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

Sommaire

Anexe 1 : Commutateur Cisco 2960 et authentification 802.1x

Je configure le commutateur :

- Je créer les différents vlan :

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, 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    VLAN0002                          active
3    VLAN0003                          active
4    VLAN0004                          active
99   VLAN0099                          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
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
2    enet  100002     1500  -      -      -        -    -        0      0
```

- Je mets en place l'authentification 802.1x sur le commutateur :

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#aaa new-mo
Switch(config)#aaa new-model
Switch(config)#aaa au
Switch(config)#aaa authen
Switch(config)#aaa authentication dotlx de
Switch(config)#aaa authentication dotlx default g
Switch(config)#aaa authentication dotlx default group radius
Switch(config)#aaa auth
Switch(config)#aaa auth
Switch(config)#aaa authau
Switch(config)#aaa authoriza
Switch(config)#aaa authorization ne
Switch(config)#aaa authorization network de
Switch(config)#aaa authorization network default grou
Switch(config)#aaa authorization network default group radius
Switch(config)#dotlx system-auth-control
Switch(config)#
```

```
Switch(config)#int f0/8
Switch(config-if)#switch
Switch(config-if)#switchport mode access
Switch(config-if)#ath
Switch(config-if)#auth
Switch(config-if)#authentication port
Switch(config-if)#authentication port-control auto
Switch(config-if)#dot
*Mar  1 00:15:53.147: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/8, changed state to downlx pae au
Switch(config-if)#dotlx pae authenticator
Switch(config-if)#
```

- J'affiche les informations de l'authentification 802.1x :

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

Dot1x Info for FastEthernet0/8
----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = SINGLE_HOST
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30

Switch#show dot1x all summary
Interface       PAE     Client          Status
---------------------------------------------------
Fa0/8           AUTH    309c.23a5.900d  UNAUTHORIZED
Switch#
```

- Je configure le reste :

```
Switch(config)#radius-server host 192.168.1.50 auth-port 1812 acct-port 191
*Mar  2 21:46:48.770: %DOT1X-5-FAIL: Authentication failed for client (309c.23a5.900d) on Interface Fa0/8 AuditSessi
nID
*Mar  2 21:46:48.770: %AUTHMGR-7-RESULT: Authentication result 'no-response' from 'dot1x' for client (309c.23a5.900d)
 on Interface Fa0/8 AuditSessionID 000000000000000409C800FB
*Mar  2 21:46:48.770: %AUTHMGR-7-FAILOVER: Failing over from 'dot1x' for client (309c.23a5.900d) on Interface Fa0/8 A
uditSessionID 000000000000000409C800FB
*Mar  2 21:46:48.770: %AUTHMGR-7-NOMOREMETHODS: Exhausted all authentication methods for client (309c.23a5.900d) on I
nterface Fa0/8 AuditSessionID 000000000000000409C800FB
*Mar  2 21:46:48.770: %AUTHMGR-5-FAIL: Authorization failed for client (309c.23a5.900d) on Interface Fa0/8 AuditSessi
onID 000000000000000409C800FB
Switch(config)#$2.168.1.50 auth-port 1812 acct-port 1813 key sio1234567
Switch(config)#int f0/7
Switch(config-if)#switchport mode access
*Mar  2 21:47:49.495: %AUTHMGR-5-START: Starting 'dot1x' for client (309c.23a5.900d) on Interface Fa0/8 AuditSessionI
D 000000000000000409C800FB
Switch(config-if)#authentification port-control auto
                 ^
% Invalid input detected at '^' marker.

Switch(config-if)#authentication port-control auto
Switch(config-if)#dot1x pae authentificator
                            ^
% Invalid input detected at '^' marker.

Switch(config-if)#dot1x pae authenticator
Switch(config-if)#int f0/8
Switch(config-if)#swit
Switch(config-if)#switchport mode access
Switch(config-if)#authentification port-control auto
                 ^
% Invalid input detected at '^' marker.

Switch(config-if)#authentication port-control auto
Switch(config-if)#dot1x pae authenticator
Switch(config-if)#
```

- Et enfin j'affiche la configuration du commutateur :

```
Switch#sh dot1x all
Sysauthcontrol              Enabled
Dot1x Protocol Version            3

Dot1x Info for FastEthernet0/7
----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = SINGLE_HOST
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30

Dot1x Info for FastEthernet0/8
----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = SINGLE_HOST
QuietPeriod               = 60

Switch#sh dot1x all
Sysauthcontrol              Enabled
Dot1x Protocol Version            3

Dot1x Info for FastEthernet0/7
----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = SINGLE_HOST
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30

Dot1x Info for FastEthernet0/8
----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = SINGLE_HOST
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30

ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30

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

Puis je configure le routeur :

- Je configure les différentes sous-interfaces du routeur :

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int g0/0
Router(config-if)#ip address 192.168.0.1 255.255.255.248
```

```
Router(config-if)#int g0/0.2
Router(config-subif)#ip address 192.168.1.1 255.255.255.240

% Configuring IP routing on a LAN subinterface is only allowed if that
subinterface is already configured as part of an IEEE 802.10, IEEE 802.1Q,
or ISL vLAN.

Router(config-subif)#enca
Router(config-subif)#encapsulation dot1Q 2
Router(config-subif)#
```

```
Router(config-subif)#int g0/0.3
Router(config-subif)#ip address 192.168.1.17 255.255.255.240

% Configuring IP routing on a LAN subinterface is only allowed if that
subinterface is already configured as part of an IEEE 802.10, IEEE 802.1Q,
or ISL vLAN.

Router(config-subif)#en
Router(config-subif)#encapsulation dot1q 3
Router(config-subif)#
```

```
Router(config-subif)#int g0/0.99
Router(config-subif)#ip address 192.168.1.33 255.255.255.240

% Configuring IP routing on a LAN subinterface is only allowed if that
subinterface is already configured as part of an IEEE 802.10, IEEE 802.1Q,
or ISL vLAN.

Router(config-subif)#eb
Router(config-subif)#en
Router(config-subif)#encapsulation dot1Q 99
Router(config-subif)#
```

```
Router(config-subif)#int g0/0.4
Router(config-subif)#ip address 192.168.1.49 255.255.255.248

% Configuring IP routing on a LAN subinterface is only allowed if that
subinterface is already configured as part of an IEEE 802.10, IEEE 802.1Q,
or ISL vLAN.

Router(config-subif)#enc
Router(config-subif)#encapsulation dot1Q 4
Router(config-subif)#
```

- Je définis les pools des différent vlan :

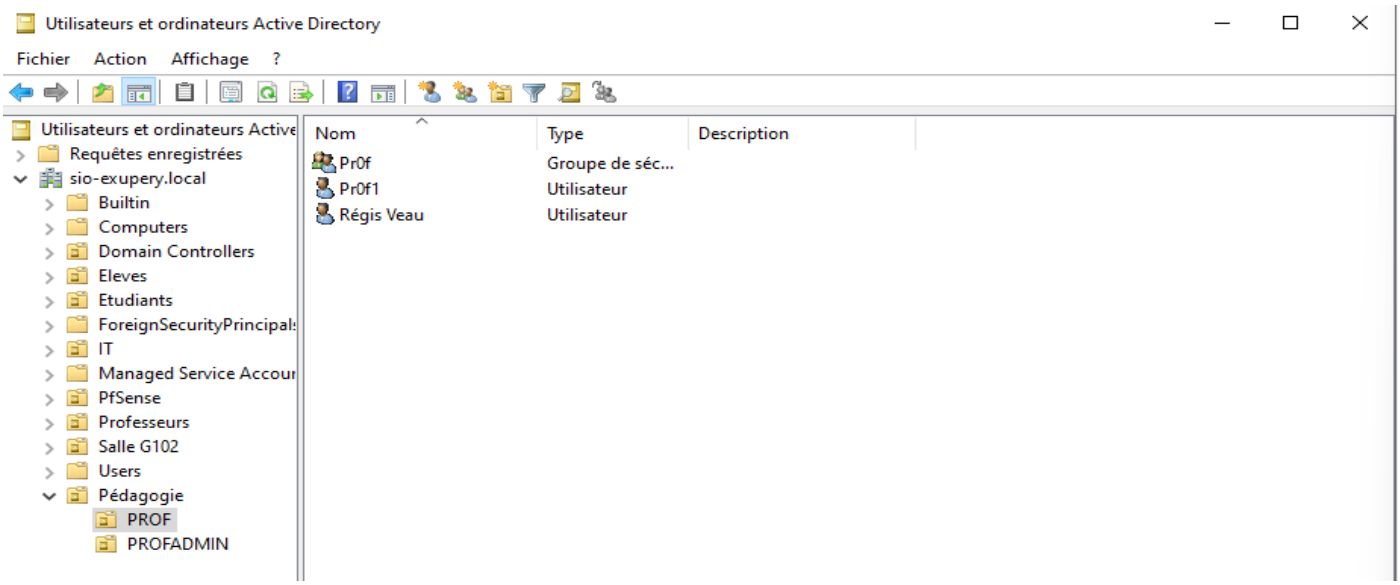
```
Router(config)#ip dhcp pool vlan2
Router(dhcp-config)#network 192.168.1.0 255.255.255.240
Router(dhcp-config)#default-router 192.168.1.1
Router(dhcp-config)#dns-server 192.168.1.50
Router(dhcp-config)#
```

```
Router(config)#ip dhcp pool vlan3
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)#
```

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

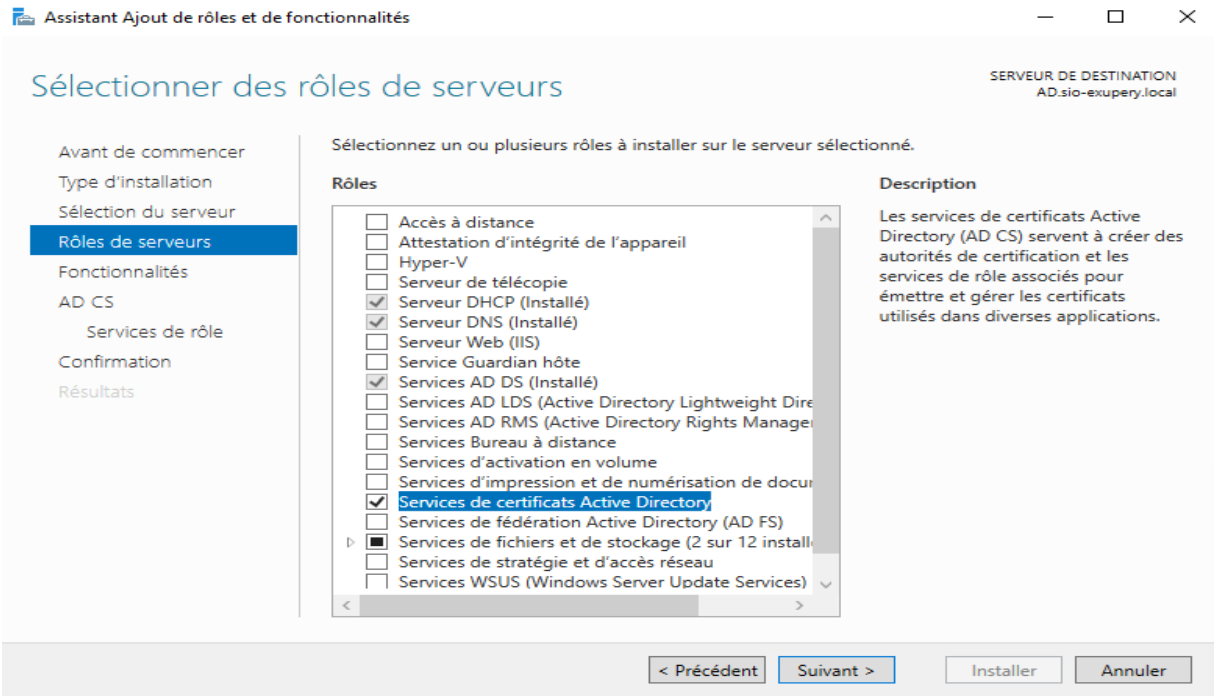
2.1 Situation de départ

- Je créer les deux unités d'organisations, avec les différents éléments à l'intérieur :

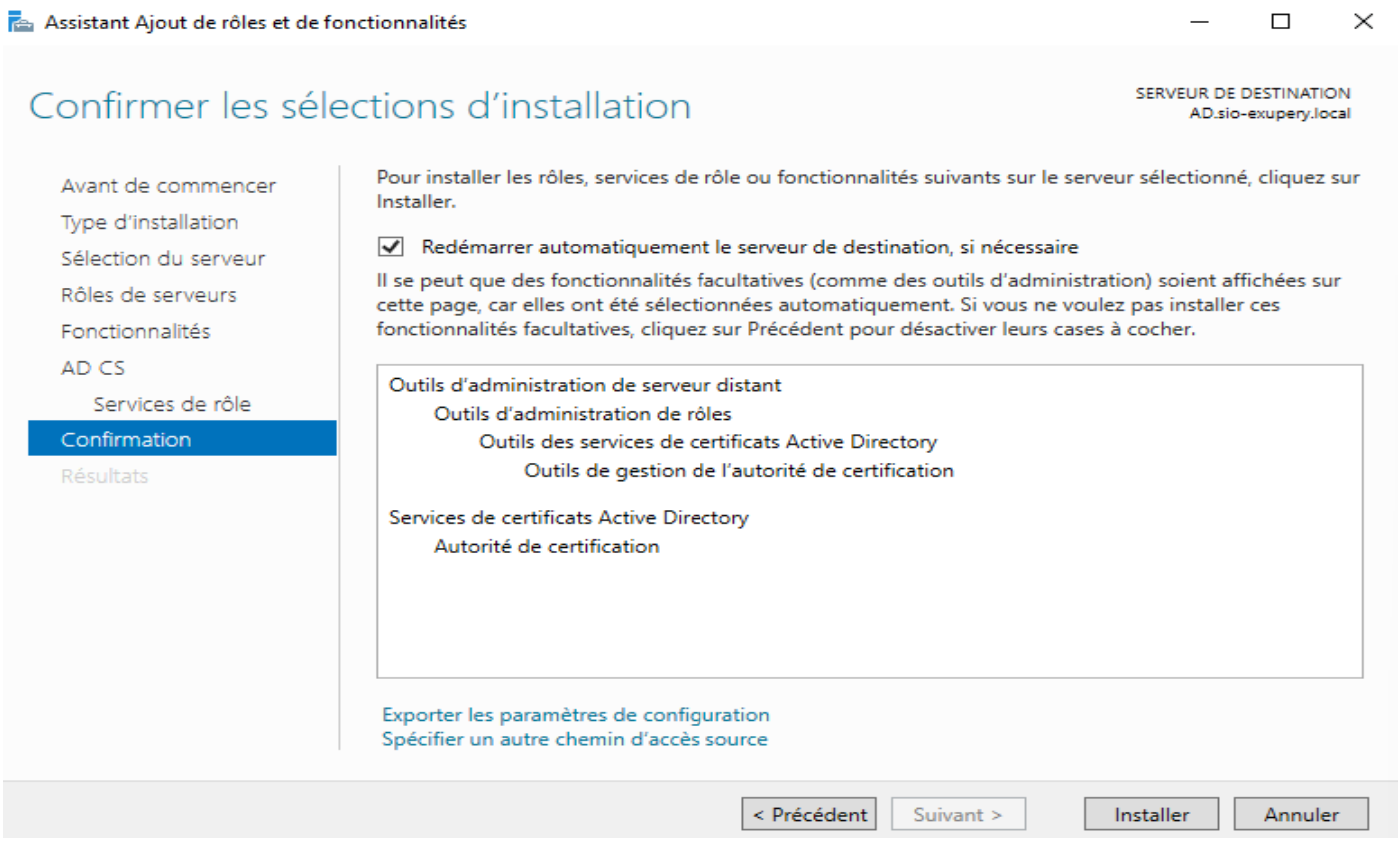


2.2 Ajout du rôle Services de certificats Active Directory

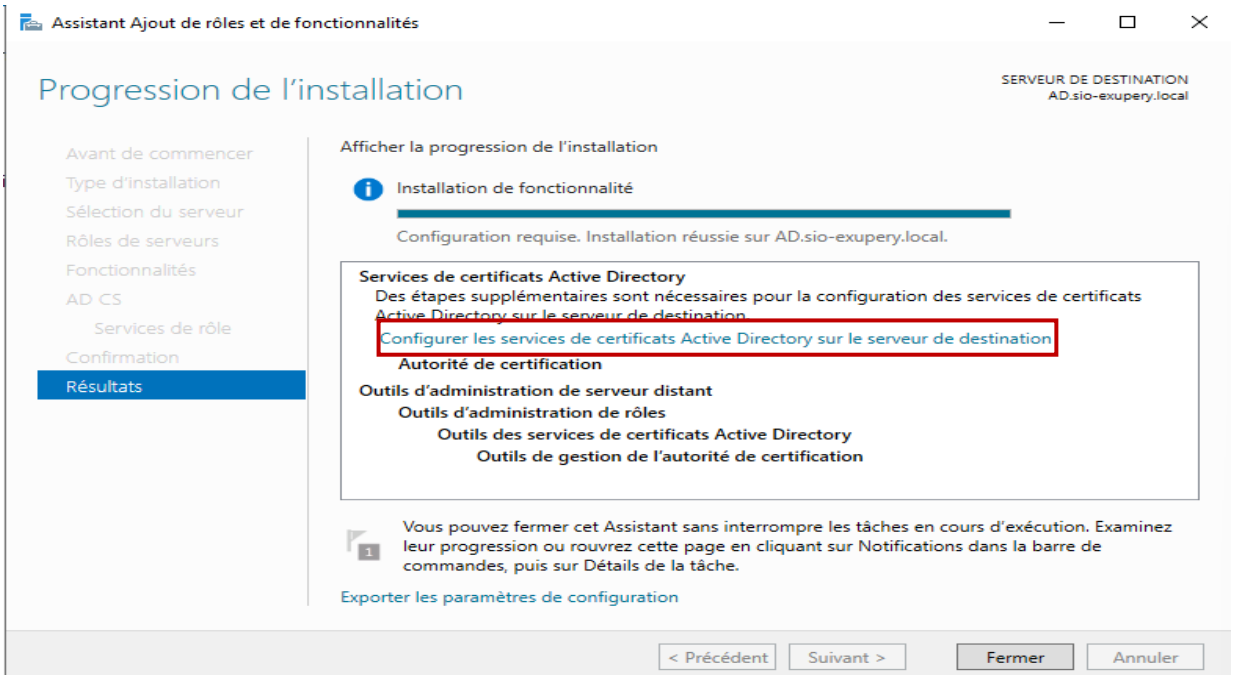
- J'ajoute le rôle Service de certificats Active Directory :



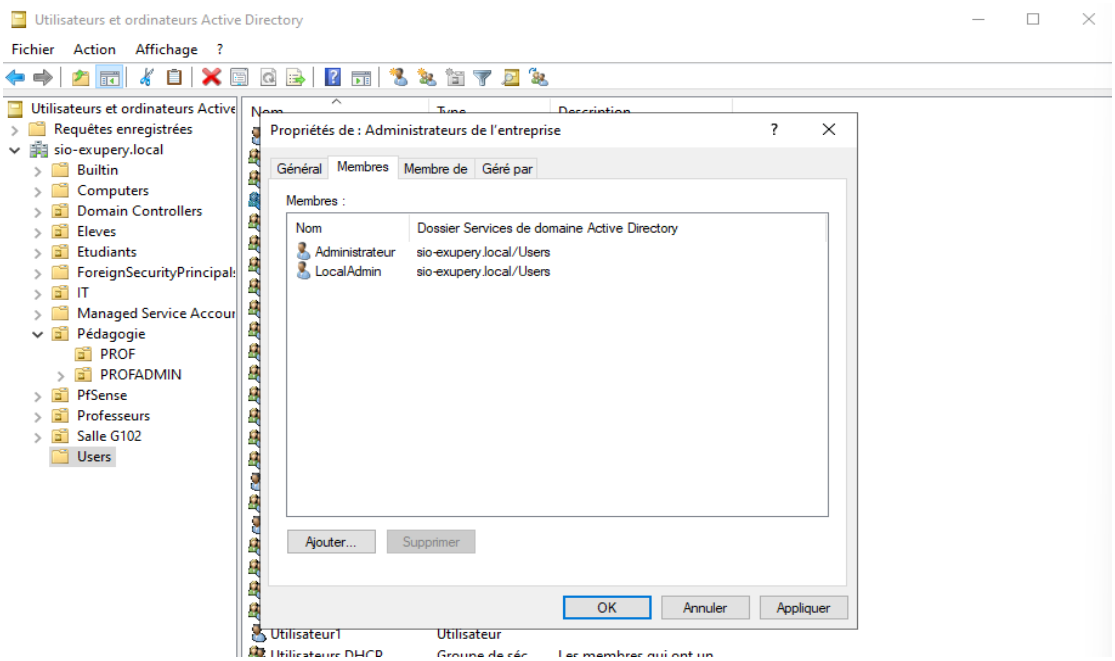
- Après avoir pris connaissance des informations de la page d'information AD CS, je clique sur suivant et je suis la procédure d'installation et j'appuis sur terminer :



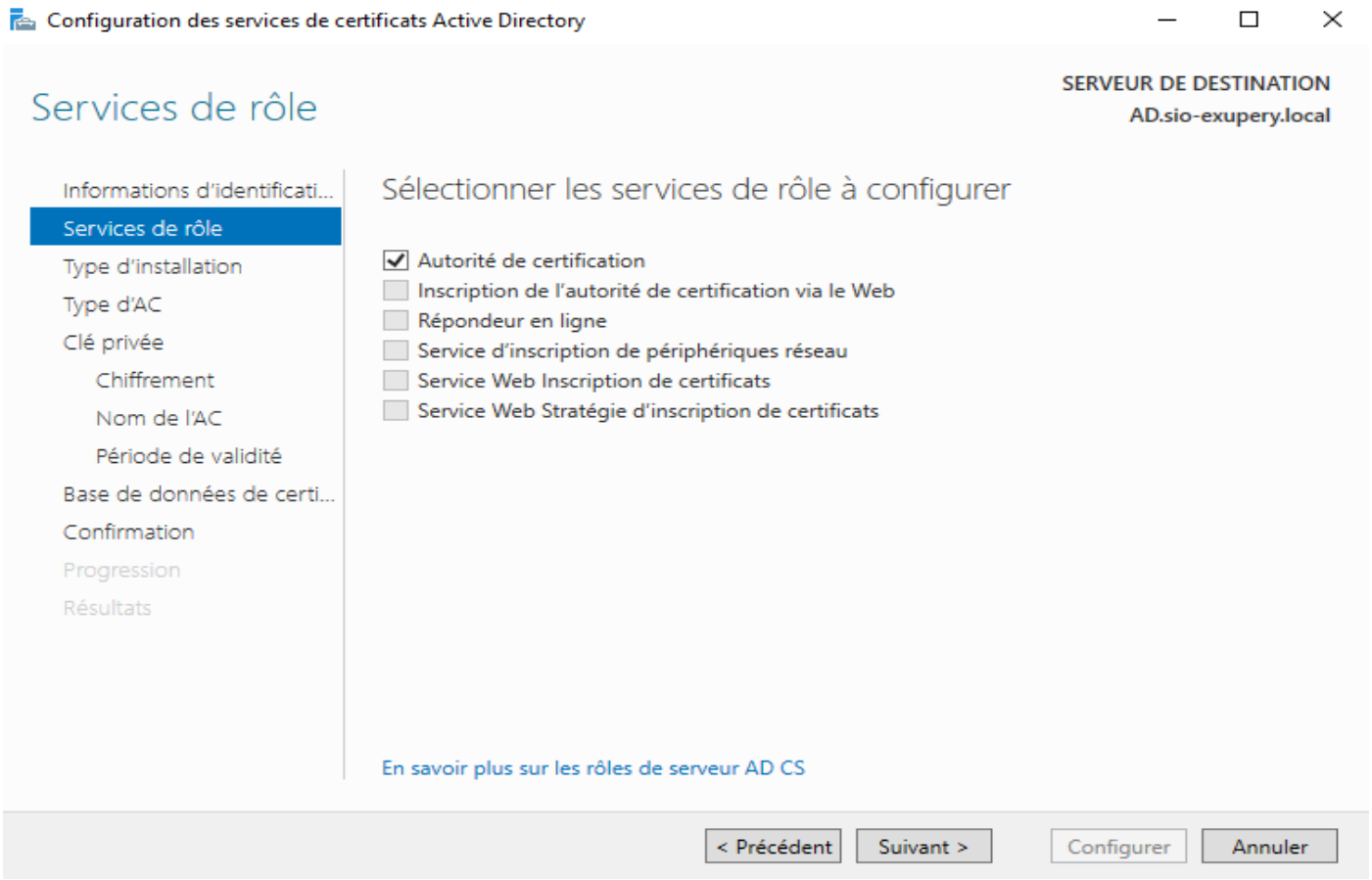
- Une fois l'installation terminée, je clique sur le lien Configurer les services de certificats Active Directory sur le serveur de destination :



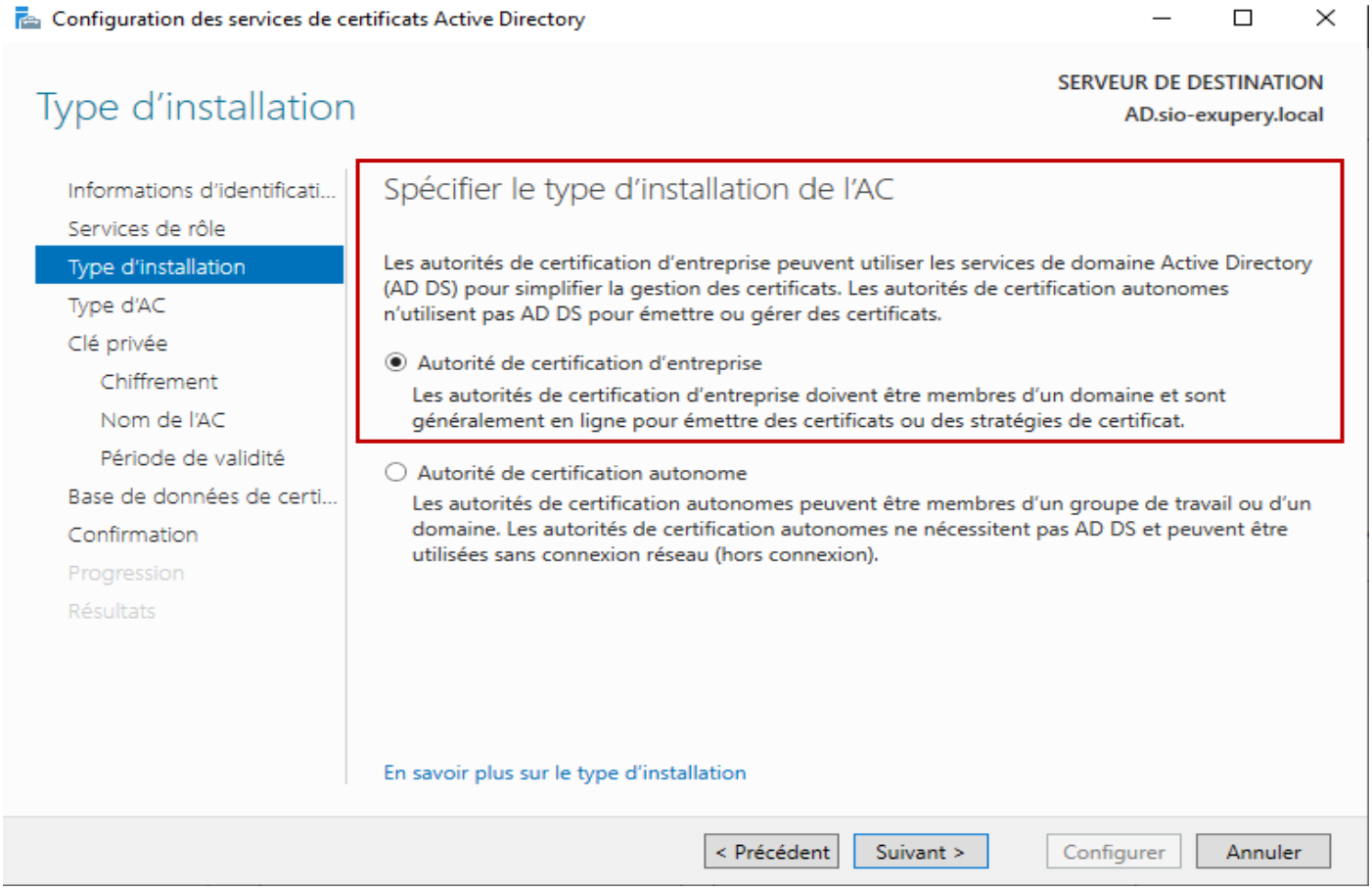
- Dans utilisateur et ordinateur Active Directory je dois être membre du groupe Administrateurs de l'entreprise :



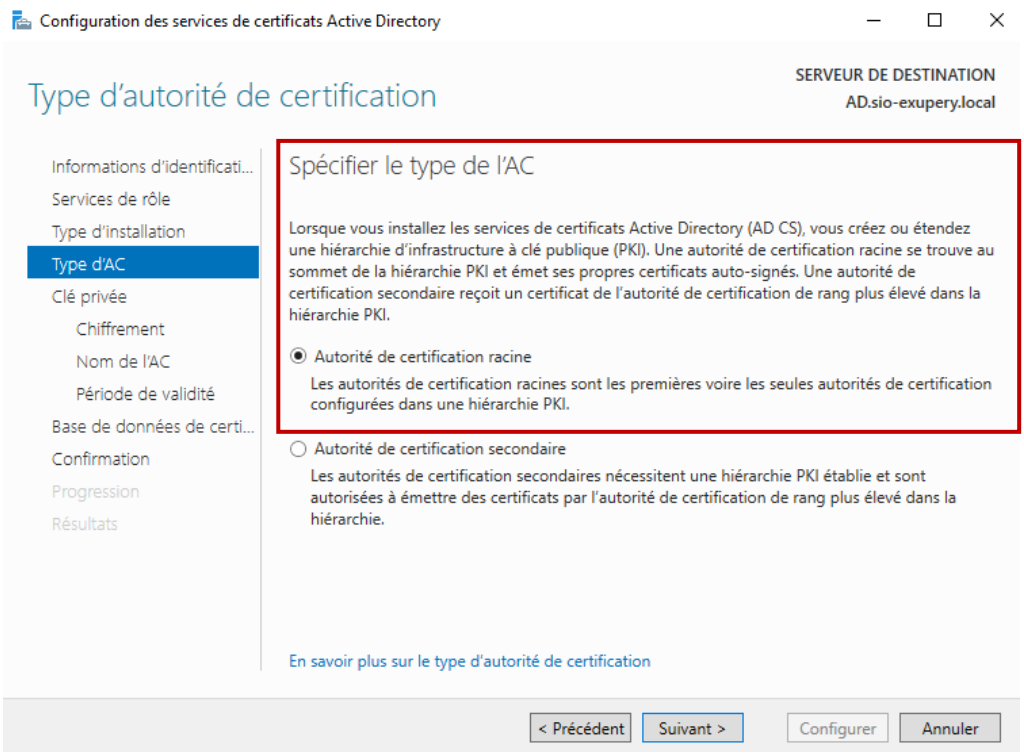
- Dans configuration des services de certificats Active Directory, je coche la case Autorité de certification pour configurer ce rôle :



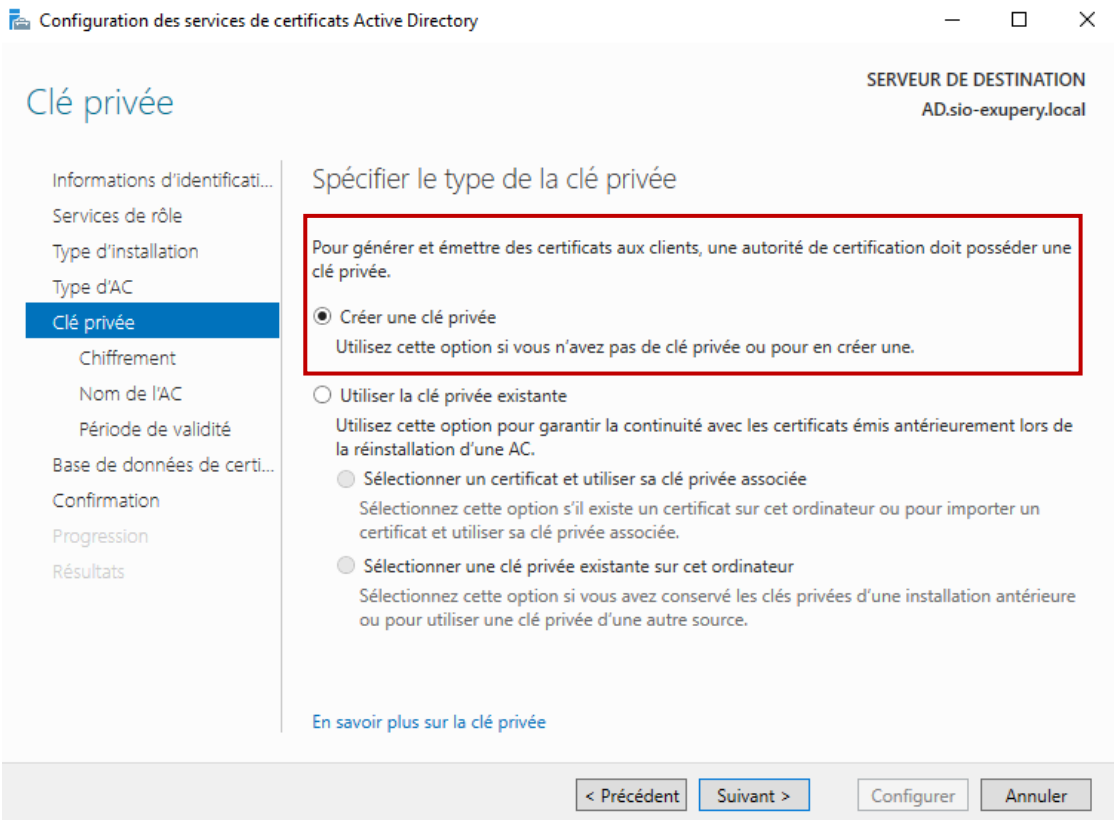
➢ Je sélectionne Autorité de certification d'entreprise :

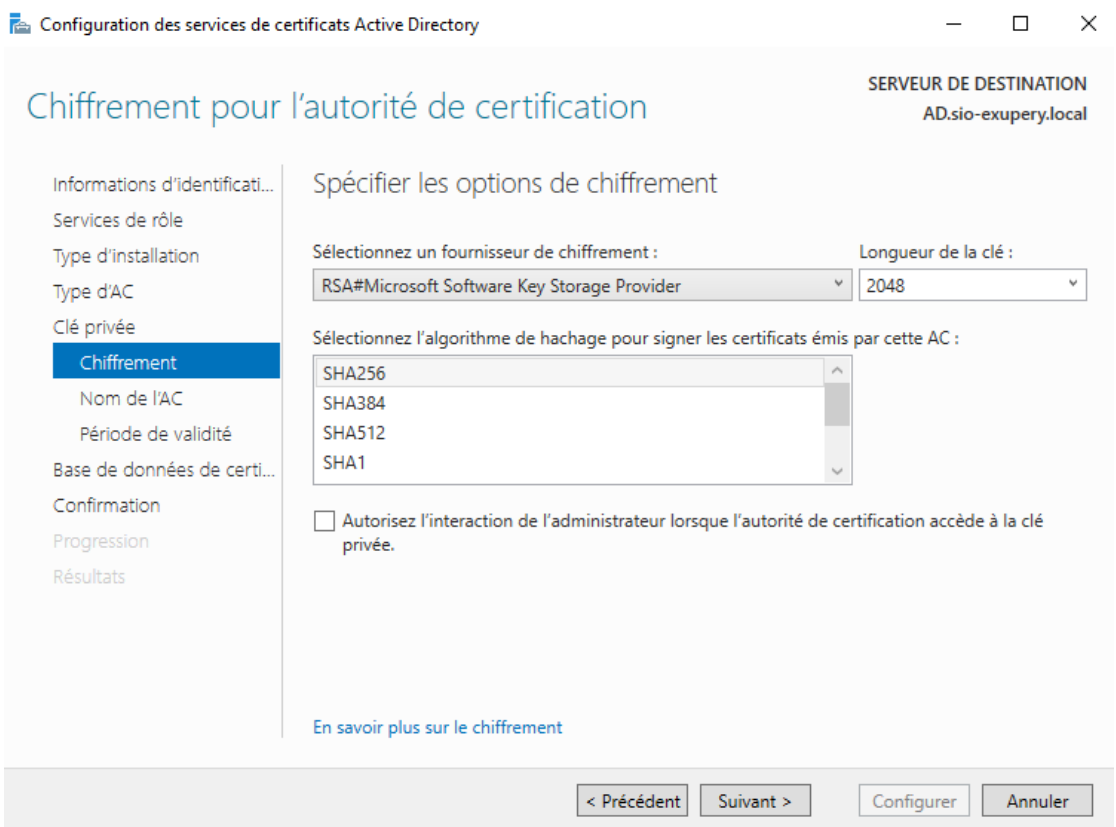


➢ Ensuite, je sélectionne Autorité de certification d'entreprise :

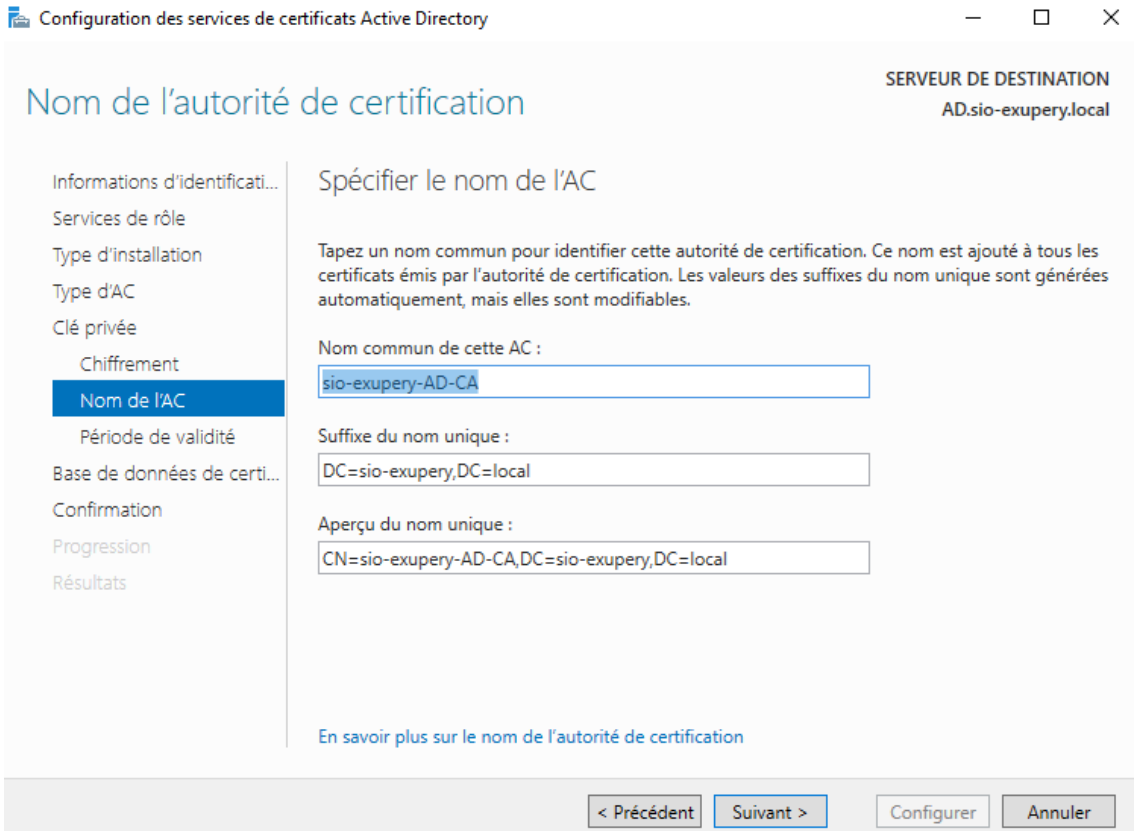


- Puis je créer une nouvelle clé privée et choisis l'algorithme de chiffrement ainsi que de hachage par défaut :

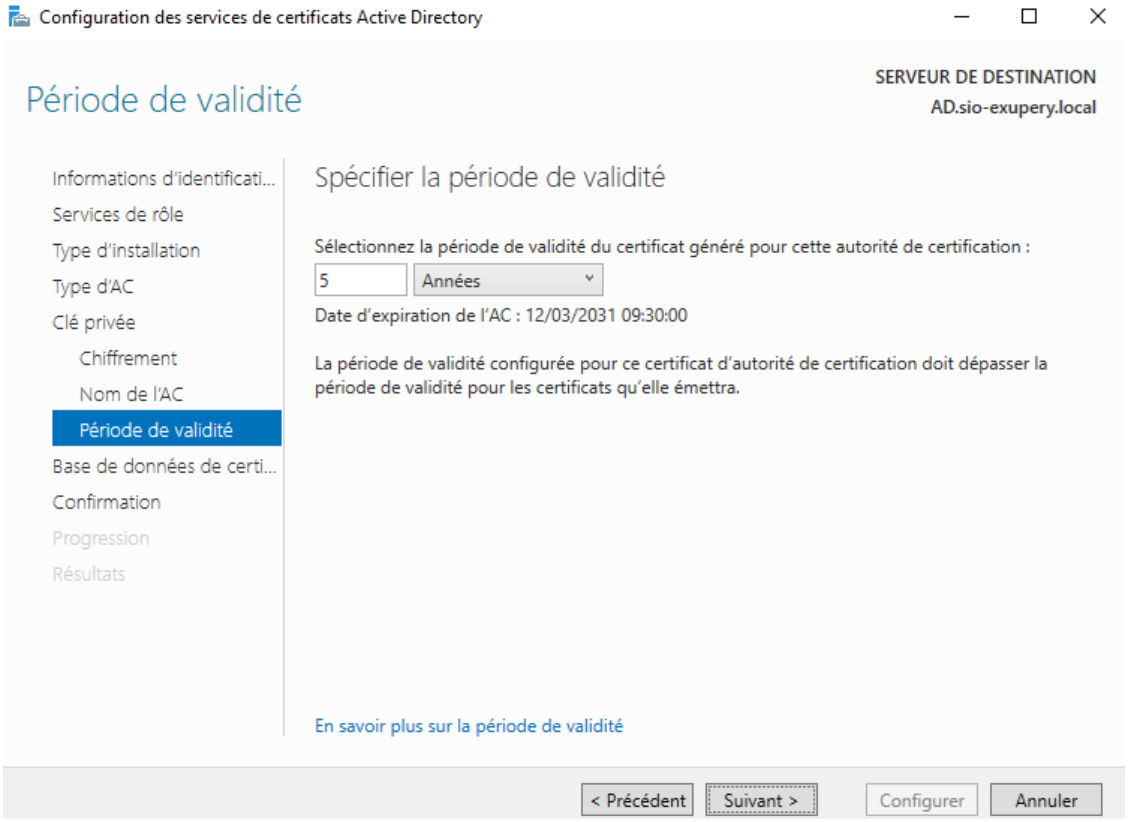




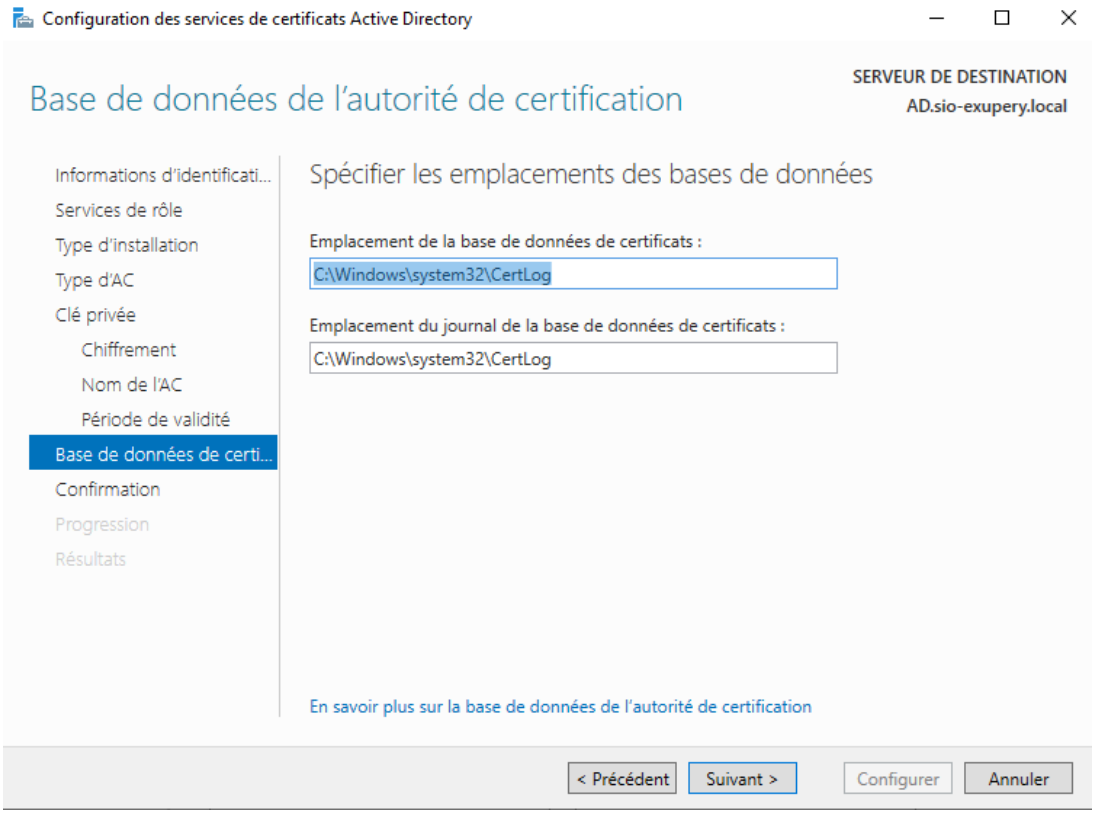
- Je laisse le nom de l'autorité de certification par défaut :



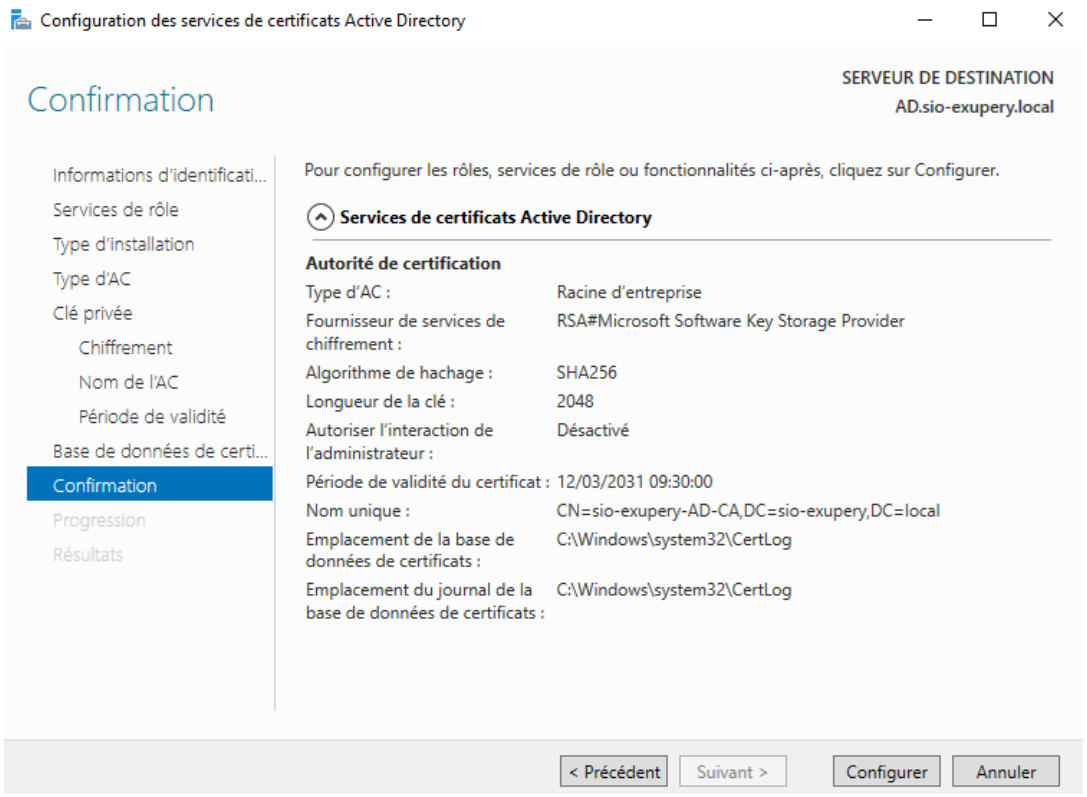
- Je laisse la période de validité par défaut :



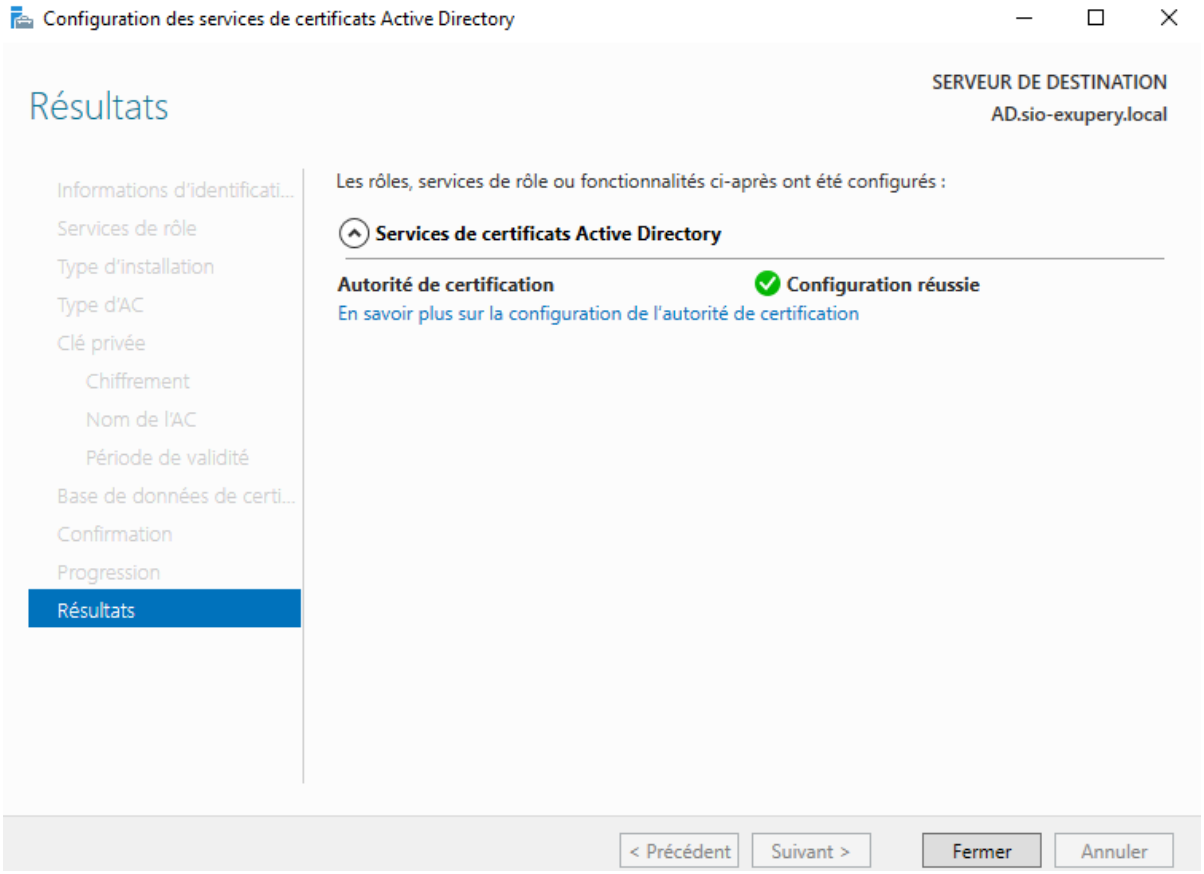
- Je laisse les dossiers des bases de données par défaut :



- L'assistant m'affiche le résumé de ma configuration, je clique sur configurer :

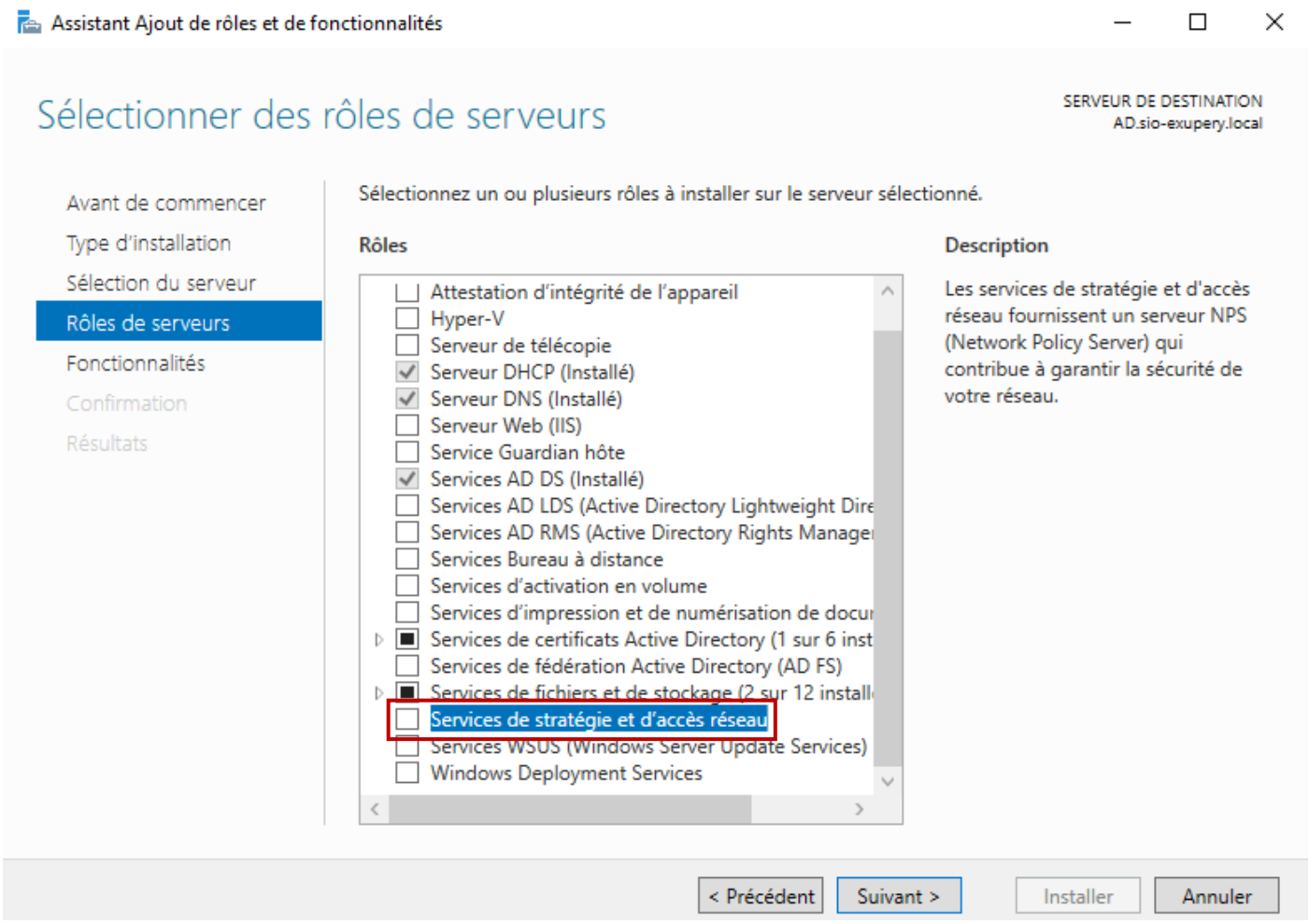


- L’autorité de certification est maintenant installée et configurer :

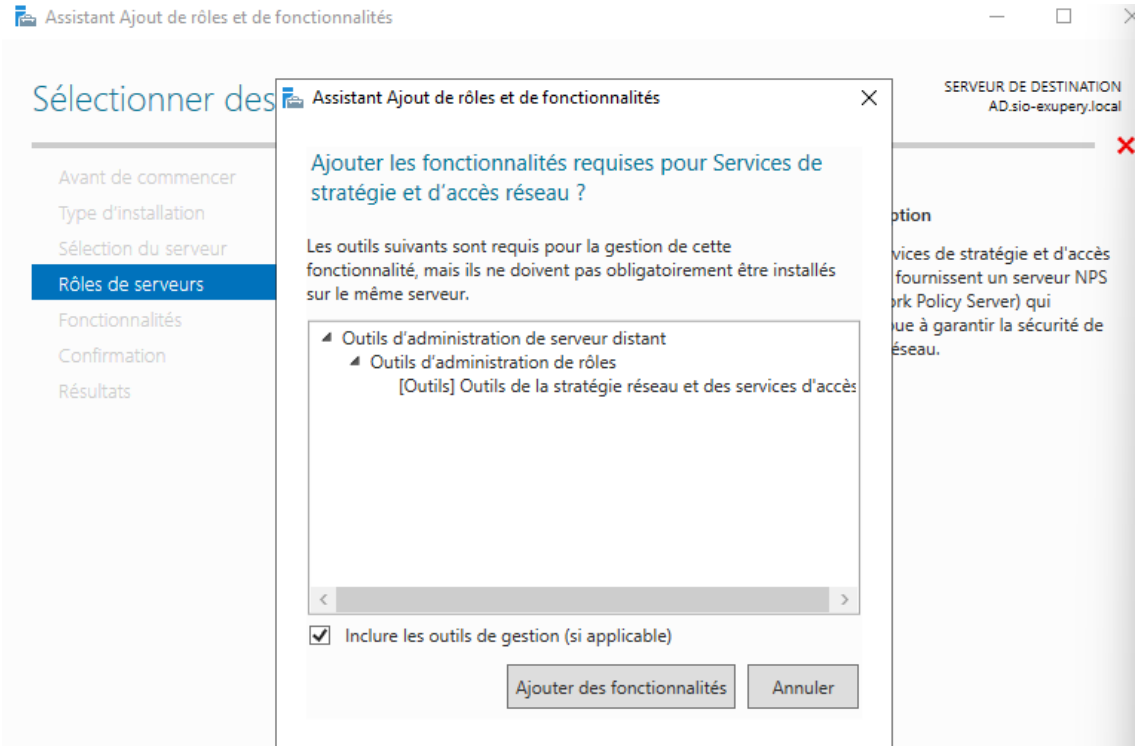


2.3 Installation du service NPS

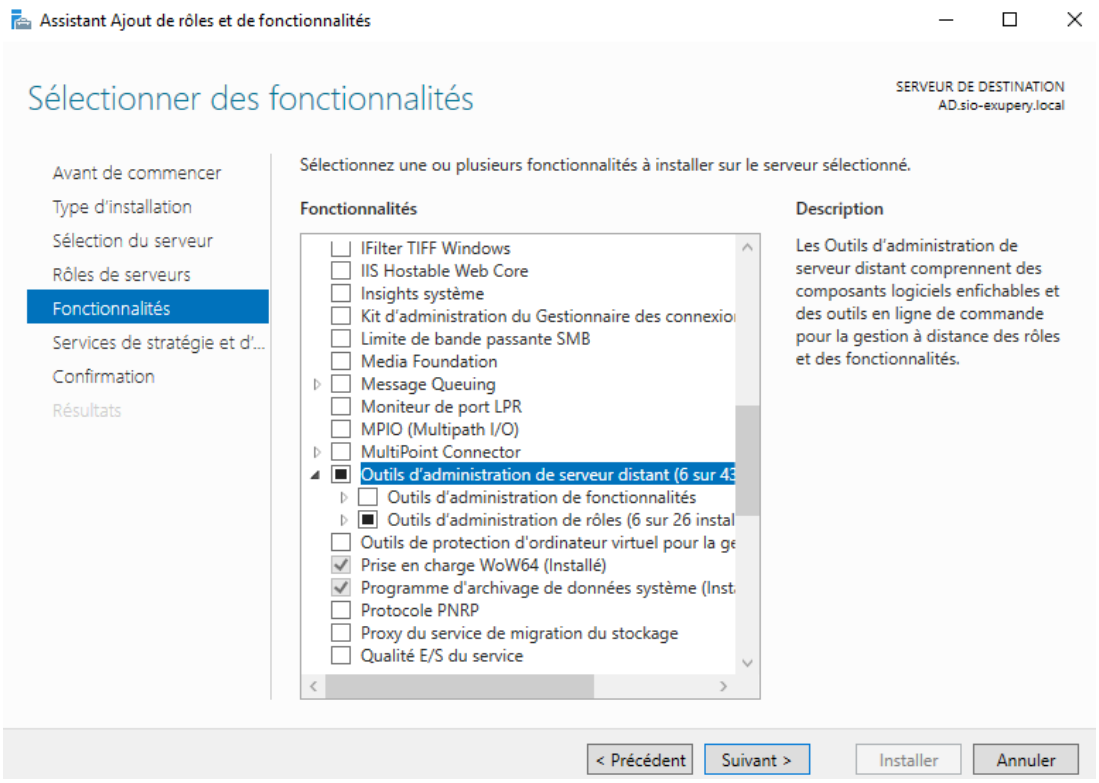
- J’ajoute le rôle Services de stratégie et d'accès réseau :



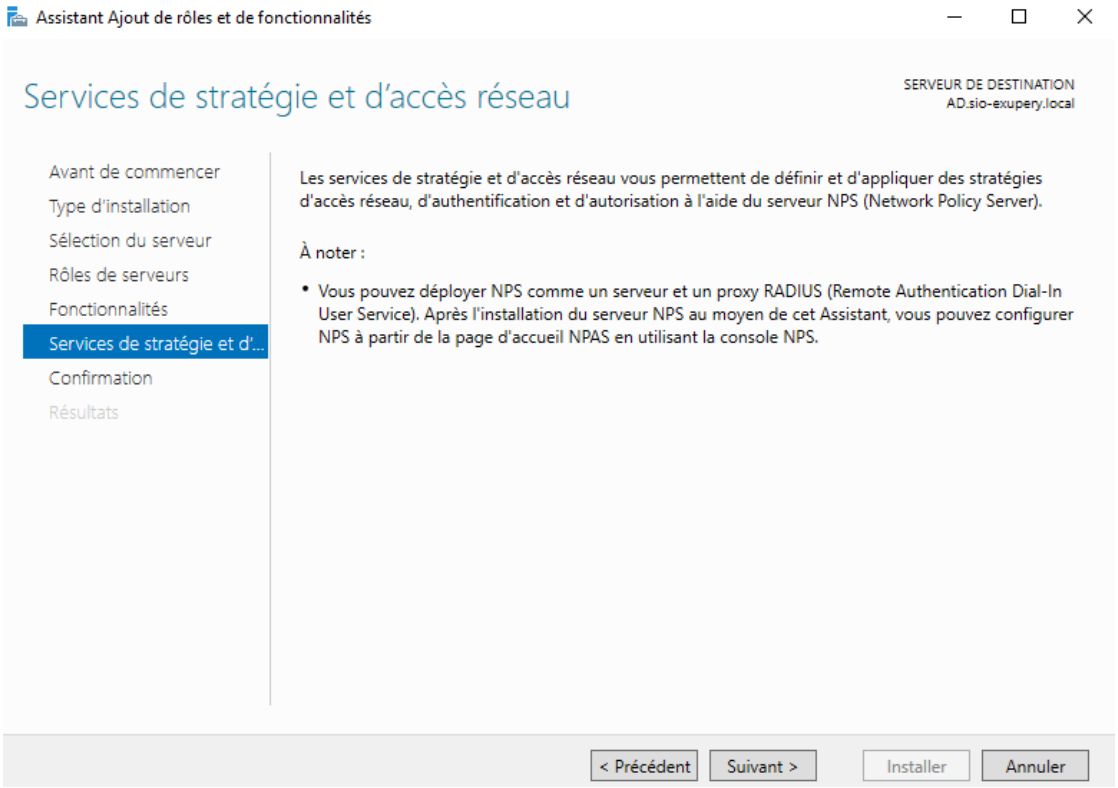
➢ Je clique sur le bouton Ajouter des fonctionnalités :



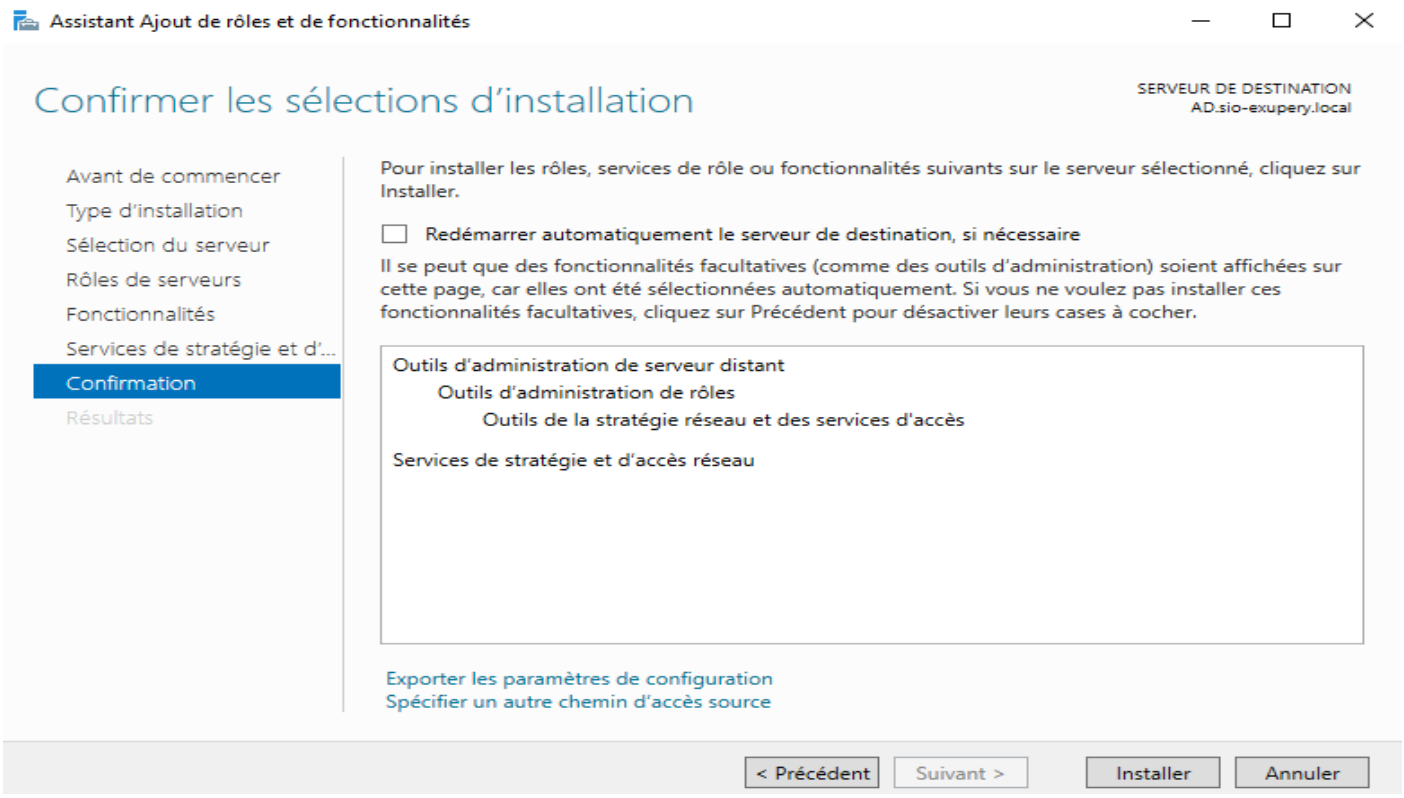
- Je clique sur le bouton suivant :



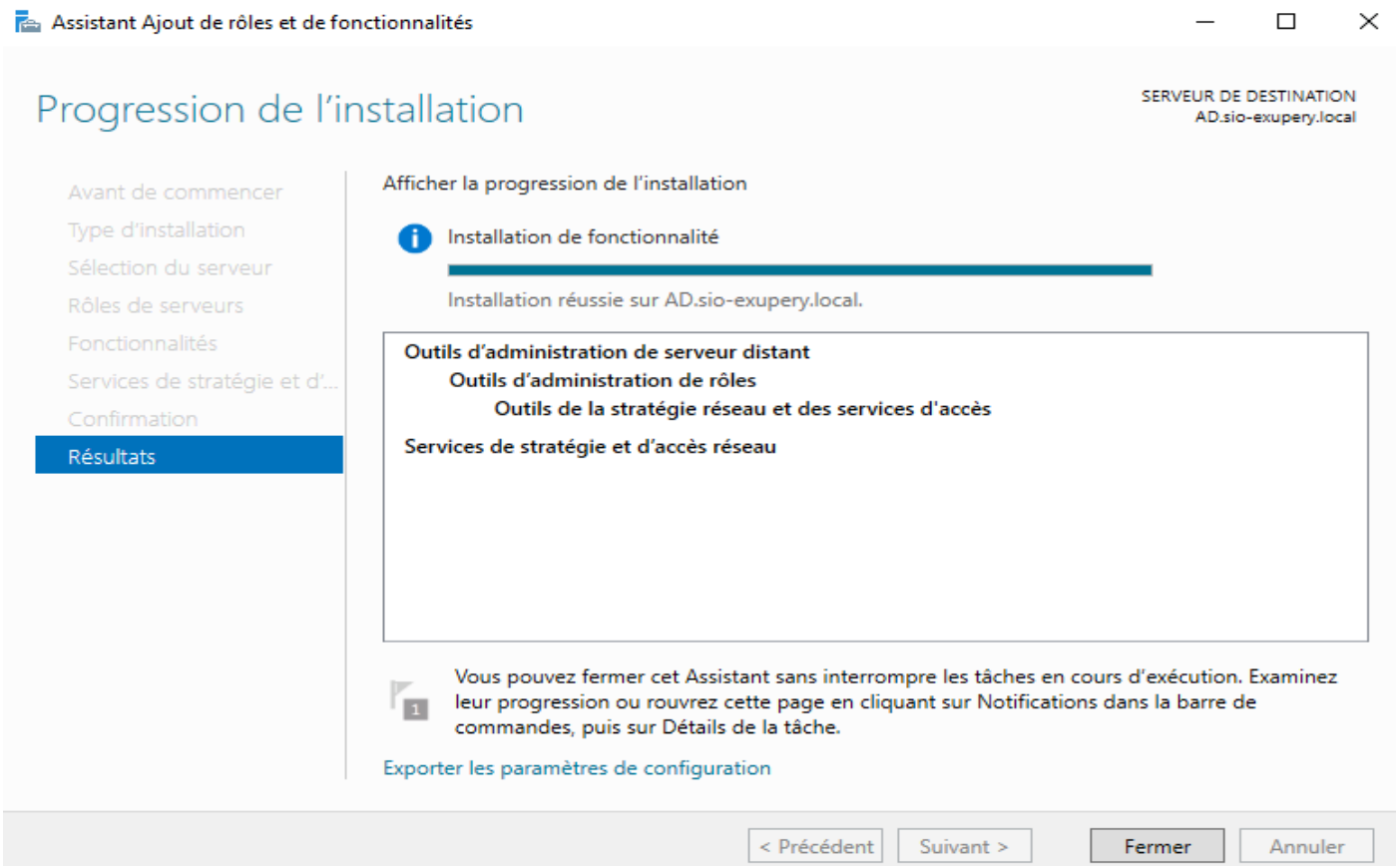
- L'écran d'information Services de stratégie et d'accès réseau s'affiche. Je clique sur le bouton Suivant :



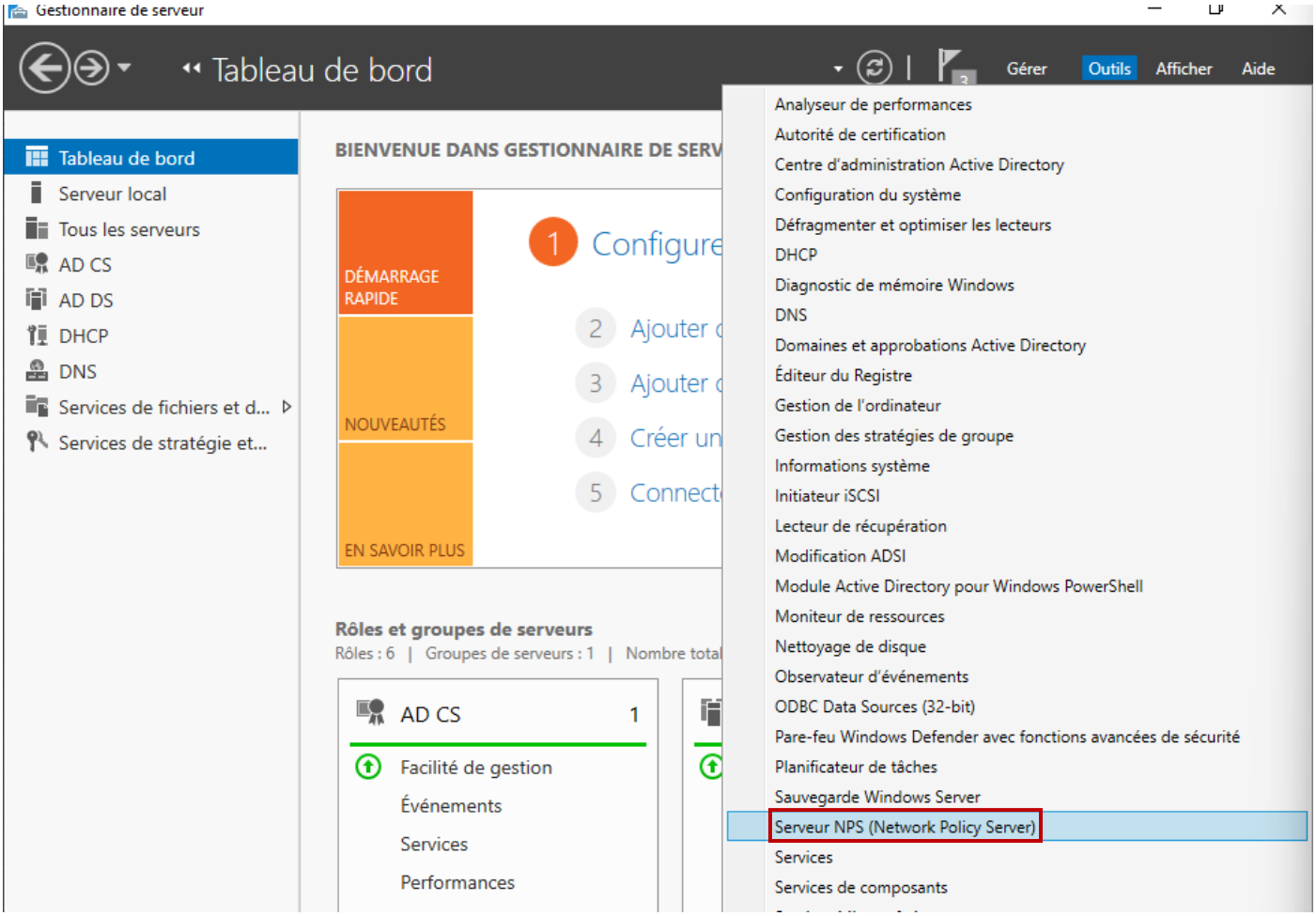
➢ Et enfin je clique sur le bouton Installer :



➢ Une fois installer je clique sur fermer :

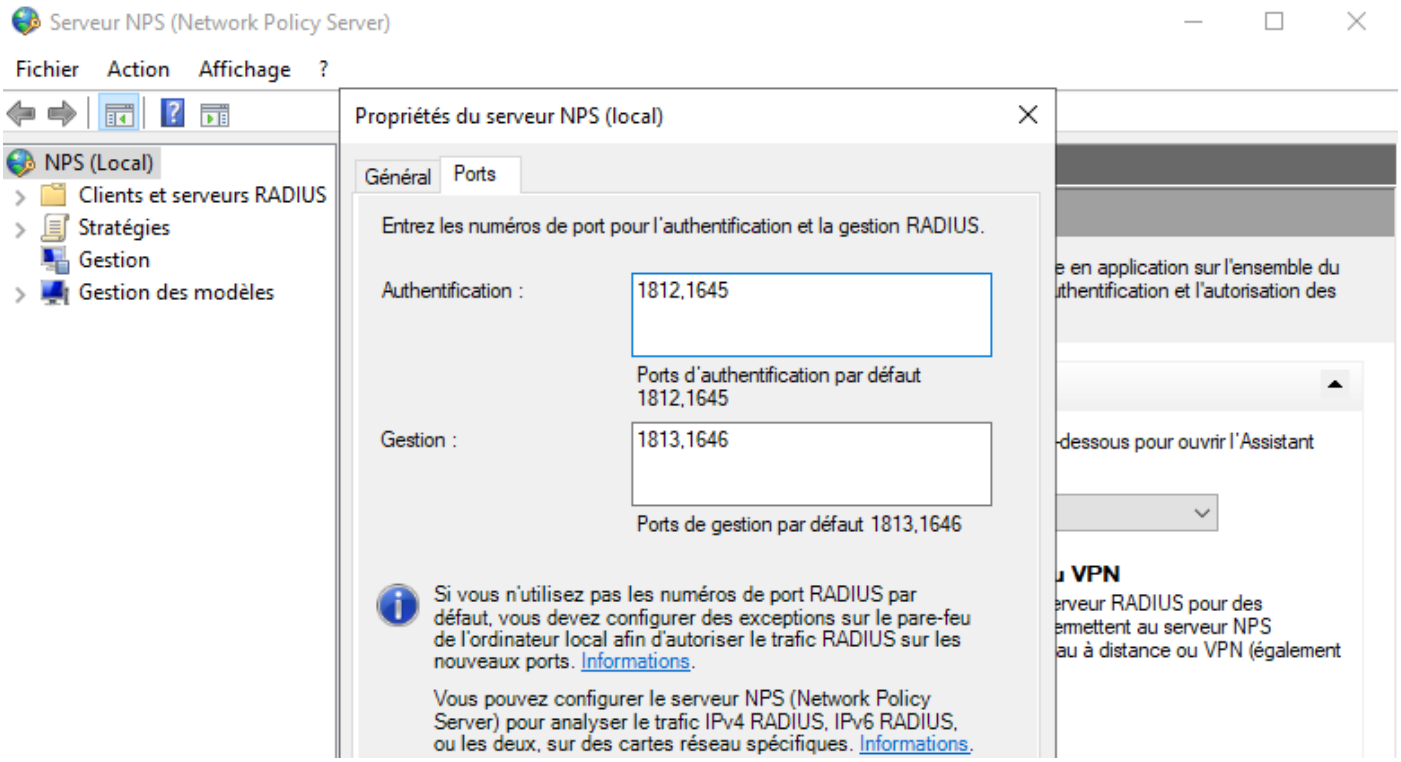


➢ Dans les outils je peux apercevoir la console Serveur NPS :



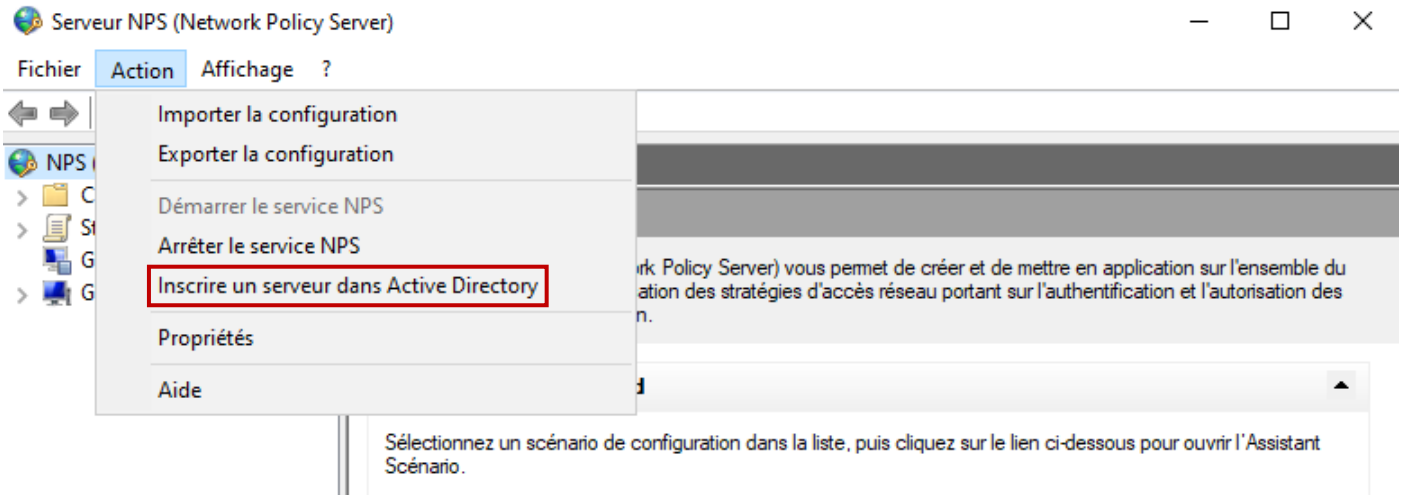
➢ Pour vérifier que le service NPS fonctionne dans un terminal j'affiche les ports en écoute :

➢ J'ouvre la console Serveur NPS et je retrouve ces ports dans les propriétés du serveur NPS :

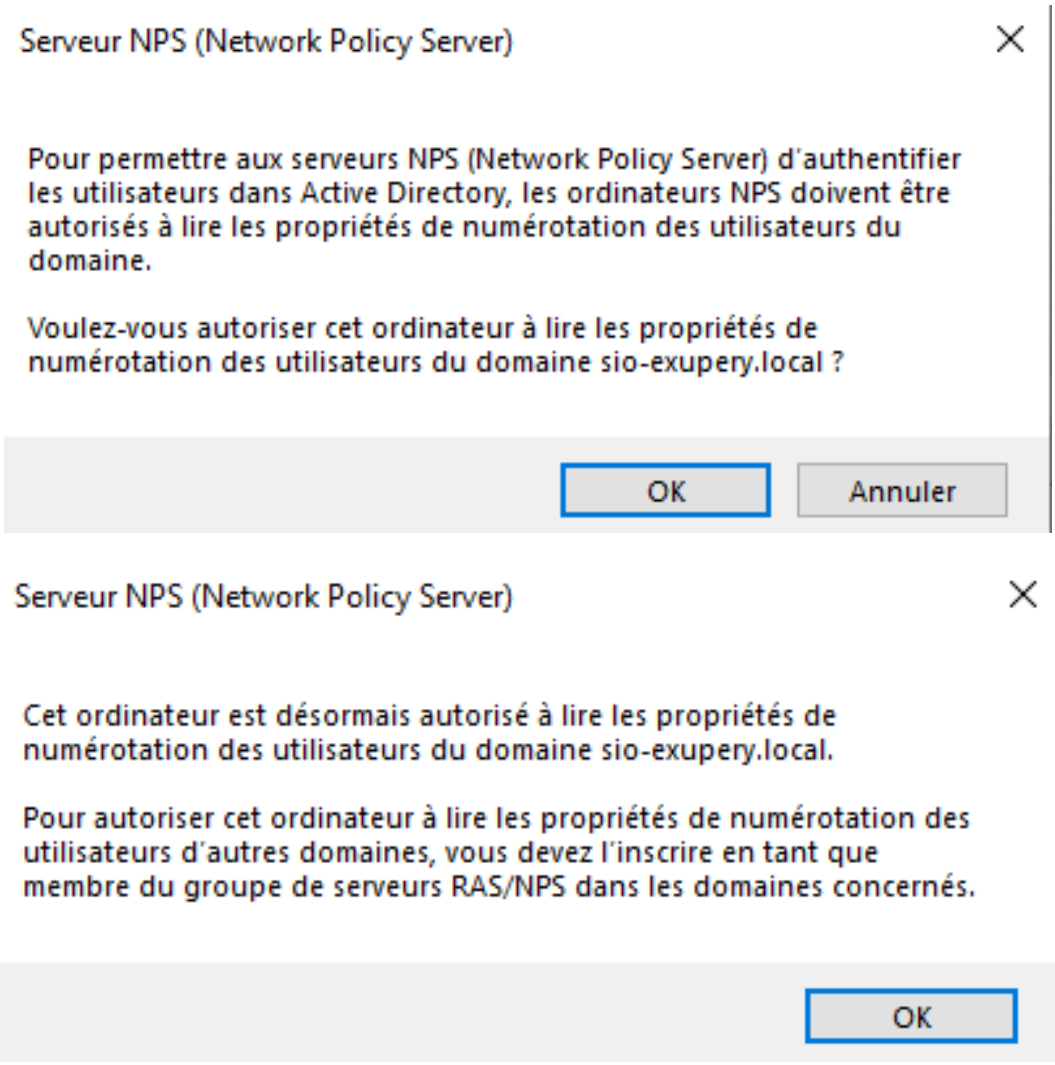


2.4 Configuration du serveur RADIUS NPS

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

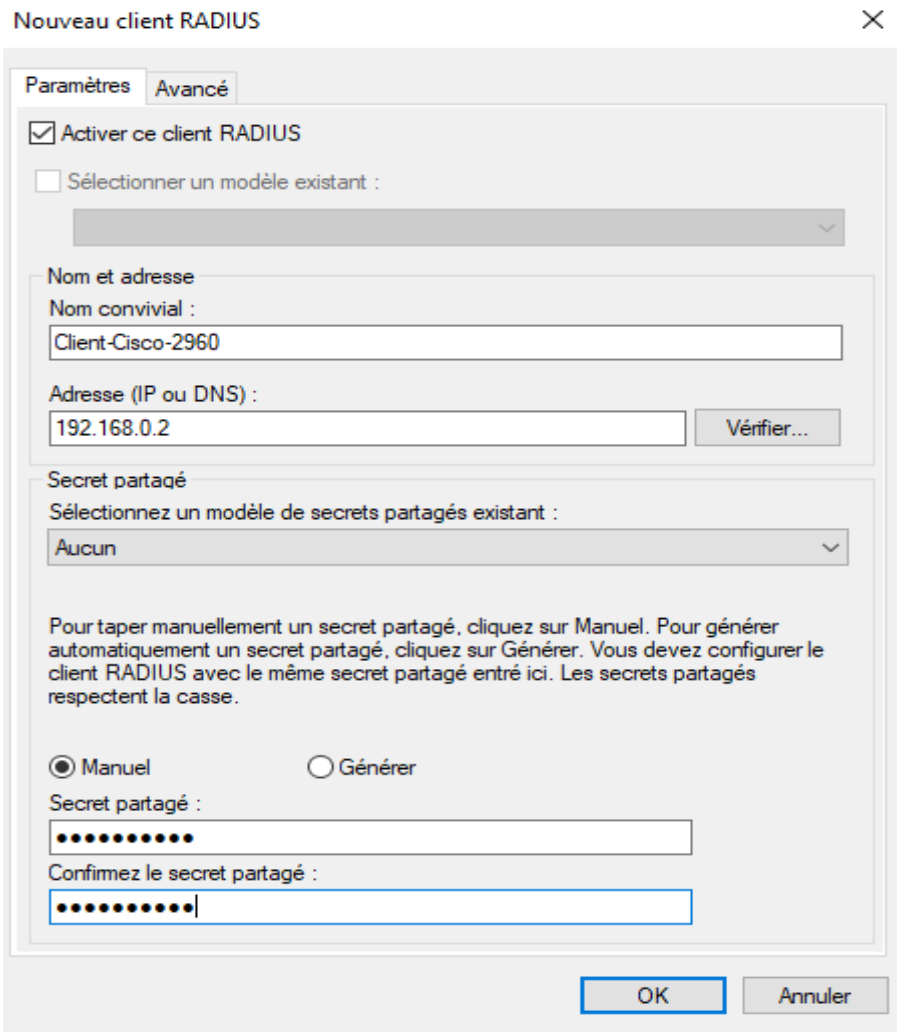


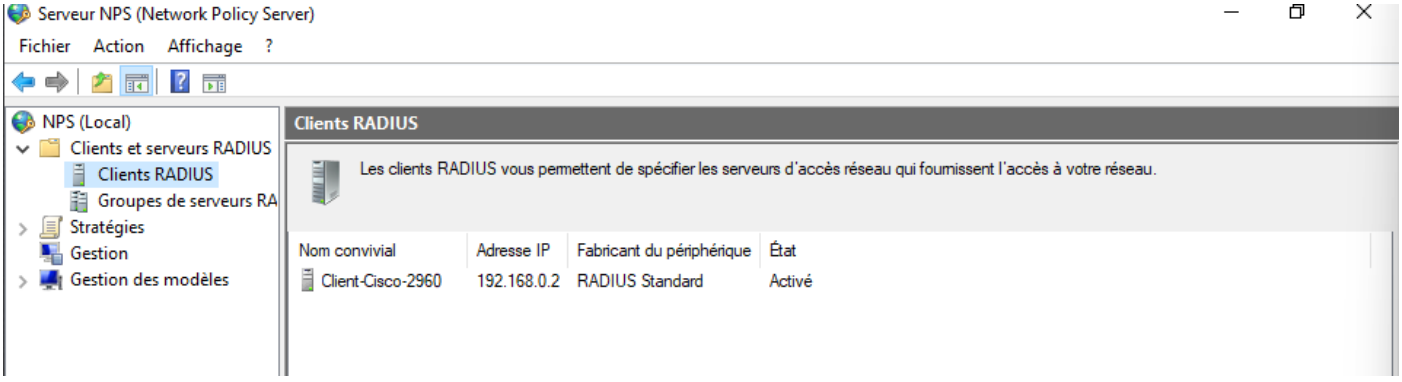
- Et j'autorise tout ce que le serveur NPS à besoin :



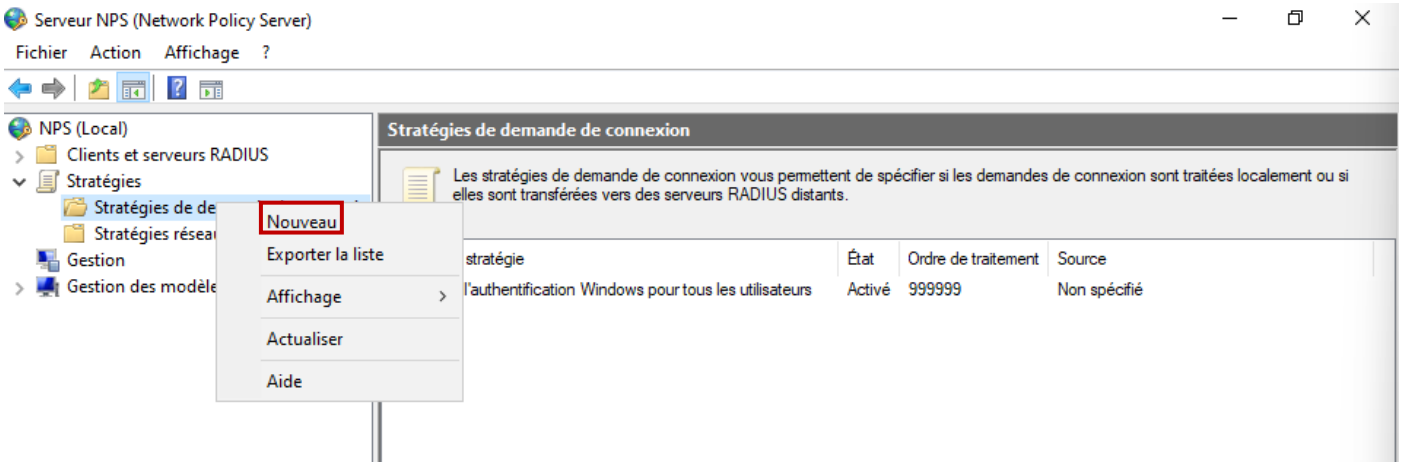
Je vais maintenant déclarer le client RADIUS :

- Je clique sur l'UO Clients et serveurs RADIUS et je clique droit sur Clients RADIUS et je clique sur Nouveaux (je n'ai pas le screen) :

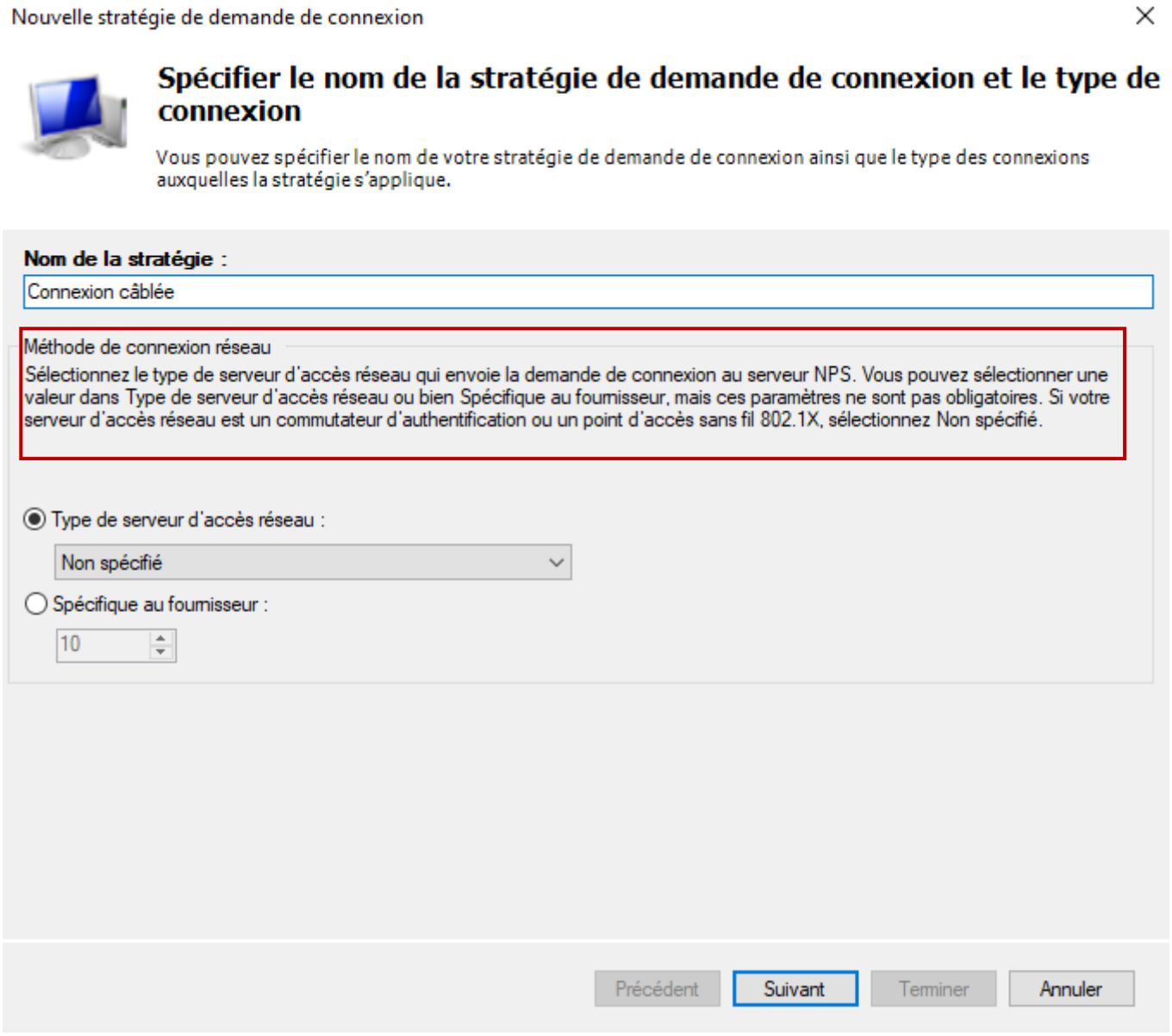




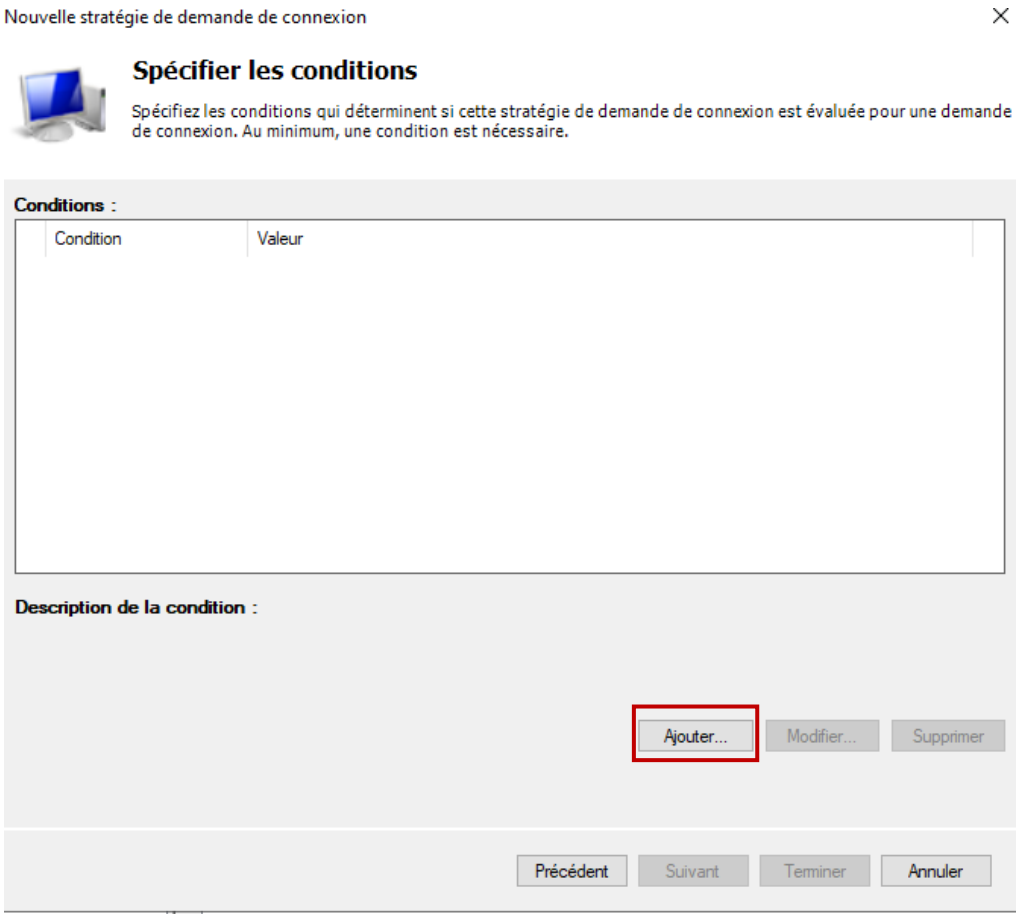
- Je clique droit sur l'entrée Stratégies de demande de connexion et je sélectionne Nouveau :



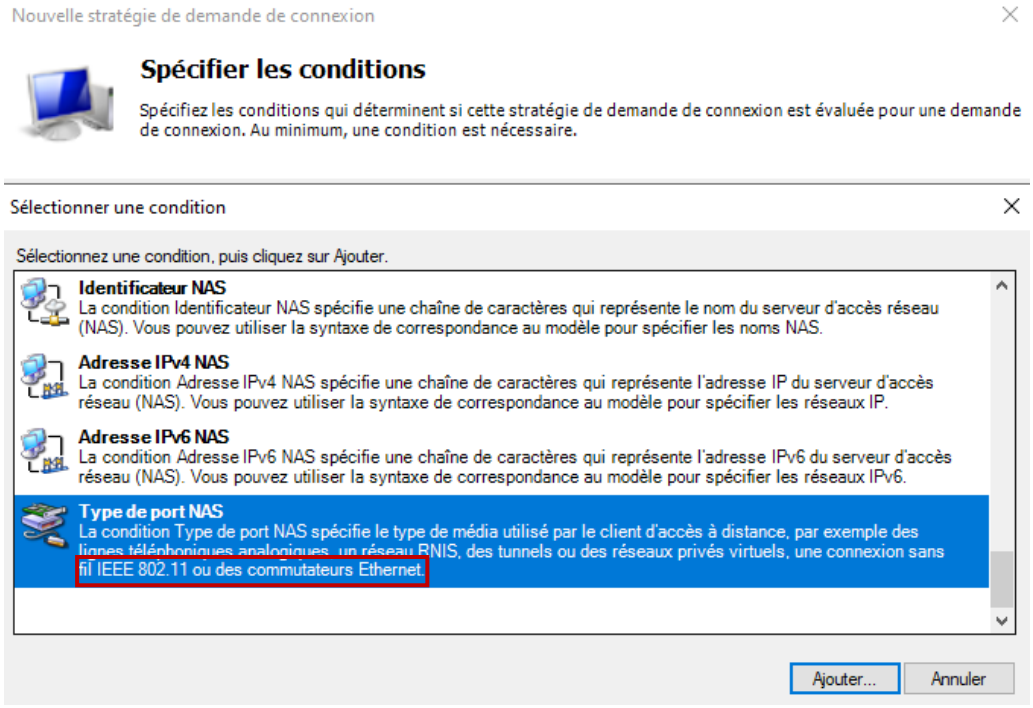
- Je clique sur suivant :



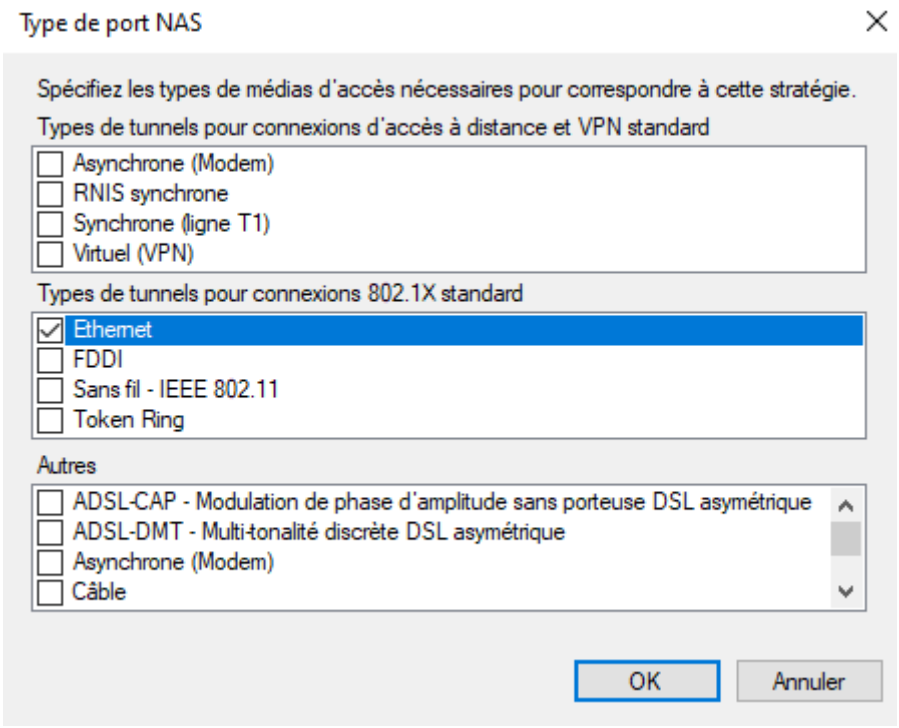
- Sur cette fenêtre je clique sur Ajouter :



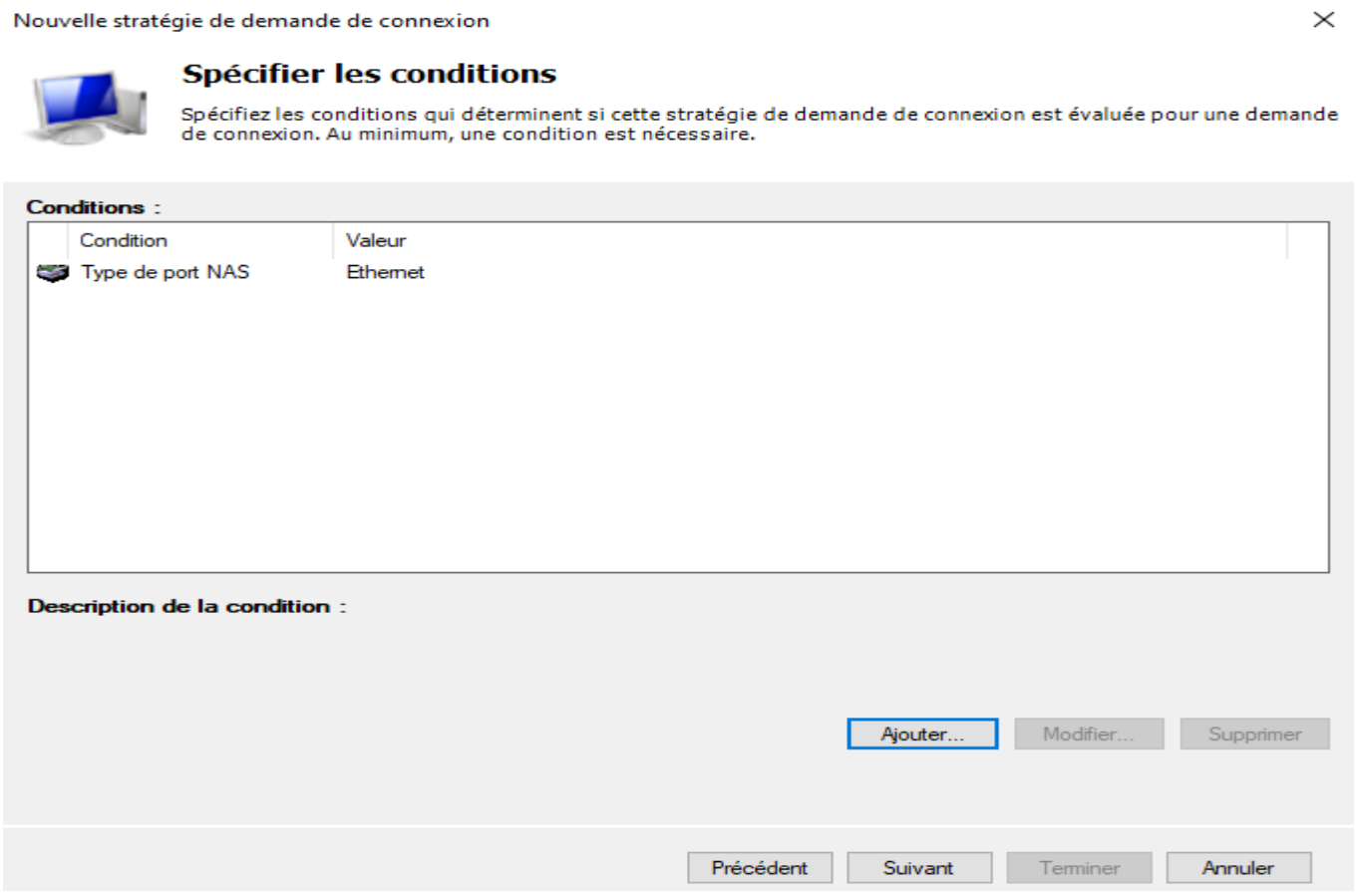
- J'indique le type de média utilisé par le client d'accès à distance (je sélectionne pour cela Type de port NAS), et Ajouter :



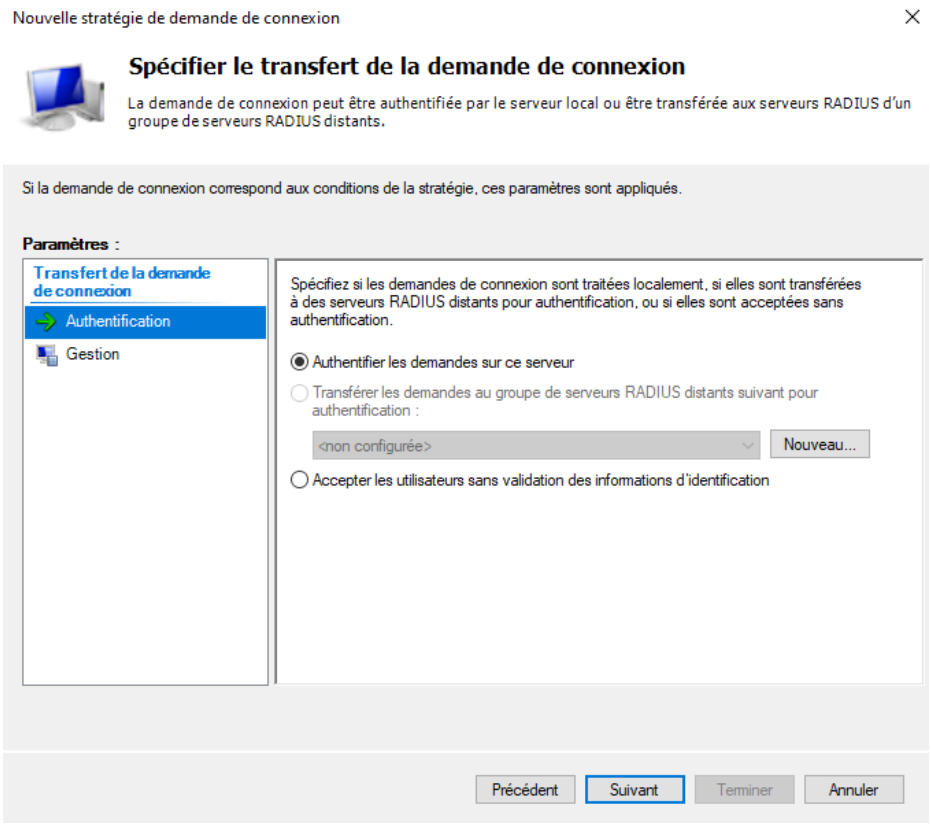
- Je coche Ethernet dans l'écran Type de port NAS :



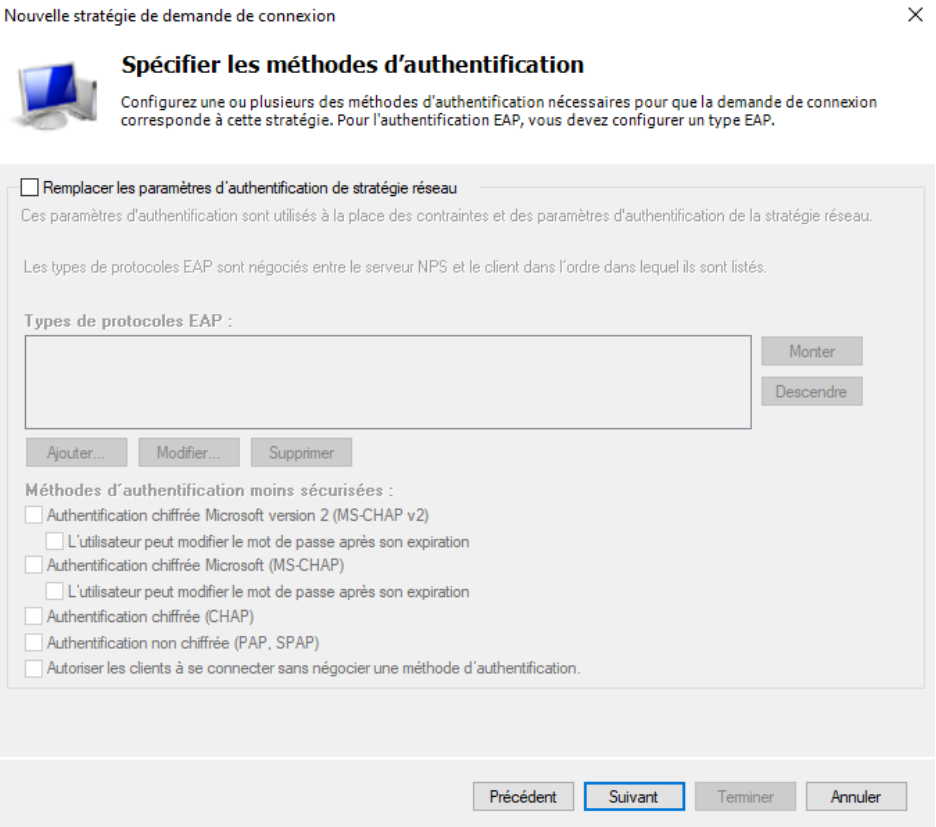
- Je clique sur le bouton Suivant :



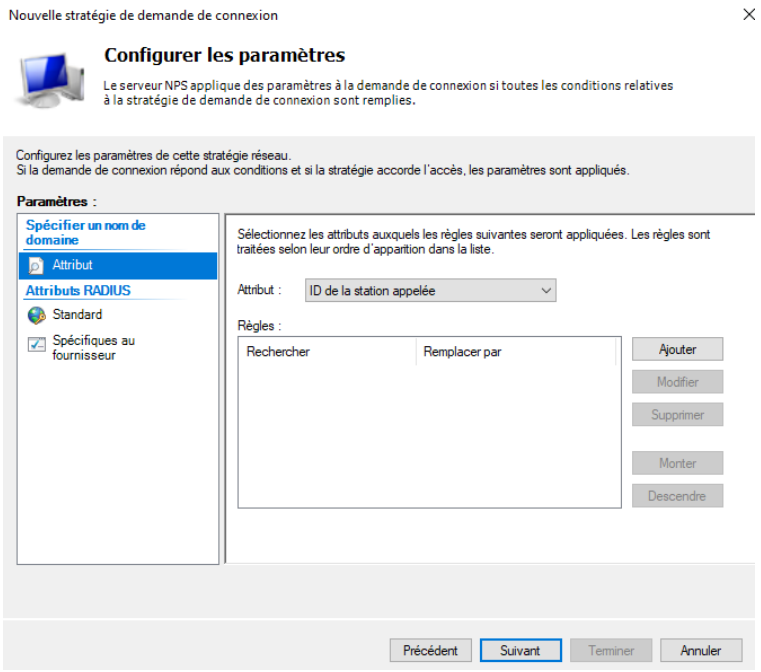
➢ Je laisse par défaut et je clique sur suivant :



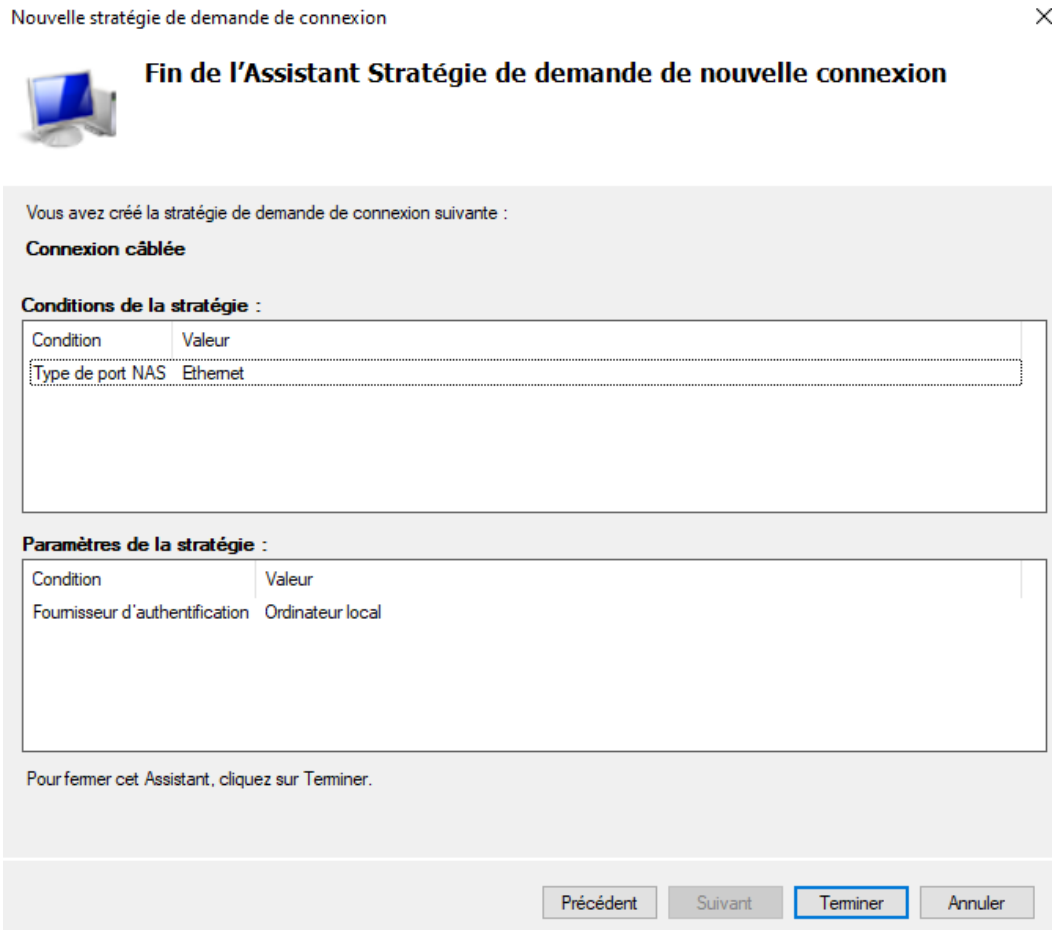
➢ Idem pour cette fenêtre :

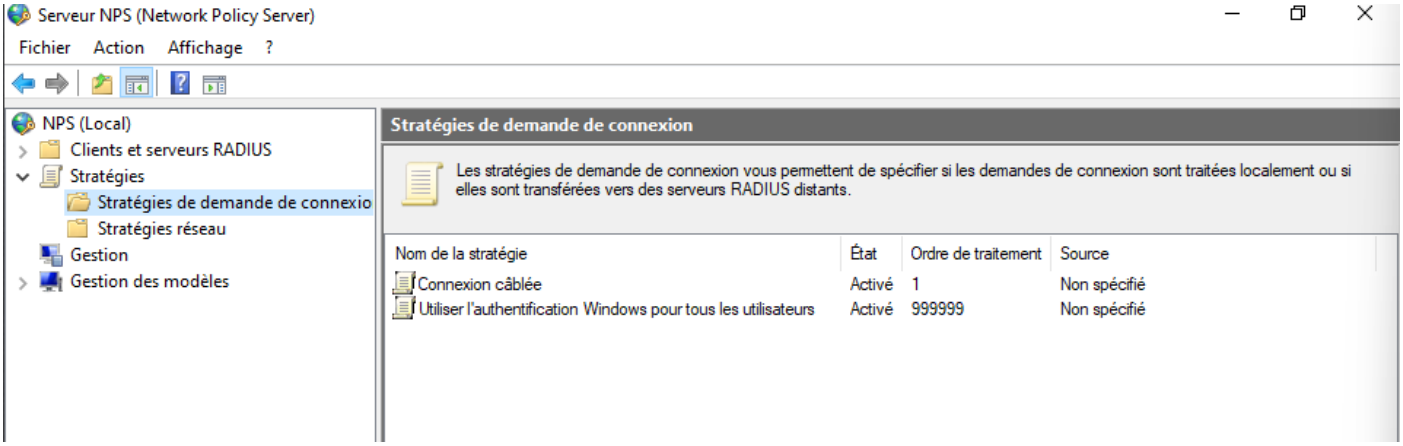


- Je clique sur le bouton Suivant :

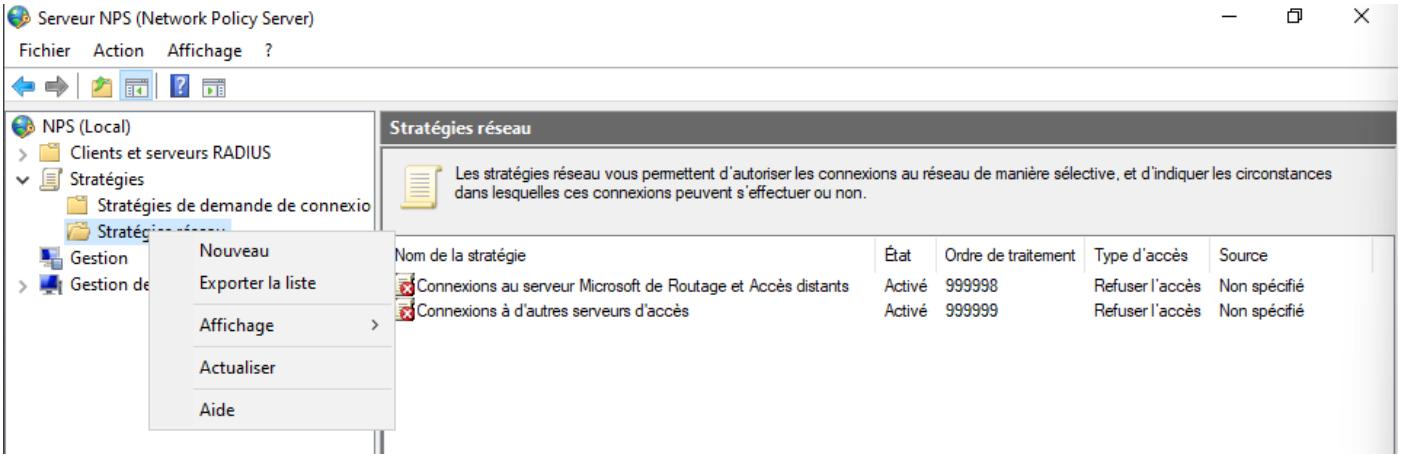


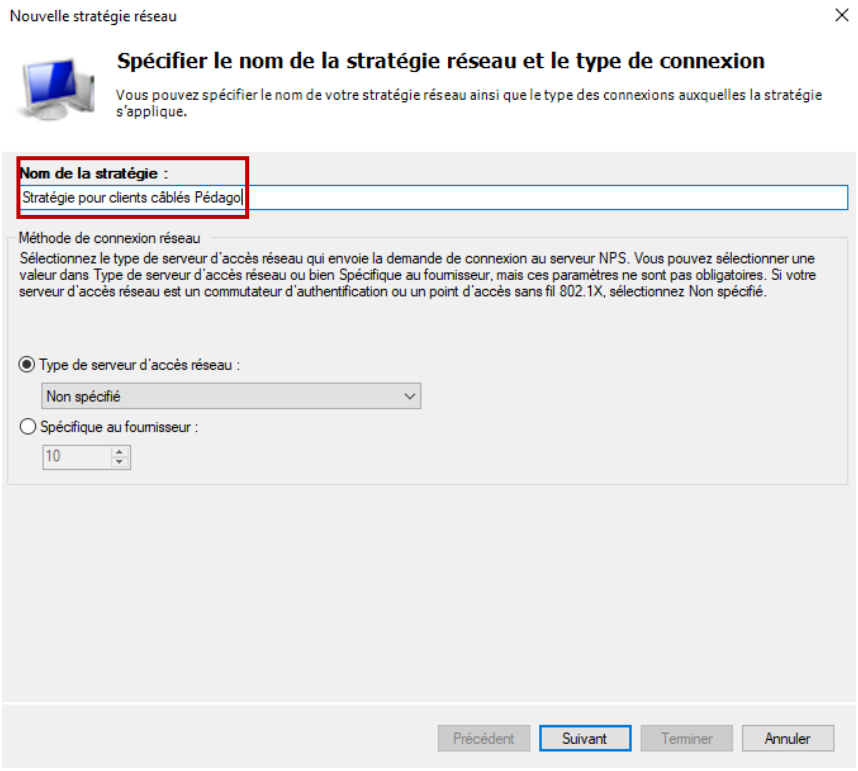
- Je clique sur le bouton Terminer dans l'écran récapitulatif de la stratégie de demande de connexion :



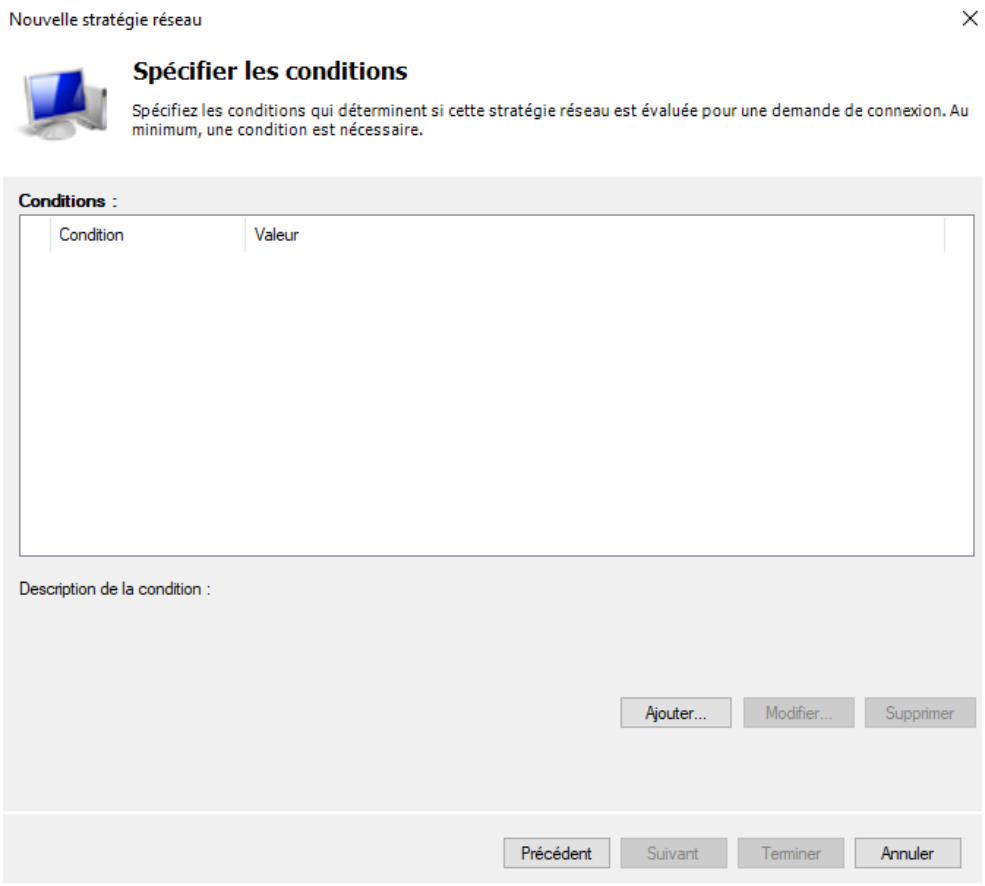


- Je clique droit sur l'entrée Stratégie Réseau et je sélectionne Nouveau et je précise le nom de cette stratégie :

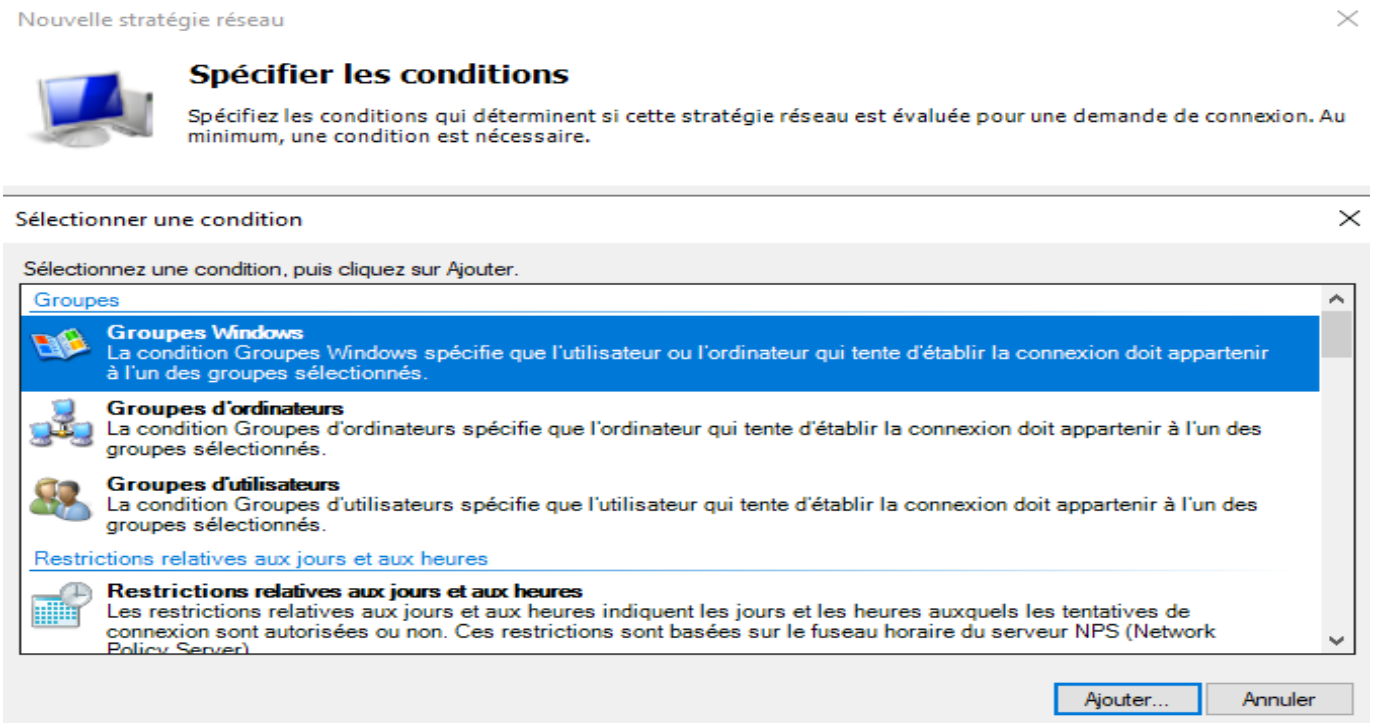




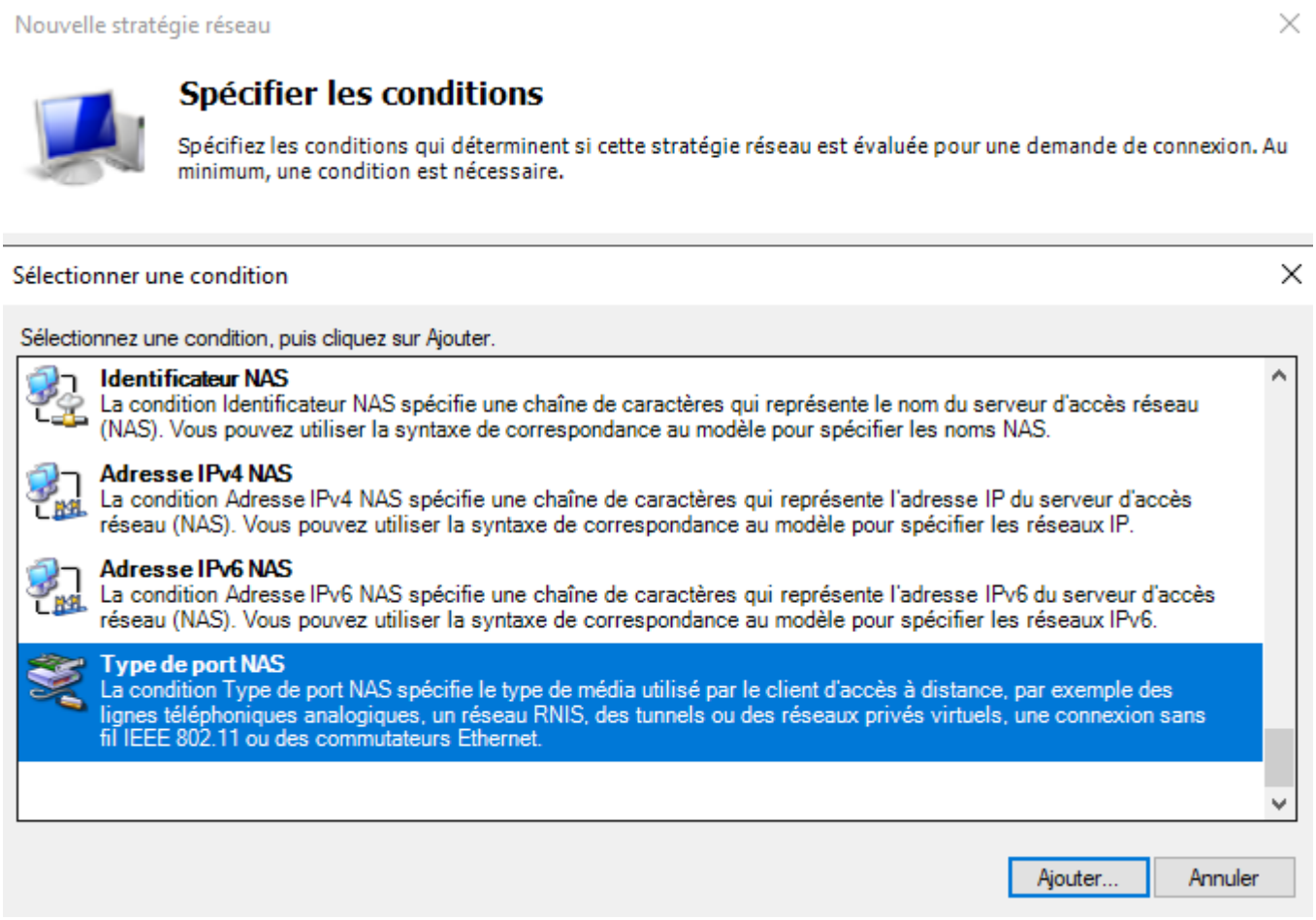
- Je clique sur Ajouter pour spécifier une condition :



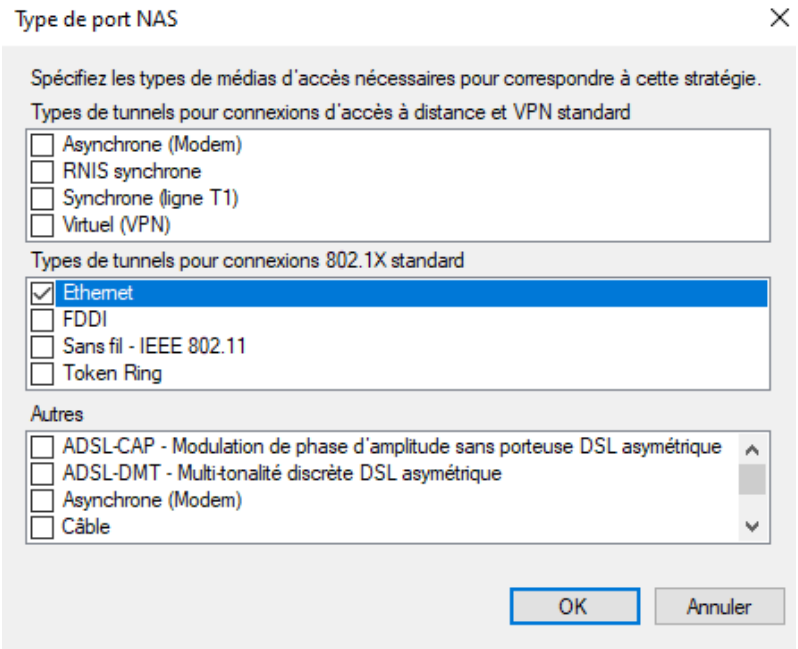
- Dans l'écran Sélectionner une condition, je choisis Groupe Windows et je clique sur Ajouter puis j'ajoute le groupe Prof (je n'ai pas fait le screen :



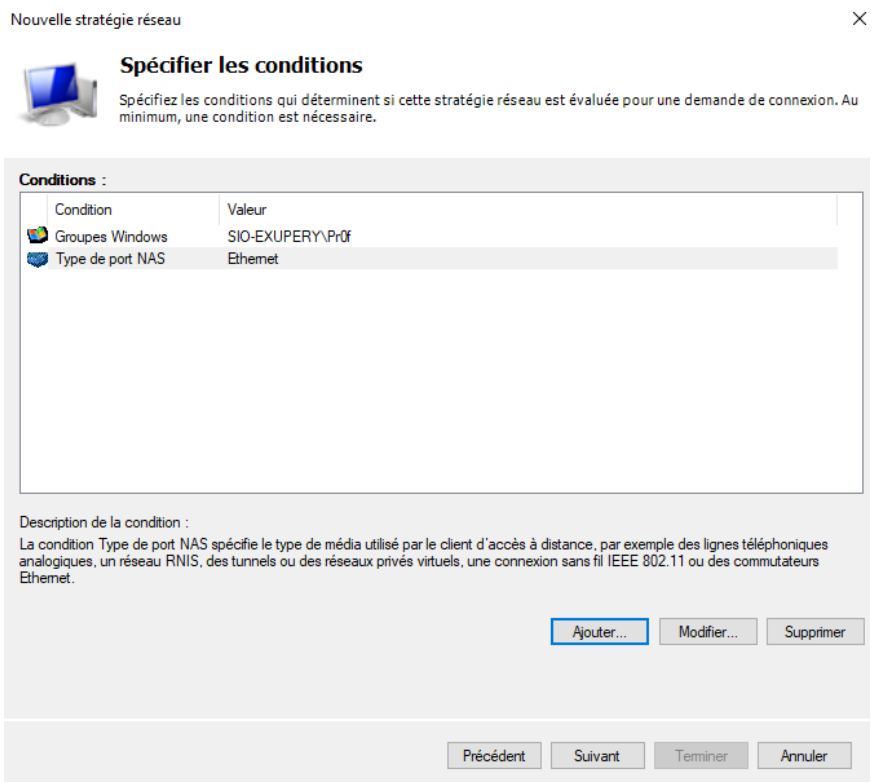
- J'ajoute une deuxième condition pour spécifier le type de port NAS :



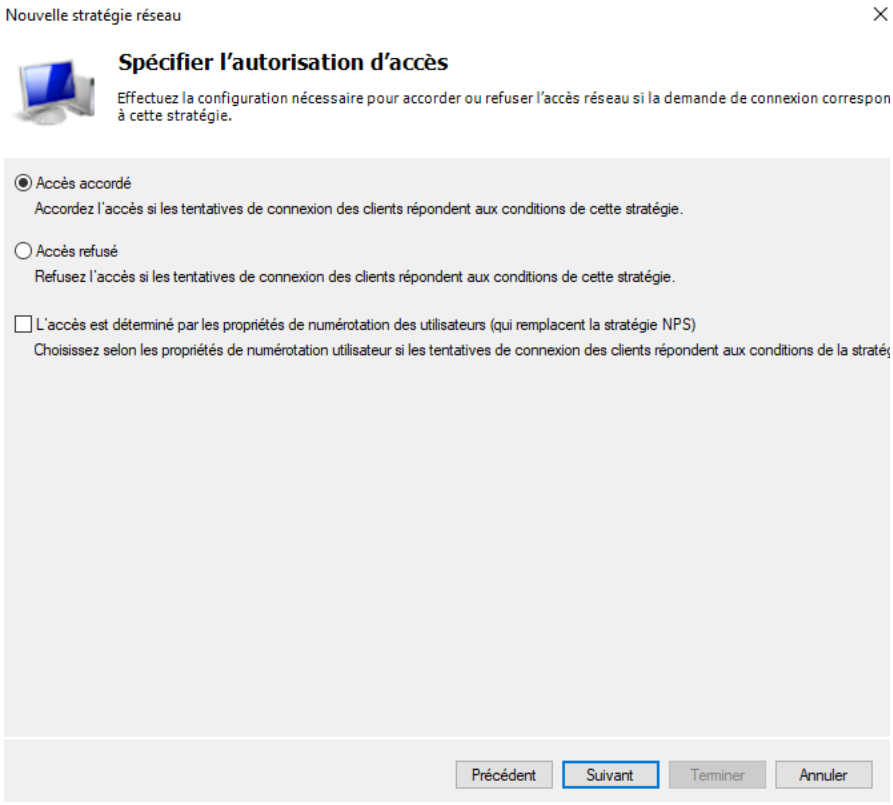
- Je coche Ethernet :



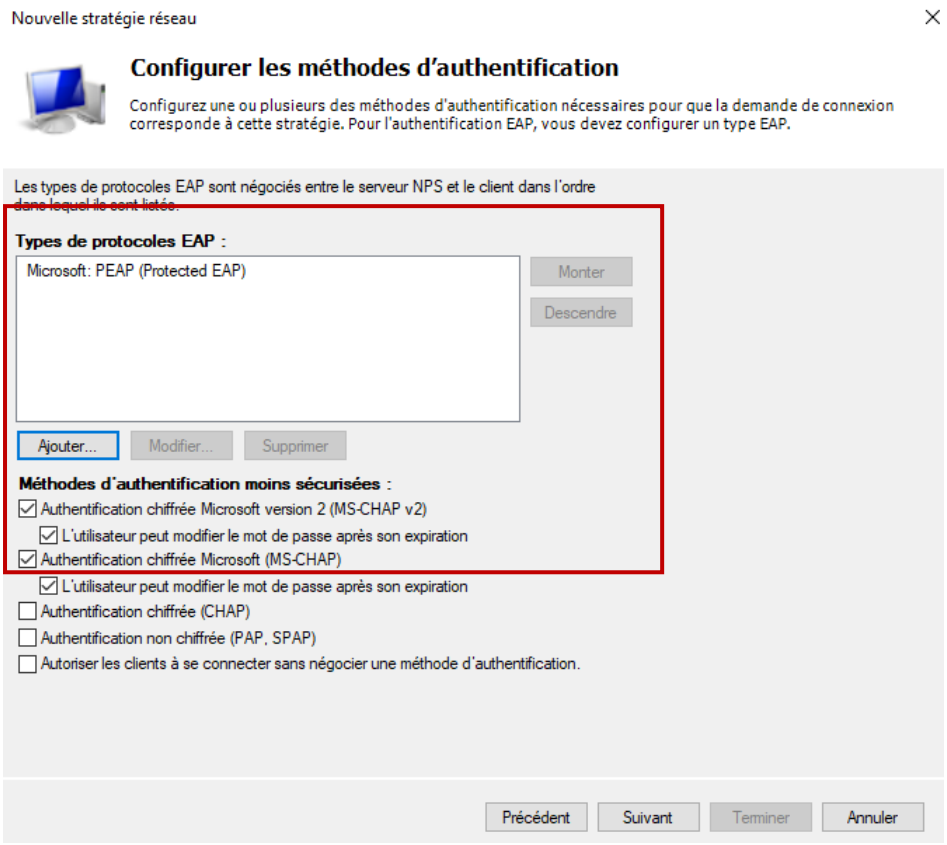
- Je clique sur suivant :



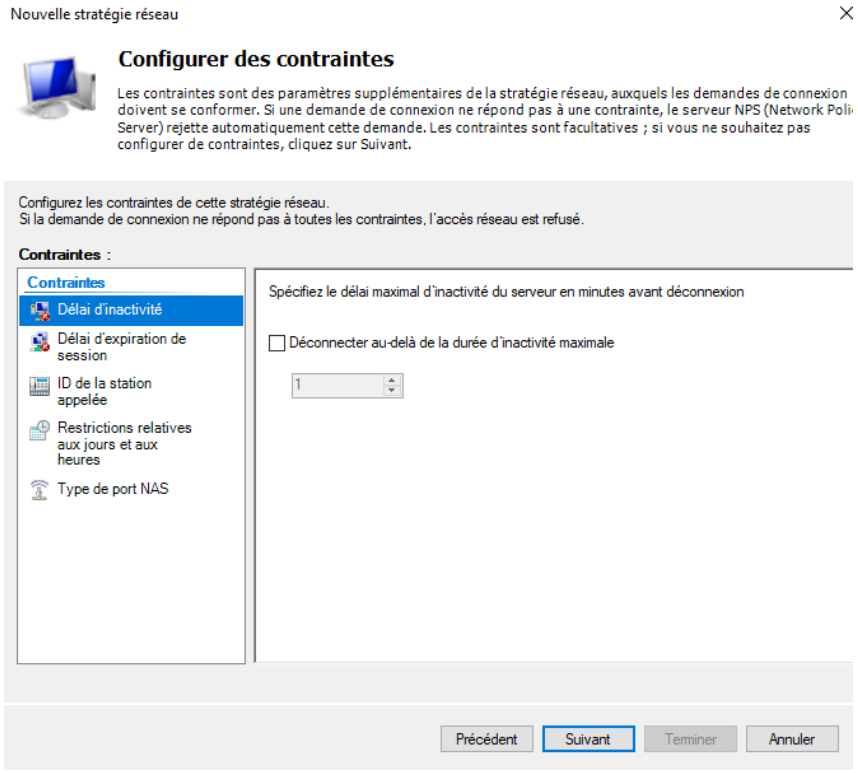
- J'accorde l'accès pour les membres de ce groupe :



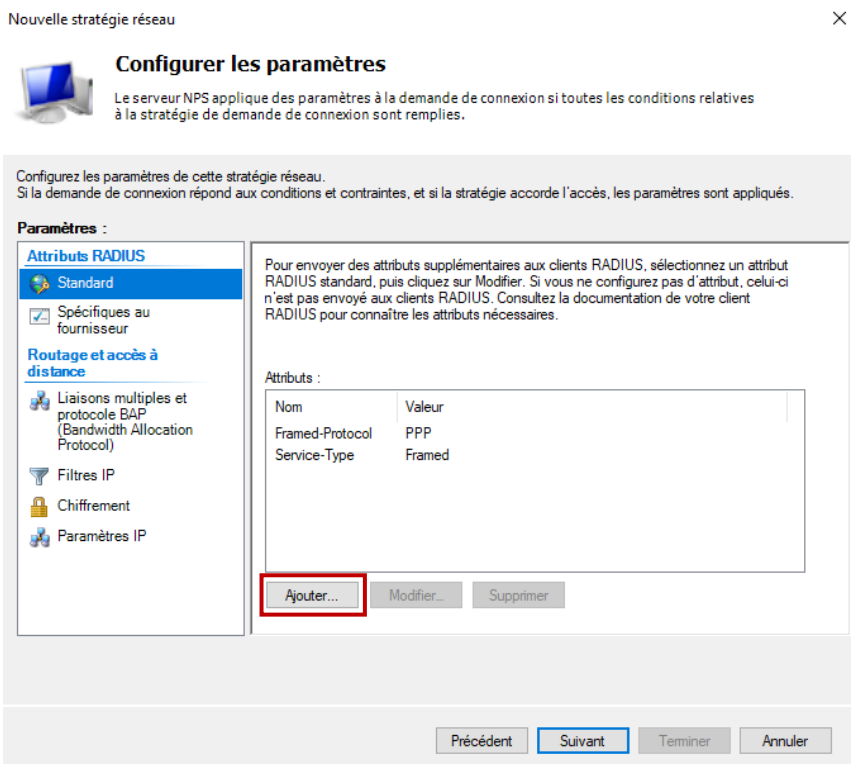
- Dans l'écran Configurer les méthodes d'authentification, je déclare le type de protocoles EAP (PEAP) en cliquant sur Ajouter :



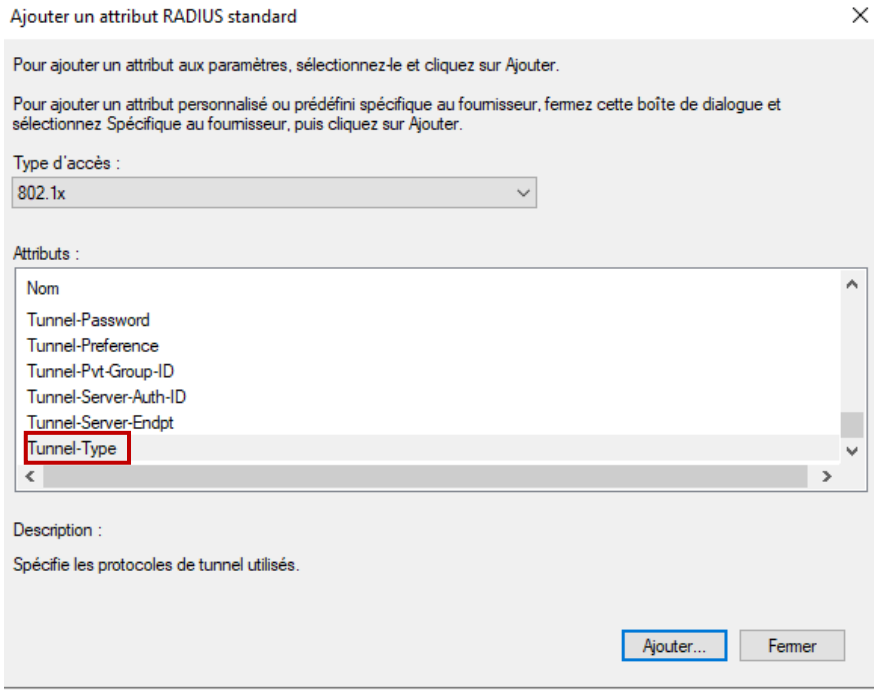
- Dans l'écran Configurer des contraintes, je clique sur Suivant :



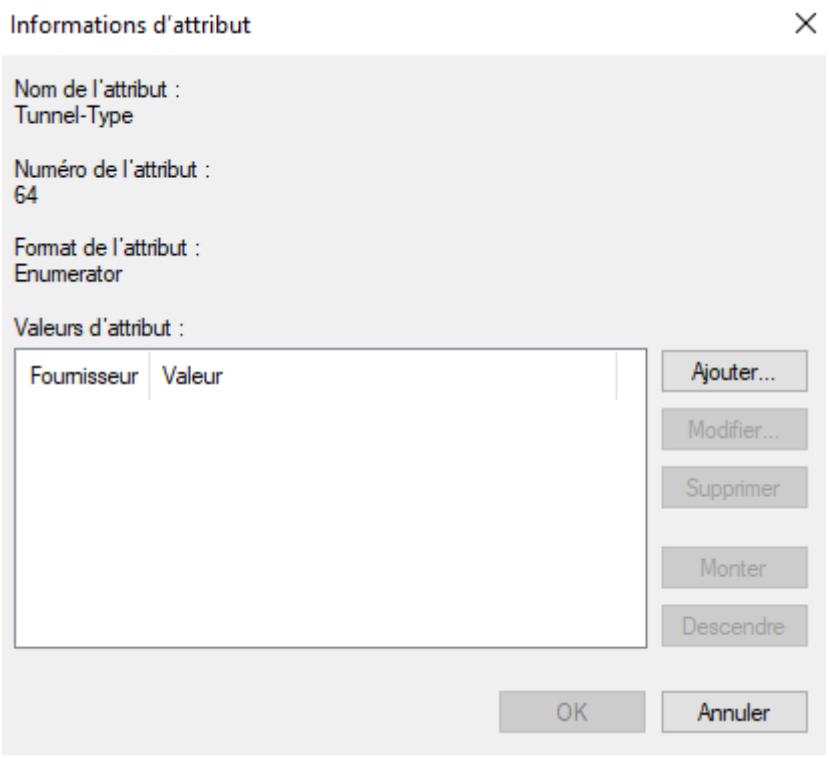
- Dans l'écran Configurer les paramètres, je clique sur Ajouter pour envoyer des attributs au client RADIUS :



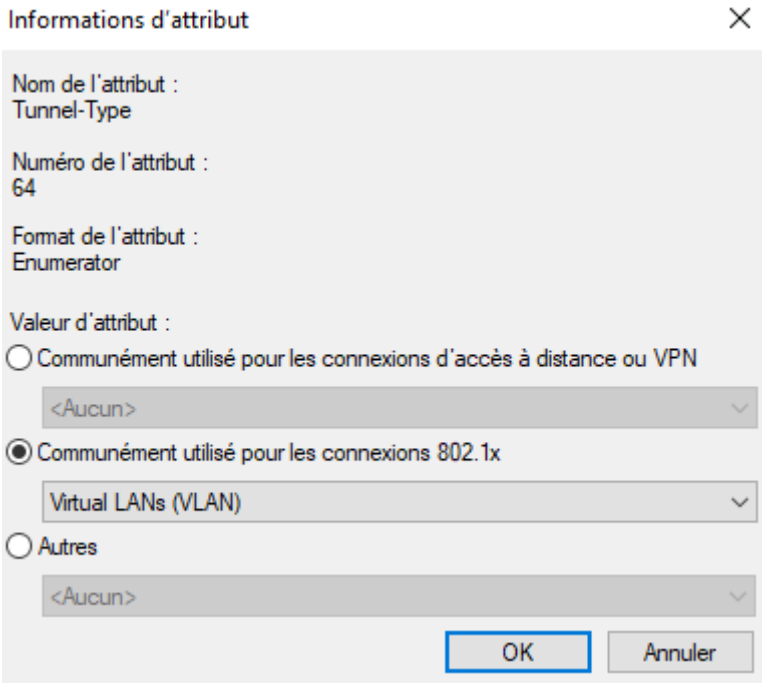
- Je sélectionne 802.1x dans Type d'accès puis sélectionnez l'attribut Tunnel-Type et je clique sur Ajouter :



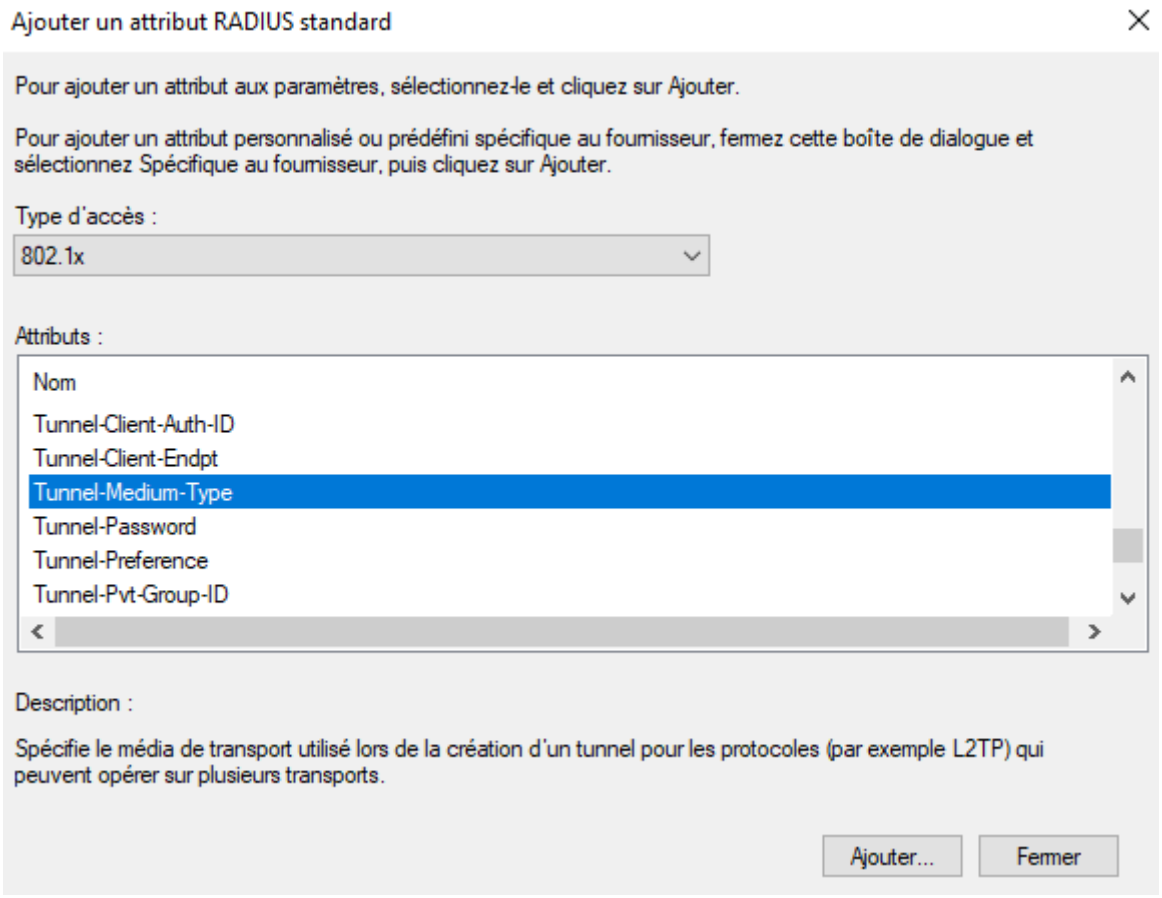
- Je clique sur Ajouter :



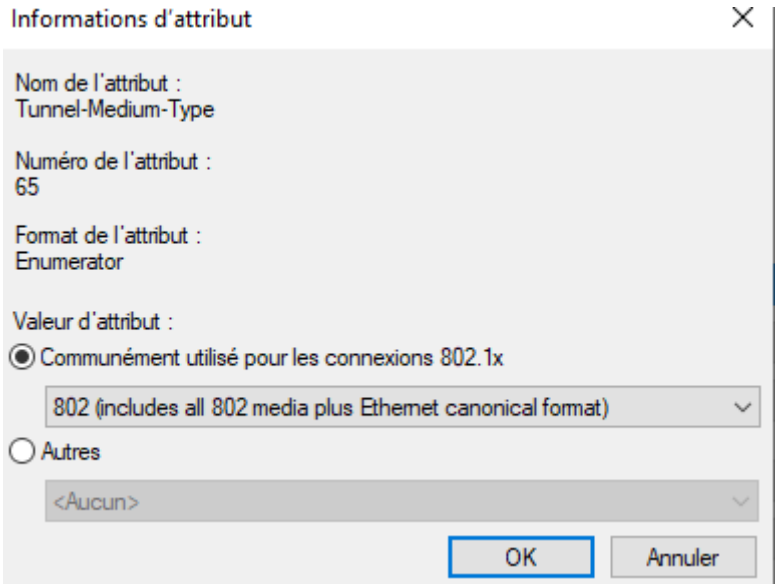
- Je sélectionne Virtual LANs :



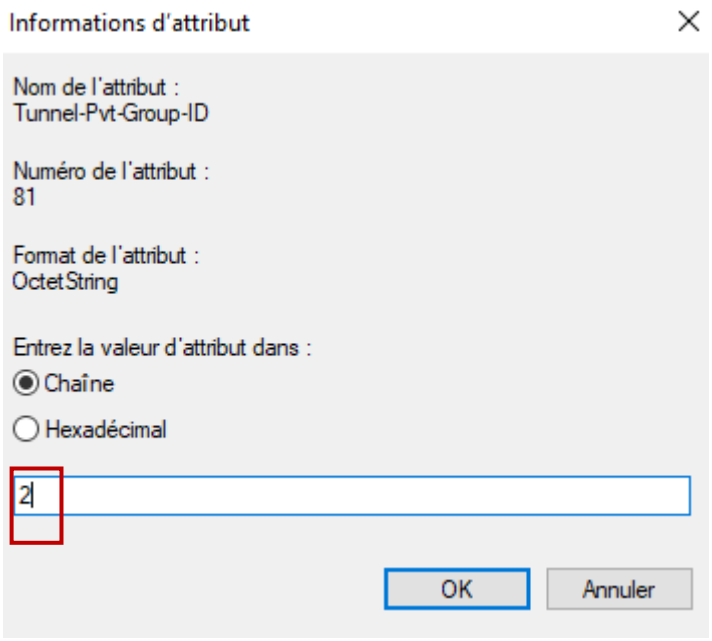
- Je clique sur OK :



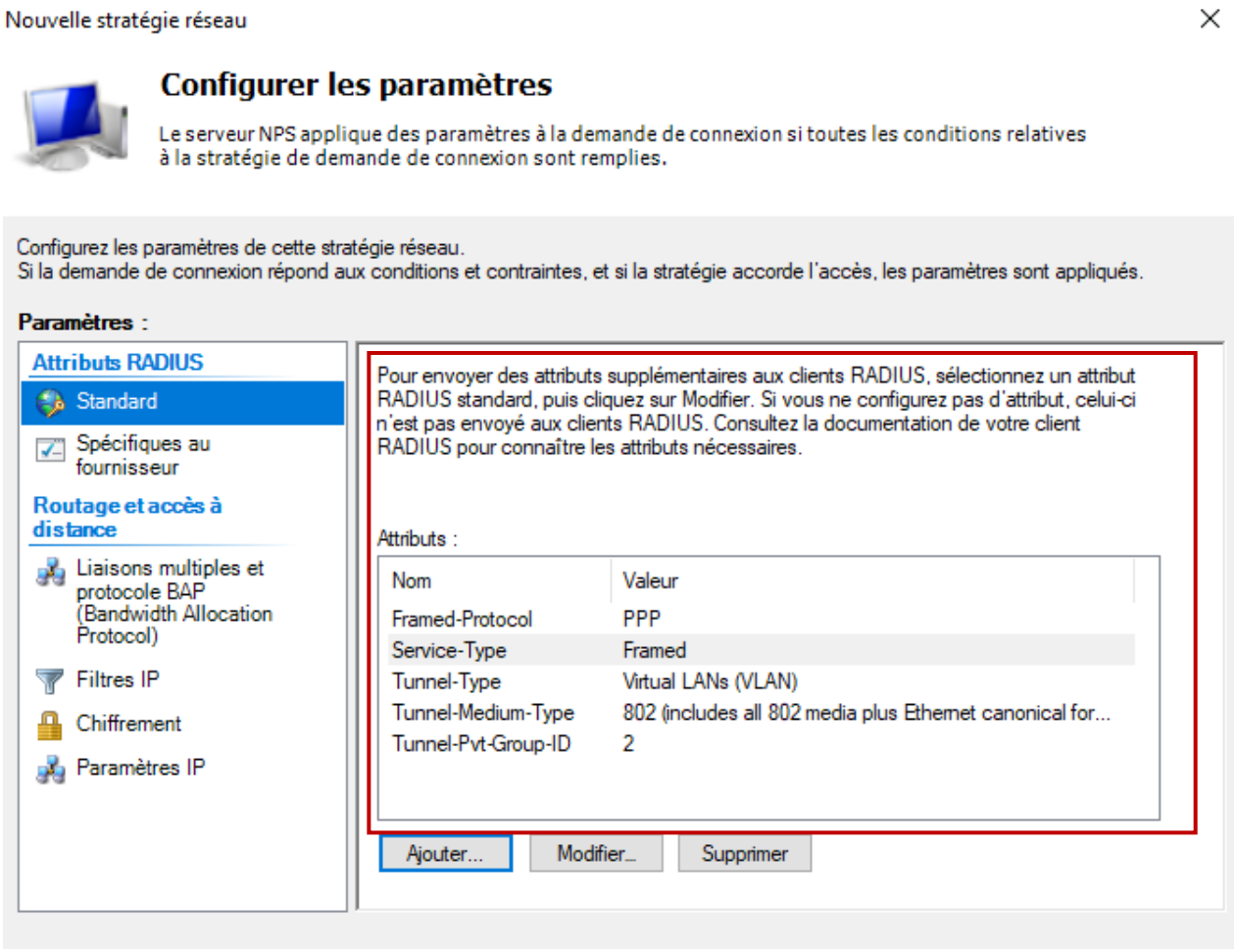
- Je sélectionne 802 includes :



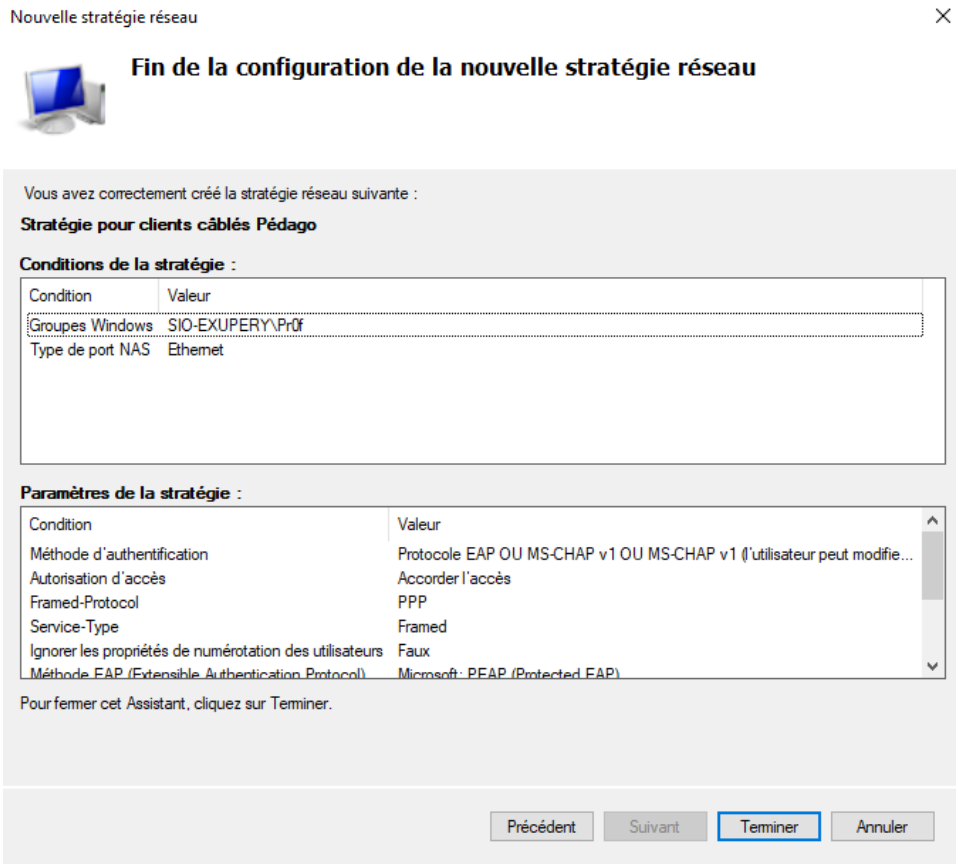
- Je spécifie le numéro de VLAN dans lequel je veux positionner les membres du groupe Prof :



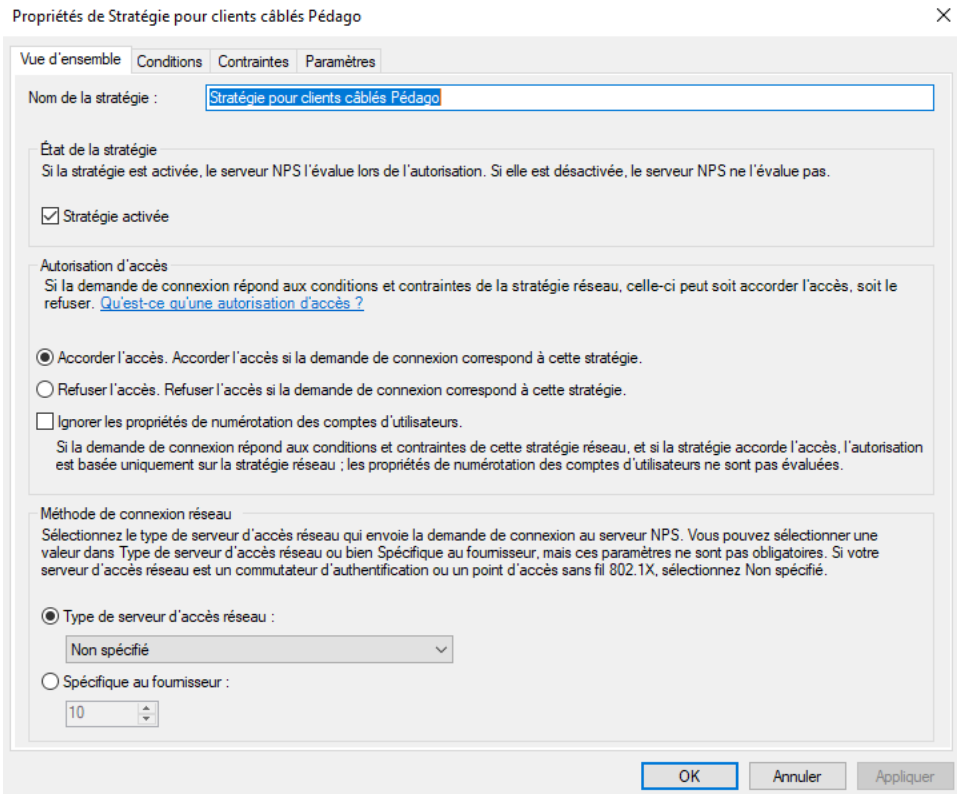
- Je clique sur Fermer dans l'écran Ajouter un attribut RADIUS standard puis sur Suivant dans l'écran récapitulatif des attributs :



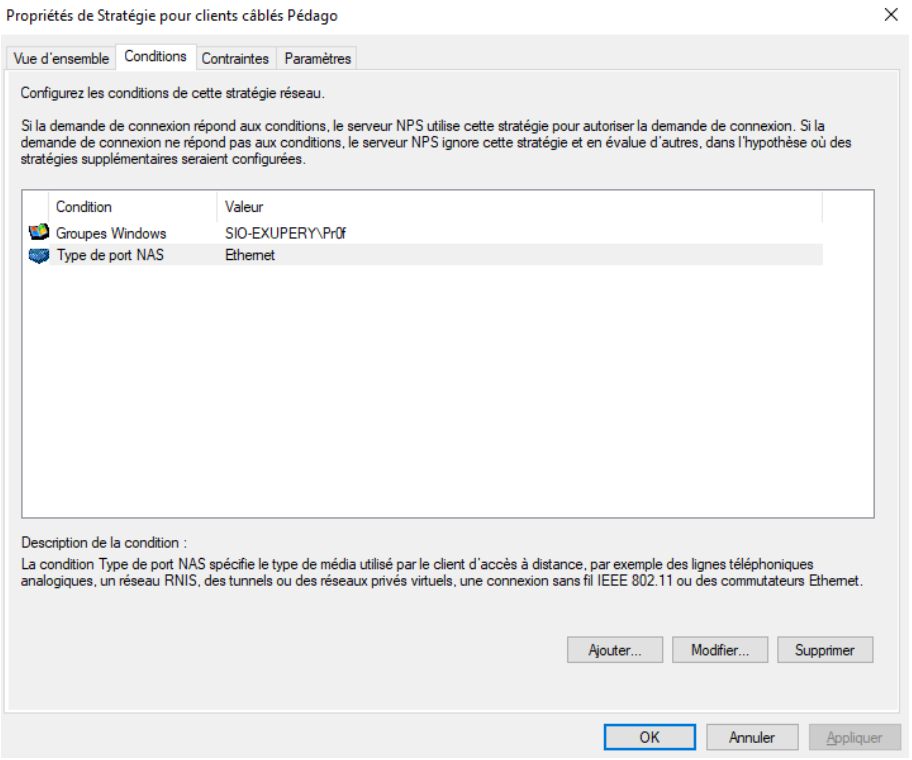
➢ Je clique sur Terminer dans l'écran Fin de la configuration de la nouvelle stratégie réseau :



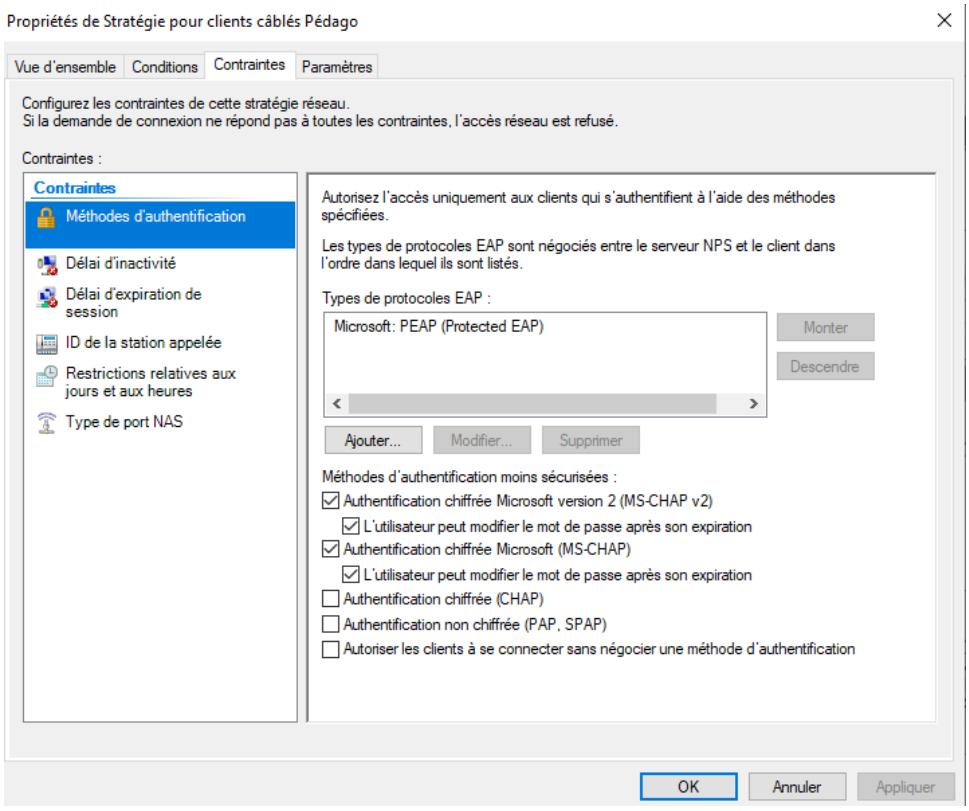
➢ Je recréer une nouvelle stratégie pour les clients câblés :

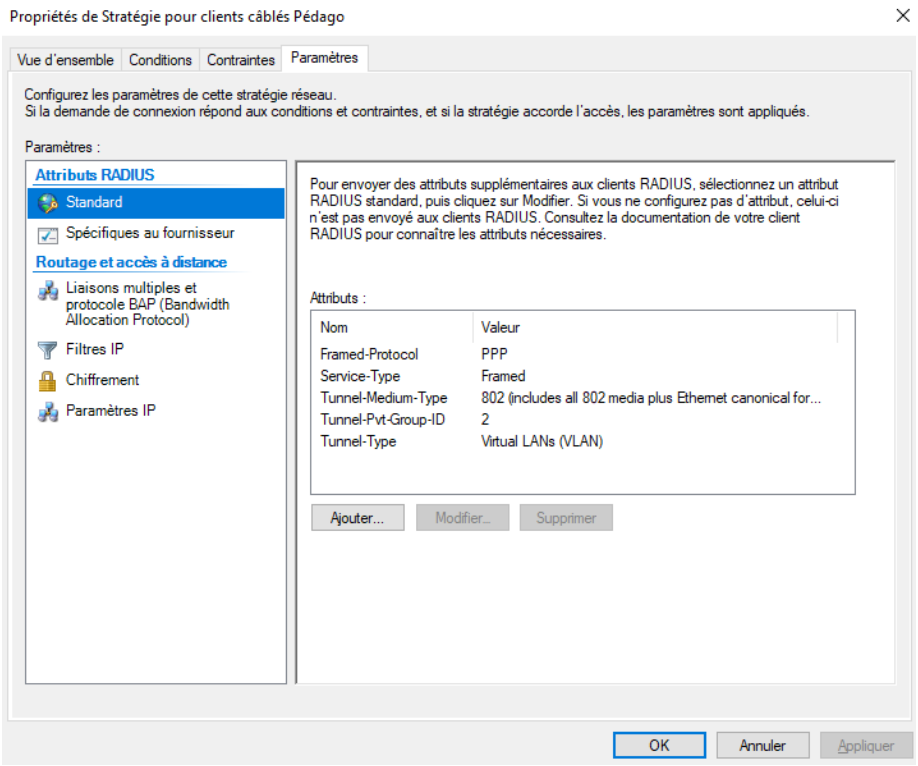


- J'ajoute Groupes Windows et Tyoe de port NAS :

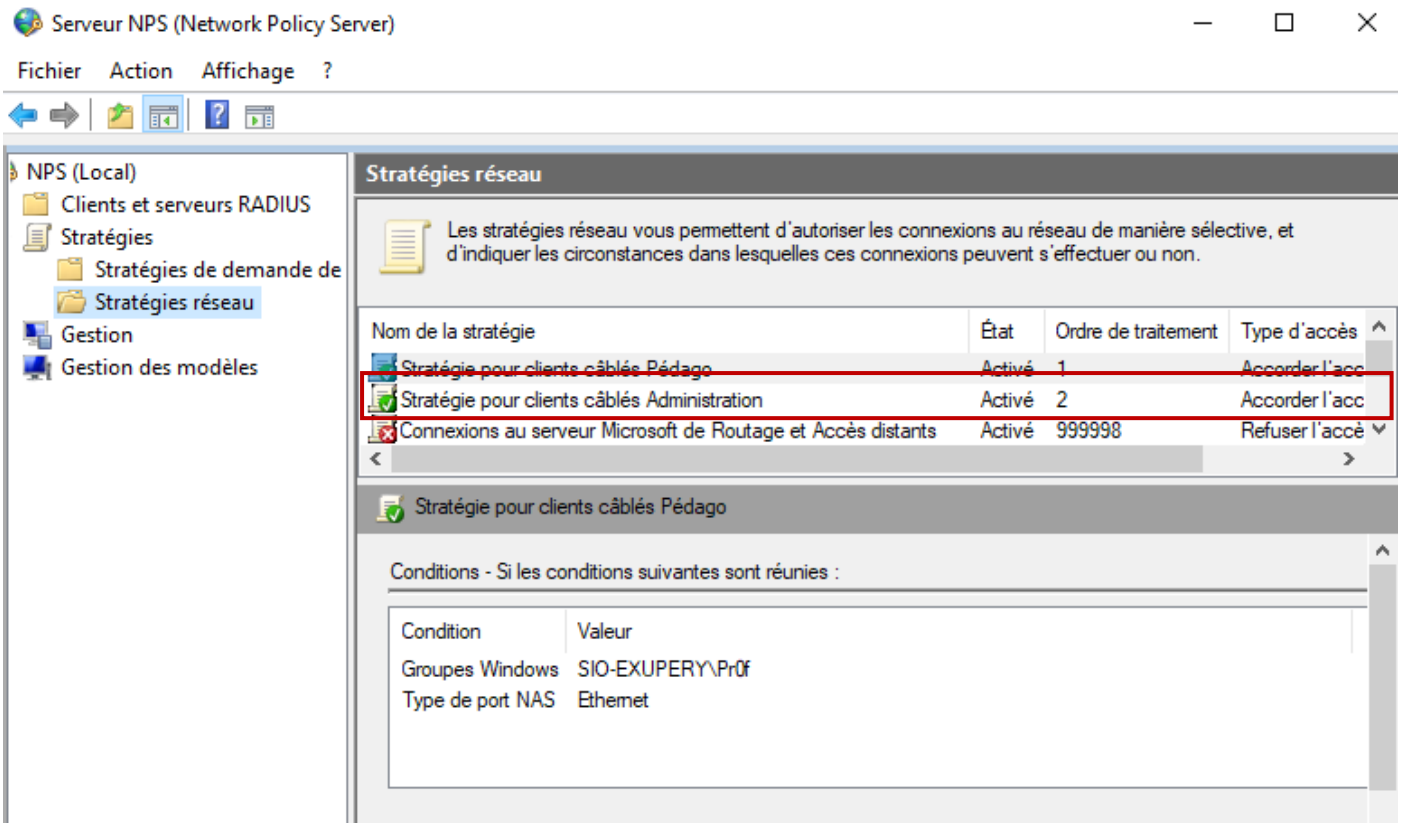


- J'ajoute la méthode d'authentification PEAP :

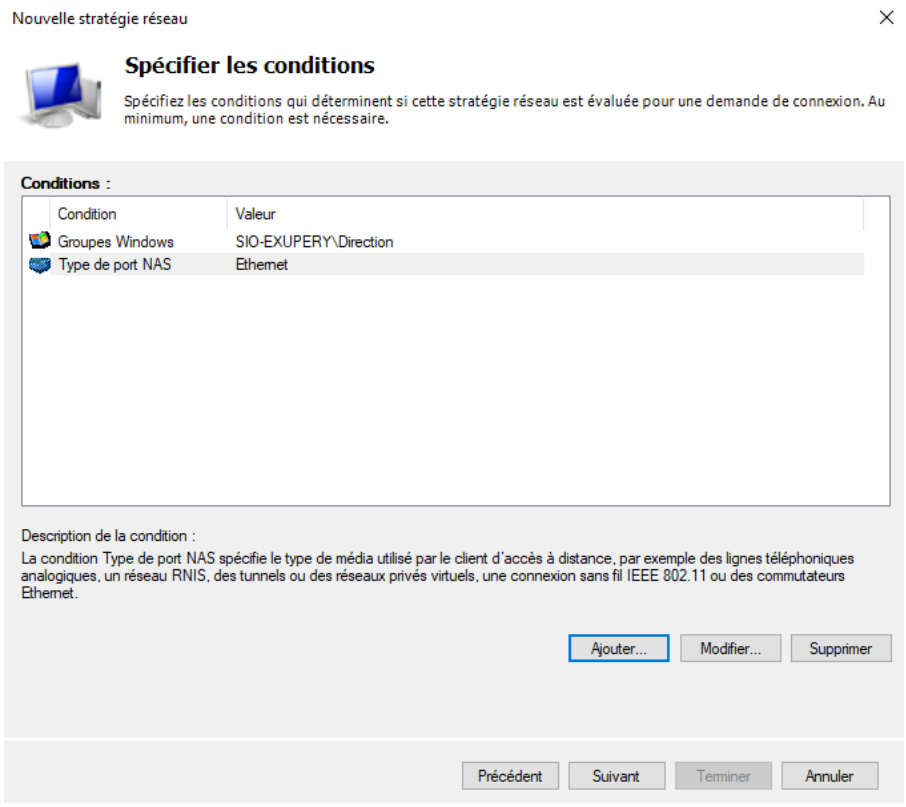




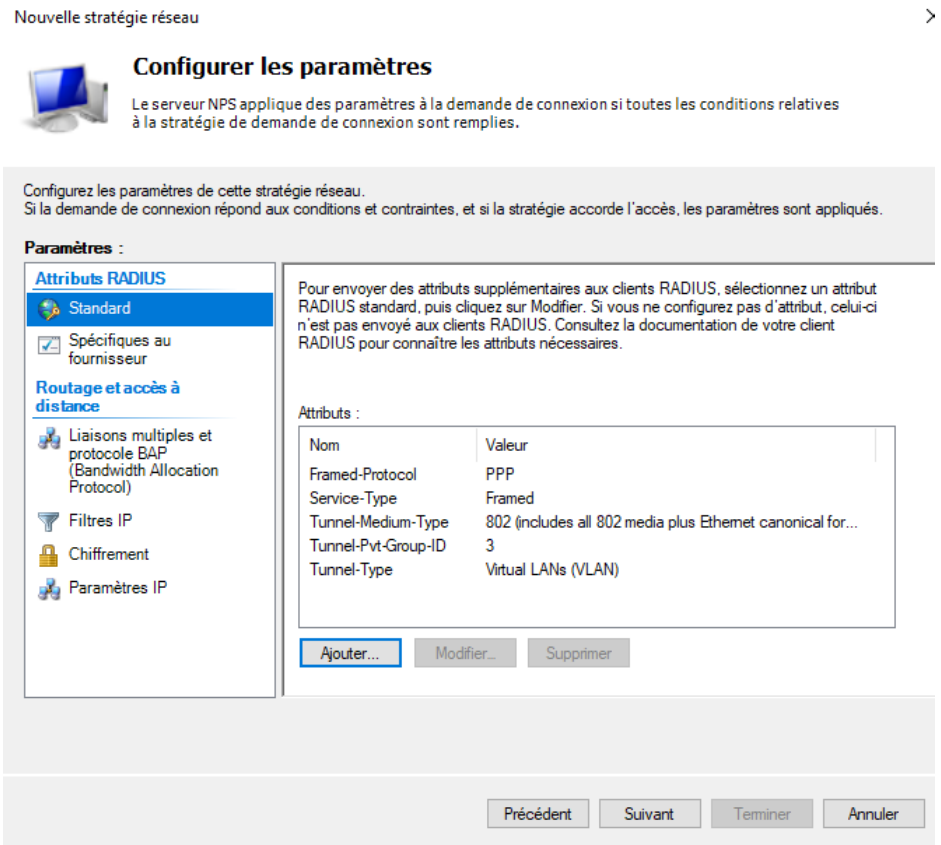
- En suivant le même procéder je créer une stratégie d'accès réseau plaçant dans le VLAN3 les membres authentifiés comme faisant partie du groupe Direction :



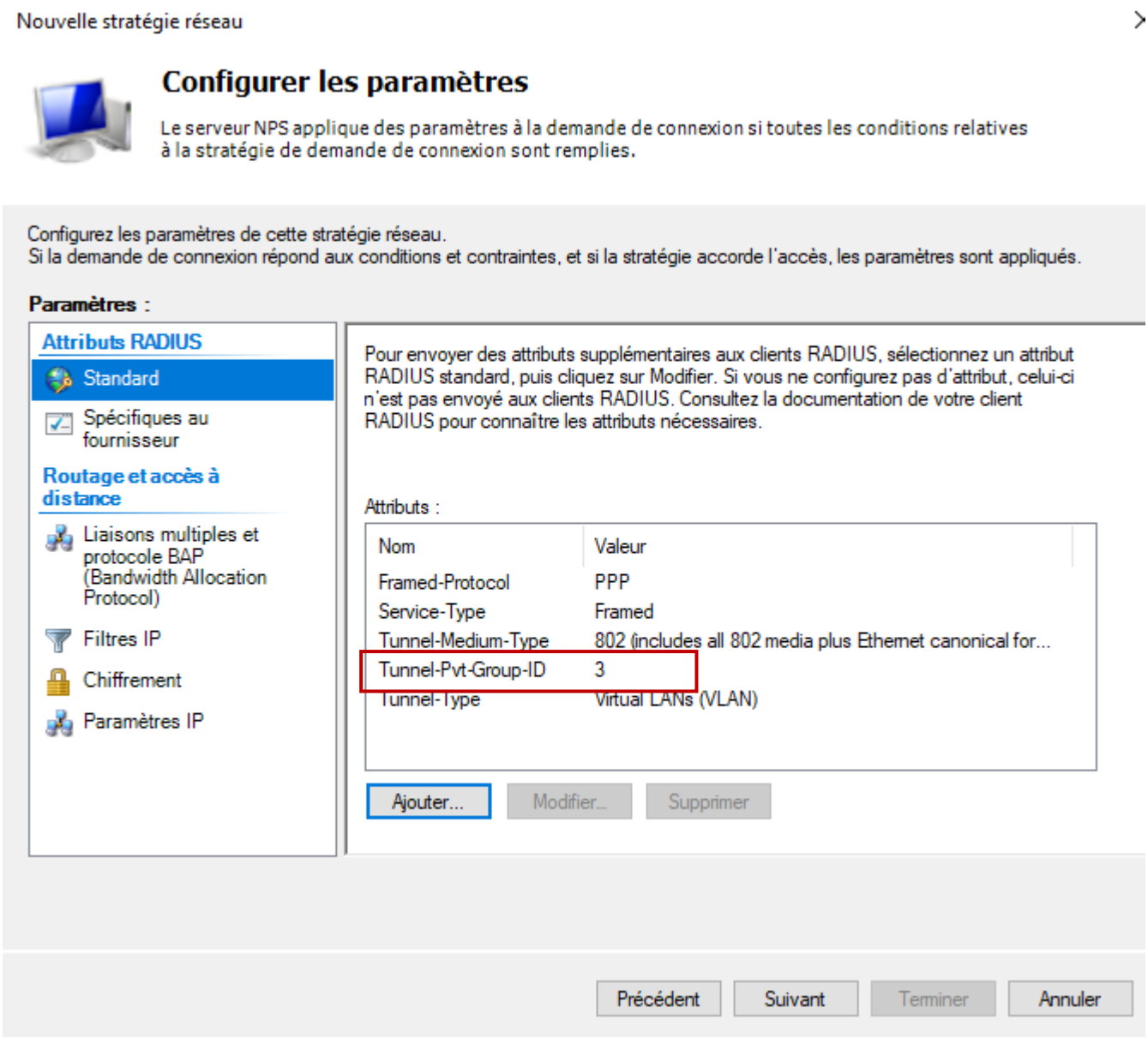
➢ J'ajoute Groupes Windows et Type de port NAS :



➢ J'ajoute la méthode d'authentification PEAP :



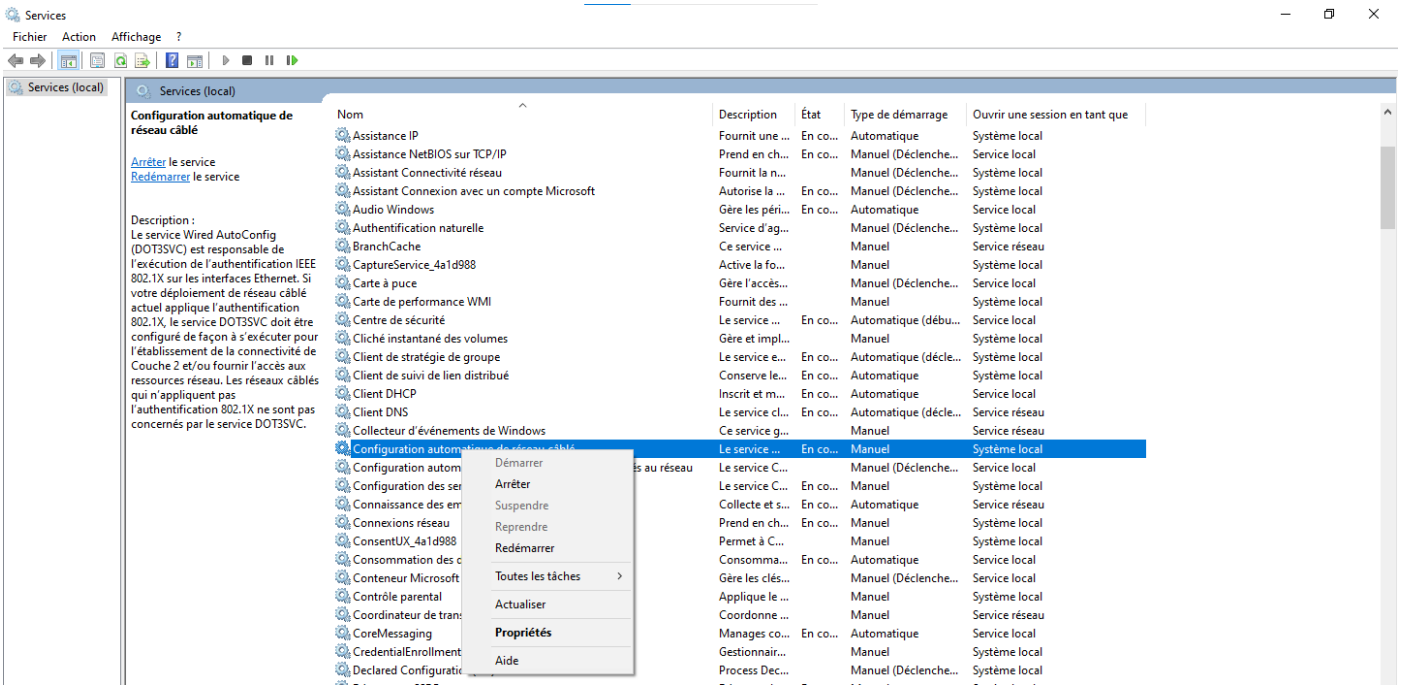
- Je veille bien à choisir le VLAN3 pour cette stratégie :



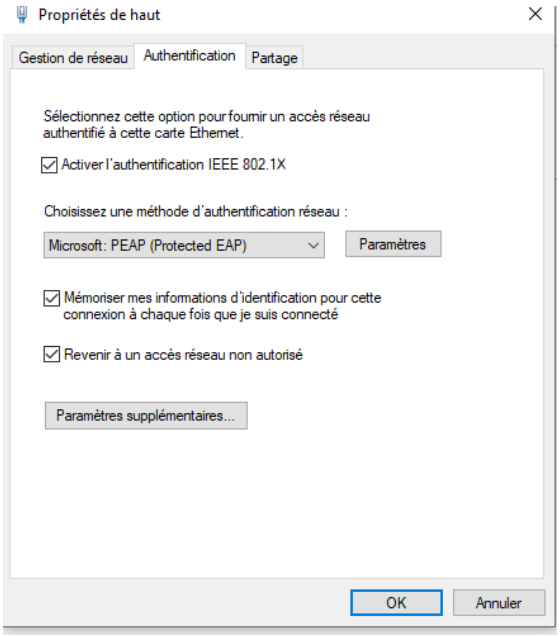
Annexe 3 : Demande de connexion des utilisateurs rveau et cgeley

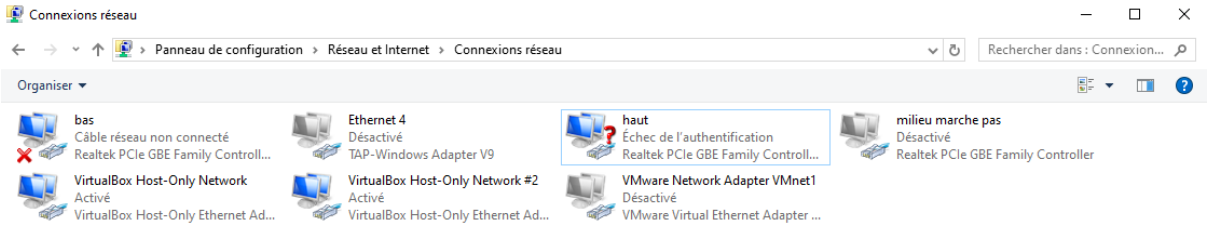
Sur le PC2 qui est un poste hors domaine

- J'active dans les services, le service Configuration automatique de réseau câblé :

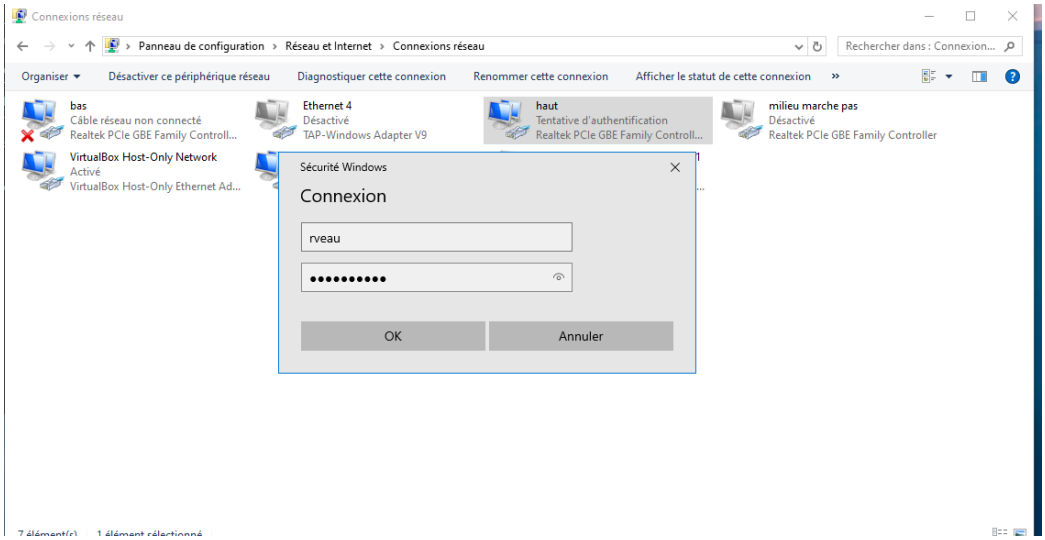


- Et puis dans les propriétés de la carte réseau du PC2 : je coche Activer et désactive l'authentification IEEE 802.1x pour faire apparaitre le menu d'authentification :

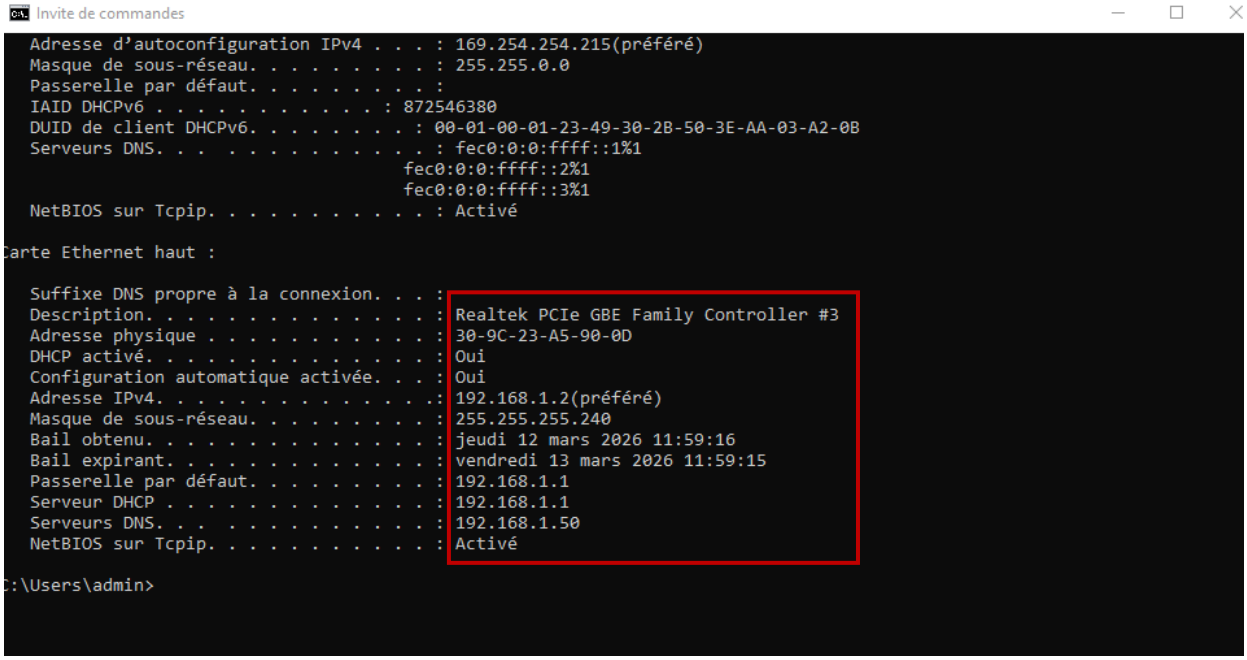




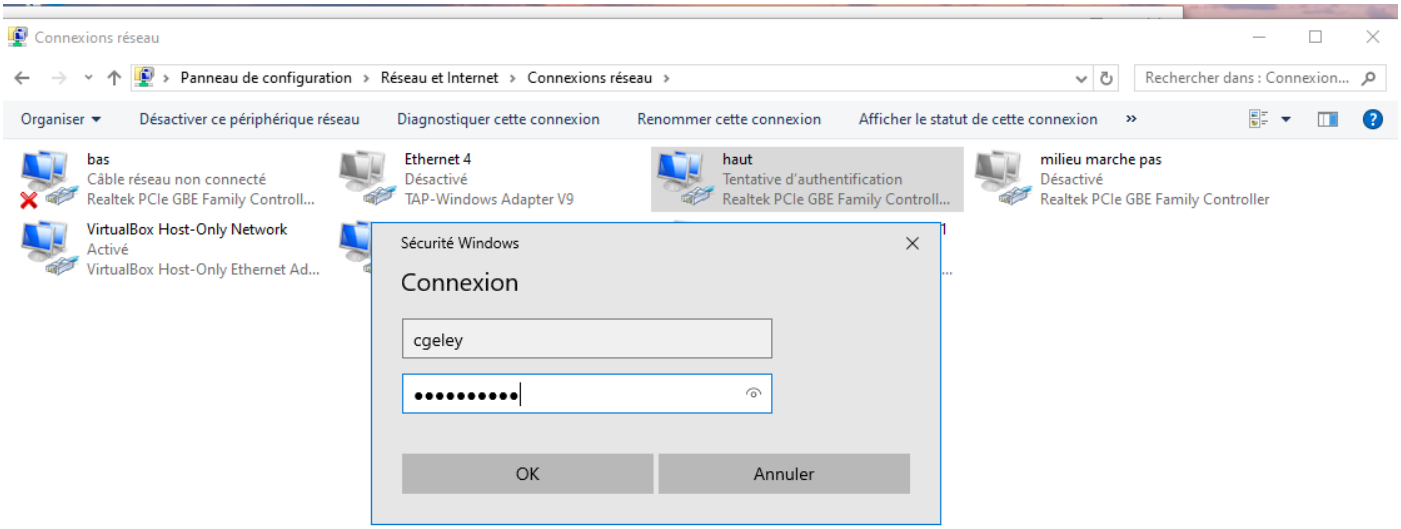
- Je me connecte avec le compte rveau :



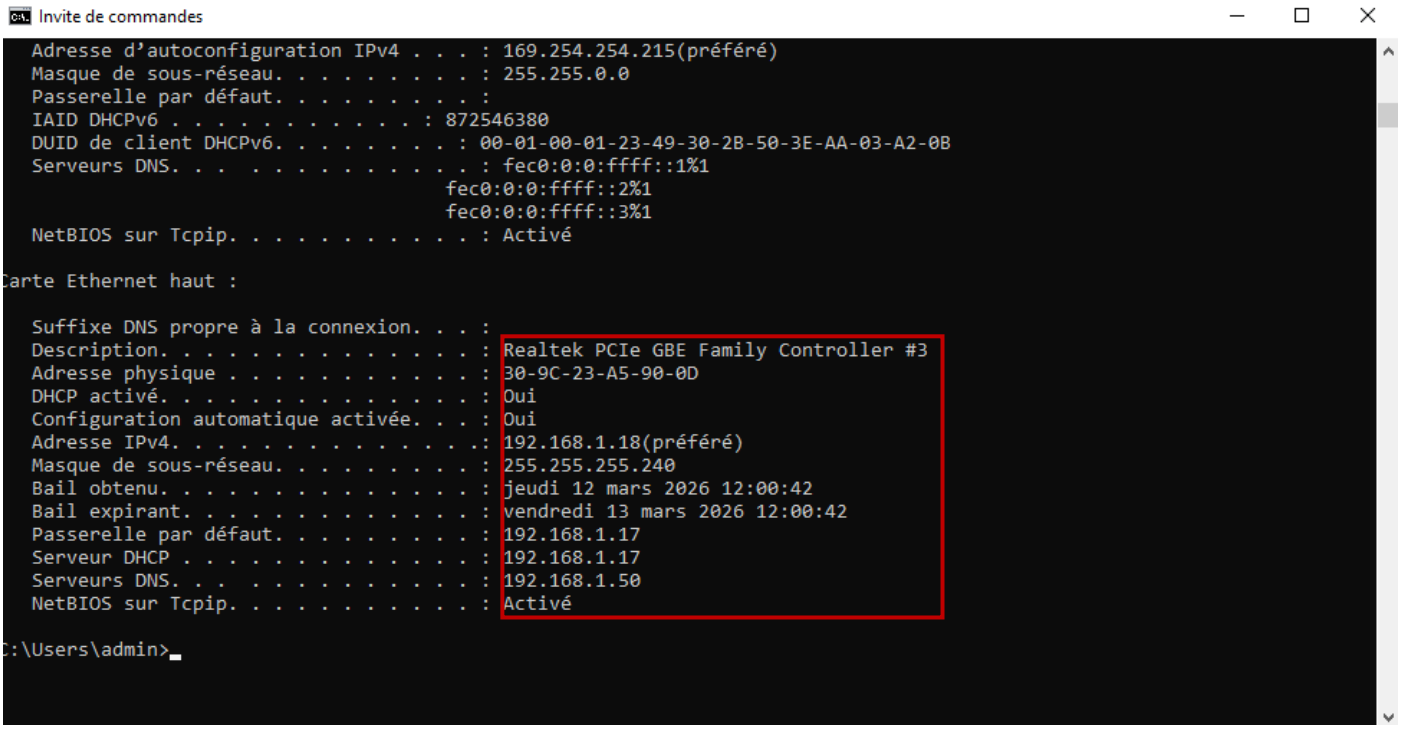
- Je me rends dans la configuration ip de la machine, je constate que celle-ci s'est mis dans le bon VLAN :



- Je me connecte aussi sur le deuxième compte cgeley :



- Je me rends aussi dans la configuration ip :



- Sur le commutateur client Radius :

```
*Mar  3 00:06:28.679: %DOT1X-5-FAIL: Authentication failed for client (309c.23a5.900d) on Interface Fa0/8 AuditSessio
nID
*Mar  3 00:06:28.679: %AUTHMGR-7-RESULT: Authentication result 'timeout' from 'dot1x' for client (309c.23a5.900d) on
Interface Fa0/8 AuditSessionID C0A80002000000110A4CFFFB
*Mar  3 00:07:26.409: %AUTHMGR-5-START: Starting 'dot1x' for client (309c.23a5.900d) on Interface Fa0/8 AuditSessionI
D C0A80002000000120A52A715
*Mar  3 00:07:36.702: %DOT1X-5-SUCCESS: Authentication successful for client (309c.23a5.900d) on Interface Fa0/8 Audi
tSessionID
*Mar  3 00:07:36.702: %AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client (309c.23a5.900d) on
Interface Fa0/8 AuditSessionID C0A80002000000120A52A715
*Mar  3 00:07:36.702: %AUTHMGR-5-VLANASSIGN: VLAN 2 assigned to Interface Fa0/8 AuditSessionID C0A80002000000120A52A7
15
*Mar  3 00:07:37.725: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/8, changed state to up
*Mar  3 00:07:37.751: %AUTHMGR-5-SUCCESS: Authorization succeeded for client (309c.23a5.900d) on Interface Fa0/8 Audi
tSessionID C0A80002000000120A52A715
Switch>
Switch>sh dot1x all summary
Interface        PAE     Client          Status
---------------------------------------------------
Fa0/7            AUTH    none            UNAUTHORIZED
Fa0/8            AUTH    309c.23a5.900d  AUTHORIZED
Switch>
```

- J'observe que l'interface Fa0/8 est relié au vlan 2 :

```
Switch>sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, 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    VLAN0002                         active    Fa0/8
3    VLAN0003                         active
4    VLAN0004                         active    Fa0/2
99   VLAN0099                         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
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
2    enet  100002     1500  -      -      -        -    -        0      0
3    enet  100003     1500  -      -      -        -    -        0      0
 --More--
```

- Dans l'observateur d'événements je filtre le journal de logs, je me rend sur l'événement correspondant et je copie les détails au format texte (je n'ai pas le screen, j'ai que les détails) :

Nom du journal :Security

Source : Microsoft-Windows-Security-Auditing

Date : 12/03/2026 11:51:52

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 : 24-01-C7-67-23-88

Identificateur de la station appelante : 30-9C-23-A5-90-0D

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 : 50008

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 clients 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.

XML de l’événement :

<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">

<System>

<Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-a5ba-3e3b0328c30d}" />

<EventID>6272</EventID>

<Version>2</Version>

<Level>0</Level>

<Task>12552</Task>

<Opcode>0</Opcode>

<Keywords>0x8020000000000000</Keywords>

<TimeCreated SystemTime="2026-03-12T10:51:52.1730698Z" />

<EventRecordID>44503</EventRecordID>

<Correlation ActivityID="{3eb3d47d-b1f6-0000-1cd5-b33ef6b1dc01}" />

<Execution ProcessID="624" ThreadID="320" />

<Channel>Security</Channel>

<Computer>AD.sio-exupery.local</Computer>

<Security />

</System>

<EventData>

<Data Name="SubjectUserSid">S-1-5-21-566680590-3389018048-3922203963-1147</Data>

<Data Name="SubjectUserName">rveau</Data>

<Data Name="SubjectDomainName">SIO-EXUPERY</Data>

<Data Name="FullyQualifiedSubjectUserName">sio-exupery.local/Pédagogie/PROF/Régis Veau</Data>

<Data Name="SubjectMachineSID">S-1-0-0</Data>

<Data Name="SubjectMachineName">-</Data>

<Data Name="FullyQualifiedSubjectMachineName">-</Data>

<Data Name="CalledStationID">24-01-C7-67-23-88</Data>

<Data Name="CallingStationID">30-9C-23-A5-90-0D</Data>

<Data Name="NASIPv4Address">192.168.0.2</Data>

<Data Name="NASIPv6Address">-</Data>

<Data Name="NASIdentifier">-</Data>

<Data Name="NASPortType">Ethernet</Data>

<Data Name="NASPort">50008</Data>

<Data Name="ClientName">Client-Cisco-2960</Data>

<Data Name="ClientIPAddress">192.168.0.2</Data>

<Data Name="ProxyPolicyName">Connexion câblée</Data>

<Data Name="NetworkPolicyName">Stratégie pour clients câblés Pédago</Data>

<Data Name="AuthenticationProvider">Windows</Data>

<Data Name="AuthenticationServer">AD.sio-exupery.local</Data>

<Data Name="AuthenticationType">PEAP</Data>

<Data Name="EAPType">Microsoft: Mot de passe sécurisé (EAP-MSCHAP version 2)</Data>

<Data Name="AccountSessionIdentifier">-</Data>

<Data Name="LoggingResult">Les informations de suivi ont été inscrites dans le fichier journal local.</Data>

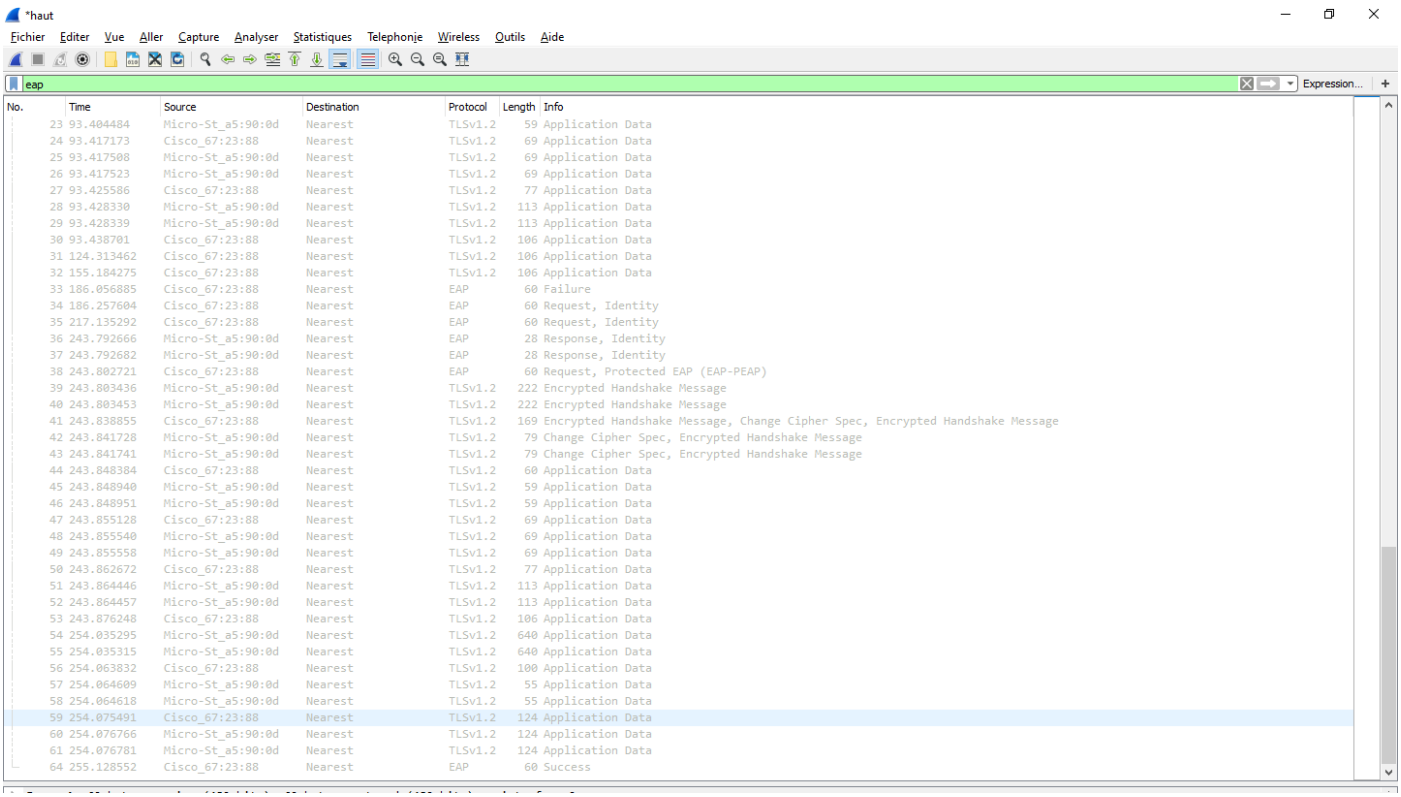
</EventData>

</Event>

Annexe 4 : Capture de trames : messages RADIUS

J'installe Wireshark sur mes deux machines PC2 et le serveur Radius et j'effectue une capture de trames :

- Sur le PC2 :



➢ Sur le serveur Radius :