

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

Table des Matières :

Annexe 1 : Commutateur Cisco 2960 et authentification 802.1x.....	2
Annexe 2 : Mise en place du serveur RADIUS (service NPS).....	8
2.1 Situation de départ.....	8
2.2 Ajout du rôle Services de certificats Active Directory.....	10
2.3 Installation du service NPS.....	18
2.4 Configuration du serveur RADIUS NPS.....	22
2.4.1 Déclaration du client RADIUS.....	24
2.4.2 Déclaration d'une stratégie de demande de connexion.....	25
2.4.3 Déclaration d'une stratégie d'accès au réseau.....	30
Annexe 3 : Demande de connexion des utilisateurs rveau et cgeley.....	45
Annexe 4 : Capture de trames : messages RADIUS.....	51

Annexe 1 : Commutateur Cisco 2960 et authentification 802.1x

- Configuration appliquée sur le switch en aval.

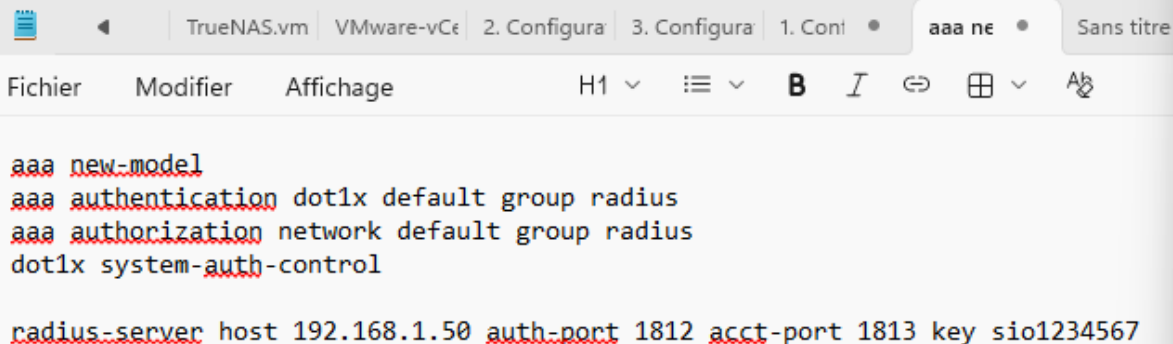
```
vlan 2
name Pedagogie
vlan 3
name Administration
vlan 4
name Serveurs
vlan 99
name Gestion

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

interface vlan 1
ip address 192.168.0.2 255.255.255.248
no shutdown

interface Fa0/2
switchport access vlan 4
switchport mode access

interface Fa0/19
switchport mode trunk
```



The screenshot shows a Cisco configuration window with a menu bar (Fichier, Modifier, Affichage) and a toolbar. The configuration text is as follows:

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

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

- Interfaces fa0/7 et fa0/8 :

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

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

- Copie du run vers le start :

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

- Configuration routeur :

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

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

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

- Copie du run vers le start :

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

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

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

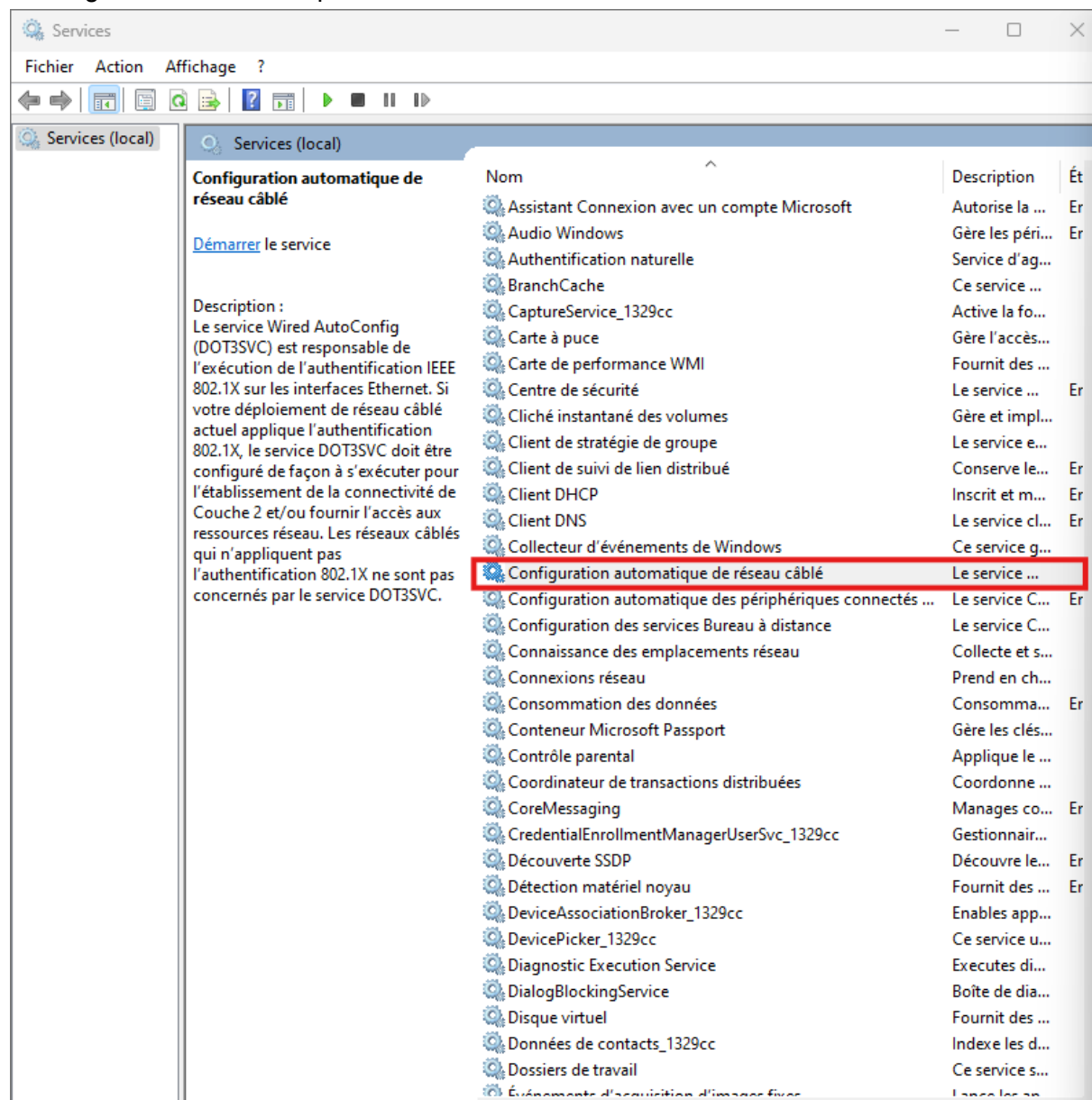
Dot1x Info for FastEthernet0/7
-----
PAE                      = AUTHENTICATOR
QuietPeriod              = 60
ServerTimeout            = 0
SuppTimeout              = 30
ReAuthMax                = 2
MaxReq                   = 2
TxPeriod                 = 30

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

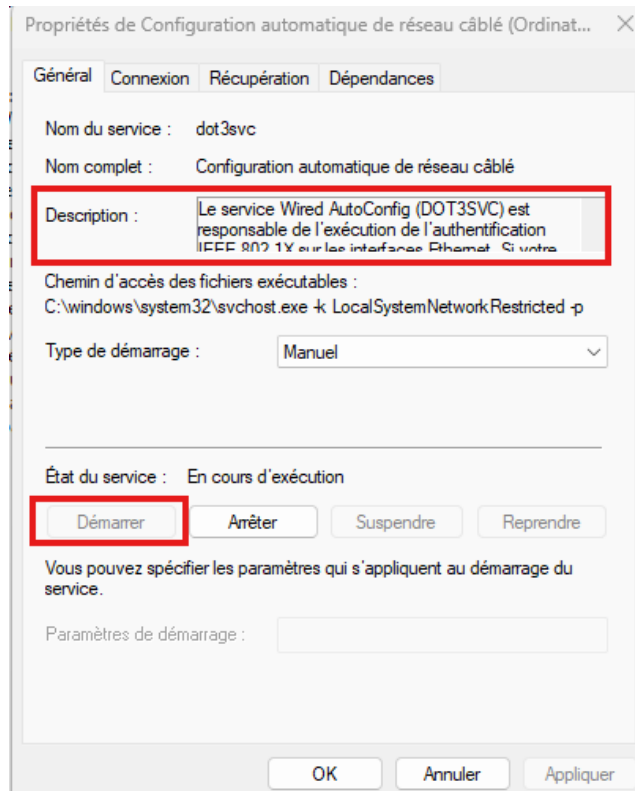
Switch#
```

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

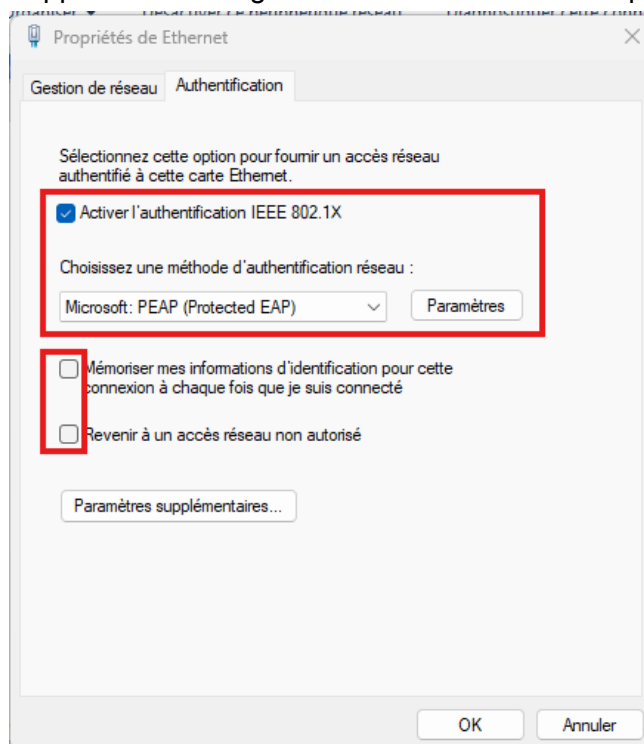
▪ Configuration du second pc :



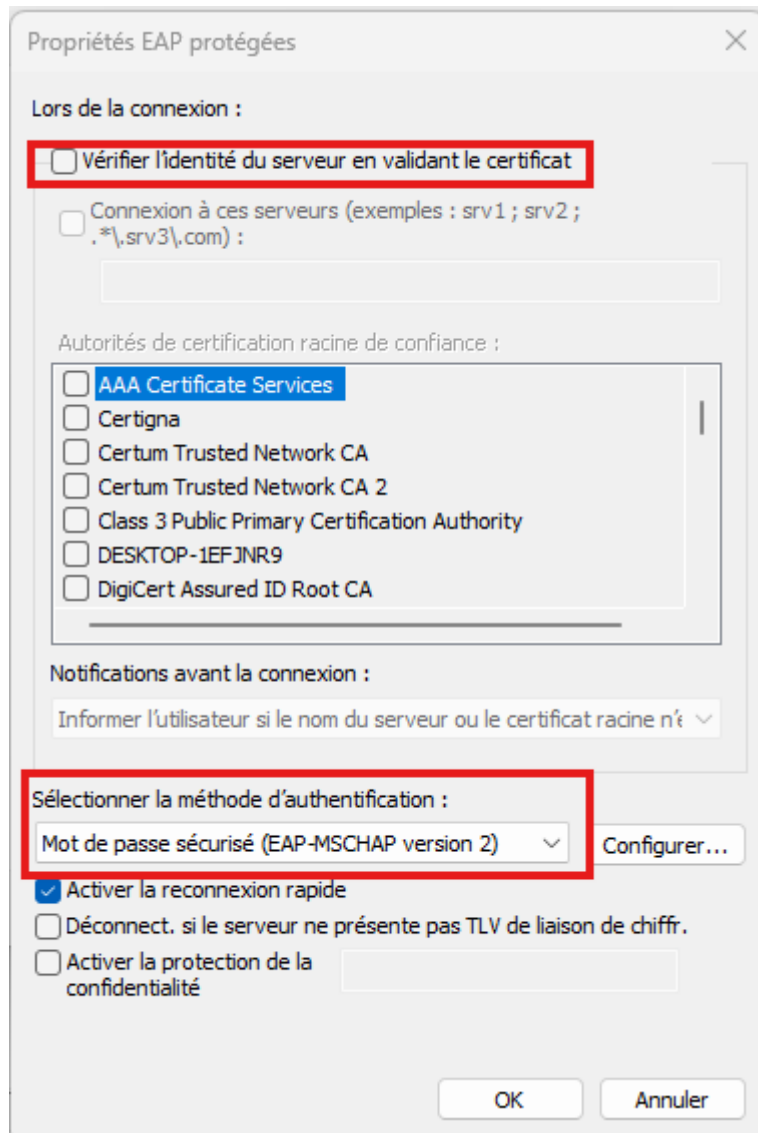
- Nous lançons le service de configuration automatique du réseau câblé.



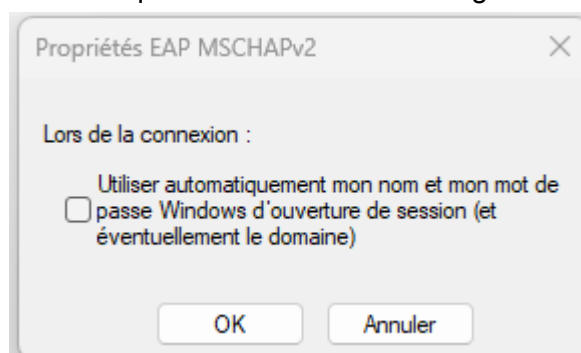
- Apparition de l'onglet authentification dans les propriétés de la carte réseau.



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



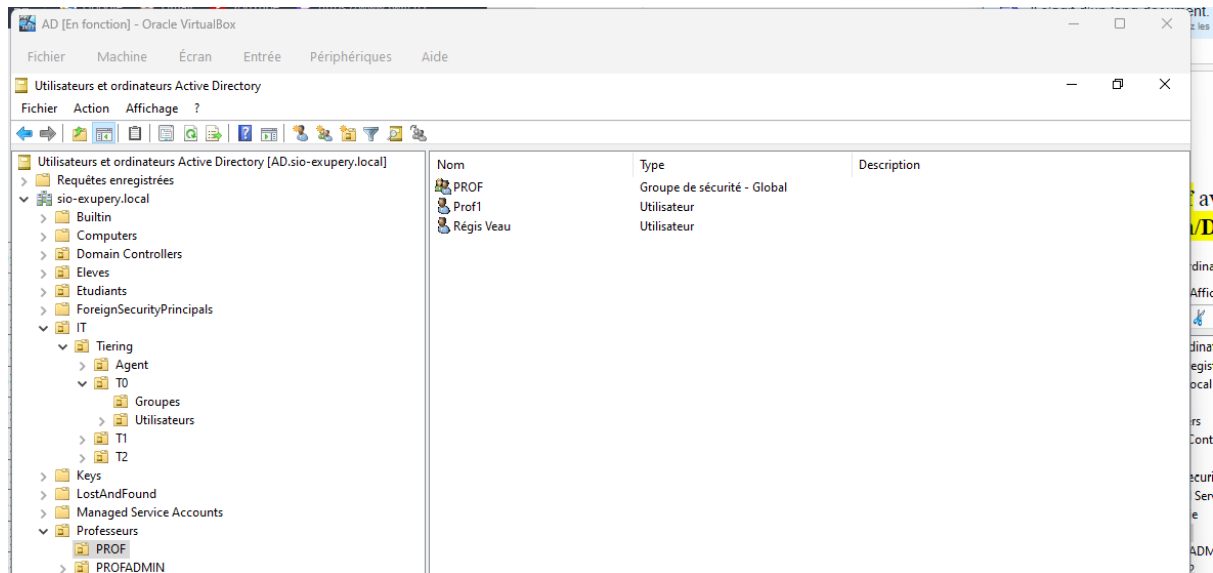
- Nous cliquons sur le bouton "Configurer"



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

2.1 Situation de départ

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



- Unité d'organisation "Administration" créé au préalable puis nous avons créé "Direction"
 - Création du compte utilisateur Corinne Geley

Nouvel objet - Utilisateur

Créer dans : sio-exupery.local/Administration/Direction

Prénom : Initiales :

Nom :

Nom complet :

Nom d'ouverture de session de l'utilisateur : @sio-exupery.local

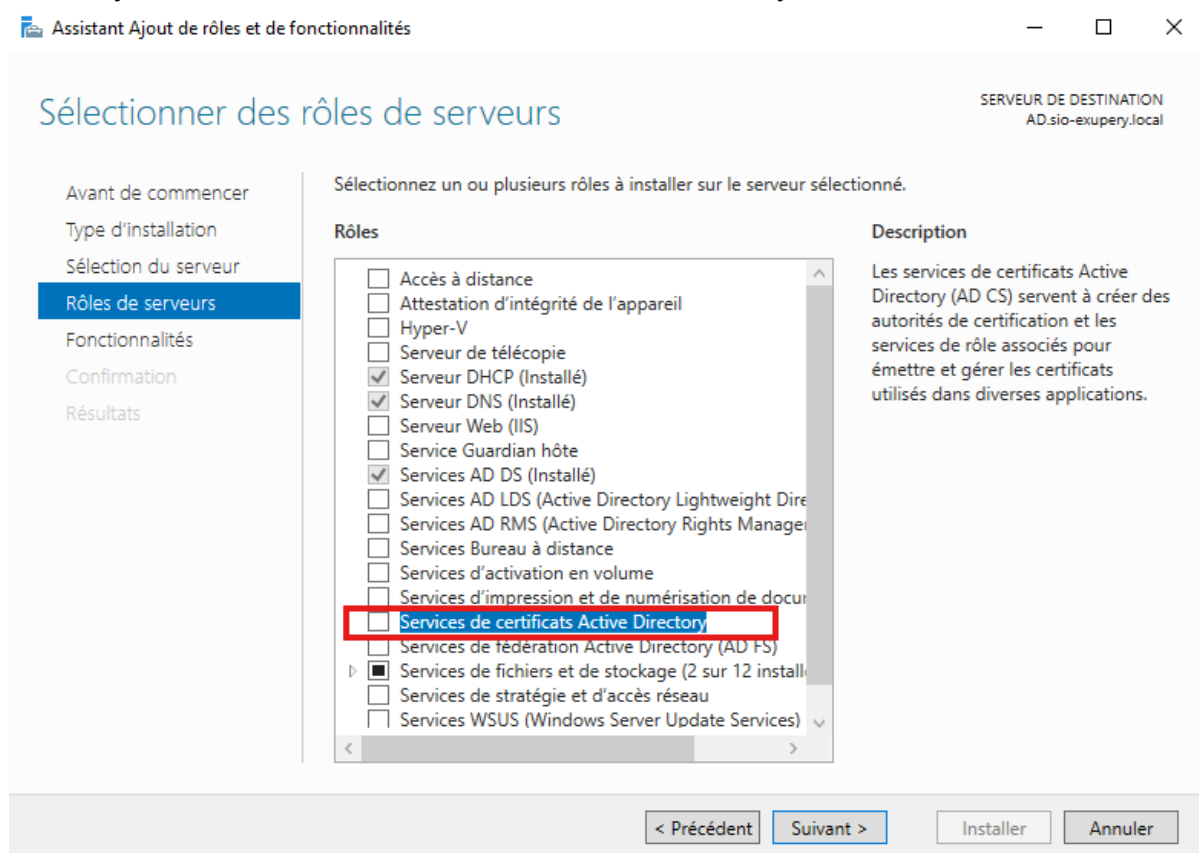
Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :

< Précédent Suivant > Annuler

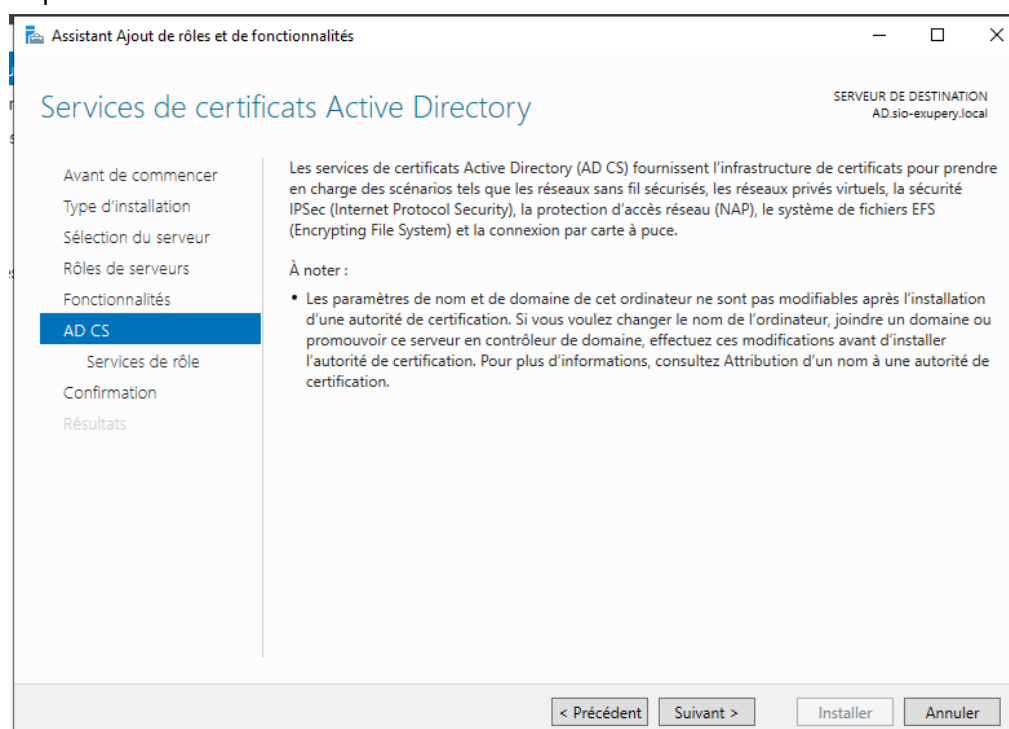
Utilisateurs et ordinateurs Active Directory			
Fichier Action Affichage ?			
Utilisateurs et ordinateurs Active Directory [AD.sio-exupery.local]			
> Requêtes enregistrées			
▼ sio-exupery.local			
▼ Administration			
Direction			
> Built-in			
> Computers			
Nom	Type	Description	
Corinne Geley	Utilisateur		
Direction	Groupe de sécurité - Global		

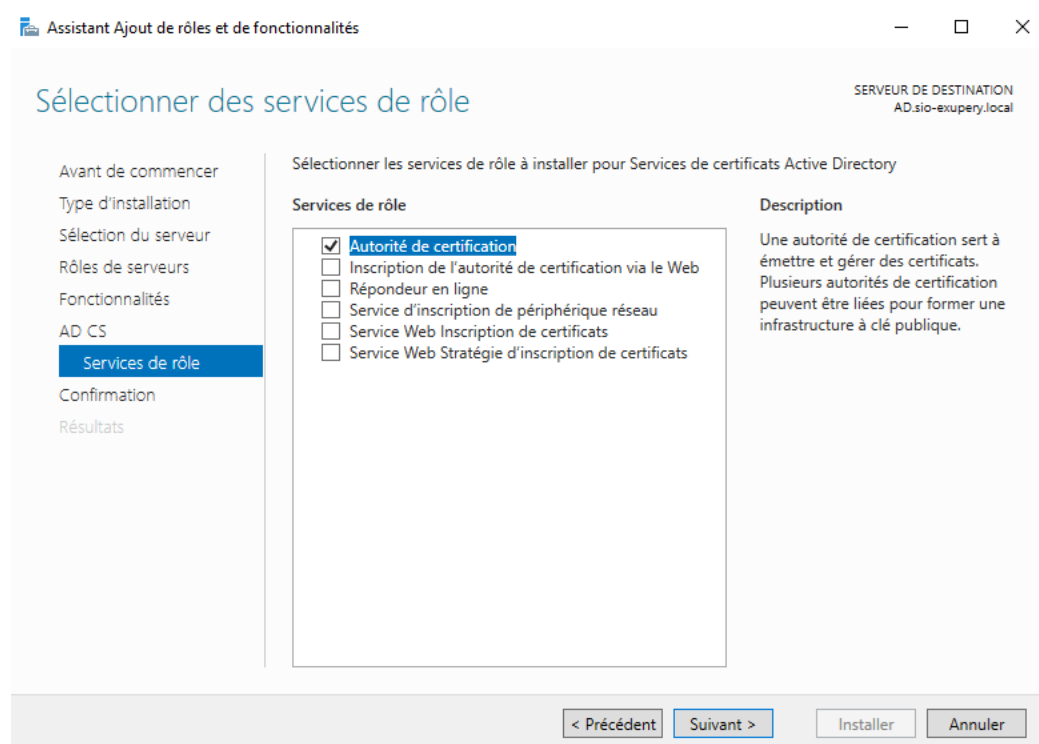
2.2 Ajout du rôle Services de certificats Active Directory

- Nous ajoutons le rôle Service de certificats Active Directory.

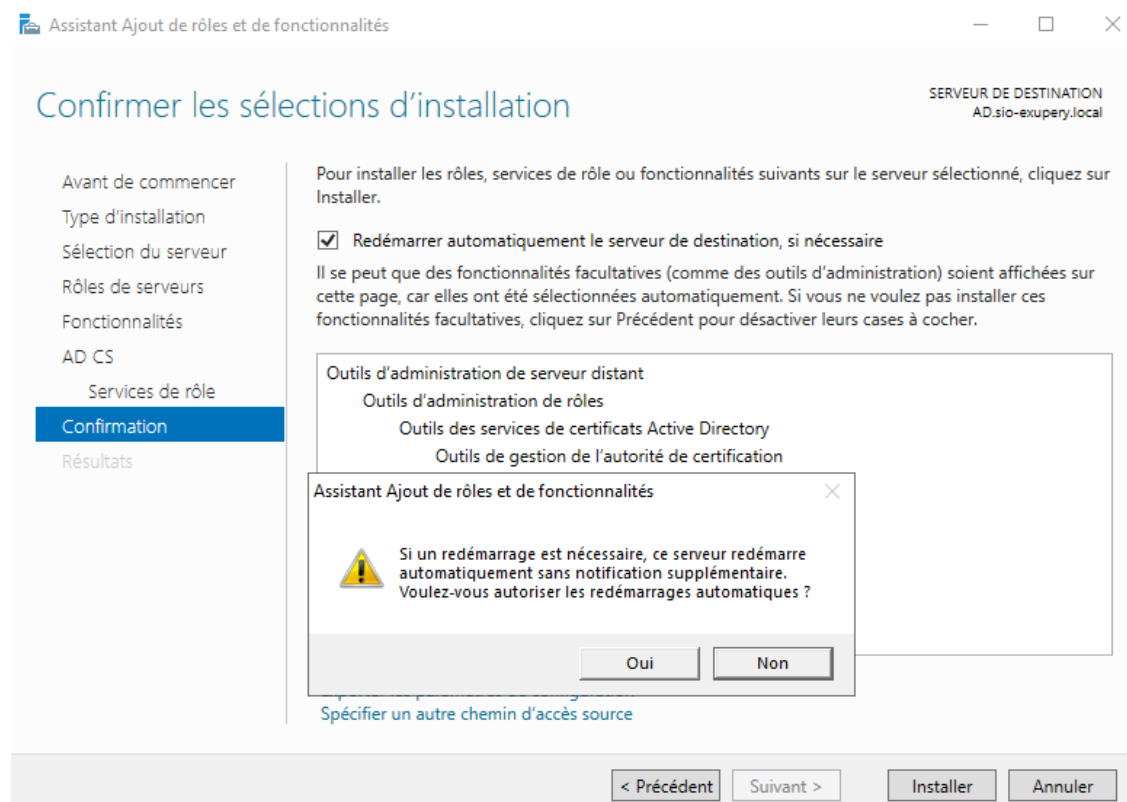


- Nous prenons connaissance des informations sur la page d'information AD CS et nous cliquons sur le bouton Suivant.

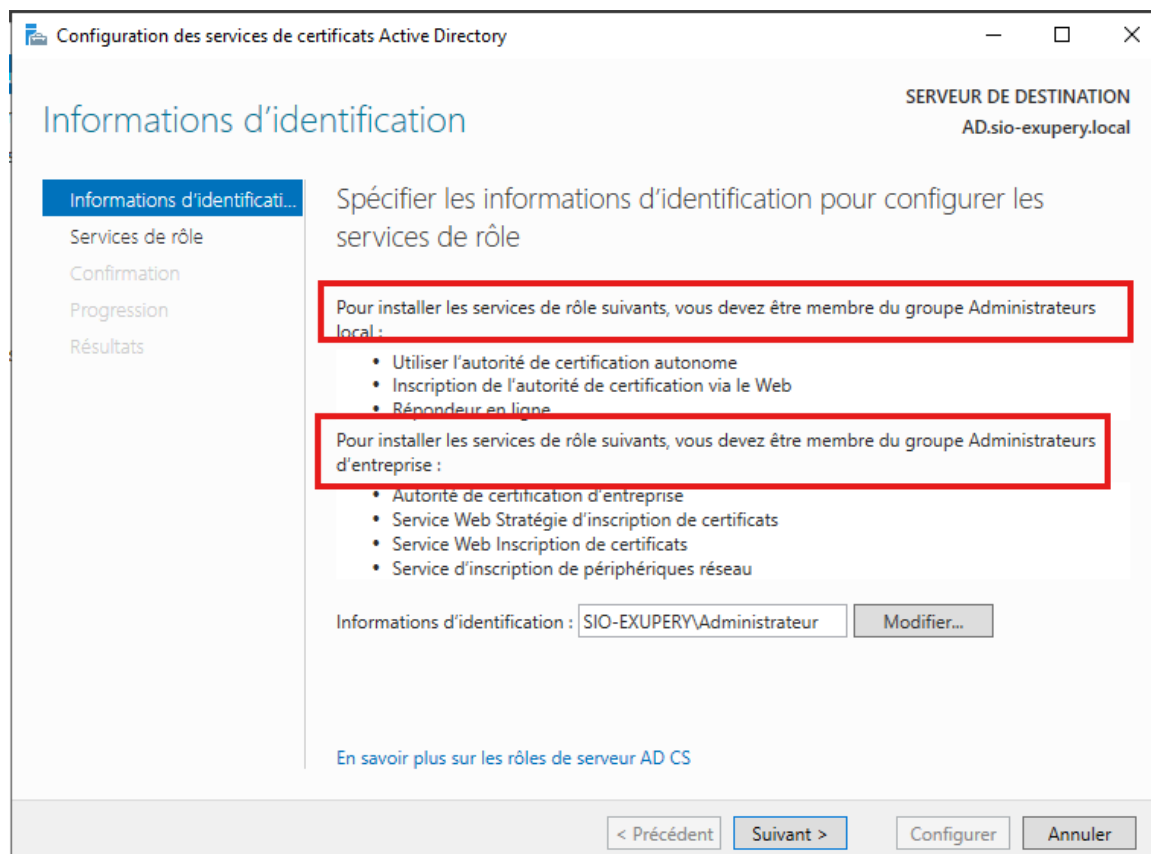
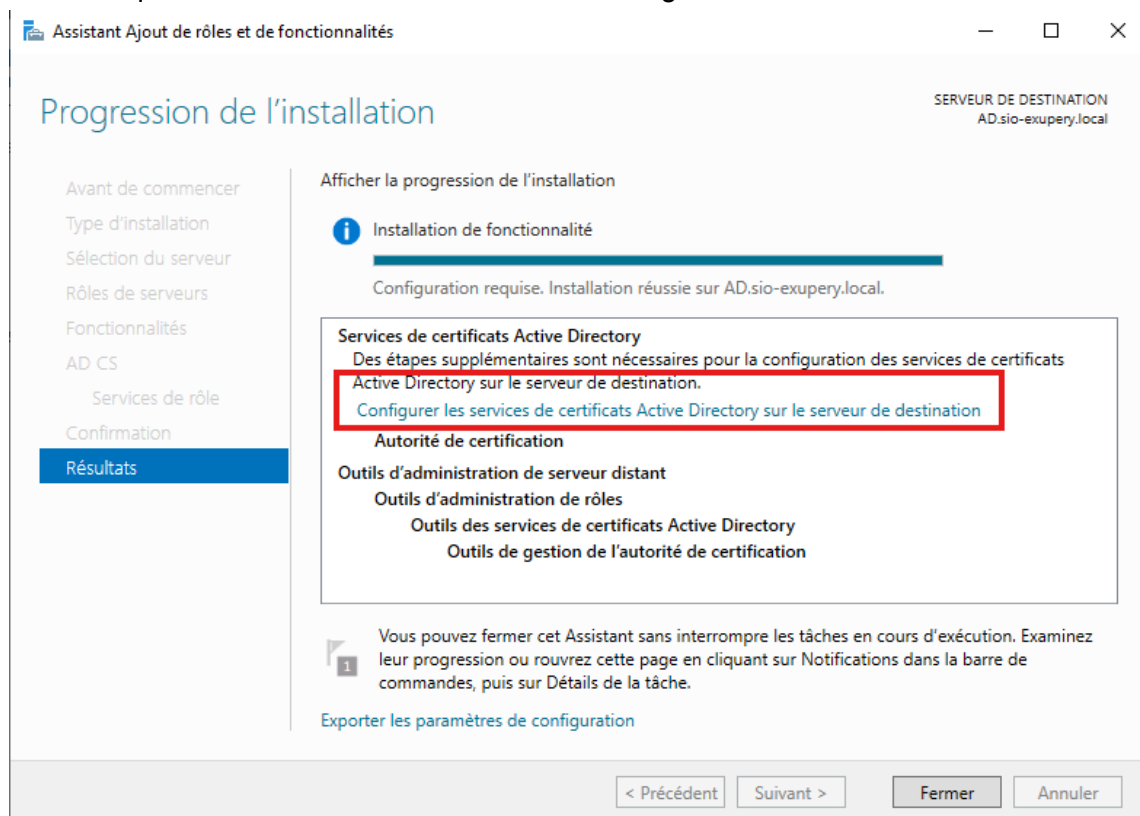




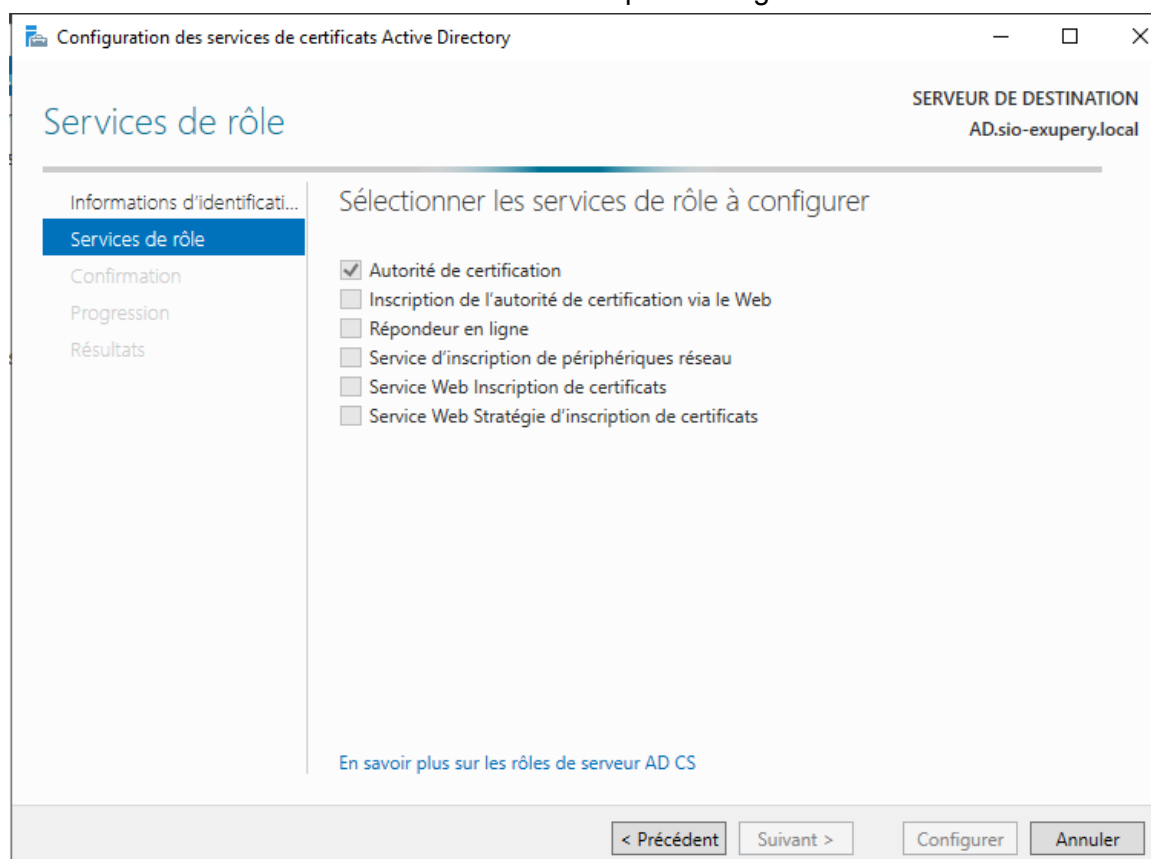
▪ Nous cochons la case



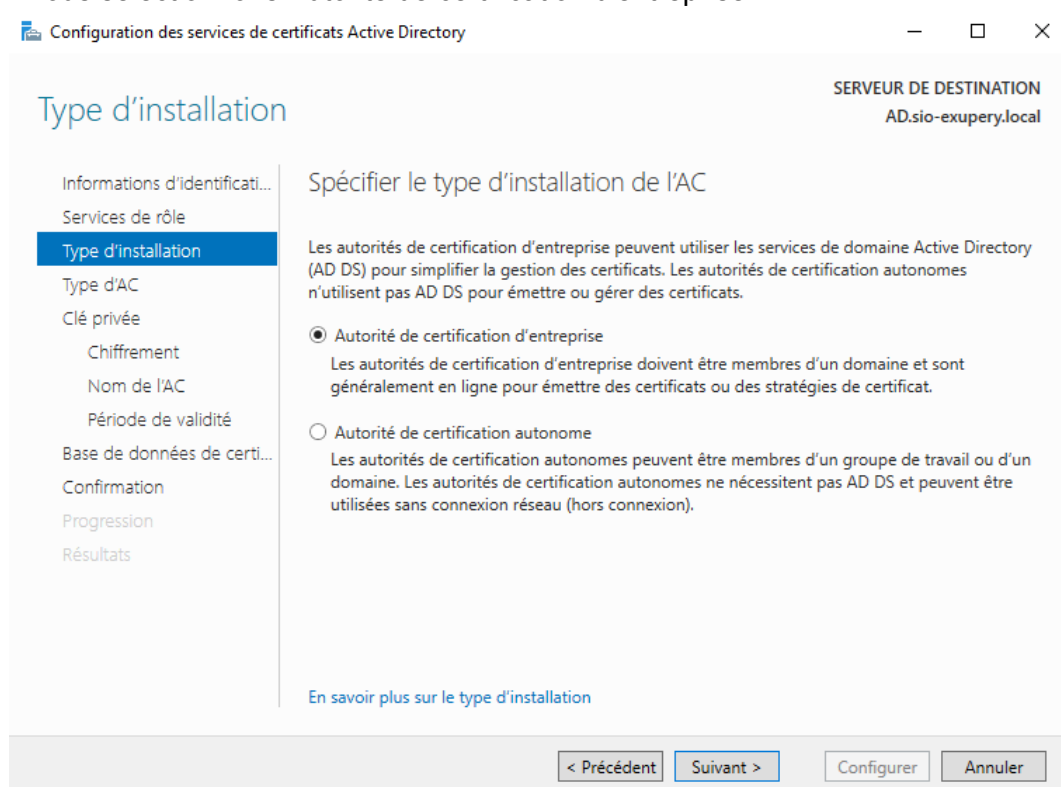
- Nous cliquons sur le lien encadré encadré en rouge ci-dessous



- Nous cochoons la case Autorité de certification pour configurer ce rôle.



- Nous sélectionnons Autorité de certification d'entreprise.



- Nous sélectionnons Autorité de certification racine :

The screenshot shows the 'Configuration des services de certificats Active Directory' window. The title bar includes the window name and standard Windows controls. The main area is titled 'Type d'autorité de certification'. On the left, a navigation pane lists steps: Informations d'identificati..., Services de rôle, Type d'installation, Type d'AC (highlighted), Clé privée, Chiffrement, Nom de l'AC, Période de validité, Base de données de certi..., Confirmation, Progression, and Résultats. The main content area is titled 'Spécifier le type de l'AC'. It contains a paragraph explaining the role of a root certification authority. Below this, two radio button options are presented: 'Autorité de certification racine' (selected and highlighted with a red box) and 'Autorité de certification secondaire'. At the bottom, there are navigation buttons: '< Précédent', 'Suivant >', 'Configurer', and 'Annuler'. The top right corner shows 'SERVEUR DE DESTINATION' as 'AD.sio-exupery.local'.

Configuration des services de certificats Active Directory

SERVEUR DE DESTINATION
AD.sio-exupery.local

Type d'autorité de certification

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

Spécifier le type de l'AC

Lorsque vous installez les services de certificats Active Directory (AD CS), vous créez ou étendez une hiérarchie d'infrastructure à clé publique (PKI). Une autorité de certification racine se trouve au sommet de la hiérarchie PKI et émet ses propres certificats auto-signés. Une autorité de certification secondaire reçoit un certificat de l'autorité de certification de rang plus élevé dans la hiérarchie PKI.

☒ **Autorité de certification racine**
Les autorités de certification racines sont les premières voire les seules autorités de certification configurées dans une hiérarchie PKI.

☐ **Autorité de certification secondaire**
Les autorités de certification secondaires nécessitent une hiérarchie PKI établie et sont autorisées à émettre des certificats par l'autorité de certification de rang plus élevé dans la hiérarchie.

[En savoir plus sur le type d'autorité de certification](#)

< Précédent Suivant > Configurer Annuler

- On sélectionne Créer une nouvelle clé privée.

The screenshot shows the 'Configuration des services de certificats Active Directory' window at the 'Clé privée' step. The navigation pane on the left highlights 'Clé privée'. The main content area is titled 'Spécifier le type de la clé privée'. It contains a paragraph explaining the need for a private key. Below this, three radio button options are presented: 'Créer une clé privée' (selected and highlighted with a red box), 'Utiliser la clé privée existante', and 'Sélectionner un certificat et utiliser sa clé privée associée'. The 'Utiliser la clé privée existante' option has two sub-options: 'Sélectionner un certificat et utiliser sa clé privée associée' and 'Sélectionner une clé privée existante sur cet ordinateur'. At the bottom, there are navigation buttons: '< Précédent', 'Suivant >', 'Configurer', and 'Annuler'. The top right corner shows 'SERVEUR DE DESTINATION' as 'AD.sio-exupery.local'.

Configuration des services de certificats Active Directory

SERVEUR DE DESTINATION
AD.sio-exupery.local

Clé privée

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

Spécifier le type de la clé privée

Pour générer et émettre des certificats aux clients, une autorité de certification doit posséder une clé privée.

☒ **Créer une clé privée**
Utilisez cette option si vous n'avez pas de clé privée ou pour en créer une.

☐ **Utiliser la clé privée existante**
Utilisez cette option pour garantir la continuité avec les certificats émis antérieurement lors de la réinstallation d'une AC.

☐ **Sélectionner un certificat et utiliser sa clé privée associée**
Sélectionnez cette option s'il existe un certificat sur cet ordinateur ou pour importer un certificat et utiliser sa clé privée associée.

☐ **Sélectionner une clé privée existante sur cet ordinateur**
Sélectionnez cette option si vous avez conservé les clés privées d'une installation antérieure ou pour utiliser une clé privée d'une autre source.

[En savoir plus sur la clé privée](#)

< Précédent Suivant > Configurer Annuler

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

The screenshot shows the 'Configuration des services de certificats Active Directory' window. The title bar indicates the window is titled 'Configuration des services de certificats Active Directory'. The main heading is 'Chiffrement pour l'autorité de certification'. The 'SERVEUR DE DESTINATION' is 'AD.sio-exupery.local'. The left sidebar shows the 'Chiffrement' step is selected. The main content area is titled 'Spécifier les options de chiffrement'. It contains two sections: 'Sélectionnez un fournisseur de chiffrement :' with a dropdown menu showing 'RSA#Microsoft Software Key Storage Provider', and 'Longueur de la clé :' with a dropdown menu showing '2048'. Below these is 'Sélectionnez l'algorithme de hachage pour signer les certificats émis par cette AC :' with a list box showing 'SHA256', 'SHA384', 'SHA512', and 'SHA1'. There is an unchecked checkbox for 'Autorisez l'interaction de l'administrateur lorsque l'autorité de certification accède à la clé privée.' and a link 'En savoir plus sur le chiffrement'. At the bottom are buttons for '< Précédent', 'Suivant >', 'Configurer', and 'Annuler'.

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

The screenshot shows the 'Configuration des services de certificats Active Directory' window. The title bar indicates the window is titled 'Configuration des services de certificats Active Directory'. The main heading is 'Nom de l'autorité de certification'. The 'SERVEUR DE DESTINATION' is 'AD.sio-exupery.local'. The left sidebar shows the 'Nom de l'AC' step is selected. The main content area is titled 'Spécifier le nom de l'AC'. It contains a text box for 'Nom commun de cette AC :' with the value 'sio-exupery-AD-CA-1'. Below this is a text box for 'Suffixe du nom unique :' with the value 'DC=sio-exupery,DC=local'. Below that is a text box for 'Aperçu du nom unique :' with the value 'CN=sio-exupery-AD-CA-1,DC=sio-exupery,DC=local'. There is a link 'En savoir plus sur le nom de l'autorité de certification'. At the bottom are buttons for '< Précédent', 'Suivant >', 'Configurer', and 'Annuler'.

- On laisse la période de validité par défaut.

The screenshot shows the 'Configuration des services de certificats Active Directory' window. The left sidebar lists various configuration steps, with 'Période de validité' highlighted. The main area is titled 'Période de validité' and 'SERVEUR DE DESTINATION AD.sio-exupery.local'. It prompts the user to 'Spécifier la période de validité' and shows a default value of '5' years. The expiration date is set to '12/03/2031 09:39:00'. A note states that the configured validity period must exceed the validity period of the certificates it will issue. Navigation buttons at the bottom include '< Précédent', 'Suivant >', 'Configurer', and 'Annuler'.

Configuration des services de certificats Active Directory

Période de validité

SERVEUR DE DESTINATION
AD.sio-exupery.local

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

Spécifier la période de validité

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

5 Années

Date d'expiration de l'AC : 12/03/2031 09:39:00

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

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

< Précédent Suivant > Configurer Annuler

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

The screenshot shows the 'Configuration des services de certificats Active Directory' window. The left sidebar lists various configuration steps, with 'Base de données de l'autorité de certification' highlighted. The main area is titled 'Base de données de l'autorité de certification' and 'SERVEUR DE DESTINATION AD.sio-exupery.local'. It prompts the user to 'Spécifier les emplacements des bases de données' and shows default paths for the certificate database and its log. Navigation buttons at the bottom include '< Précédent', 'Suivant >', 'Configurer', and 'Annuler'.

Configuration des services de certificats Active Directory

Base de données de l'autorité de certification

SERVEUR DE DESTINATION
AD.sio-exupery.local

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

Spécifier les emplacements des bases de données

Emplacement de la base de données de certificats :

C:\Windows\system32\CertLog

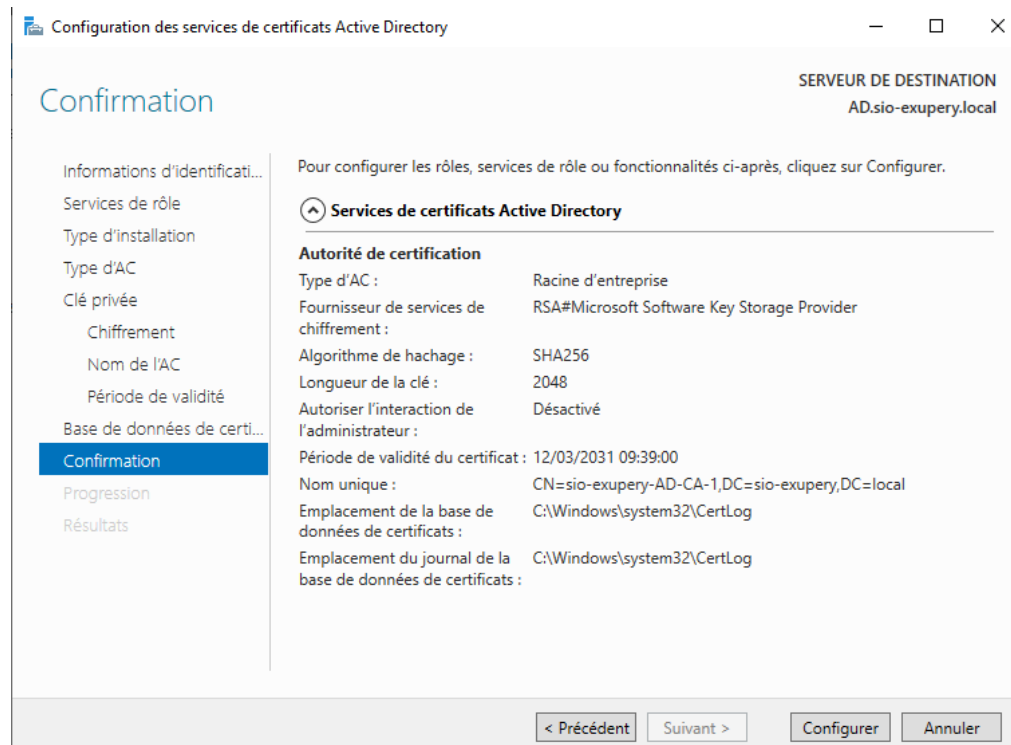
Emplacement du journal de la base de données de certificats :

C:\Windows\system32\CertLog

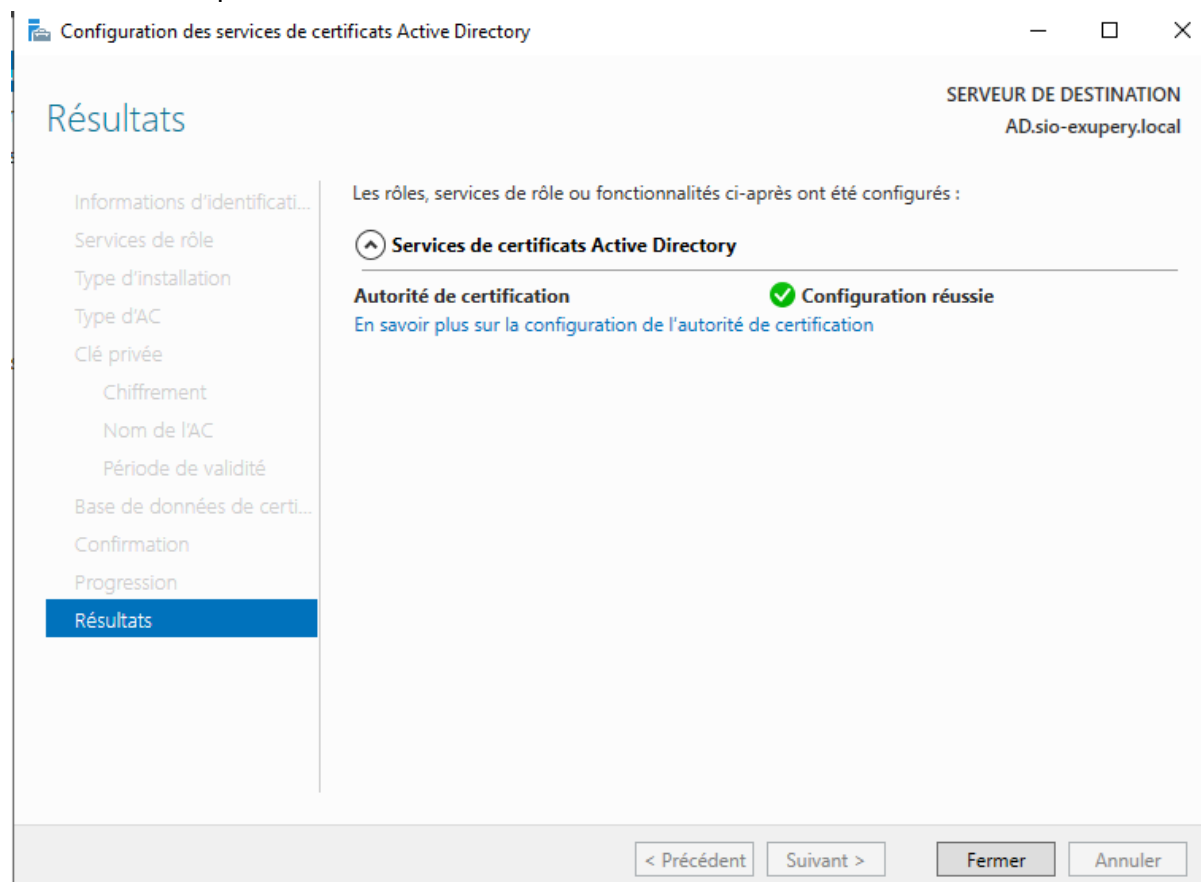
[En savoir plus sur la base de données de l'autorité de certification](#)

< Précédent Suivant > Configurer Annuler

- Nous cliquons sur Configurer.

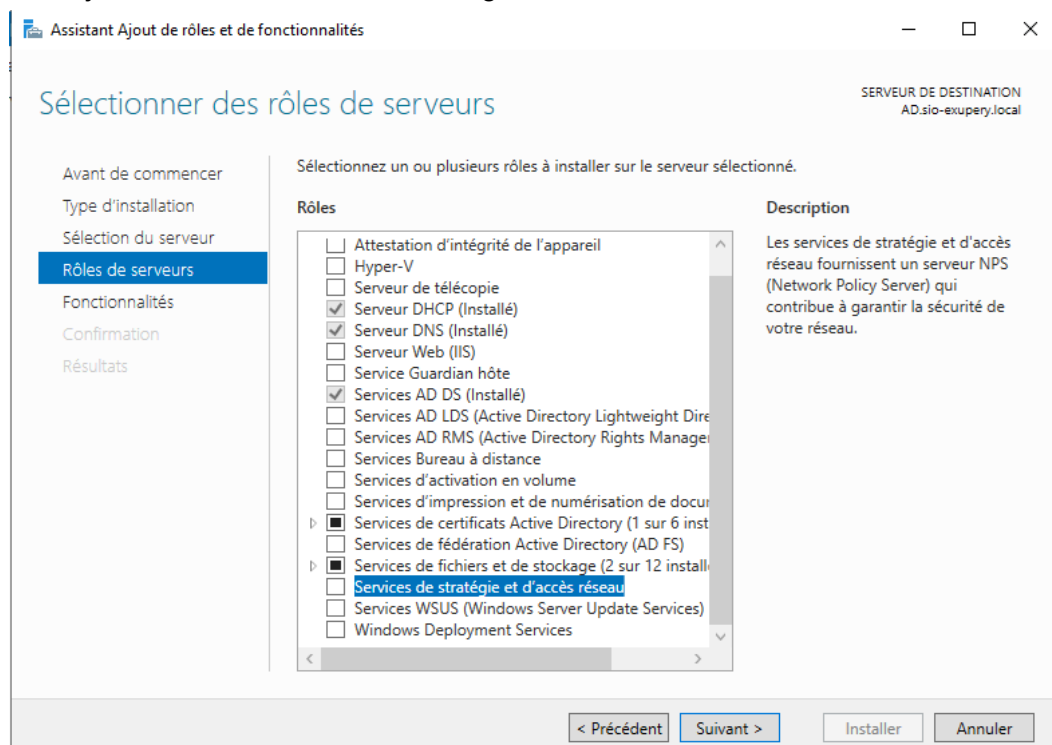


- Notre autorité de certification est maintenant installée et configurée.
 - Nous cliquons sur Fermer.

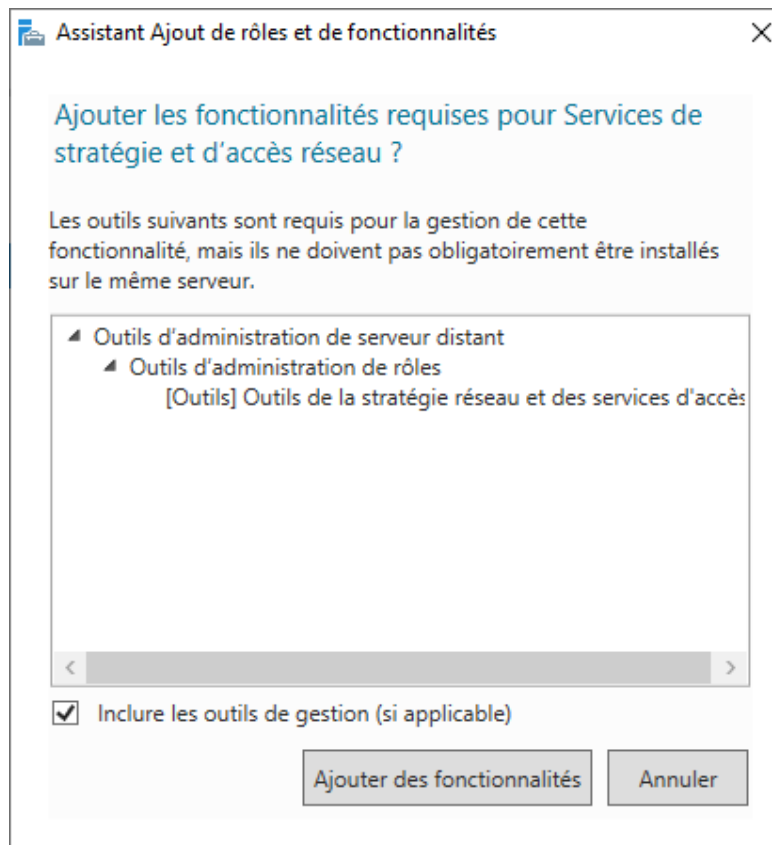


2.3 Installation du service NPS

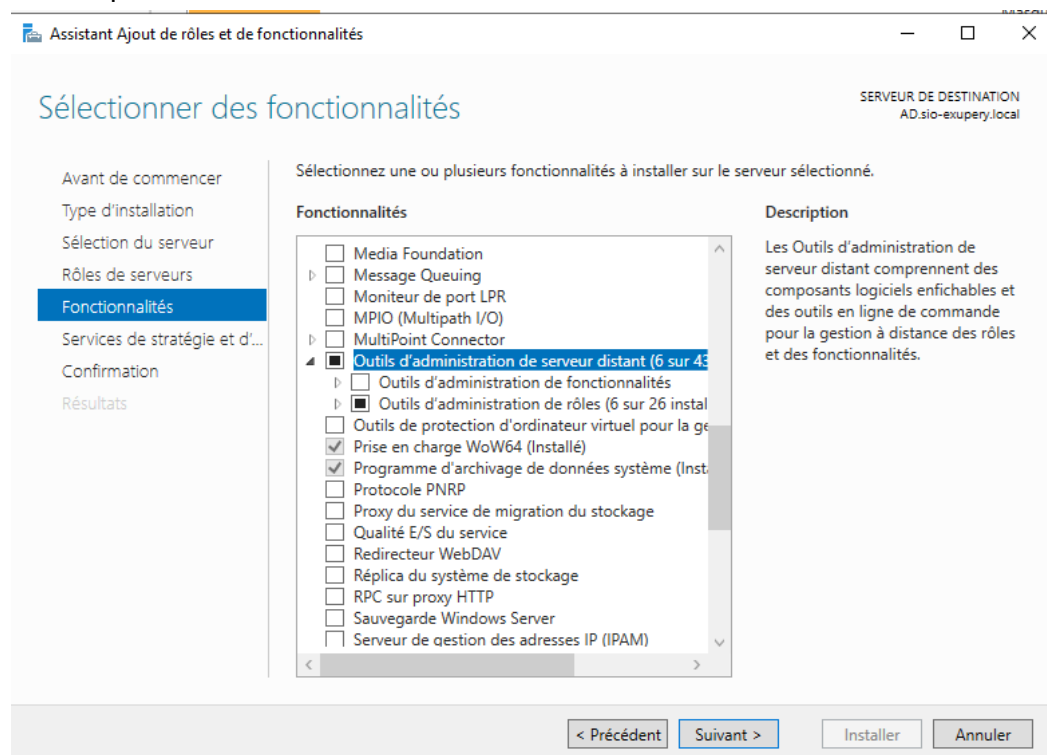
- On ajoute le rôle Services de stratégie et d'accès réseau.



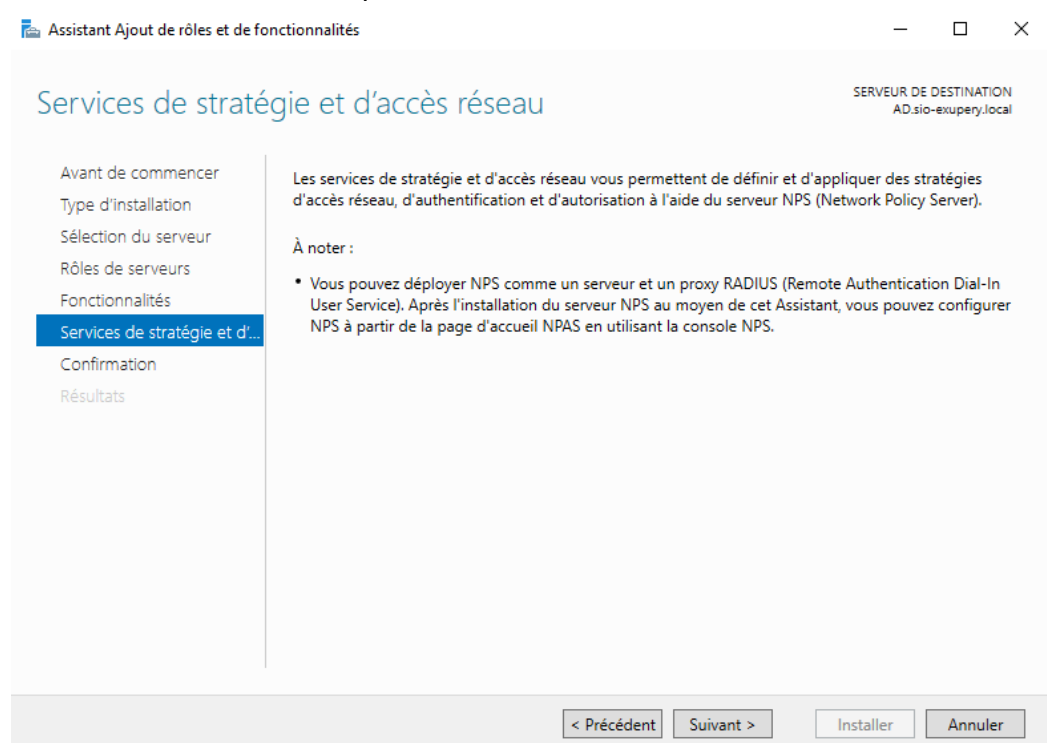
- Nous cliquons sur le bouton Ajouter des fonctionnalités.



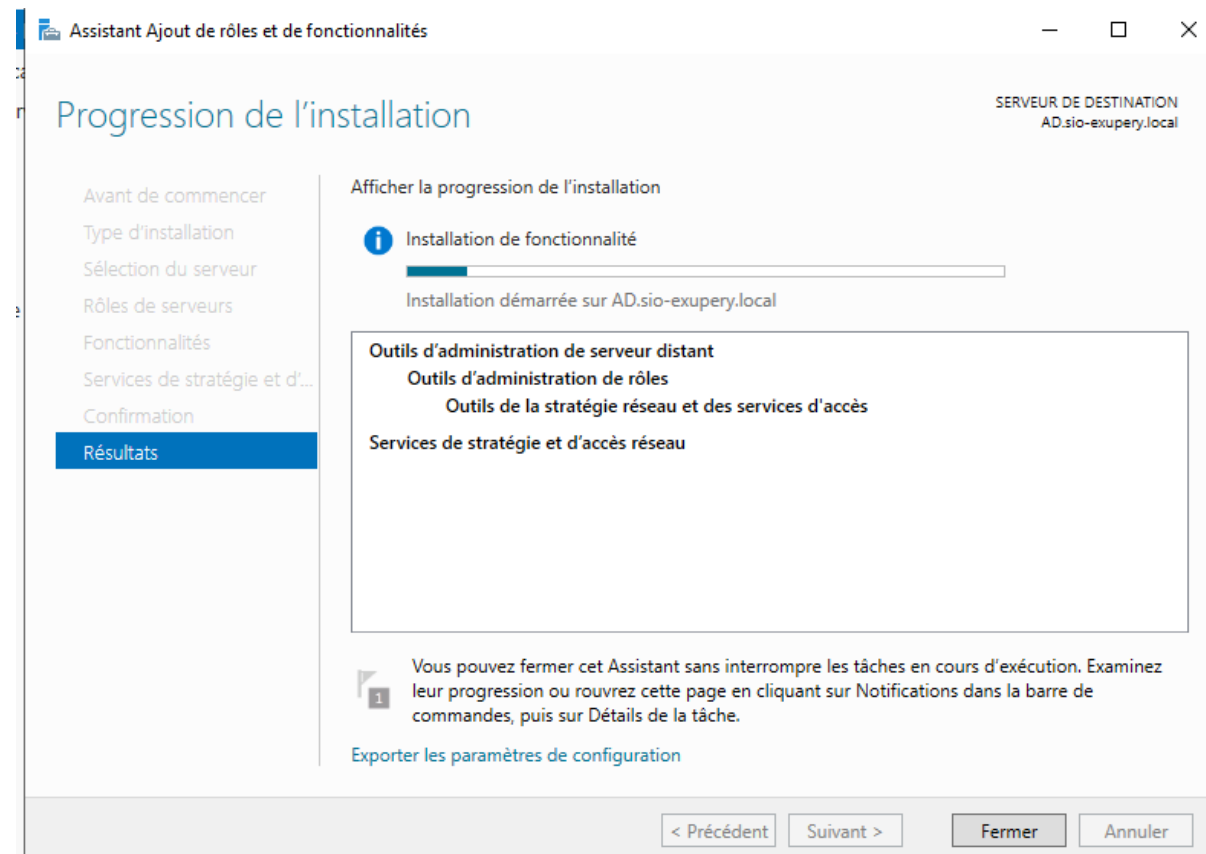
- On clique sur le bouton Suivant.



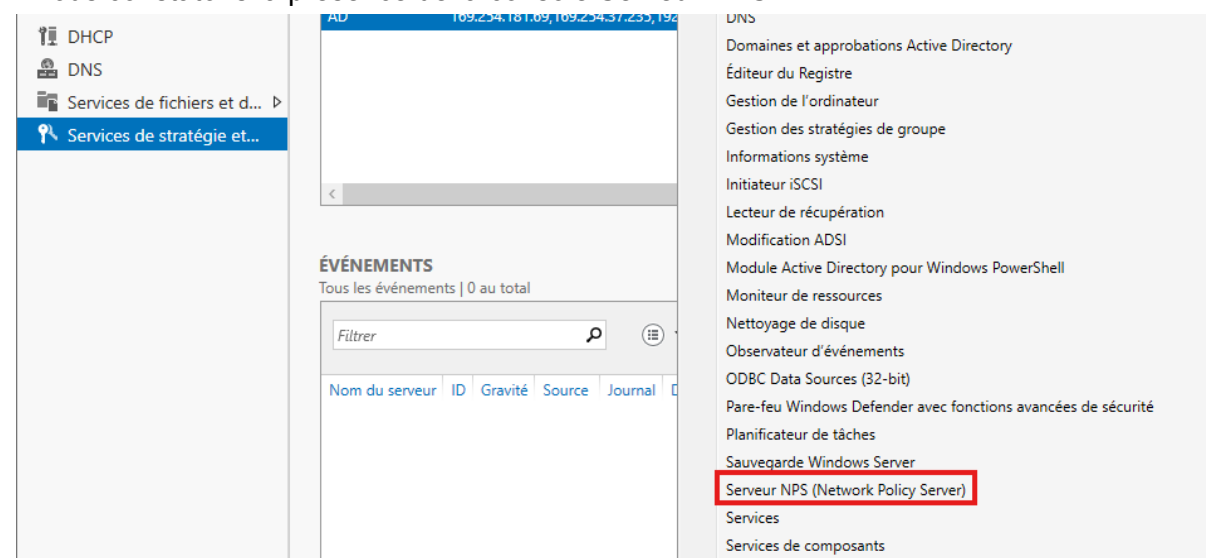
- De nouveau, on clique sur suivant :
 - Puis nous allons cliquer sur installer.



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



- Nous constatons la présence de la console Serveur NPS.



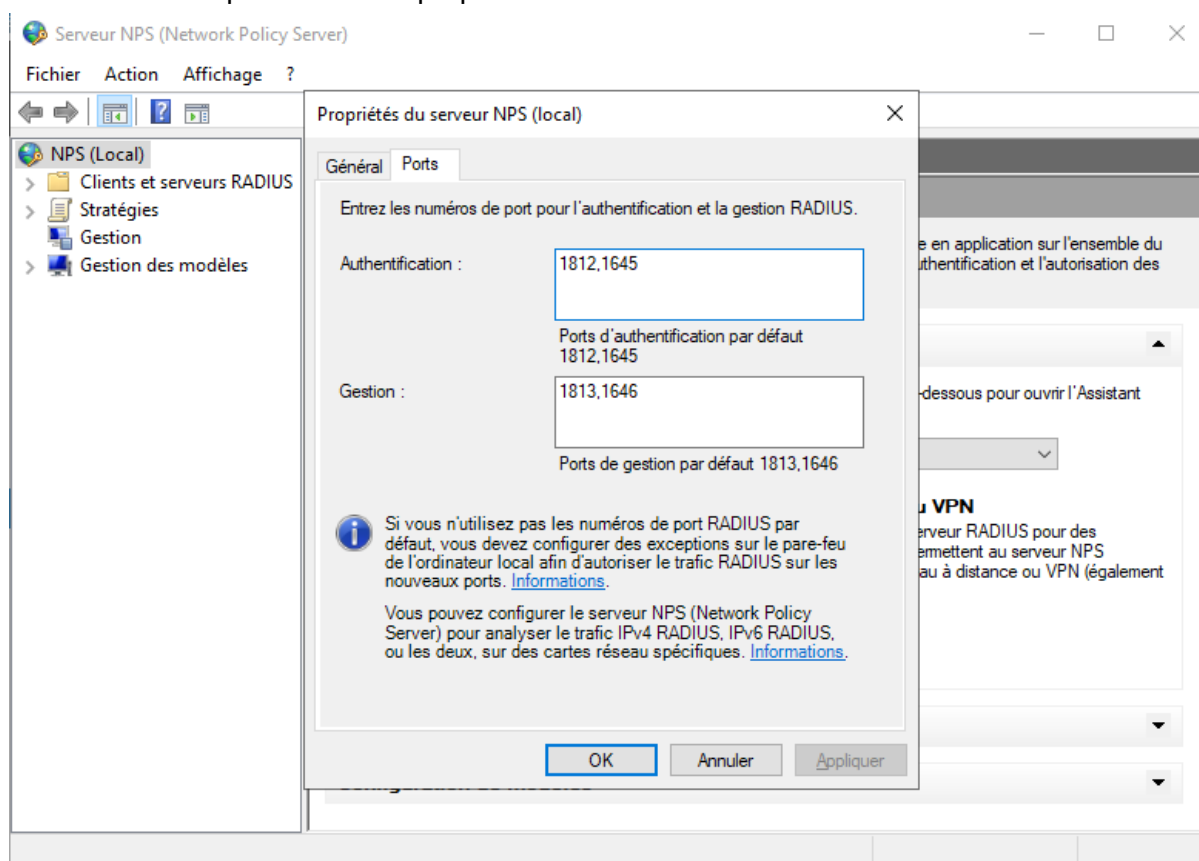
- Afin de vérifier le bon fonctionnement du service NPS sur le serveur, nous affichons les ports en écoute sur celui-ci avec la commande netstat -a -p udp :

```
UDP 169.254.181.69:1646 *:*
UDP 169.254.181.69:1812 *:*
UDP 169.254.181.69:1813 *:*
UDP 192.168.1.50:53 *:*
UDP 192.168.1.50:67 *:*
UDP 192.168.1.50:68 *:*
UDP 192.168.1.50:88 *:*
UDP 192.168.1.50:137 *:*
UDP 192.168.1.50:138 *:*
UDP 192.168.1.50:164 *:*
UDP 192.168.1.50:1645 *:*
UDP 192.168.1.50:1646 *:*
UDP 192.168.1.50:1812 *:*
UDP 192.168.1.50:1813 *:*
UDP 192.168.1.50:2535 *:*

C:\Users\Administrateur>ping 192.168.1.51

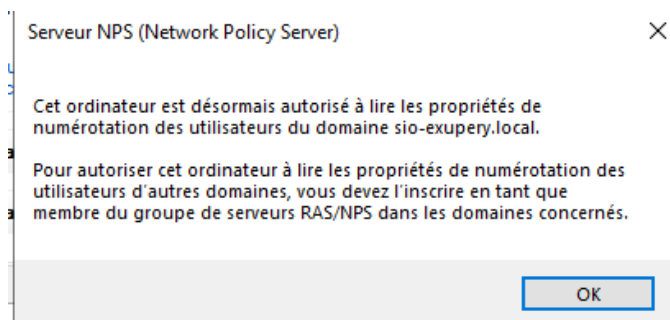
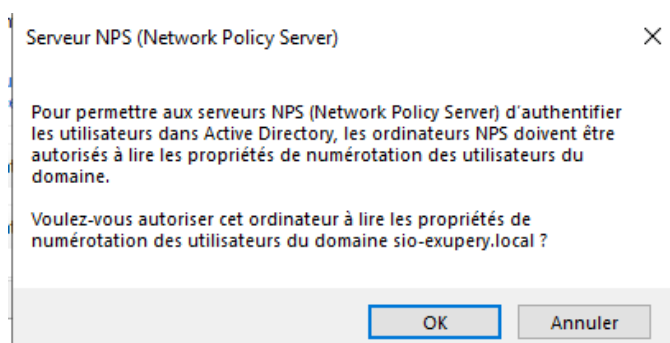
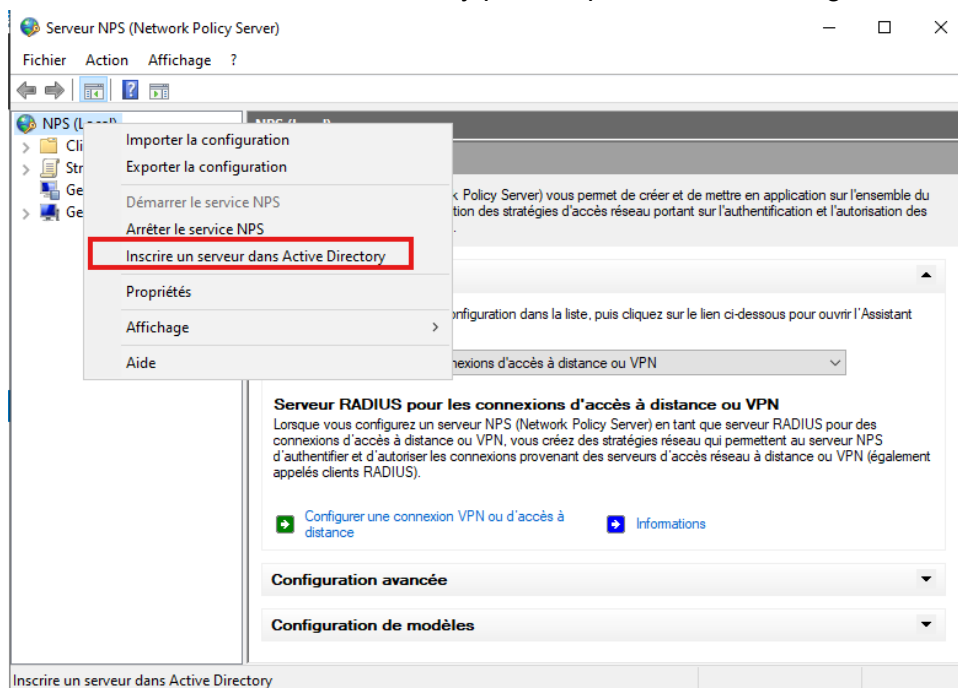
Envoi d'une requête 'Ping' 192.168.1.51 avec 32 octets de données :
```

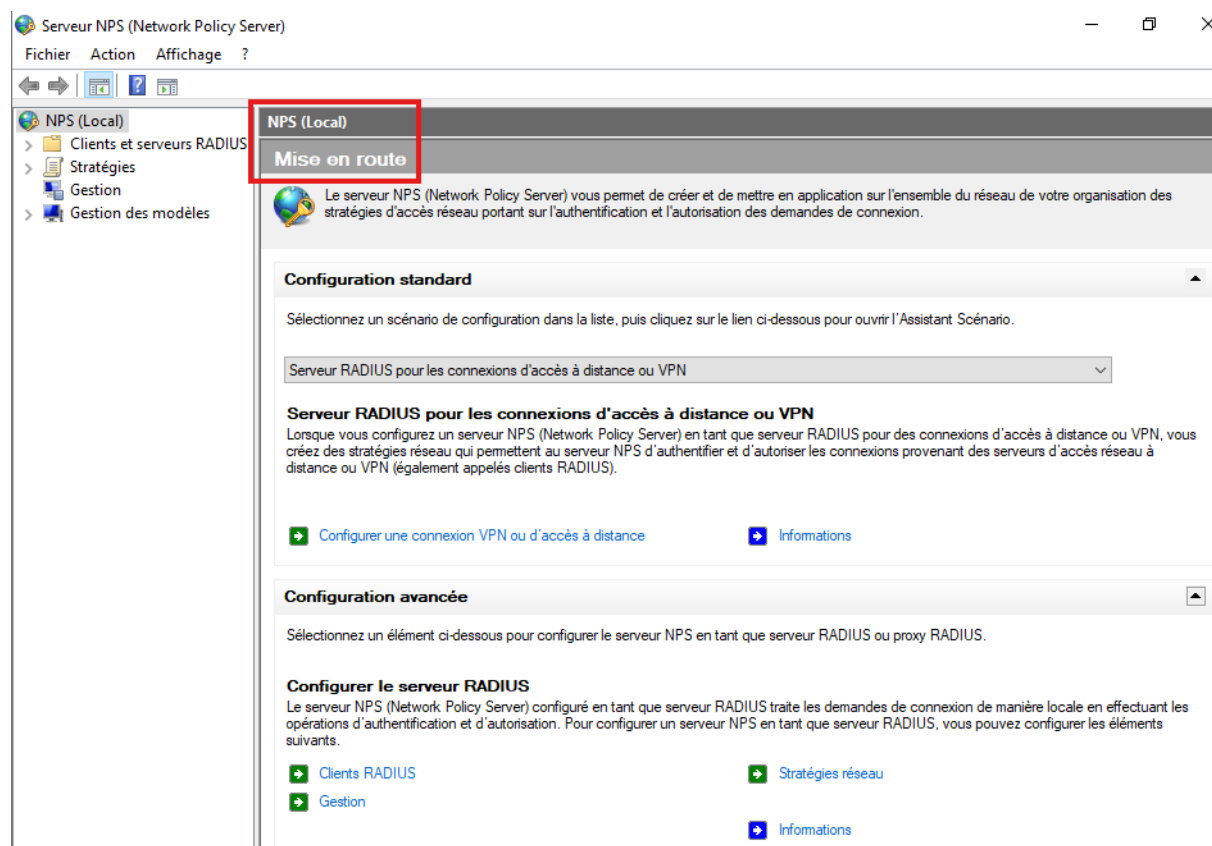
- Ouverture de la console du Serveur NPS :
 - Liste des ports dans les propriétés du serveur NPS :



2.4 Configuration du serveur RADIUS NPS

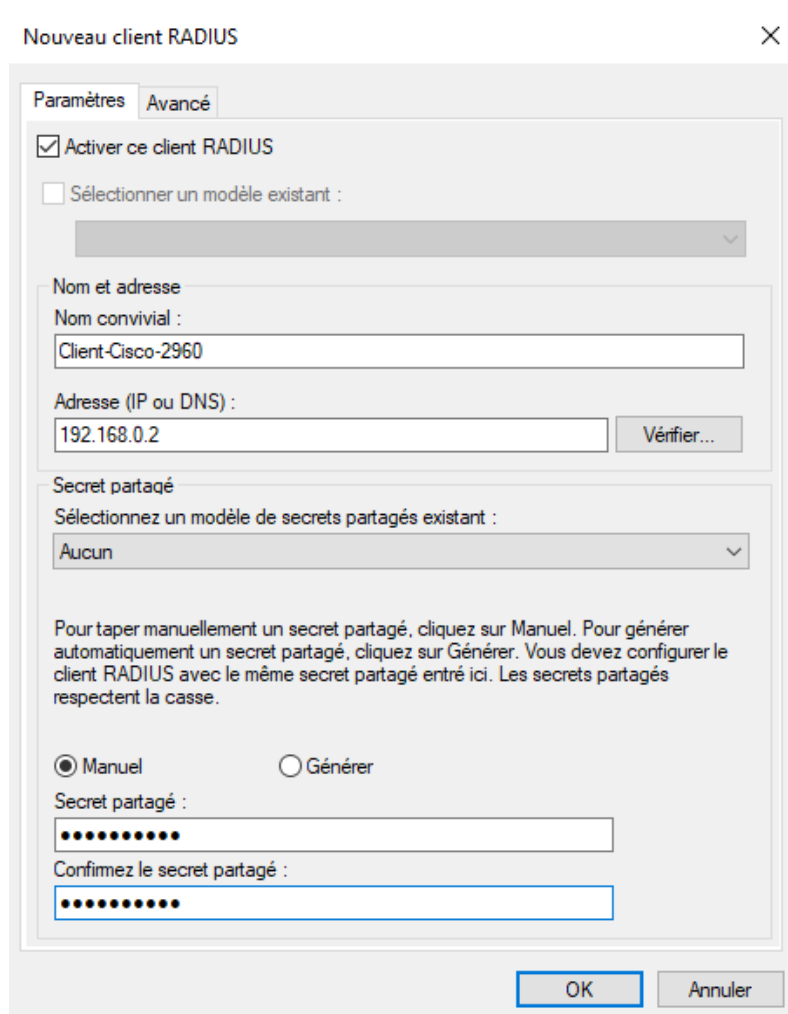
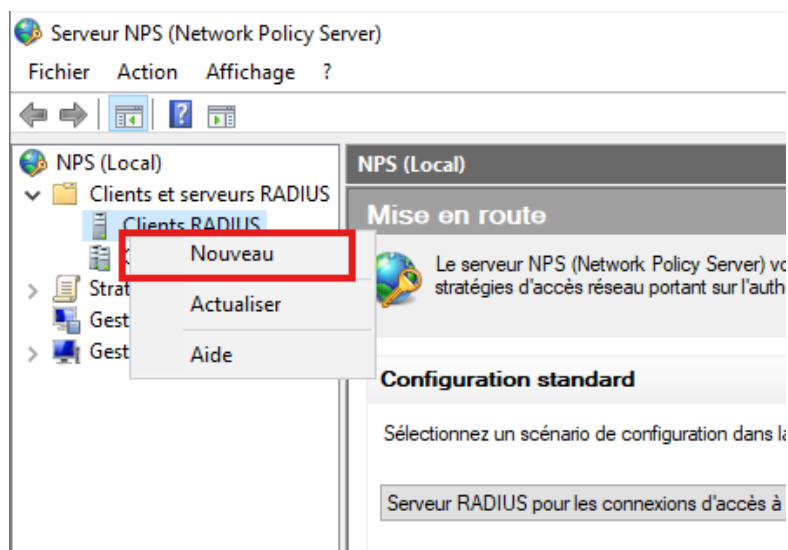
- Nous cliquons depuis le menu Action sur Inscrire un serveur dans Active Directory, afin d'inscrire NPS dans Active Directory pour lui permettre d'interroger la base des utilisateurs.





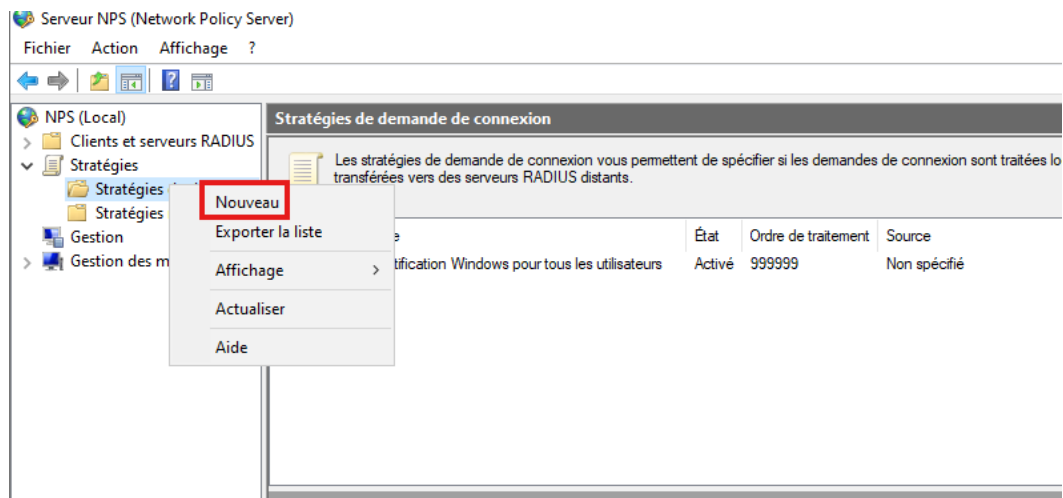
2.4.1 Déclaration du client RADIUS

- Nous effectuons un clic droit sur l'entrée Clients RADIUS puis nous sélectionnons "Nouveau".



2.4.2 Déclaration d'une stratégie de demande de connexion

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



- Nous y spécifions un nom de stratégie (Connexion câblée).
 - On laisse le type de serveur d'accès réseau sur non spécifié car nous utilisons un commutateur en tant que client Radius.

Nouvelle stratégie de demande de connexion

Spécifier le nom de la stratégie de demande de connexion et le type de connexion

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

Nom de la stratégie :

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

☒ Type de serveur d'accès réseau :

☐ Spécifique au fournisseur :

Précédent **Suivant** Terminer Annuler

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

Nouvelle stratégie de demande de connexion

Spécifier les conditions

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

Sélectionner une condition

Sélectionnez une condition, puis cliquez sur Ajouter.

- Identificateur NAS**
La condition Identificateur NAS spécifie une chaîne de caractères qui représente le nom du serveur d'accès réseau (NAS). Vous pouvez utiliser la syntaxe de correspondance au modèle pour spécifier les noms NAS.
- Adresse IPv4 NAS**
La condition Adresse IPv4 NAS spécifie une chaîne de caractères qui représente l'adresse IP du serveur d'accès réseau (NAS). Vous pouvez utiliser la syntaxe de correspondance au modèle pour spécifier les réseaux IP.
- Adresse IPv6 NAS**
La condition Adresse IPv6 NAS spécifie une chaîne de caractères qui représente l'adresse IPv6 du serveur d'accès réseau (NAS). Vous pouvez utiliser la syntaxe de correspondance au modèle pour spécifier les réseaux IPv6.
- Type de port NAS**
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... Annuler

Ajouter... Modifier... Supprimer

Précédent Suivant Terminer Annuler

Type de port NAS

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

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

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

Types de tunnels pour connexions 802.1X standard

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

Autres

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

OK Annuler

Nous cliquons sur le bouton Suivant.

Nouvelle stratégie de demande de connexion ×

 **Spécifier les conditions**

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

Conditions :

Condition	Valeur
 Type de port NAS	Ethernet

Description de la condition :

[Ajouter...](#) [Modifier...](#) [Supprimer](#)

[Précédent](#) [Suivant](#) [Terminer](#) [Annuler](#)

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

Nouvelle stratégie de demande de connexion ×

 **Spécifier le transfert de la demande de connexion**

La demande de connexion peut être authentifiée par le serveur local ou être transférée aux serveurs RADIUS d'un groupe de serveurs RADIUS distants.

Si la demande de connexion correspond aux conditions de la stratégie, ces paramètres sont appliqués.

Paramètres :

Transfert de la demande de connexion

 **Authentification**

 Gestion

Spécifiez si les demandes de connexion sont traitées localement, si elles sont transférées à des serveurs RADIUS distants pour authentification, ou si elles sont acceptées sans authentification.

☒ Authentifier les demandes sur ce serveur

☐ Transférer les demandes au groupe de serveurs RADIUS distants suivant pour authentification :

[Nouveau...](#)

☐ Accepter les utilisateurs sans validation des informations d'identification

[Précédent](#) [Suivant](#) [Terminer](#) [Annuler](#)

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

Nouvelle stratégie de demande de connexion

✕



Spécifier les méthodes d'authentification

Configurez une ou plusieurs des méthodes d'authentification nécessaires pour que la demande de connexion corresponde à cette stratégie. Pour l'authentification EAP, vous devez configurer un type EAP.

☐ Remplacer les paramètres d'authentification de stratégie réseau

Ces paramètres d'authentification sont utilisés à la place des contraintes et des paramètres d'authentification de la stratégie réseau.

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 :

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.

Précédent

Suivant

Terminer

Annuler

- Suivant

Nouvelle stratégie de demande de connexion

✕



Configurer les paramètres

Le serveur NPS applique des paramètres à la demande de connexion si toutes les conditions relatives à la stratégie de demande de connexion sont remplies.

Configurez les paramètres de cette stratégie réseau.

Si la demande de connexion répond aux conditions et si la stratégie accorde l'accès, les paramètres sont appliqués.

Paramètres :

Spécifier un nom de domaine

Attribut

Attributs RADIUS

Standard

☒ Spécifiques au fournisseur

Sélectionnez les attributs auxquels les règles suivantes seront appliquées. Les règles sont traitées selon leur ordre d'apparition dans la liste.

Attribut : ID de la station appelée

Règles :

Rechercher	Remplacer par

Ajouter

Modifier

Supprimer

Monter

Descendre

Précédent

Suivant

Terminer

Annuler

▪ Nous cliquons sur terminer

Nouvelle stratégie de demande de connexion

×



Fin de l'Assistant Stratégie de demande de nouvelle connexion

Vous avez créé la stratégie de demande de connexion suivante :

Connexion câblée

Conditions de la stratégie :

Condition	Valeur
Type de port NAS	Ethernet

Paramètres de la stratégie :

Condition	Valeur
Fournisseur d'authentification	Ordinateur local

Pour fermer cet Assistant, cliquez sur Terminer.

Précédent

Suivant

Terminer

Annuler

Serveur NPS (Network Policy Server)

Fichier Action Affichage ?

NPS (Local)

- Clients et serveurs RADIUS
- Stratégies
 - Stratégies de demande
 - Stratégies réseau
- Gestion
- Gestion des modèles

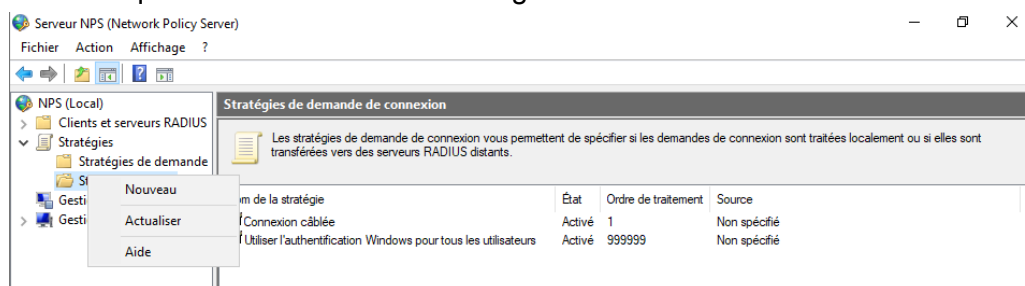
Stratégies de demande de connexion

Les stratégies de demande de connexion vous permettent de spécifier si les demandes de connexion sont traitées localement ou si elles sont transférées vers des serveurs RADIUS distants.

Nom de la stratégie	État	Ordre de traitement	Source
Connexion câblée	Activé	1	Non spécifié
Utiliser l'authentification Windows pour tous les utilisateurs	Activé	999999	Non spécifié

2.4.3 Déclaration d'une stratégie d'accès au réseau

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



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

Nouvelle stratégie réseau

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

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

Nom de la stratégie :
Stratégie pour cliente câblée Pédago

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

☒ Type de serveur d'accès réseau :
Non spécifié

☐ Spécifique au fournisseur :
10

Précédent Suivant Terminer Annuler

- Nous cliquons sur ajouter afin de spécifier une condition :

Nouvelle stratégie réseau

Spécifier les conditions

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

Condition	Valeur
-----------	--------

Description de la condition :

Ajouter... Modifier... Supprimer

Précédent Suivant Terminer Annuler

- Nous sélectionnons pour les groupes Windows

Nouvelle stratégie réseau

Spécifier les conditions

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

Sélectionner une condition

Sélectionnez une condition, puis cliquez sur Ajouter.

Groupes

Groupes Windows
La condition Groupes Windows spécifie que l'utilisateur ou l'ordinateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.

Groupes d'ordinateurs
La condition Groupes d'ordinateurs spécifie que l'ordinateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.

Groupes d'utilisateurs
La condition Groupes d'utilisateurs spécifie que l'utilisateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.

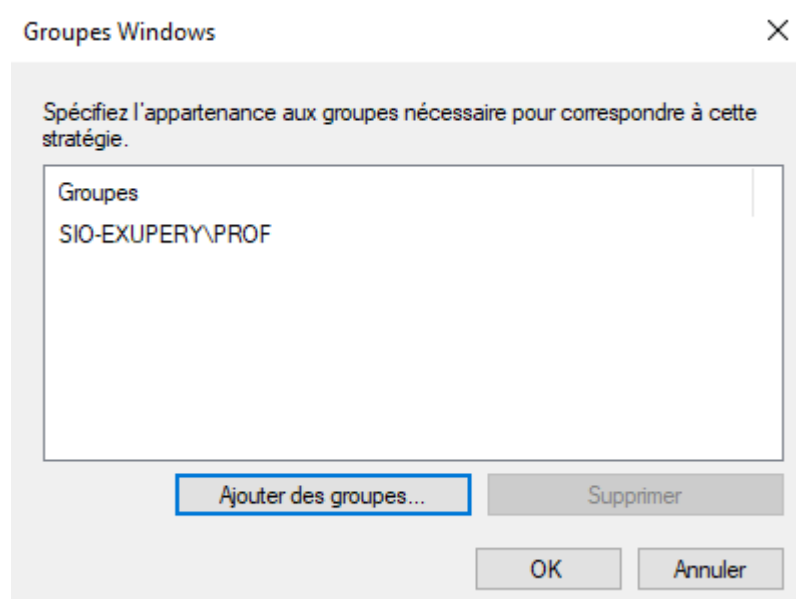
Restrictions relatives aux jours et aux heures
Les restrictions relatives aux jours et aux heures indiquent les jours et les heures auxquels les tentatives de connexion sont autorisées ou non. Ces restrictions sont basées sur le fuseau horaire du serveur NPS (Network Policy Server).

Ajouter... Annuler

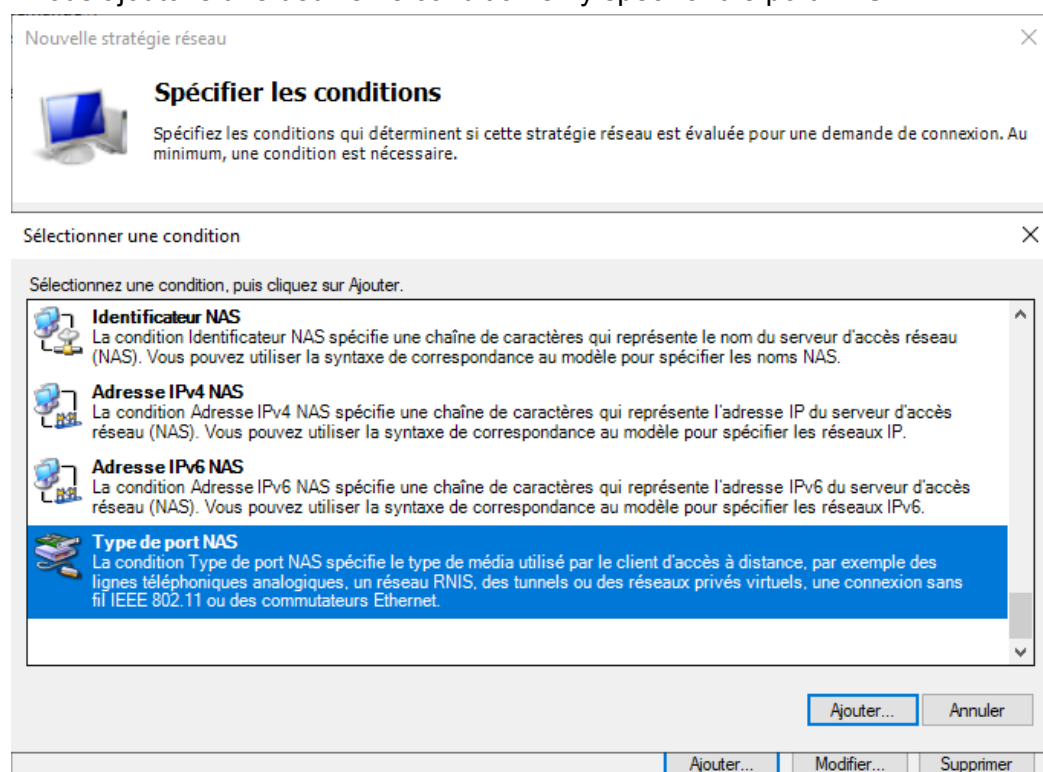
Ajouter... Modifier... Supprimer

Précédent Suivant Terminer Annuler

- Nous y ajoutons le groupe "Prof"



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



▪ Nous cochons Ethernet.

Type de port NAS

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

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

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

Types de tunnels pour connexions 802.1X standard

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

Autres

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

OK Annuler

▪ Nous cliquons sur Suivant

Nouvelle stratégie réseau

 **Spécifier les conditions**

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

Conditions :

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

Précédent Suivant Terminer Annuler

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

Nouvelle stratégie réseau

Spécifier l'autorisation d'accès

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

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

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

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

Précédent Suivant Terminer Annuler

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

Nouvelle stratégie réseau

Configurer les méthodes d'authentification

Configurez une ou plusieurs des méthodes d'authentification nécessaires pour que la demande de connexion corresponde à cette stratégie. Pour l'authentification EAP, vous devez configurer un type EAP.

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.

Précédent Suivant Terminer Annuler

▪ Nous cliquons sur suivant :

Nouvelle stratégie réseau

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, nous cliquons sur Ajouter afin d'envoyer des attributs au client RADIUS.

Nouvelle stratégie réseau

Configurer les paramètres

Le serveur NPS applique des paramètres à la demande de connexion si toutes les conditions relatives à la stratégie de demande de connexion sont remplies.

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.

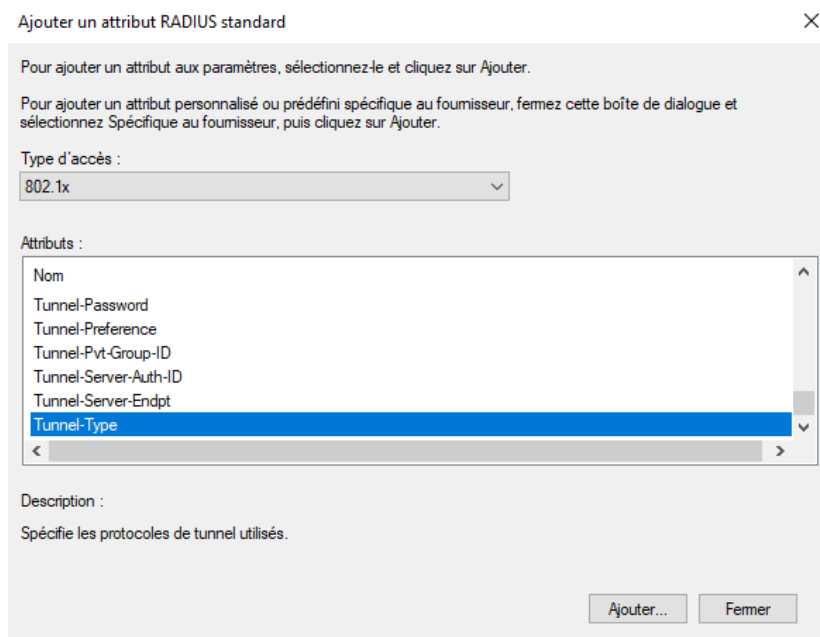
Attributs :

Nom	Valeur
Framed-Protocol	PPP
Service-Type	Framed

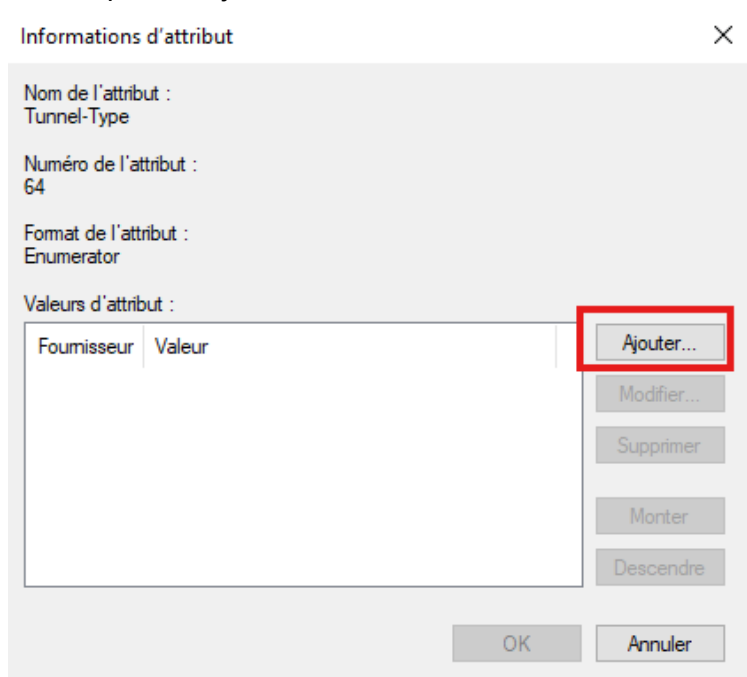
Ajouter... Modifier... Supprimer

Précédent Suivant Terminer Annuler

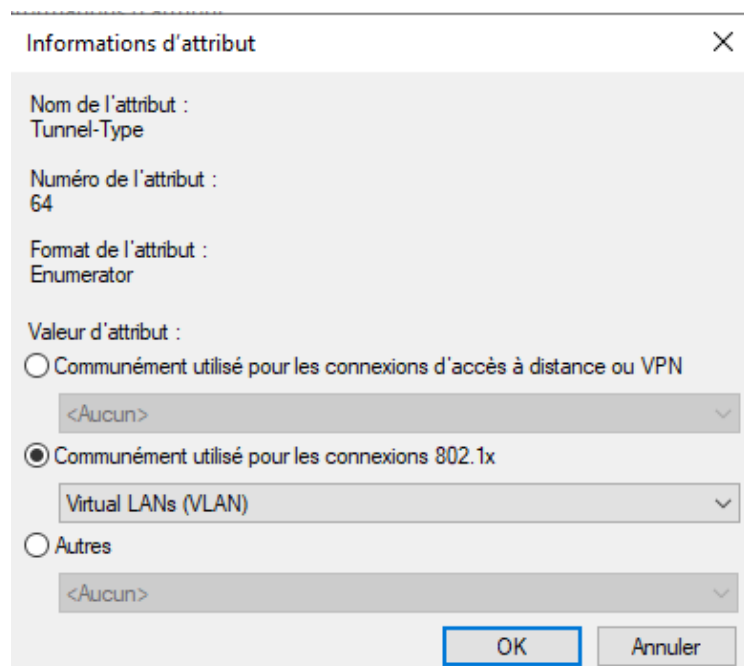
- Nous sélectionnons 802.1x dans Type d'accès puis nous sélectionnons l'attribut Tunnel-Type :
 - Nous cliquons sur Ajouter.



- On clique sur Ajouter.



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



Informations d'attribut

Nom de l'attribut :
Tunnel-Type

Numéro de l'attribut :
64

Format de l'attribut :
Enumerator

Valeur d'attribut :

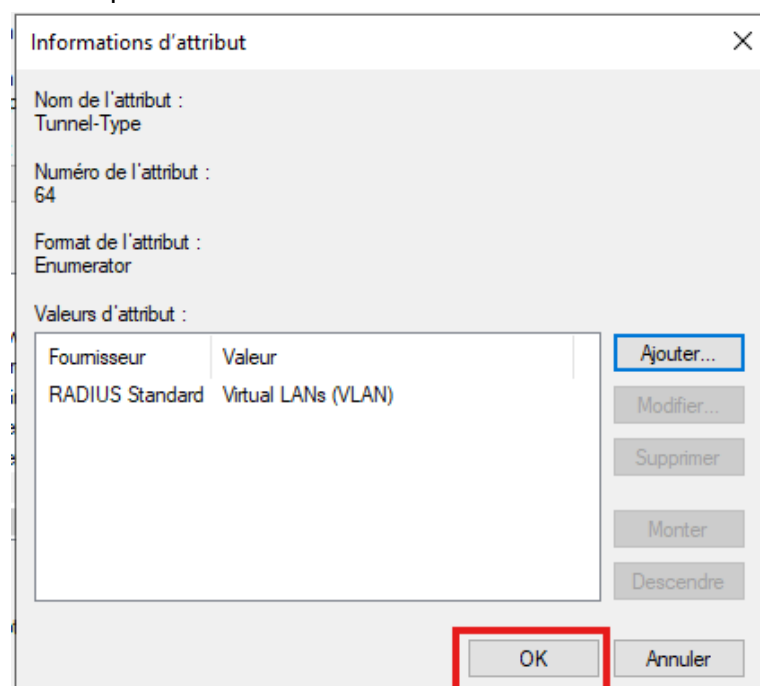
☐ Communément utilisé pour les connexions d'accès à distance ou VPN
<Aucun>

☒ Communément utilisé pour les connexions 802.1x
Virtual LANs (VLAN)

☐ Autres
<Aucun>

OK Annuler

- On clique sur OK.



Informations d'attribut

Nom de l'attribut :
Tunnel-Type

Numéro de l'attribut :
64

Format de l'attribut :
Enumerator

Valeurs d'attribut :

Fournisseur	Valeur
RADIUS Standard	Virtual LANs (VLAN)

Ajouter...
Modifier...
Supprimer
Monter
Descendre

OK Annuler

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

Ajouter un attribut RADIUS standard

Pour ajouter un attribut aux paramètres, sélectionnez-le et cliquez sur Ajouter.

Pour ajouter un attribut personnalisé ou prédéfini spécifique au fournisseur, fermez cette boîte de dialogue et sélectionnez Spécifique au fournisseur, puis cliquez sur Ajouter.

Type d'accès :
802.1x

Attributs :

- Nom
- Tunnel-Client-Auth-ID
- Tunnel-Client-Endpt
- Tunnel-Medium-Type**
- Tunnel-Password
- Tunnel-Preference
- Tunnel-Pvt-Group-ID

Description :

Spécifie le média de transport utilisé lors de la création d'un tunnel pour les protocoles (par exemple L2TP) qui peuvent opérer sur plusieurs transports.

Ajouter... Fermer

- On sélectionne 802 (includes...).

Informations d'attribut

Nom de l'attribut :
Tunnel-Medium-Type

Numéro de l'attribut :
65

Format de l'attribut :
Enumerator

Valeur d'attribut :

☒ Communément utilisé pour les connexions 802.1x

802 (includes all 802 media plus Ethernet canonical format)

☐ Autres

<Aucun>

OK Annuler

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

Ajouter un attribut RADIUS standard

Pour ajouter un attribut aux paramètres, sélectionnez-le et cliquez sur Ajouter.

Pour ajouter un attribut personnalisé ou prédéfini spécifique au fournisseur, fermez cette boîte de dialogue et sélectionnez Spécifique au fournisseur, puis cliquez sur Ajouter.

Type d'accès :
802.1x

Attributs :

- Nom
- Tunnel-Password
- Tunnel-Preference
- Tunnel-Pvt-Group-ID**
- Tunnel-Server-Auth-ID
- Tunnel-Server-Endpt
- Tunnel-Type

Description :
Spécifie l'ID de groupe pour une session par tunnel.

Ajouter... Fermer

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

Informations d'attribut

Nom de l'attribut :
Tunnel-Pvt-Group-ID

Numéro de l'attribut :
81

Format de l'attribut :
OctetString

Entrez la valeur d'attribut dans :

☒ Chaîne
☐ Hexadécimal

21

OK Annuler

▪ Nous cliquons sur suivant :

Nouvelle stratégie réseau

Configurer les paramètres

Le serveur NPS applique des paramètres à la demande de connexion si toutes les conditions relatives à la stratégie de demande de connexion sont remplies.

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

Précédent Suivant Terminer Annuler

▪ On clique sur Terminer.

Nouvelle stratégie réseau

Fin de la configuration de la nouvelle stratégie réseau

Vous avez correctement créé la stratégie réseau suivante :

Stratégie pour cliente câblée Pédago

Conditions de la stratégie :

Condition	Valeur
Groupes Windows	SIO-EXUPERY-PROF
Type de port NAS	Ethernet

Paramètres de la stratégie :

Condition	Valeur
Méthode d'authentification	Protocole EAP OU MS-CHAP v1 OU MS-CHAP v1 (l'utilisateur peut modifier...)
Autorisation d'accès	Accorder l'accès
Framed-Protocol	PPP
Service-Type	Framed
Ignorer les propriétés de numérotation des utilisateurs	Faux
Méthode EAP (Extensible Authentication Protocol)	Microsoft: PEAP (Protected EAP)

Pour fermer cet Assistant, cliquez sur Terminer.

Précédent Suivant Terminer Annuler

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

Propriétés de Stratégie pour cliente câblée Pédago

Vue d'ensemble Conditions Contraintes Paramètres

Nom de la stratégie : Stratégie pour cliente câblée Pédago

État de la stratégie
Si la stratégie est activée, le serveur NPS l'évalue lors de l'autorisation. Si elle est désactivée, le serveur NPS ne l'évalue pas.

☒ Stratégie activée

Autorisation d'accès
Si la demande de connexion répond aux conditions et contraintes de la stratégie réseau, celle-ci peut soit accorder l'accès, soit le refuser. [Qu'est-ce qu'une autorisation d'accès ?](#)

☒ Accorder l'accès. Accorder l'accès si la demande de connexion correspond à cette stratégie.
☐ Refuser l'accès. Refuser l'accès si la demande de connexion correspond à cette stratégie.
☐ Ignorer les propriétés de numérotation des comptes d'utilisateurs.
 Si la demande de connexion répond aux conditions et contraintes de cette stratégie réseau, et si la stratégie accorde l'accès, l'autorisation est basée uniquement sur la stratégie réseau ; les propriétés de numérotation des comptes d'utilisateurs ne sont pas évaluées.

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

☒ Type de serveur d'accès réseau :
 Non spécifié

☐ Spécifique au fournisseur :
 10

OK Annuler Appliquer

Propriétés de Stratégie pour cliente câblée Pédago

Vue d'ensemble Conditions Contraintes Paramètres

Configurez les conditions de cette stratégie réseau.

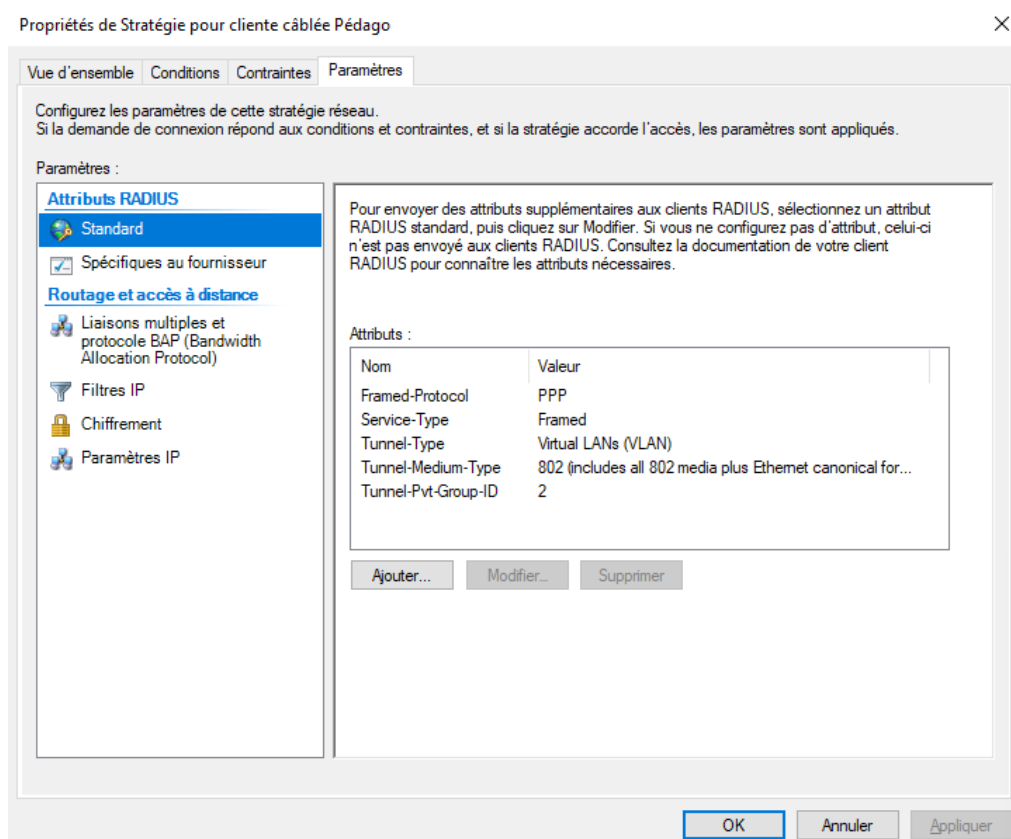
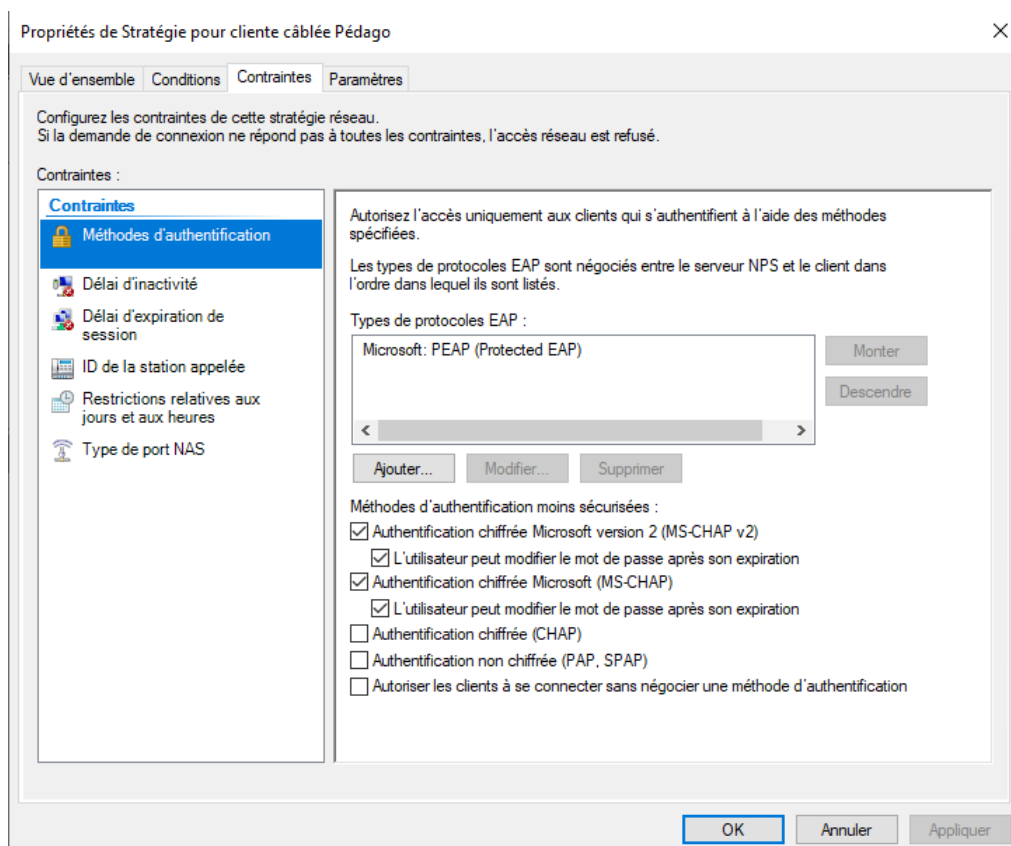
Si la demande de connexion répond aux conditions, le serveur NPS utilise cette stratégie pour autoriser la demande de connexion. Si la demande de connexion ne répond pas aux conditions, le serveur NPS ignore cette stratégie et en évalue d'autres, dans l'hypothèse où des stratégies supplémentaires seraient configurées.

Condition	Valeur
Groupes Windows	SIO-EXUPERY\PROF
Type de port NAS	Ethernet

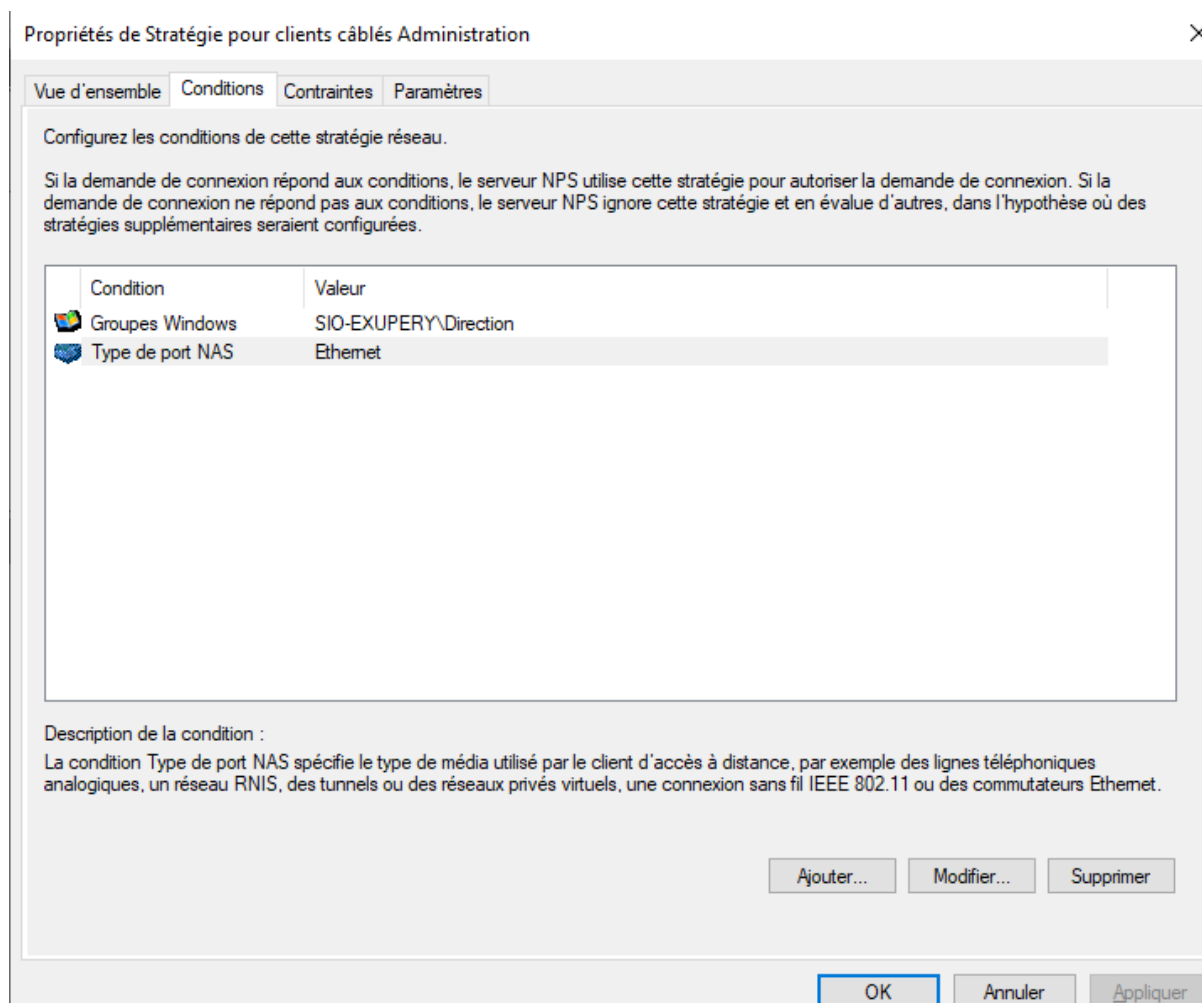
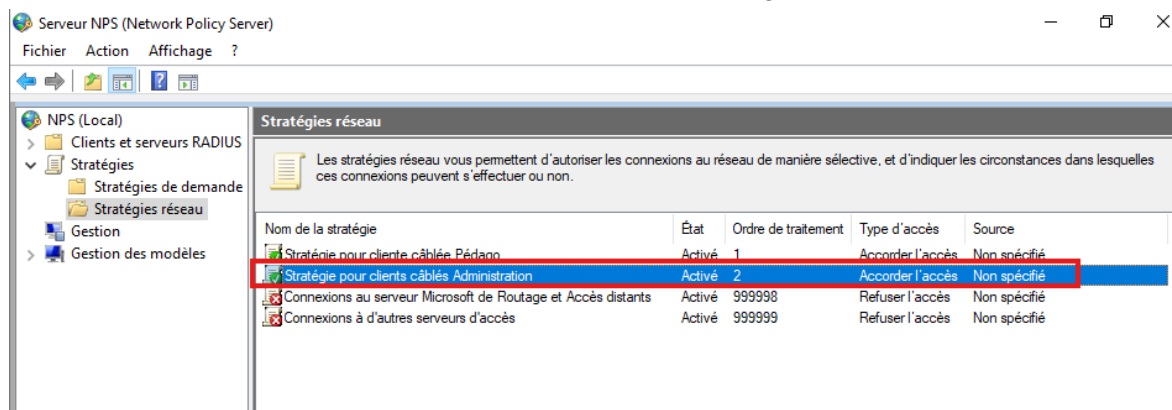
Description de la condition :
 La condition Type de port NAS spécifie le type de média utilisé par le client d'accès à distance, par exemple des lignes téléphoniques analogiques, un réseau RNIS, des tunnels ou des réseaux privés virtuels, une connexion sans fil IEEE 802.11 ou des commutateurs Ethernet.

Ajouter... Modifier... Supprimer

OK Annuler Appliquer



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



Propriétés de Stratégie pour clients câblés Administration

Vue d'ensemble Conditions Contraintes Paramètres

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

Contraintes :

Contraintes

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

Autorisez l'accès uniquement aux clients qui s'authentifient à l'aide des méthodes spécifiées.

Les types de protocoles EAP sont négociés entre le serveur NPS et le client dans l'ordre dans lequel ils sont listés.

Types de protocoles EAP :

Microsoft: PEAP (Protected EAP)

Monter Descendre

Ajouter... Modifier... Supprimer

Méthodes d'authentification moins sécurisées :

- ☒ Authentification chiffrée Microsoft version 2 (MS-CHAP v2)
 - ☒ L'utilisateur peut modifier le mot de passe après son expiration
- ☒ Authentification chiffrée Microsoft (MS-CHAP)
 - ☒ L'utilisateur peut modifier le mot de passe après son expiration
- ☐ Authentification chiffrée (CHAP)
- ☐ Authentification non chiffrée (PAP, SPAP)
- ☐ Autoriser les clients à se connecter sans négocier une méthode d'authentification

OK Annuler Appliquer

Propriétés de Stratégie pour clients câblés Administration

Vue d'ensemble Conditions Contraintes Paramètres

Configurez les paramètres de cette stratégie réseau.
Si la demande de connexion répond aux conditions et contraintes, et si la stratégie accorde l'accès, les paramètres sont appliqués.

Paramètres :

Attributs RADIUS

- Standard
- ☒ Spécifiques au fournisseur

Routing et accès à distance

- Liaisons multiples et protocole BAP (Bandwidth Allocation Protocol)
- Filtres IP
- Chiffrement
- Paramètres IP

Pour envoyer des attributs supplémentaires aux clients RADIUS, sélectionnez un attribut RADIUS standard, puis cliquez sur Modifier. Si vous ne configurez pas d'attribut, celui-ci n'est pas envoyé aux clients RADIUS. Consultez la documentation de votre client RADIUS pour connaître les attributs nécessaires.

Attributs :

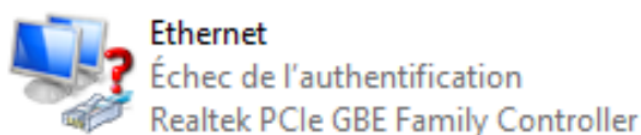
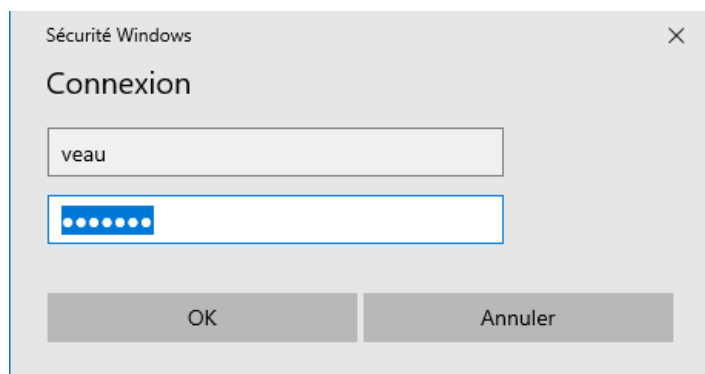
Nom	Valeur
Framed-Protocol	PPP
Service-Type	Framed
Tunnel-Type	Virtual LANs (VLAN)
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical for...
Tunnel-Pvt-Group-ID	3

Ajouter... Modifier... Supprimer

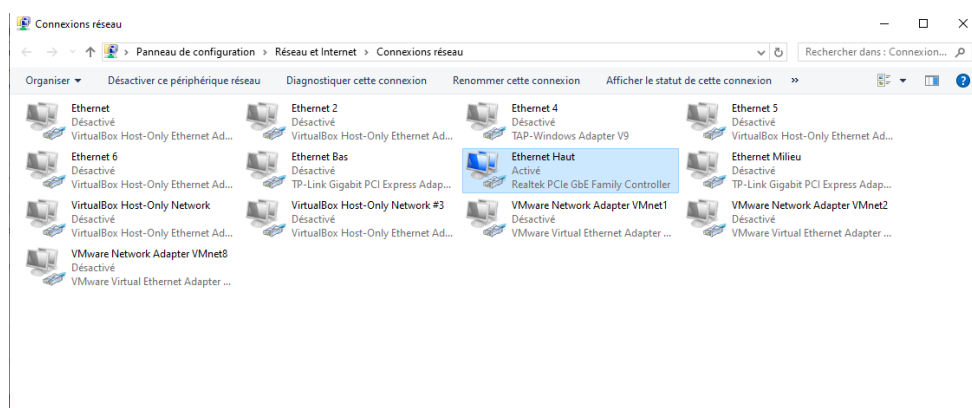
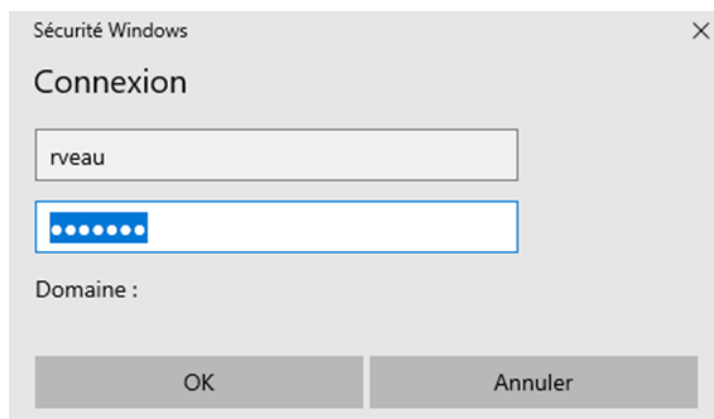
OK Annuler Appliquer

Annexe 3 : Demande de connexion des utilisateurs rveau et cgeley

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



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



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

```

C:\Users\admin>ipconfig /all

Configuration IP de Windows

Nom de l'hôte . . . . . : G101-MSI-C
Suffixe DNS principal . . . . . :
Type de noeud . . . . . : Hybride
Routage IP activé . . . . . : Non
Proxy WINS activé . . . . . : Non

Carte Ethernet Ethernet Haut :

Suffixe DNS propre à la connexion. . . :
Description. . . . . : Realtek PCIe GbE Family Controller
Adresse physique . . . . . : 30-9C-23-A5-90-CA
DHCP activé. . . . . : Oui
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . : fe80::7c5c:f03f:366c:5a2a%6(préfééré)
Adresse IPv4. . . . . : 192.168.1.2(préfééré)
Masque de sous-réseau. . . . . : 255.255.255.240
Bail obtenu. . . . . : jeudi 26 mars 2026 12:10:52
Bail expirant. . . . . : vendredi 27 mars 2026 12:10:51
Passerelle par défaut. . . . . : 192.168.1.1
Serveur DHCP . . . . . : 192.168.1.1
IAID DHCPv6 . . . . . : 523279395
DUID de client DHCPv6. . . . . : 00-01-00-01-23-3F-D2-C9-50-3E-AA-03-ED-39
Serveurs DNS. . . . . : 192.168.1.50
NetBIOS sur Tcpip. . . . . : Activé

C:\Users\admin>

```

- Nous vérifions sur le commutateur radius :

```

S1#sh dot1x all summary
Interface      PAE      Client      Status
-----
Fa0/7          AUTH     309c.23a5.90ca AUTHORIZED
Fa0/8          AUTH     none        UNAUTHORIZED
S1#

```

```

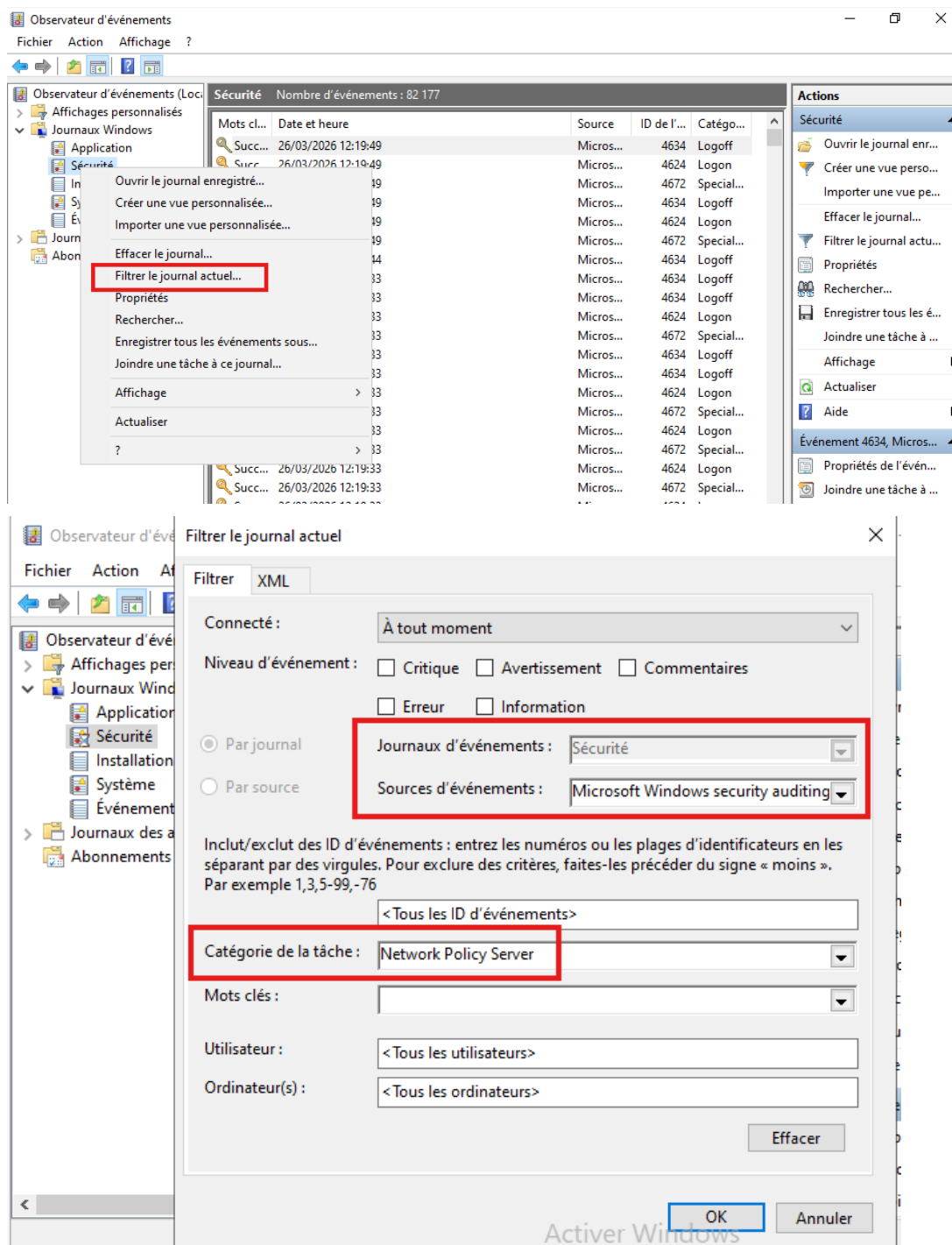
S1#sh vlan

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   Gestion                 active
1002 fddi-default            act/unsup
1003 token-ring-default     act/unsup
1004 fddinet-default        act/unsup
1005 trnet-default          act/unsup

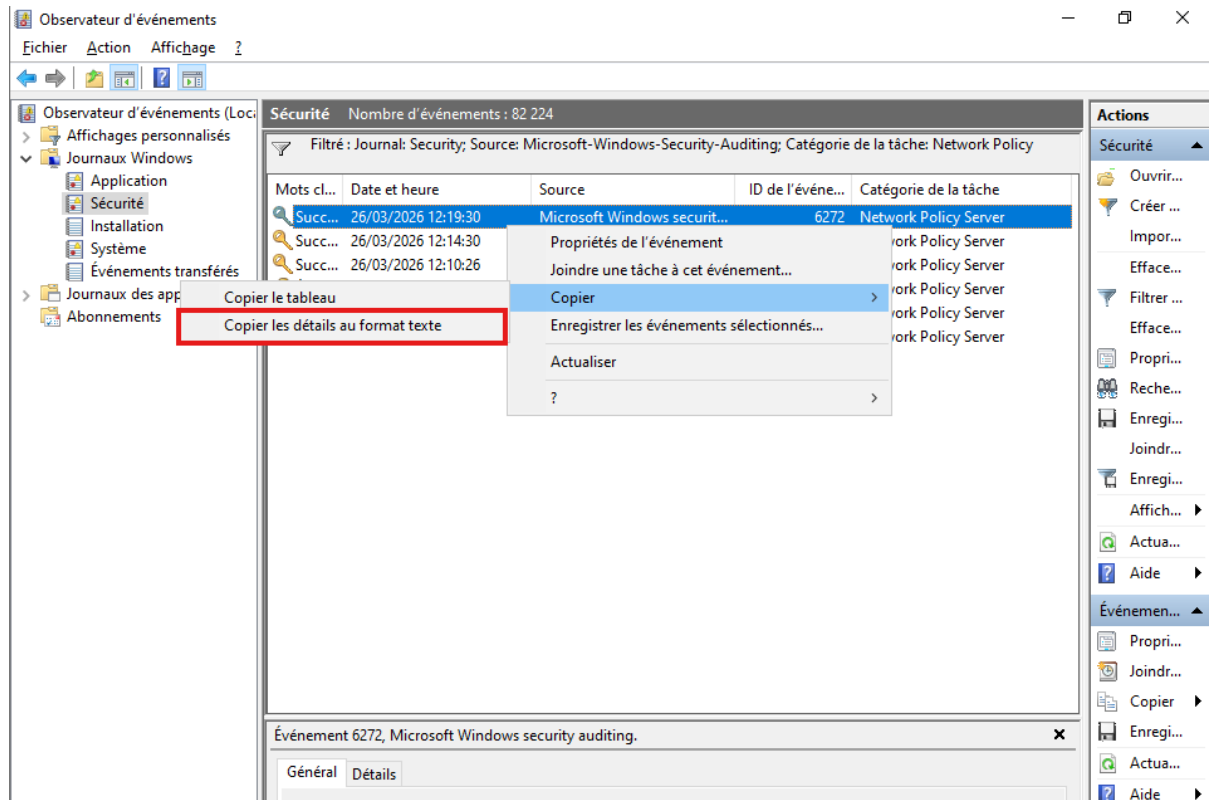
VLAN Type  SAID      MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
-----
1    enet   100001    1500  -     -     -     -   -       0       0
2    enet   100002    1500  -     -     -     -   -       0       0
3    enet   100003    1500  -     -     -     -   -       0       0

```

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



- Nous copions les informations au format texte :



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

Le serveur NPS a accordé l'accès à un utilisateur.

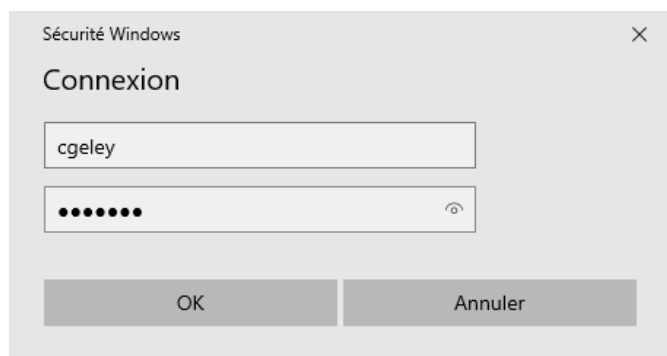
Utilisateur :
ID de sécurité : SIO-EXUPERY\iveau
Nom de compte : iveau
Domaine de compte : SIO-EXUPERY
Nom de compte complet : sio-exupery.local/Pédagogie/PROF/Régis VEAU

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

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

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

Informations détaillées sur l'authentification :
Nom de stratégie de demande de connexion : Connexion câblée
Nom de stratégie réseau : Stratégie pour 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.



Annexe 4 : Capture de trames : messages RADIUS

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

The image shows a Wireshark packet capture window titled "Capture en cours de Ethernet". The filter is set to "radius". The packet list shows a series of RADIUS messages between 192.168.1.50 and 192.168.0.2. The selected packet is number 1125, a RADIUS Access-Accept message with ID 39, which is highlighted with a red box. Below the packet list, the packet details pane shows the structure of the RADIUS message: Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and RADIUS Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1105	763.120780	192.168.0.2	192.168.1.50	RADIUS	284	Access-Request id=30
1106	763.123565	192.168.1.50	192.168.0.2	RADIUS	132	Access-Challenge id=30
1107	763.130325	192.168.0.2	192.168.1.50	RADIUS	483	Access-Request id=31
1109	763.131881	192.168.1.50	192.168.0.2	RADIUS	152	Access-Challenge id=31
1110	763.141045	192.168.0.2	192.168.1.50	RADIUS	317	Access-Request id=32
1111	763.141263	192.168.1.50	192.168.0.2	RADIUS	779	Access-Challenge id=32
1112	763.153083	192.168.0.2	192.168.1.50	RADIUS	486	Access-Request id=33
1113	763.154233	192.168.1.50	192.168.0.2	RADIUS	187	Access-Challenge id=33
1114	763.167815	192.168.0.2	192.168.1.50	RADIUS	317	Access-Request id=34
1115	763.168123	192.168.1.50	192.168.0.2	RADIUS	162	Access-Challenge id=34
1116	763.175372	192.168.0.2	192.168.1.50	RADIUS	353	Access-Request id=35
1117	763.175584	192.168.1.50	192.168.0.2	RADIUS	177	Access-Challenge id=35
1118	763.182952	192.168.0.2	192.168.1.50	RADIUS	362	Access-Request id=36
1119	763.183745	192.168.1.50	192.168.0.2	RADIUS	185	Access-Challenge id=36
1120	763.192446	192.168.0.2	192.168.1.50	RADIUS	407	Access-Request id=37
1121	763.193465	192.168.1.50	192.168.0.2	RADIUS	208	Access-Challenge id=37
1122	763.204453	192.168.0.2	192.168.1.50	RADIUS	348	Access-Request id=38
1123	763.204750	192.168.1.50	192.168.0.2	RADIUS	232	Access-Challenge id=38
1124	763.212931	192.168.0.2	192.168.1.50	RADIUS	417	Access-Request id=39
1125	763.213410	192.168.1.50	192.168.0.2	RADIUS	346	Access-Accept id=39

Frame 1125: 346 bytes on wire (2768 bits), 346 bytes captured (2768 bits) on interface 0
 Ethernet II, Src: PCSSystemtec_f7:4e:f7 (08:00:27:f7:4e:f7), Dst: 08:00:00:00:00:00
 Internet Protocol Version 4, Src: 192.168.1.50, Dst: 192.168.0.2
 User Datagram Protocol, Src Port: 1812, Dst Port: 1645
 RADIUS Protocol

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

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

Capture en cours de Ethernet

Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

radius

> Frame 1124: 417 bytes on wire (3336 bits), 417 bytes captured (3336 bits) on interface 0
 > Ethernet II, Src: Cisco_9f:d3:50 (e0:2f:6d:9f:d3:50), Dst: PCSSys_08:00:27:f7:4e:f7
 > Internet Protocol Version 4, Src: 192.168.0.2, Dst: 192.168.1.50
 > User Datagram Protocol, Src Port: 1645, Dst Port: 1812

▼ RADIUS Protocol

Code: Access-Request (1)

Packet Identifier: 0x27 (39)

Length: 375

Authenticator: 6503c15c43f077489203c62a38c56e15
 [The response to this request is in frame 1125]

▼ Attribute Value Pairs

> AVP: t=User-Name(1) l=8 val=cgeley

> AVP: t=Service-Type(6) l=6 val=Framed(2)

> AVP: t=Vendor-Specific(26) l=27 vnd=ciscoSystems(9)

> AVP: t=Framed-MTU(12) l=6 val=1500

> AVP: t=Called-Station-Id(30) l=19 val=00-08-2F-45-CD-87

> AVP: t=Calling-Station-Id(31) l=19 val=30-9C-23-A5-90-CA

▼ AVP: t=EAP-Message(79) l=108 Last Segment[1]

Type: 79

Length: 108

EAP fragment: 020b006a1900170303005f0000000000000053f4f

▼ Extensible Authentication Protocol

Code: Response (2)

Id: 11

Length: 106

Type: Protected EAP (EAP-PEAP) (25)

> EAP-TLS Flags: 0x00

> Transport Layer Security

> AVP: t=Message-Authenticator(80) l=18 val=d3a332cbb690ac7f3

> AVP: t=EAP-Key-Name(102) l=2 val=[wrong length]

> AVP: t=Vendor-Specific(26) l=49 vnd=ciscoSystems(9)

> AVP: t=Vendor-Specific(26) l=20 vnd=ciscoSystems(9)

> AVP: t=NAS-IP-Address(4) l=6 val=192.168.0.2

> AVP: t=NAS-Port-Id(87) l=17 val=FastEthernet0/7

> AVP: t=NAS-Port-Type(61) l=6 val=Ethernet(15)

> AVP: t=NAS-Port(5) l=6 val=50107

> AVP: t=State(24) l=38 val=5cb2077b0000013700011700fe8000000