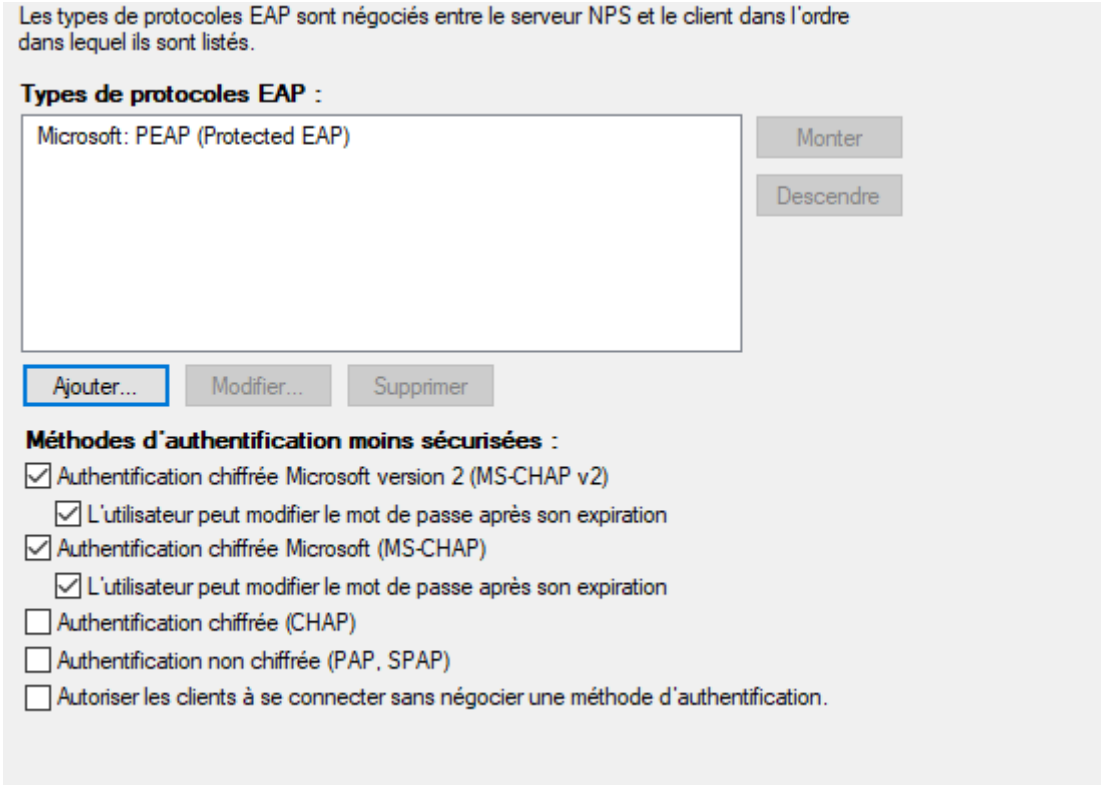


Les deux conditions on bien été ajouter

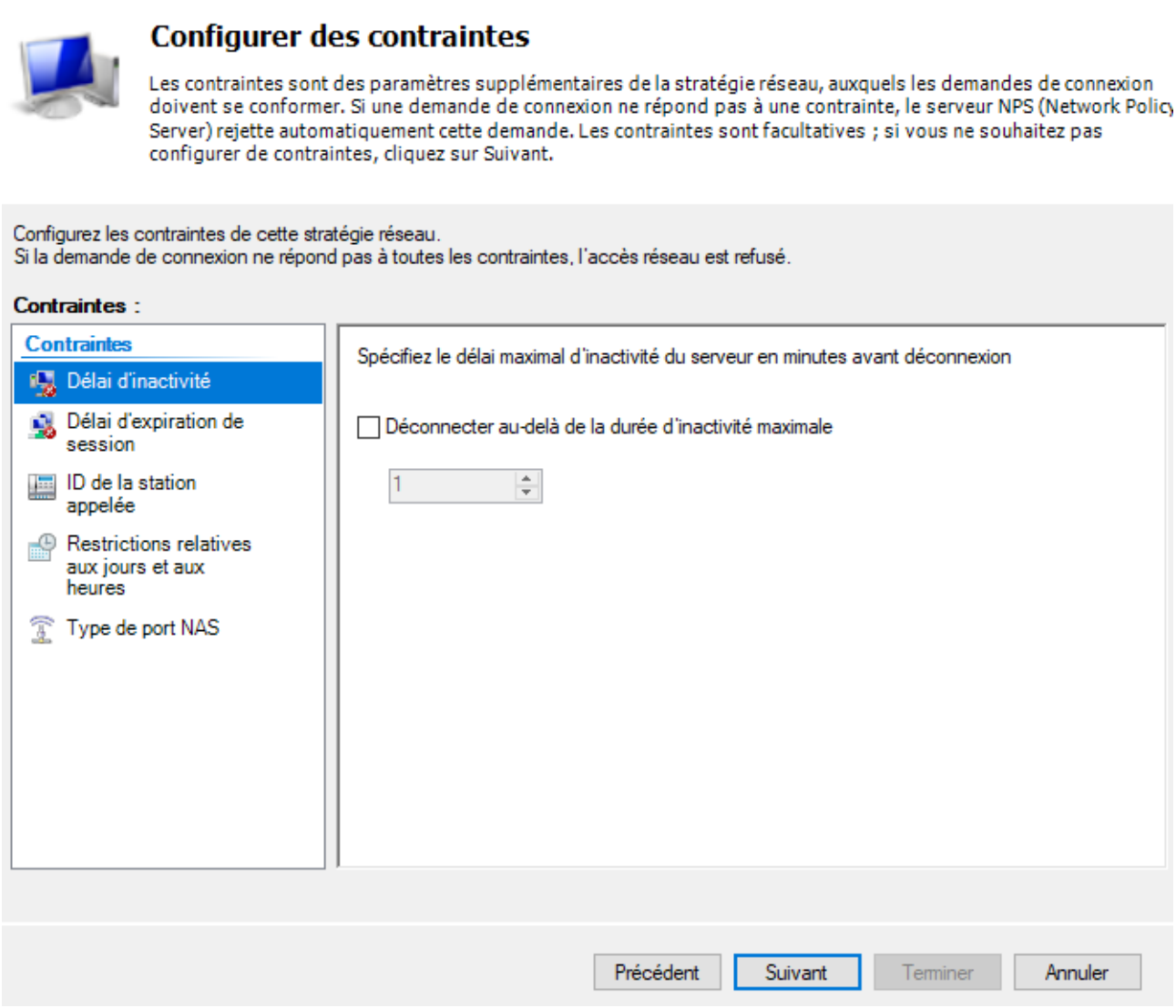


on clique sur suivant on garde accès accordé

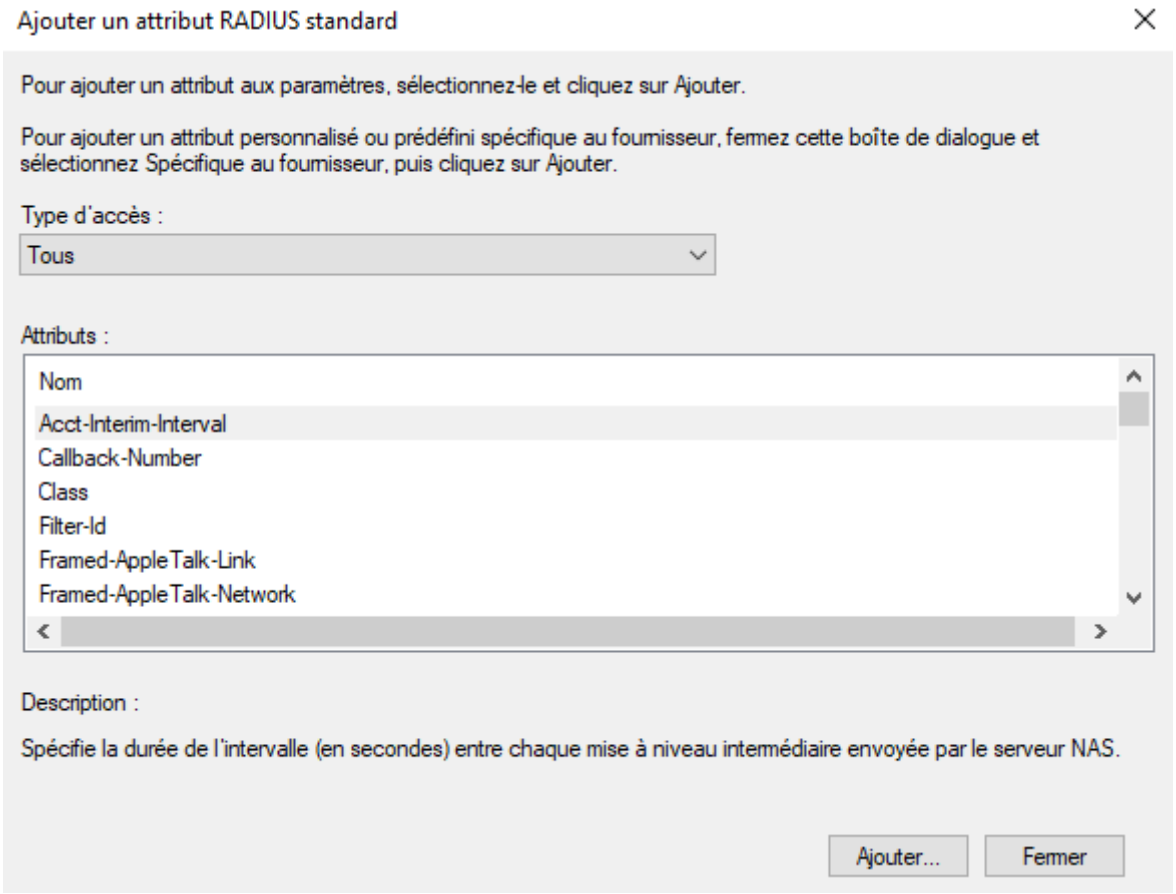
Dans l’écran Configurer les méthodes d’authentification, je déclare le type de protocoles EAP (PEAP) en cliquant sur Ajouter



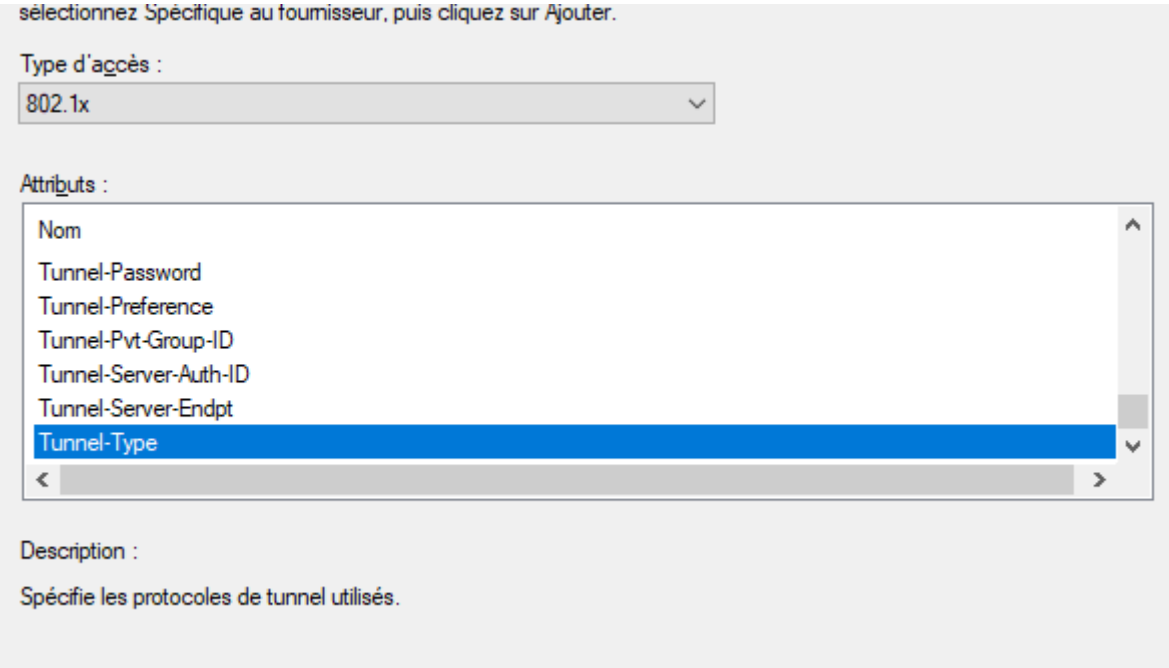
Dans l’écran Configurer des contraintes, je clique sur Suivant


Configurer des contraintes
Les contraintes sont des paramètres supplémentaires de la stratégie réseau, auxquels les demandes de connexion doivent se conformer. Si une demande de connexion ne répond pas à une contrainte, le serveur NPS (Network Policy Server) rejette automatiquement cette demande. Les contraintes sont facultatives ; si vous ne souhaitez pas configurer de contraintes, cliquez sur Suivant.
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
Délai d'inactivité
Délai d'expiration de session
ID de la station appelée
Restrictions relatives aux jours et aux heures
Type de port NAS
Spécifiez le délai maximal d'inactivité du serveur en minutes avant déconnexion
Déconnecter au-delà de la durée d'inactivité maximale
1
Précédent
Suivant
Terminer
Annuler

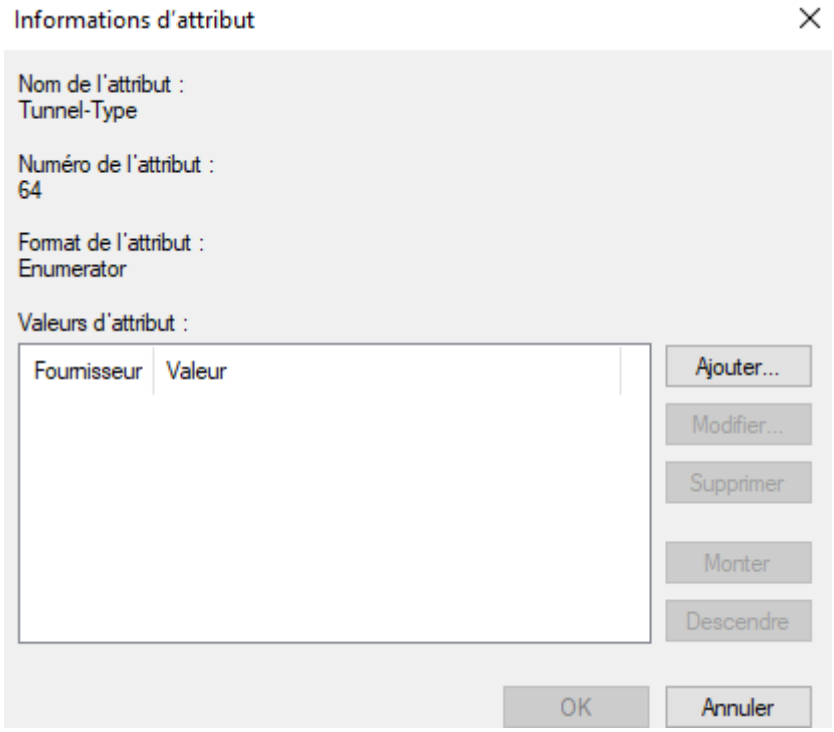
Dans l’écran Configurer les paramètres,je clique sur Ajouter pour envoyer des attributs au client RADIUS.



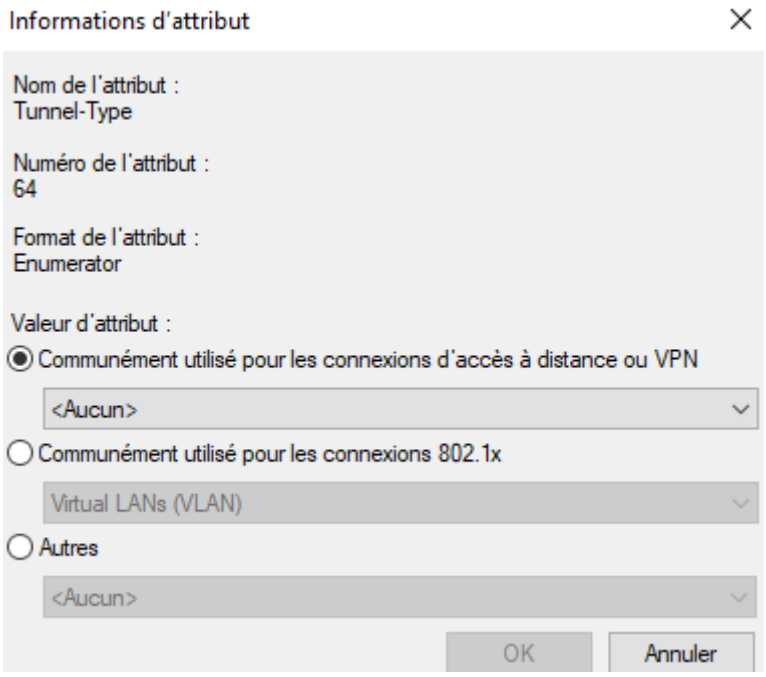
Je sélectionne 802.1x dans Type d’accès puis sélectionnez l’attribut Tunnel-Type et cliquez sur Ajouter.



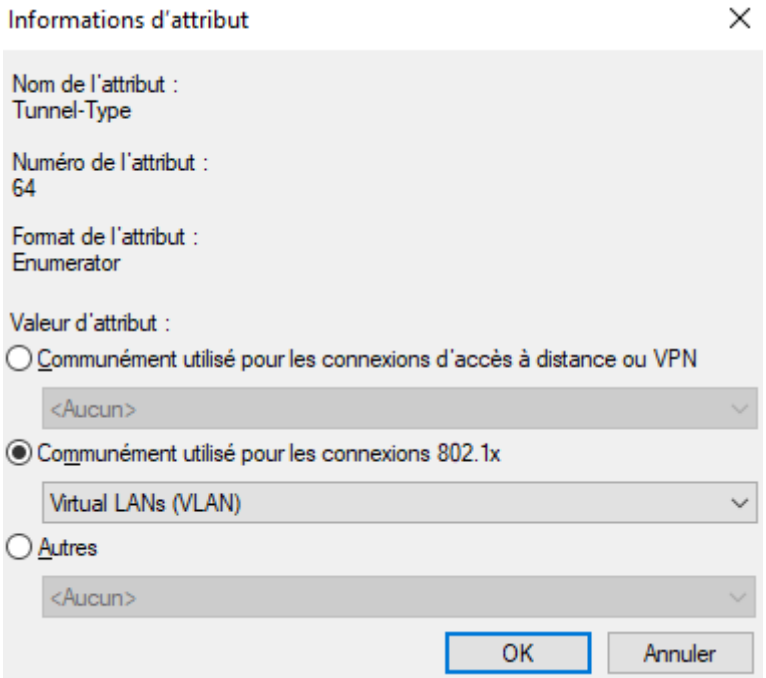
Je clique sur Ajouter



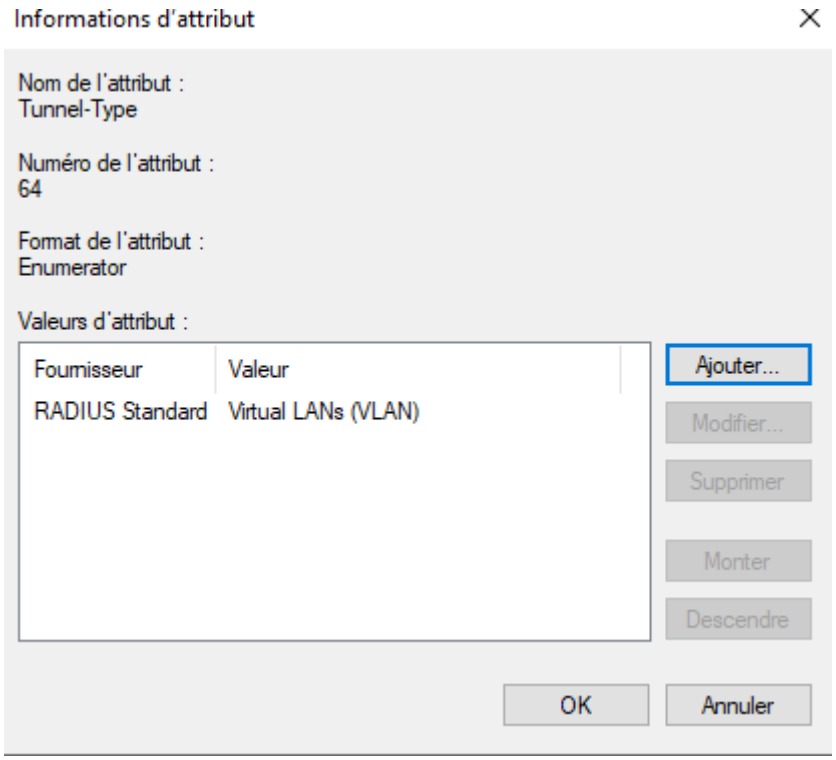
On clique encore sur ajouter



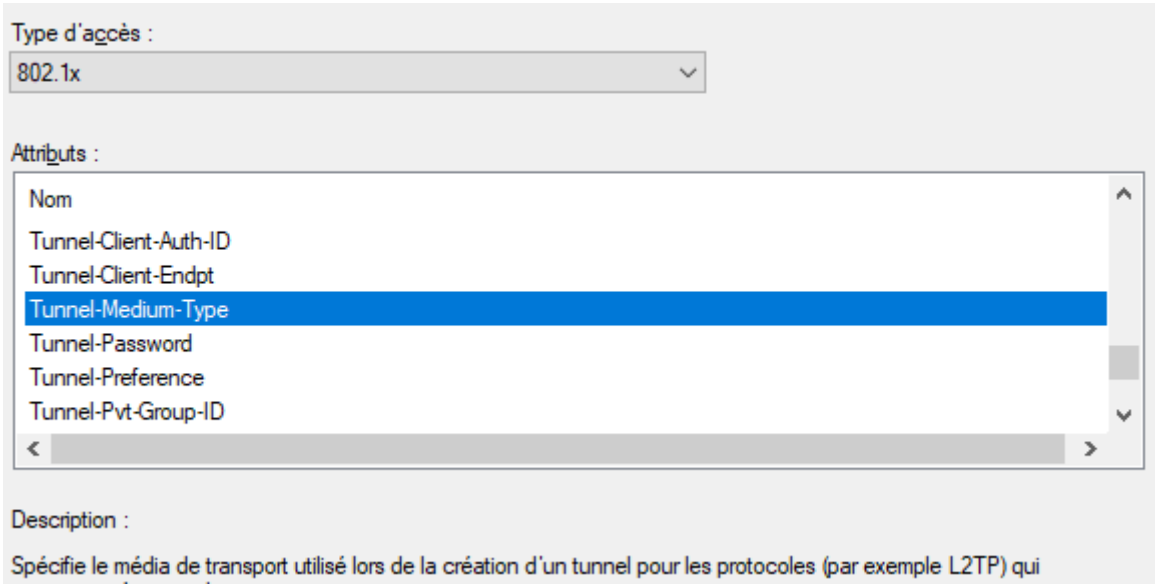
Je sélectionne Virtual LANs (VLAN) dans Communément utilisé pour les connexions 802.1x



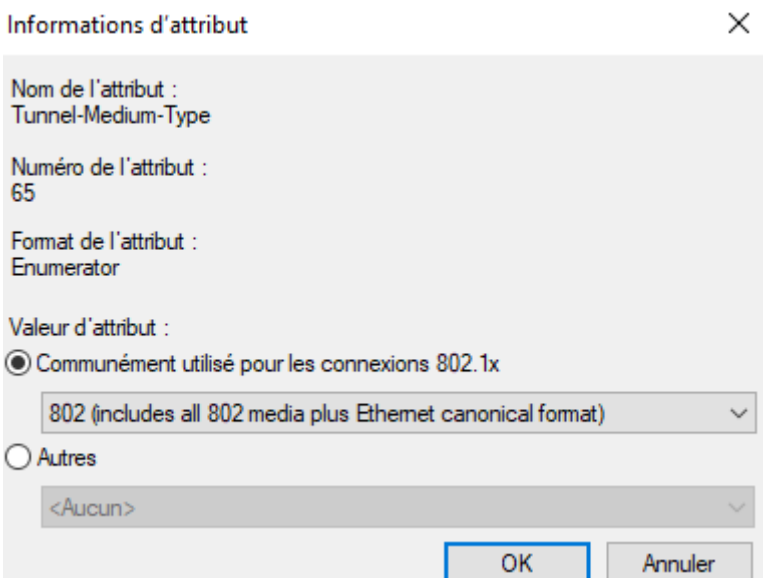
Je clique sur OK



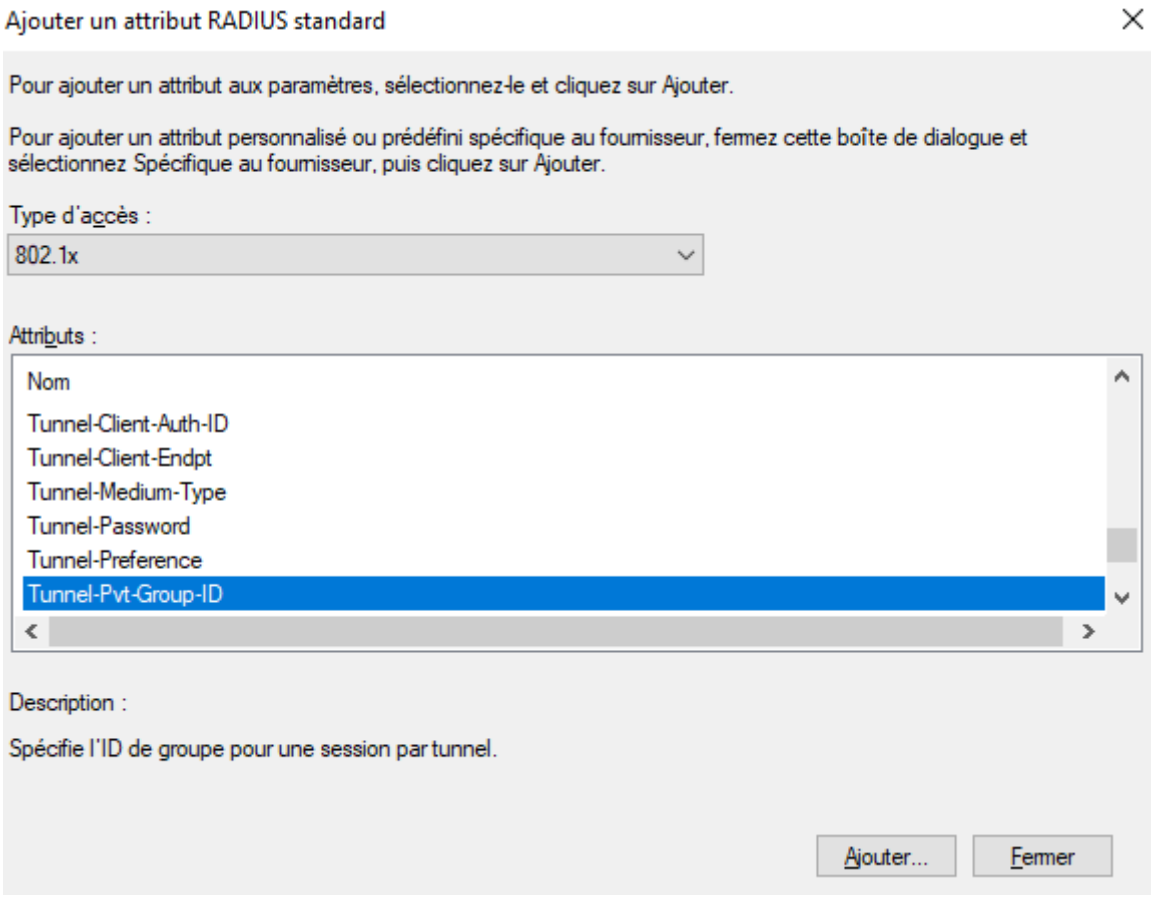
On procède de la même manière pour Tunnel-medium-type



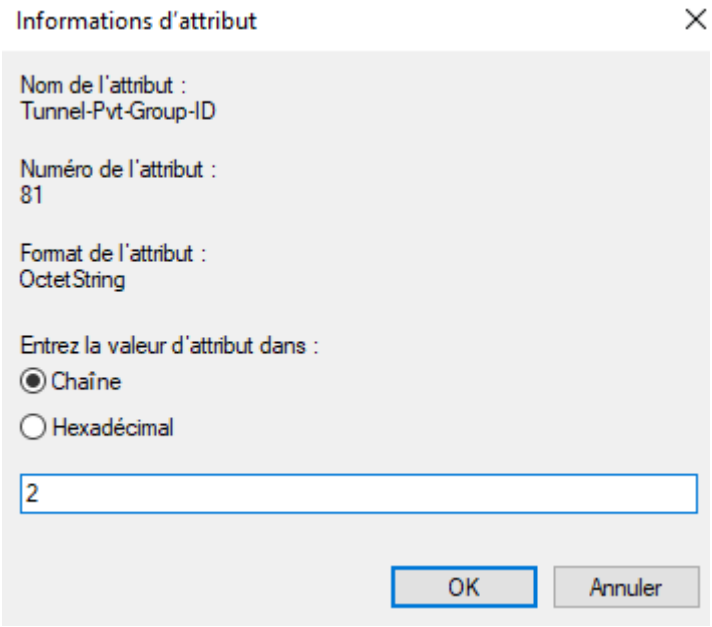
Je sélectionne 802,,,



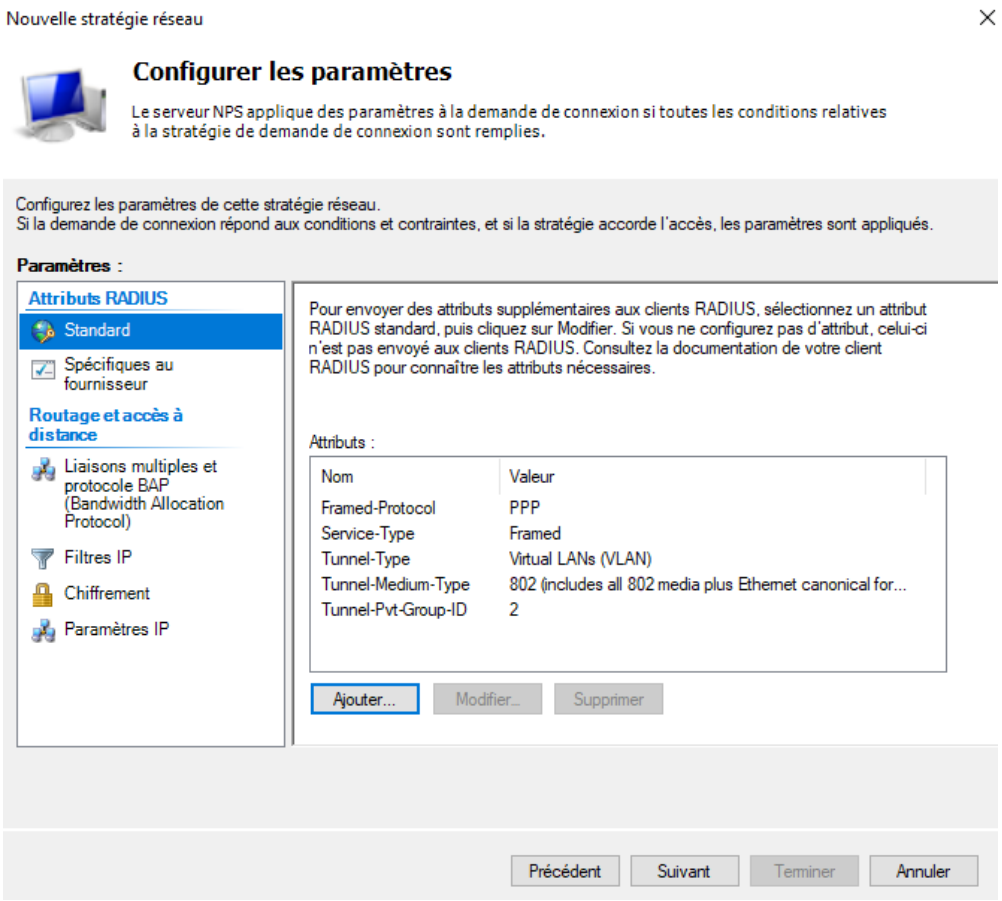
Je sélectionne ensuite tunnel-PVT-GROUP-ID



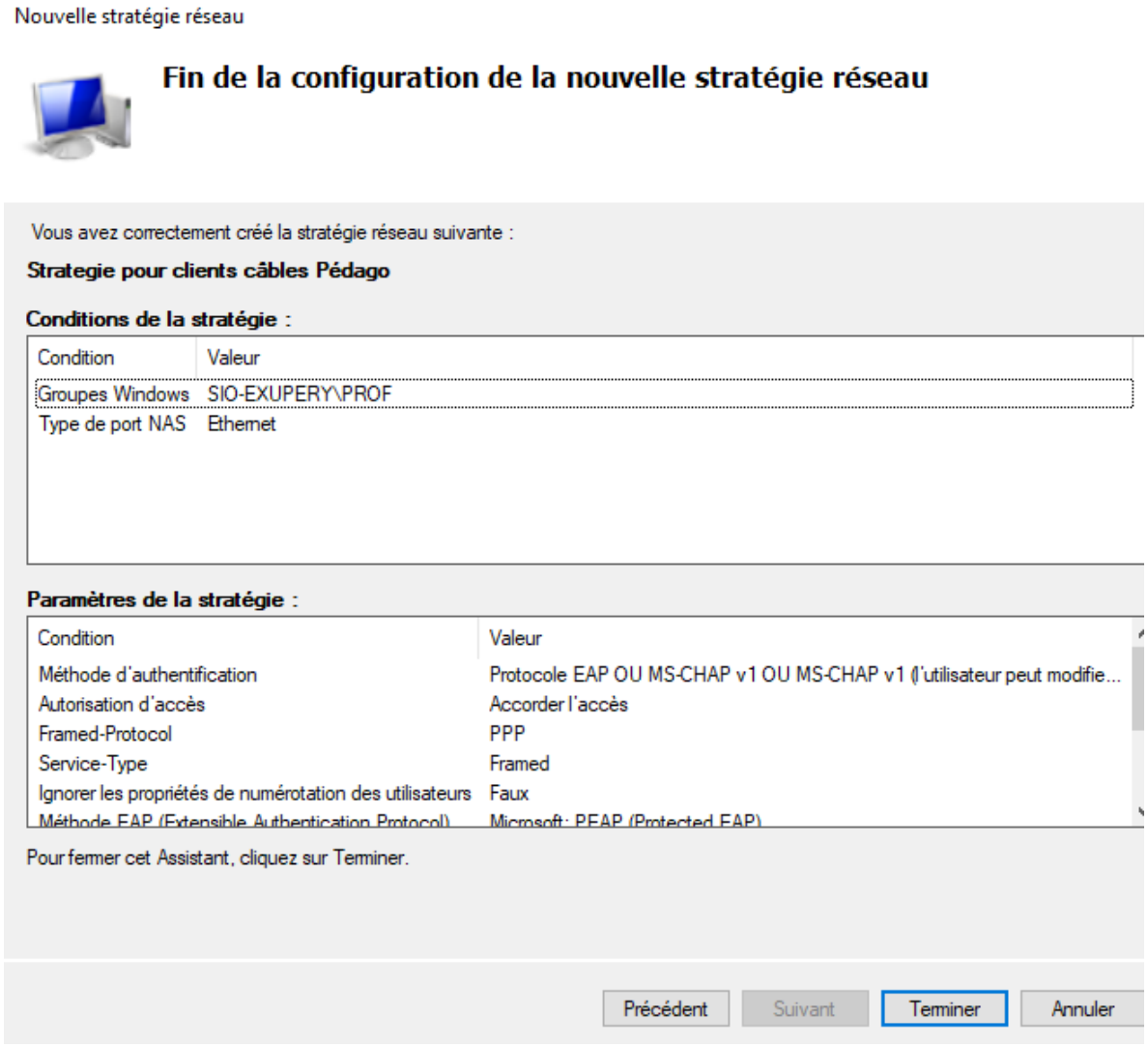
Je spécifie le numéro de VLAN dans lequel on veut positionner les membres du groupe Prof



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

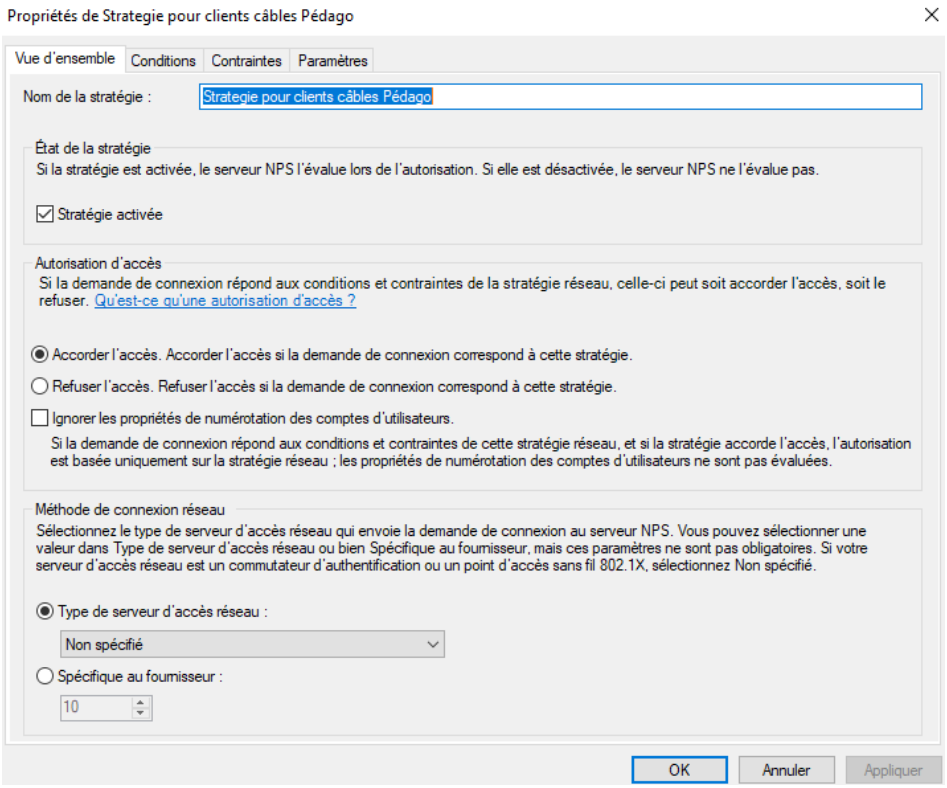


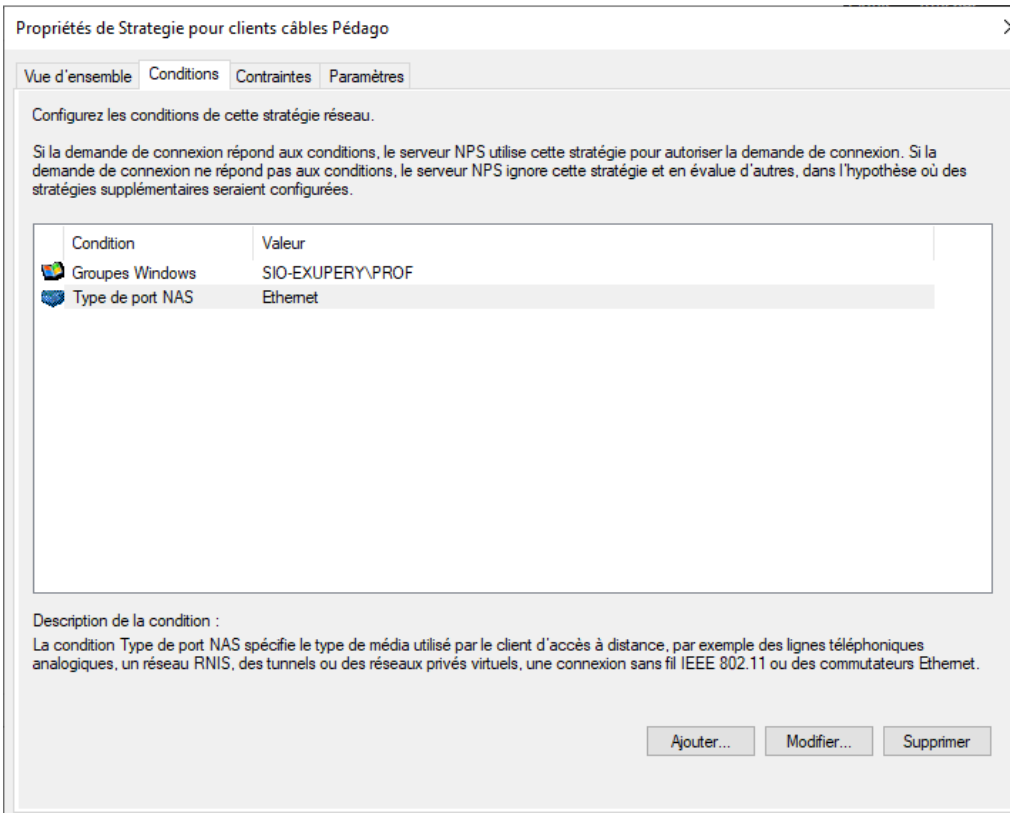
Je clique sur Terminer dans l’écran Fin de la configuration de la nouvelle stratégie réseau.

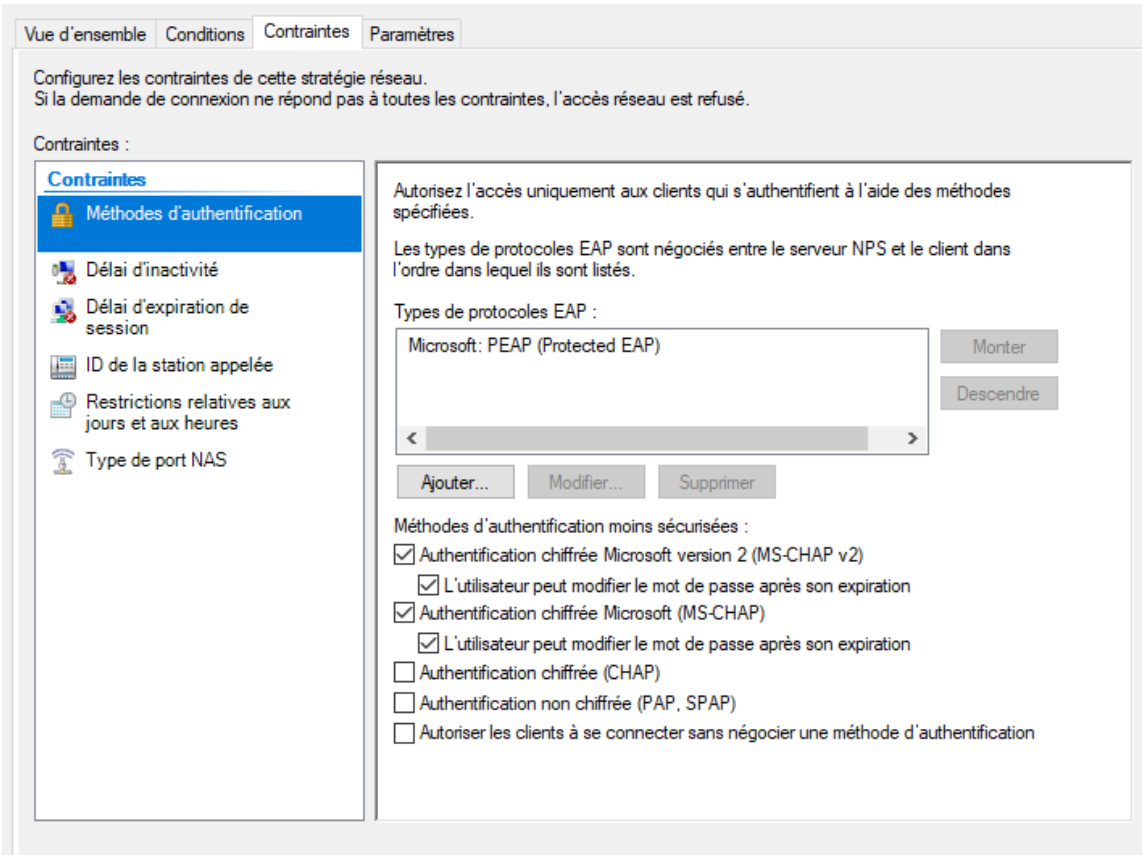


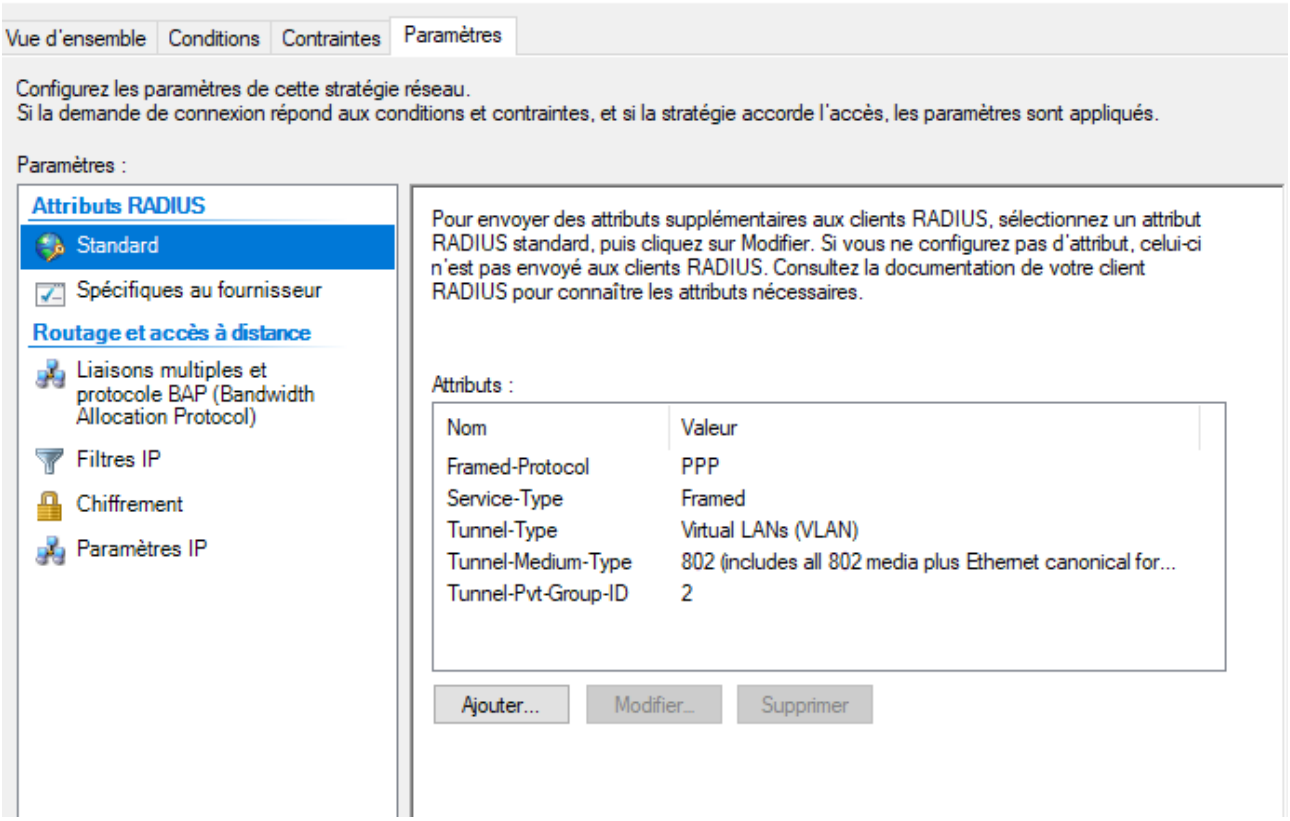
J'ai mis en place sur le serveur NPS :
Une stratégie de demande de connexion associée aux connexions filaire Ethernet ;
Une stratégie d'accès réseau Ethernet 802.1x plaçant dans le VLAN2 les membres authentifiés comme faisant partie du groupe Prof
Précisant le groupe autorisé (Prof) ainsi que la stratégie de demande de connexion (NAS Ethernet) : notion de condition ;
Précisant la méthode d'authentification (PEAP/MSCHAPV2) : notion de contrainte ;
Précisant les paramètres renvoyés au client radius (VLAN) : notion d'attribut.

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

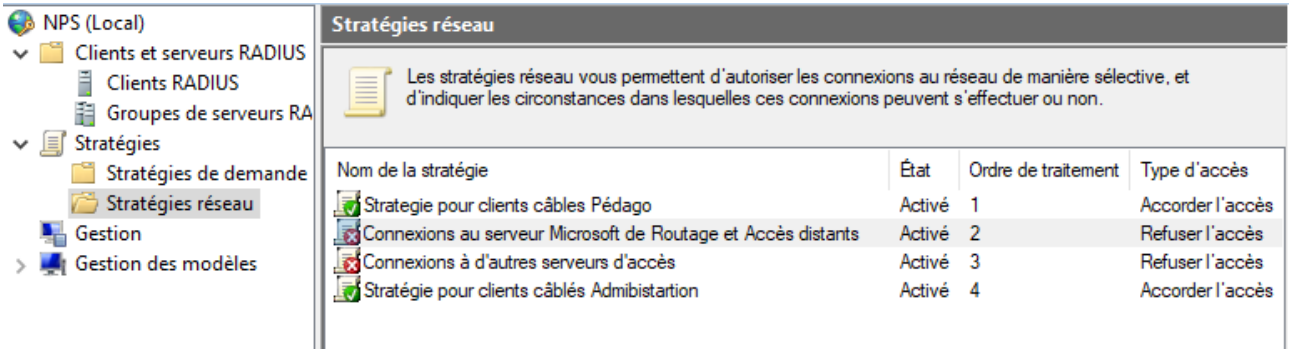





Vue d'ensemble
Conditions
Contraintes
Paramètres
Configurez les contraintes de cette stratégie réseau.
Si la demande de connexion ne répond pas à toutes les contraintes, l'accès réseau est refusé.
Contraintes :
Contraintes
Méthodes d'authentification
Délai d'inactivité
Délai d'expiration de session
ID 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

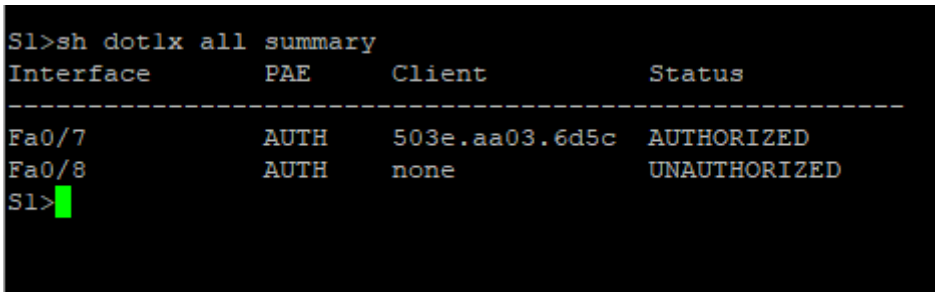


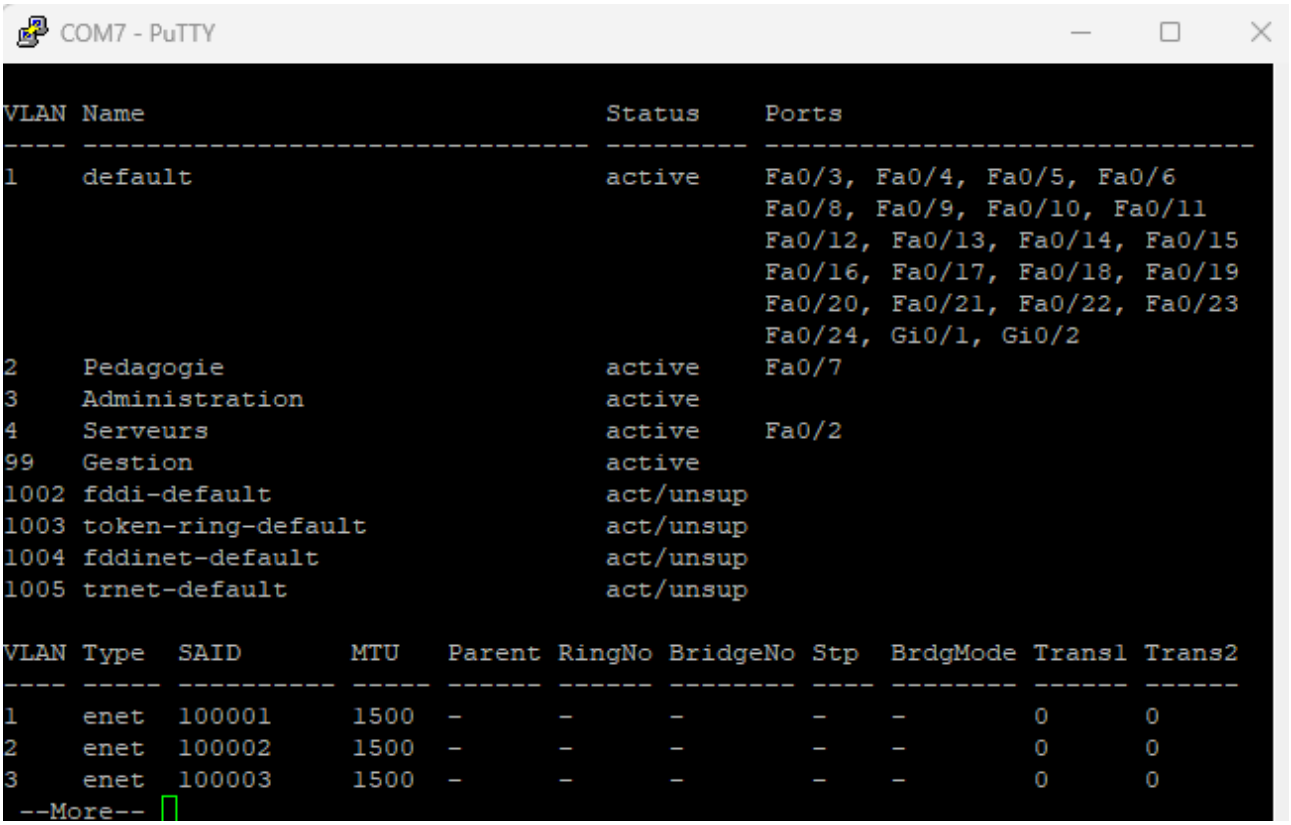
Je définis de manière analogue une stratégie d'accès réseau plaçant dans le VLAN3 les membres authentifiés comme faisant partie du groupe Direction



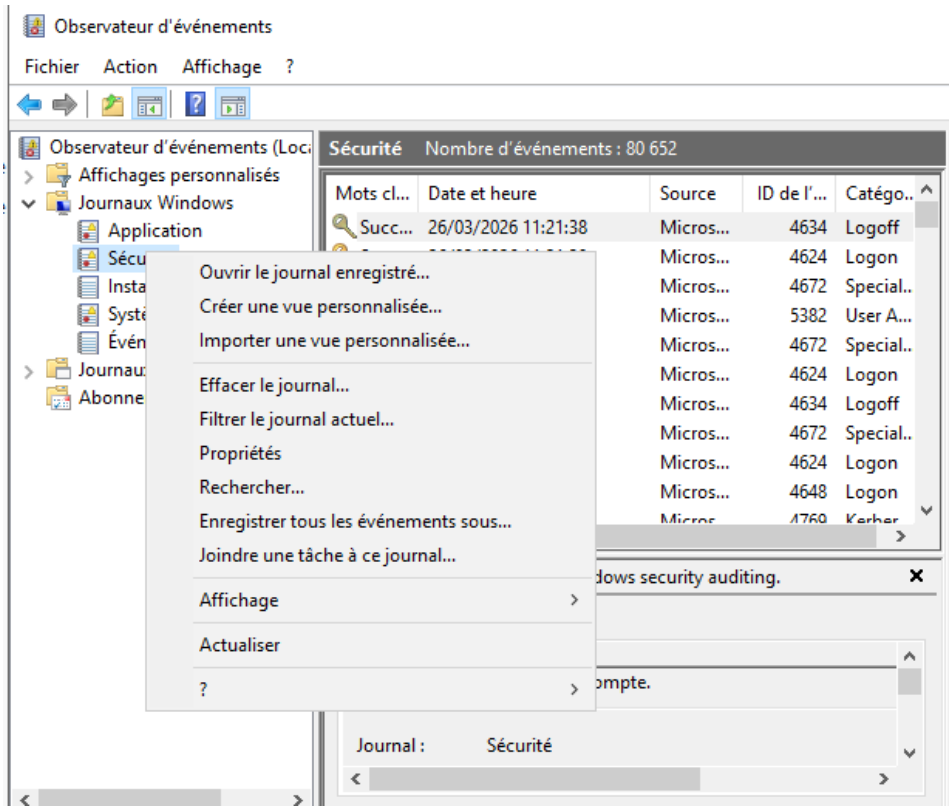
REVOIR L'ORDRE DES SCREEN

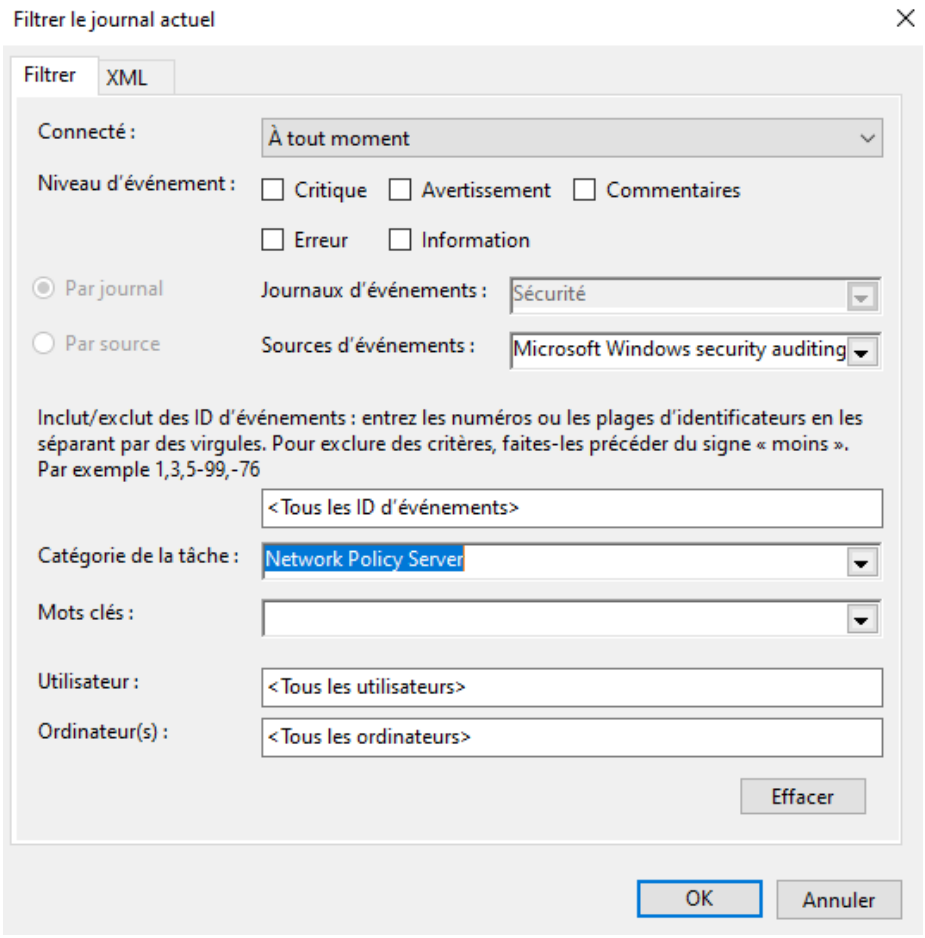
Commutateur client Radius

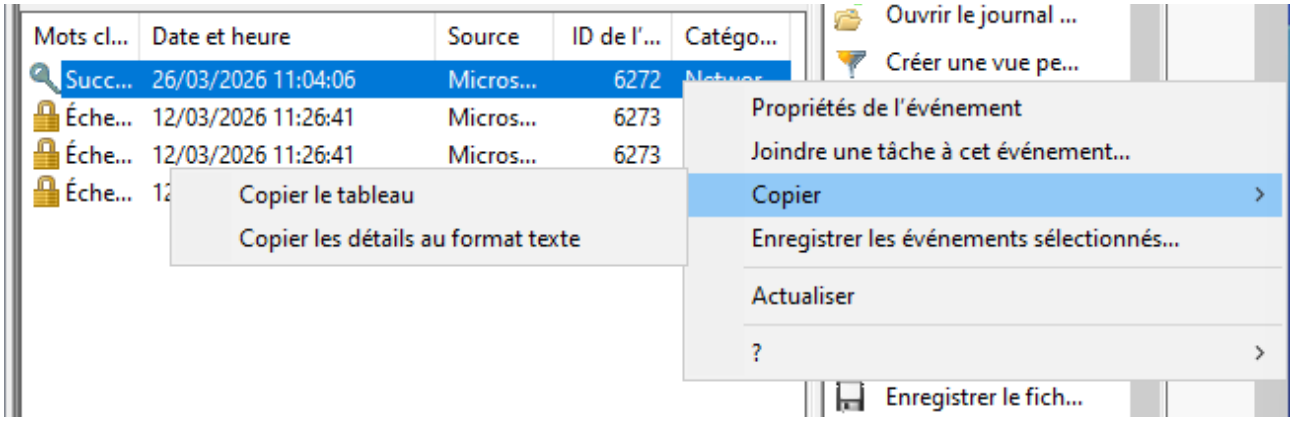

S1>sh dot1x all summary
Interface PAE Client Status
Fa0/7 AUTH 503e.aa03.6d5c AUTHORIZED
Fa0/8 AUTH none UNAUTHORIZED
S1>



Exportation du fichier XML depuis l'AD




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


Mots cl...
Date et heure
Source
ID de l'...
Catégo...
Succ...
26/03/2026 11:04:06
Micros...
6272
Éche...
12/03/2026 11:26:41
Micros...
6273
Éche...
12/03/2026 11:26:41
Micros...
6273
Éche...
Copier le tableau
Copier les détails au format texte
Ouvrir le journal ...
Créer une vue pe...
Propriétés de l'événement
Joindre une tâche à cet événement...
Copier
Enregistrer les événements sélectionnés...
Actualiser
?
Enregistrer le fich...

Nom du journal :Security
Source : Microsoft-Windows-Security-Auditing
Date : 26/03/2026 11:04:06
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/Professeurs/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-F7-8C-87
Identificateur de la station appelante : 50-3E-AA-03-6D-5C

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-Cisco2960
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 : Strategie pour clients câbles 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.

J’installe wireshark et j’effectue une capture de trames radius pendant une connexion entre le serveur radius et le client radius

No.	Time	Source	Destination	Protocol	Lengtl	Info
75	48.616877	192.168.0.2	192.168.1.50	RADIUS	282	Access-Request id=31
76	48.619412	192.168.1.50	192.168.0.2	RADIUS	132	Access-Challenge id=31
77	48.626054	192.168.0.2	192.168.1.50	RADIUS	514	Access-Request id=32
78	48.626464	192.168.1.50	192.168.0.2	RADIUS	277	Access-Challenge id=32
79	48.635258	192.168.0.2	192.168.1.50	RADIUS	371	Access-Request id=33
80	48.635770	192.168.1.50	192.168.0.2	RADIUS	232	Access-Challenge id=33
81	48.646634	192.168.0.2	192.168.1.50	RADIUS	356	Access-Request id=34
82	48.646869	192.168.1.50	192.168.0.2	RADIUS	162	Access-Challenge id=34
83	48.653733	192.168.0.2	192.168.1.50	RADIUS	351	Access-Request id=35
84	48.653953	192.168.1.50	192.168.0.2	RADIUS	177	Access-Challenge id=35
85	48.661246	192.168.0.2	192.168.1.50	RADIUS	361	Access-Request id=36
86	48.661837	192.168.1.50	192.168.0.2	RADIUS	185	Access-Challenge id=36
87	48.670845	192.168.0.2	192.168.1.50	RADIUS	405	Access-Request id=37
88	48.671772	192.168.1.50	192.168.0.2	RADIUS	208	Access-Challenge id=37
89	48.679317	192.168.0.2	192.168.1.50	RADIUS	347	Access-Request id=38
90	48.704826	192.168.1.50	192.168.0.2	RADIUS	232	Access-Challenge id=38
91	48.712612	192.168.0.2	192.168.1.50	RADIUS	416	Access-Request id=39
92	48.713151	192.168.1.50	192.168.0.2	RADIUS	346	Access-Accept id=39

Je recense au travers d’une capture les différents types de message radius