

Sommaire

Anexe 1 : Commutateur Cisco 2960 et authentification 802.1x	2
Annexe 2 : Mise en place du serveur RADIUS (service NPS).....	6
2.1 Situation de départ.....	6
2.2 Ajout du rôle Services de certificats Active Directory	6
2.3 Installation du service NPS	13
2.4 Configuration du serveur RADIUS NPS.....	18
Annexe 3 : Demande de connexion des utilisateurs rveau et cgeley.....	40
Annexe 4 : Capture de trames : messages RADIUS.....	47

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 dot1x de
Switch(config)#aaa authentication dot1x default g
Switch(config)#aaa authentication dot1x 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)#dot1x 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)#dot1x 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 AuditSessionID
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 00000000000000409C800FB
*Mar 2 21:46:48.770: %AUTHMGR-7-FAILOVER: Failing over from 'dot1x' for client (309c.23a5.900d) on Interface Fa0/8
AuditSessionID 00000000000000409C800FB
*Mar 2 21:46:48.770: %AUTHMGR-7-NOMOREMETHODS: Exhausted all authentication methods for client (309c.23a5.900d) on I
nterface Fa0/8 AuditSessionID 00000000000000409C800FB
*Mar 2 21:46:48.770: %AUTHMGR-5-FAIL: Authorization failed for client (309c.23a5.900d) on Interface Fa0/8 AuditSess
ionID 00000000000000409C800FB
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 00000000000000409C800FB
Switch(config-if)#authentication port-control auto
^
% Invalid input detected at '^' marker.

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

```
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 :

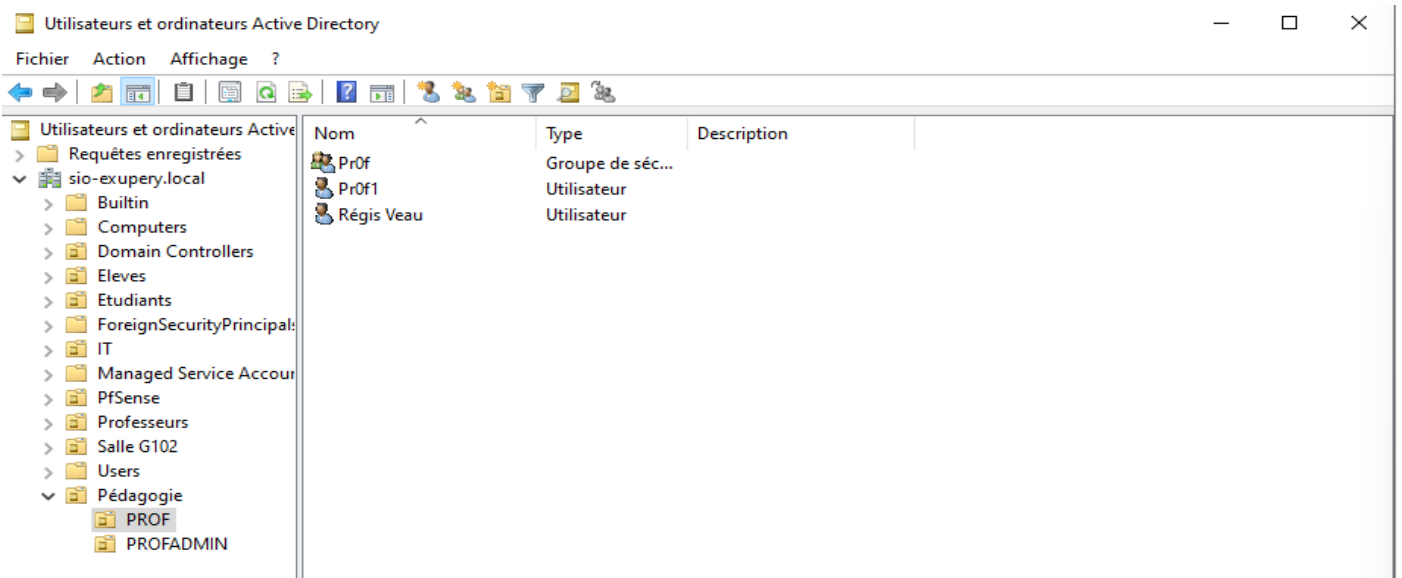
```
Router(config)#ip dhcp pool vlan2
Router(dhcp-config)#network 192.168.1.0 255.255.255.240
Router(dhcp-config)#default-router 192.168.1.1
Router(dhcp-config)#dns-server 192.168.1.50
Router(dhcp-config)#
```

```
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)

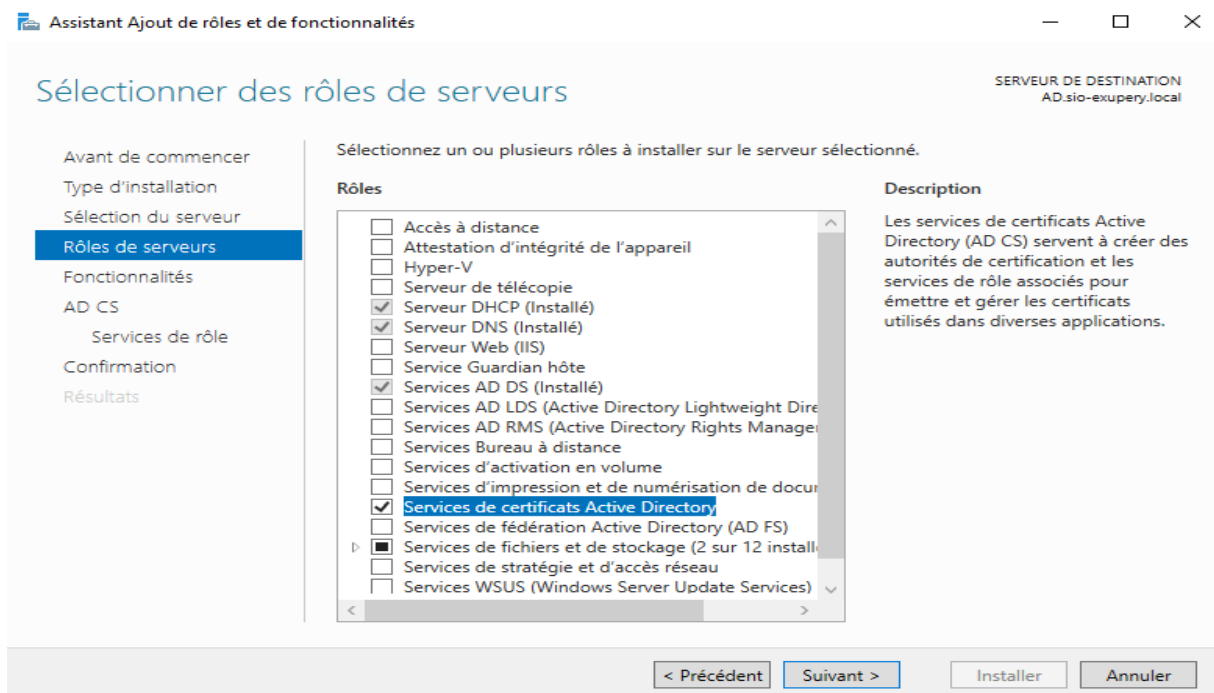
2.1 Situation de départ

➤ 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 :

Assistant Ajout de rôles et de fonctionnalités

Confirmer les sélections d'installation

SERVEUR DE DESTINATION
AD.sio-exupery.local

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
AD CS
Services de rôle
Confirmation
Résultats

Pour installer les rôles, services de rôle ou fonctionnalités suivants sur le serveur sélectionné, cliquez sur Installer.

Redémarrer automatiquement le serveur de destination, si nécessaire

Il se peut que des fonctionnalités facultatives (comme des outils d'administration) soient affichées sur cette page, car elles ont été sélectionnées automatiquement. Si vous ne voulez pas installer ces fonctionnalités facultatives, cliquez sur Précédent pour désactiver leurs cases à cocher.

Outils d'administration de serveur distant
Outils d'administration de rôles
Outils des services de certificats Active Directory
Outils de gestion de l'autorité de certification

Services de certificats Active Directory
Autorité de certification

[Exporter les paramètres de configuration](#)
[Spécifier un autre chemin d'accès source](#)

< Précédent Suivant > Installer Annuler

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

Assistant Ajout de rôles et de fonctionnalités

Progression de l'installation

SERVEUR DE DESTINATION
AD.sio-exupery.local

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
AD CS
Services de rôle
Confirmation
Résultats

Afficher la progression de l'installation

i Installation de fonctionnalité
Configuration requise. Installation réussie sur AD.sio-exupery.local.

Services de certificats Active Directory
Des étapes supplémentaires sont nécessaires pour la configuration des services de certificats Active Directory sur le serveur de destination.
Configurer les services de certificats Active Directory sur le serveur de destination
Autorité de certification

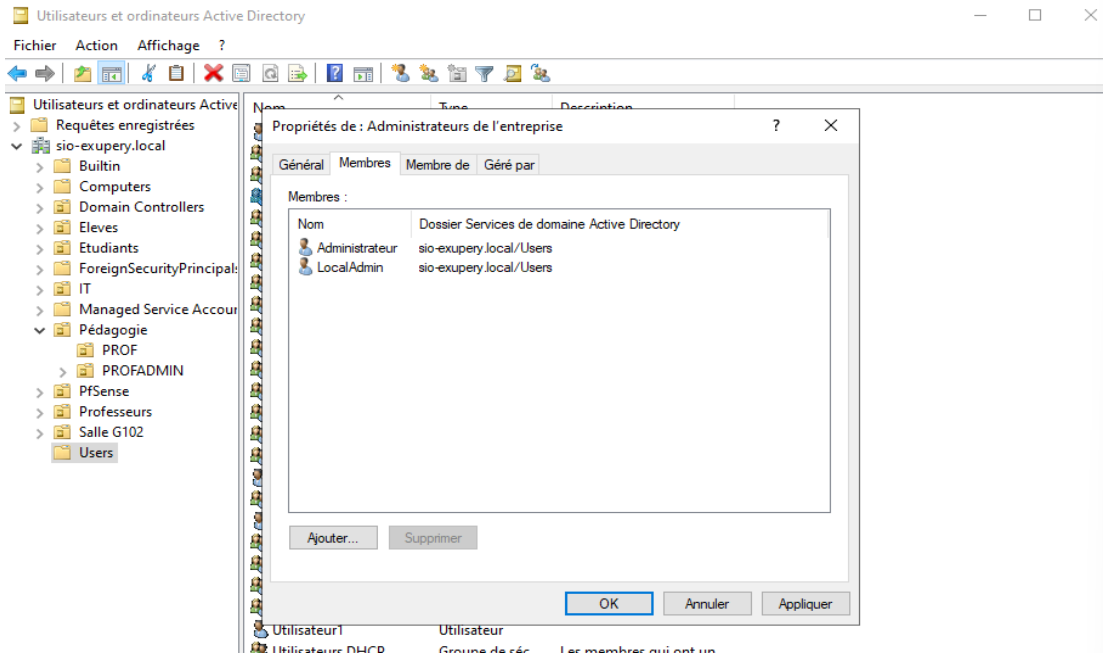
Outils d'administration de serveur distant
Outils d'administration de rôles
Outils des services de certificats Active Directory
Outils de gestion de l'autorité de certification

1 Vous pouvez fermer cet Assistant sans interrompre les tâches en cours d'exécution. Examinez leur progression ou rouvrez cette page en cliquant sur Notifications dans la barre de commandes, puis sur Détails de la tâche.

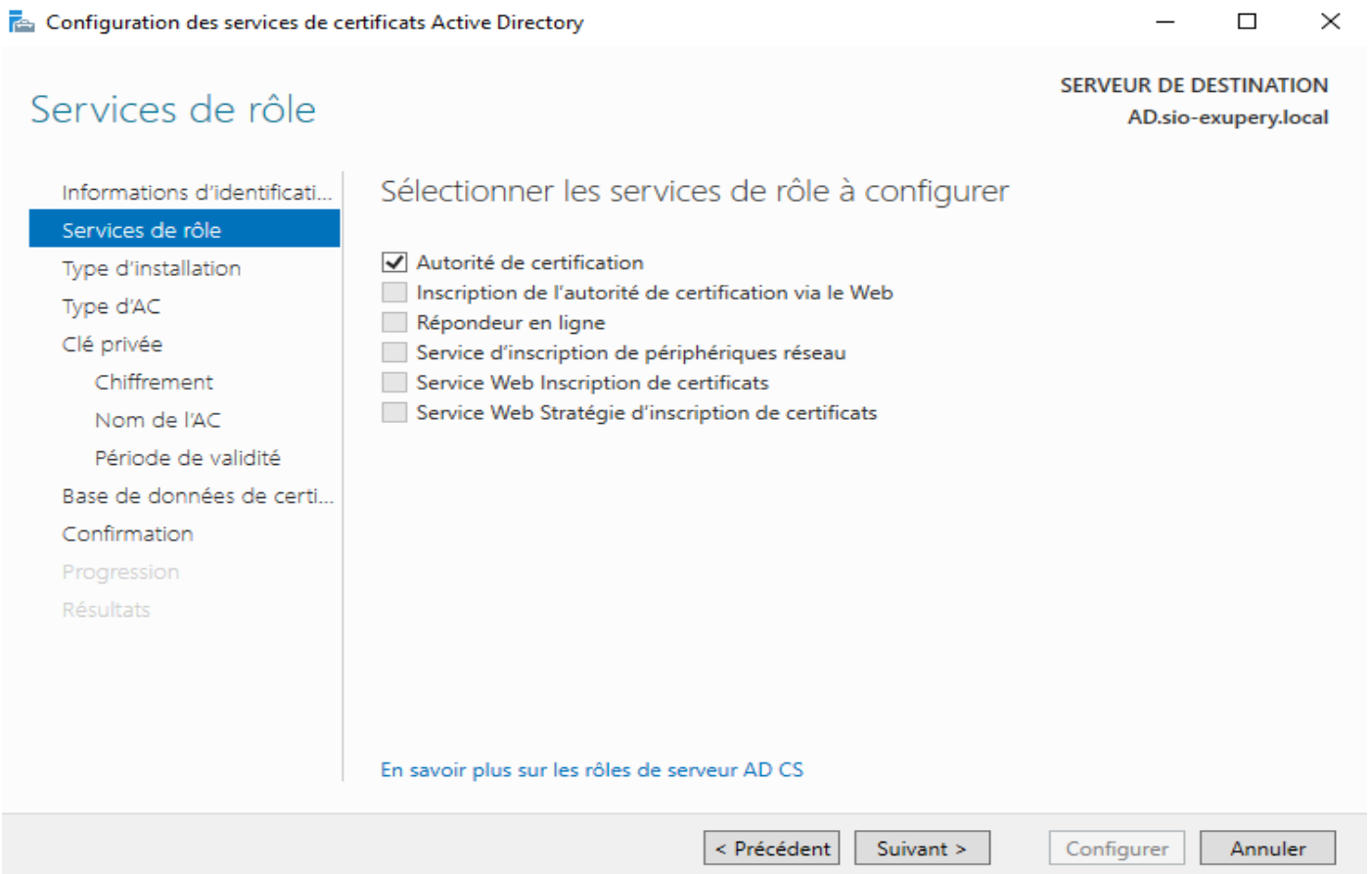
[Exporter les paramètres de configuration](#)

< Précédent Suivant > Fermer Annuler

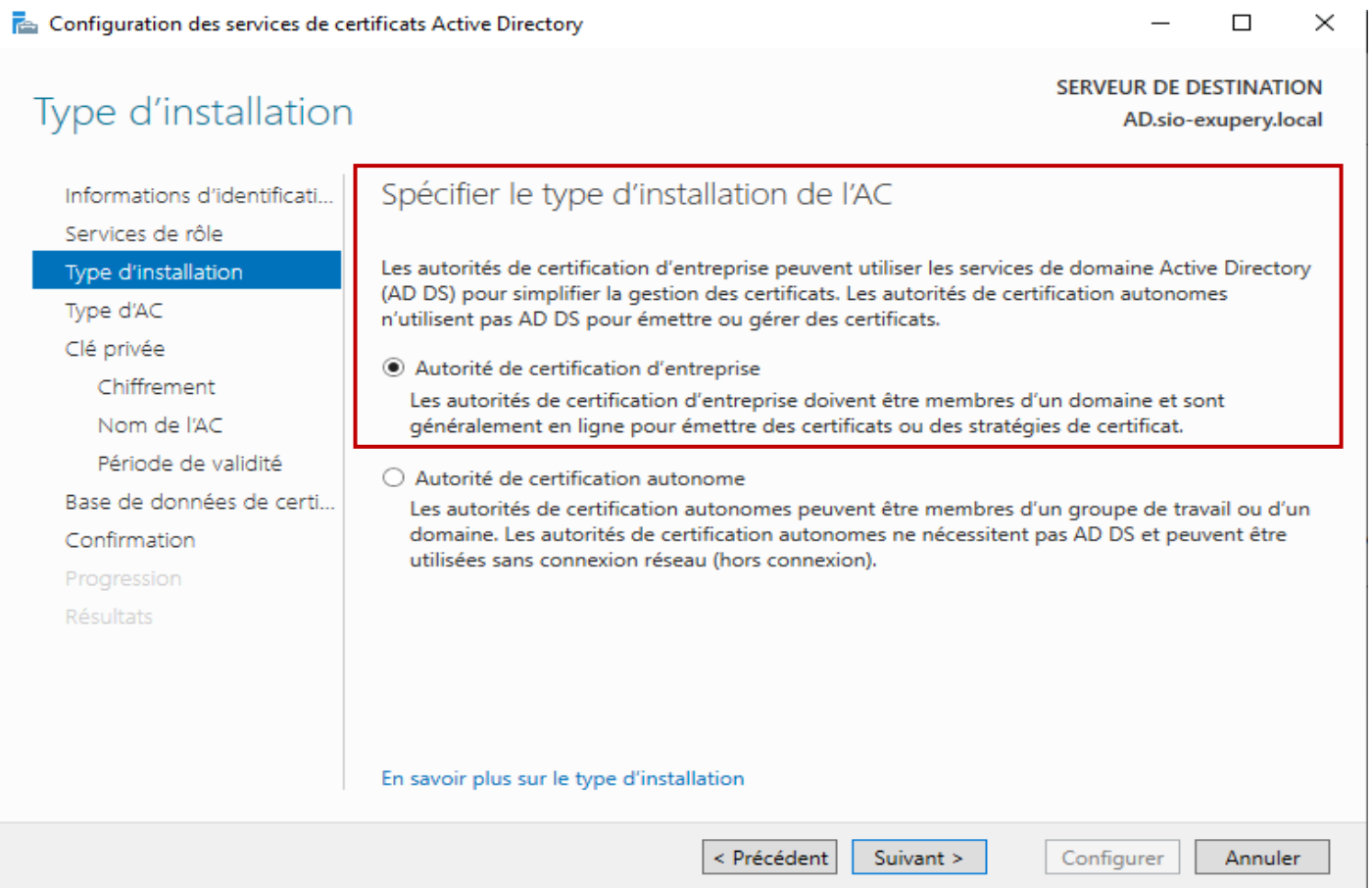
- Dans utilisateur et ordinateur Active Directory je dois être membre du groupe Administrateurs de l'entreprise :



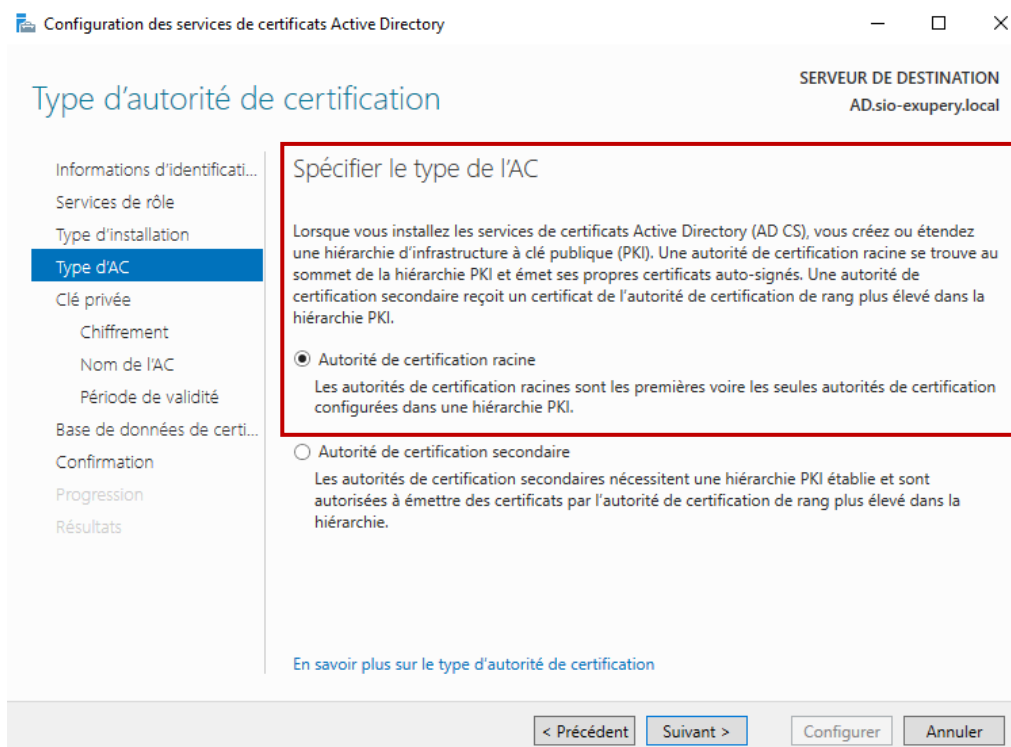
- Dans configuration des services de certificats Active Directory, je coche la case Autorité de certification pour configurer ce rôle :



➤ 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 :

Configuration des services de certificats Active Directory

— □ ×

Clé privée

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 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

Configuration des services de certificats Active Directory

— □ ×

Chiffrement pour 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 certi...
Confirmation
Progression
Résultats

Spécifier les options de chiffrement

Sélectionnez un fournisseur de chiffrement : Longueur de la clé :

RSA#Microsoft Software Key Storage Provider 2048

Sélectionnez l'algorithme de hachage pour signer les certificats émis par cette AC :

SHA256
SHA384
SHA512
SHA1

Autorisez l'interaction de l'administrateur lorsque l'autorité de certification accède à la clé privée.

[En savoir plus sur le chiffrement](#)

< Précédent Suivant > Configurer Annuler

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

Configuration des services de certificats Active Directory

SERVEUR DE DESTINATION
AD.sio-exupery.local

Nom de l'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 nom de l'AC

Tapez un nom commun pour identifier cette autorité de certification. Ce nom est ajouté à tous les certificats émis par l'autorité de certification. Les valeurs des suffixes du nom unique sont générées automatiquement, mais elles sont modifiables.

Nom commun de cette AC :

Suffixe du nom unique :

Aperçu du nom unique :

[En savoir plus sur le nom de l'autorité de certification](#)

< Précédent Suivant > Configurer Annuler

- Je laisse la période de validité par défaut :

Configuration des services de certificats Active Directory

SERVEUR DE DESTINATION
AD.sio-exupery.local

Période de validité

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 :

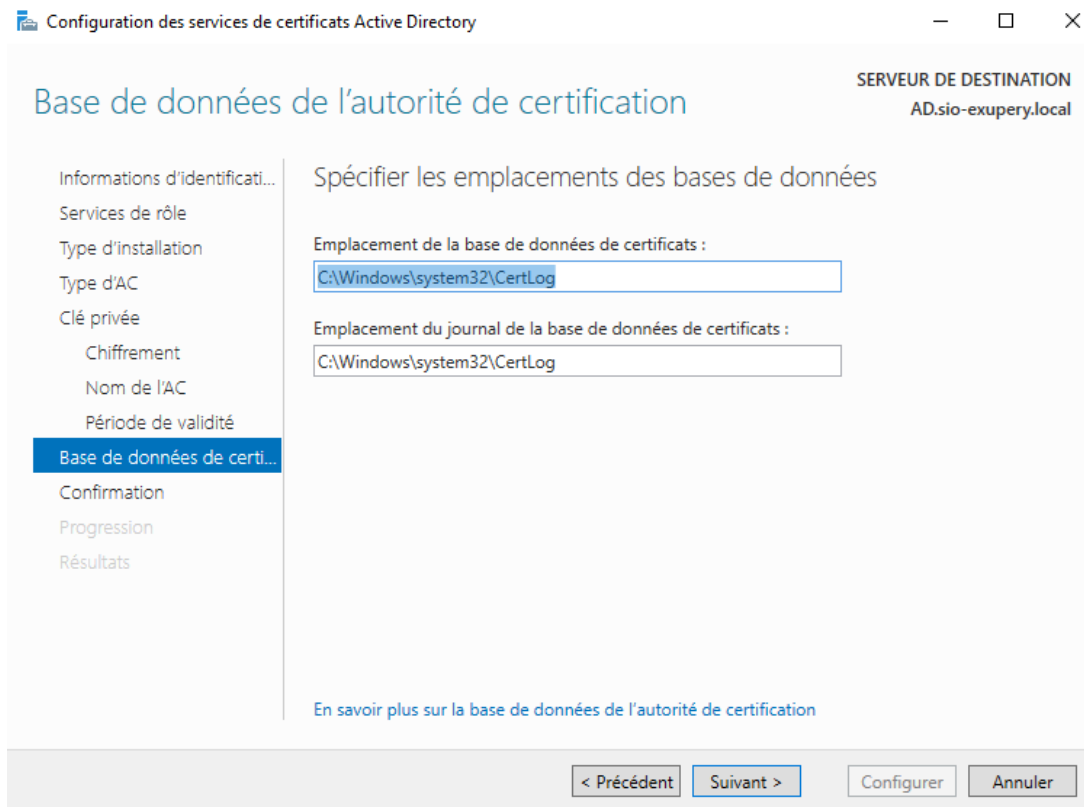
Date d'expiration de l'AC : 12/03/2031 09:30:00

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

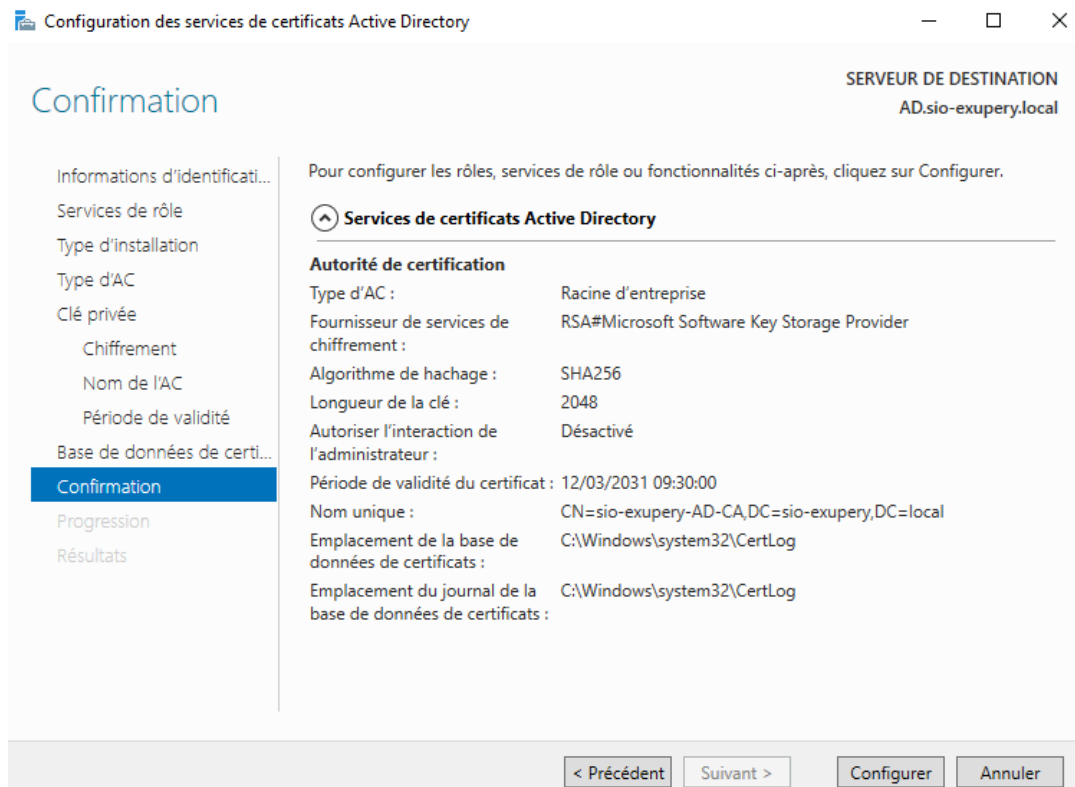
[En savoir plus sur la période de validité](#)

< Précédent Suivant > Configurer Annuler

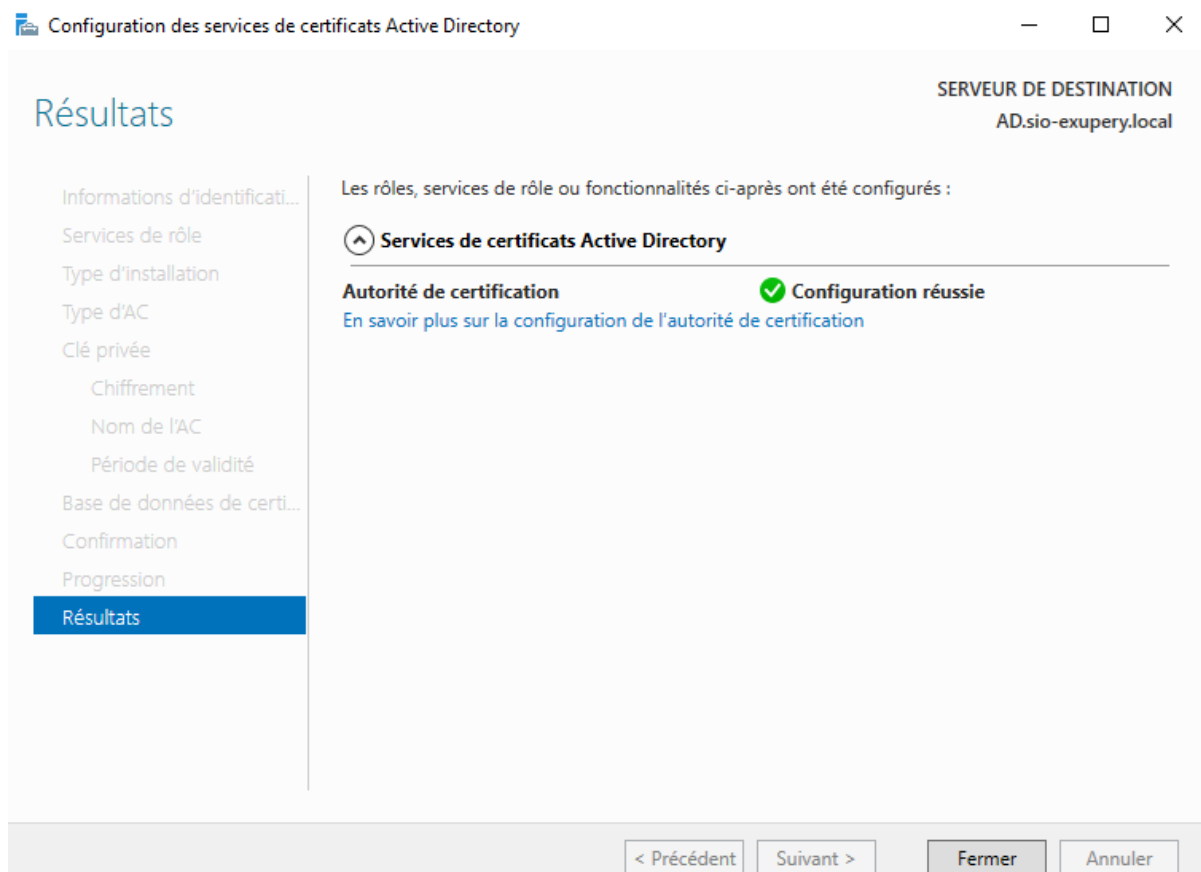
- Je laisse les dossiers des bases de données par défaut :



- 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 :

Sélectionner des rôles de serveurs

SERVEUR DE DESTINATION
AD.sio-exuperly.local

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

Confirmation

Résultats

Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.

Rôles

- Attestation d'intégrité de l'appareil
- Hyper-V
- Serveur de télécopie
- Serveur DHCP (Installé)
- Serveur DNS (Installé)
- Serveur Web (IIS)
- Service Guardian hôte
- Services AD DS (Installé)
- Services AD LDS (Active Directory Lightweight Directory Services)
- Services AD RMS (Active Directory Rights Management Services)
- Services Bureau à distance
- Services d'activation en volume
- Services d'impression et de numérisation de documents
- Services de certificats Active Directory (1 sur 6 installés)
- Services de fédération Active Directory (AD FS)
- Services de fichiers et de stockage (2 sur 12 installés)
- Services de stratégie et d'accès réseau
- Services WSUS (Windows Server Update Services)
- Windows Deployment Services

Description

Les services de stratégie et d'accès réseau fournissent un serveur NPS (Network Policy Server) qui contribue à garantir la sécurité de votre réseau.

< Précédent

Suivant >

Installer

Annuler

➤ Je clique sur le bouton Ajouter des fonctionnalités :

Sélectionner des rôles de serveurs

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

Confirmation

Résultats

Assistant Ajout de rôles et de fonctionnalités

Ajouter les fonctionnalités requises pour Services de stratégie et d'accès réseau ?

Les outils suivants sont requis pour la gestion de cette fonctionnalité, mais ils ne doivent pas obligatoirement être installés sur le même serveur.

- ▾ Outils d'administration de serveur distant
 - ▾ Outils d'administration de rôles
 - [Outils] Outils de la stratégie réseau et des services d'accès

 Inclure les outils de gestion (si applicable)

Ajouter des fonctionnalités

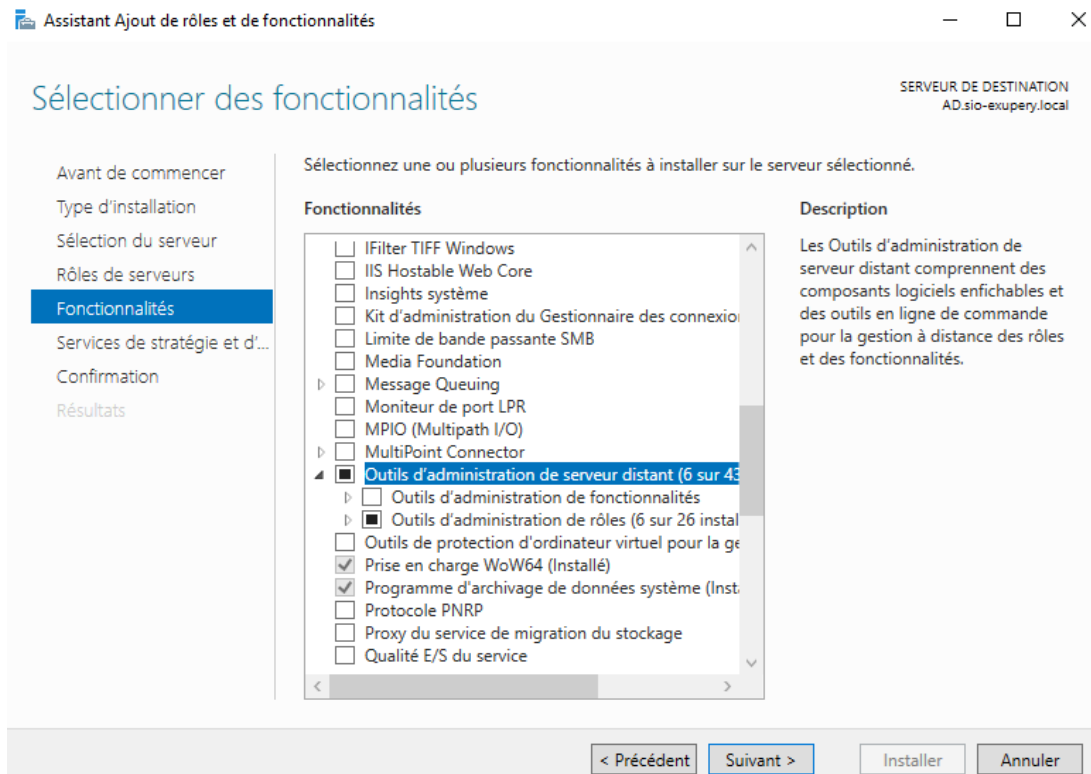
Annuler

SERVEUR DE DESTINATION
AD.sio-exuperly.local

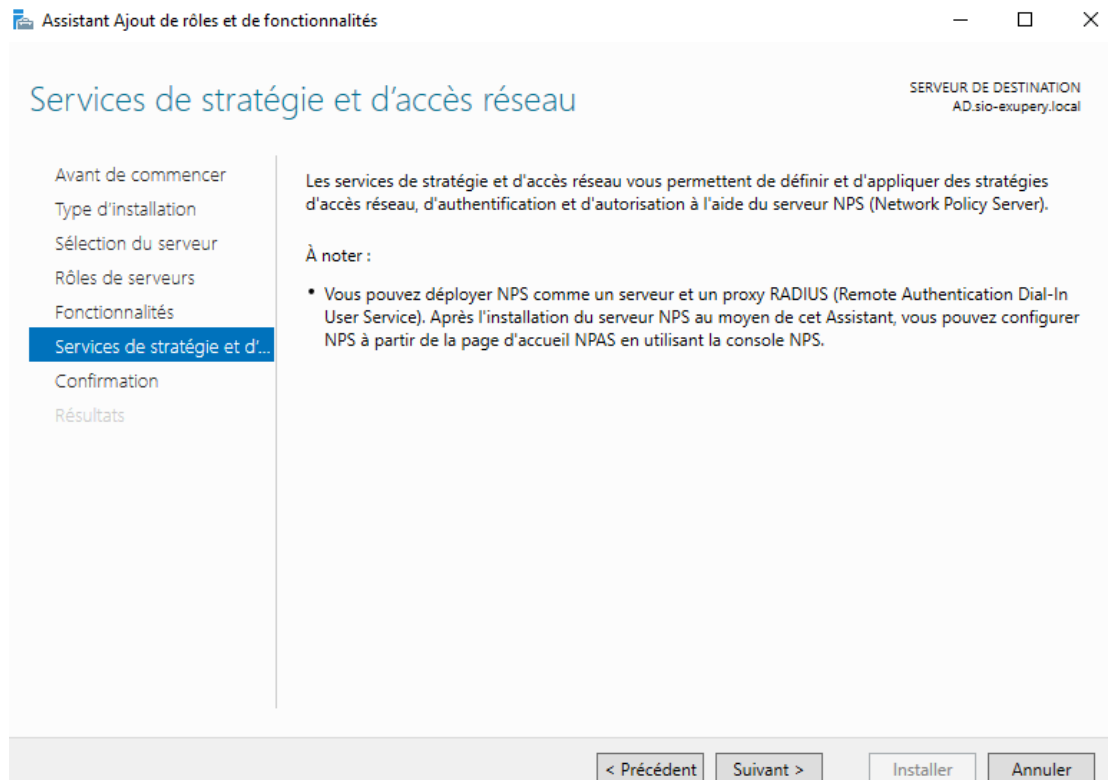
Description

Les services de stratégie et d'accès réseau fournissent un serveur NPS (Network Policy Server) qui contribue à garantir la sécurité de votre réseau.

➤ 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 :

Assistant Ajout de rôles et de fonctionnalités

SERVEUR DE DESTINATION
AD.sio-exupery.local

Confirmer les sélections d'installation

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Services de stratégie et d'...
Confirmation
Résultats

Pour installer les rôles, services de rôle ou fonctionnalités suivants sur le serveur sélectionné, cliquez sur Installer.

Redémarrer automatiquement le serveur de destination, si nécessaire

Il se peut que des fonctionnalités facultatives (comme des outils d'administration) soient affichées sur cette page, car elles ont été sélectionnées automatiquement. Si vous ne voulez pas installer ces fonctionnalités facultatives, cliquez sur Précédent pour désactiver leurs cases à cocher.

Outils d'administration de serveur distant
Outils d'administration de rôles
Outils de la stratégie réseau et des services d'accès

Services de stratégie et d'accès réseau

[Exporter les paramètres de configuration](#)
[Spécifier un autre chemin d'accès source](#)

< Précédent Suivant > Installer Annuler

➤ Une fois installer je clique sur fermer :

Assistant Ajout de rôles et de fonctionnalités

SERVEUR DE DESTINATION
AD.sio-exupery.local

Progression de l'installation

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Services de stratégie et d'...
Confirmation
Résultats

Afficher la progression de l'installation

i Installation de fonctionnalité

Installation réussie sur AD.sio-exupery.local.

Outils d'administration de serveur distant
Outils d'administration de rôles
Outils de la stratégie réseau et des services d'accès

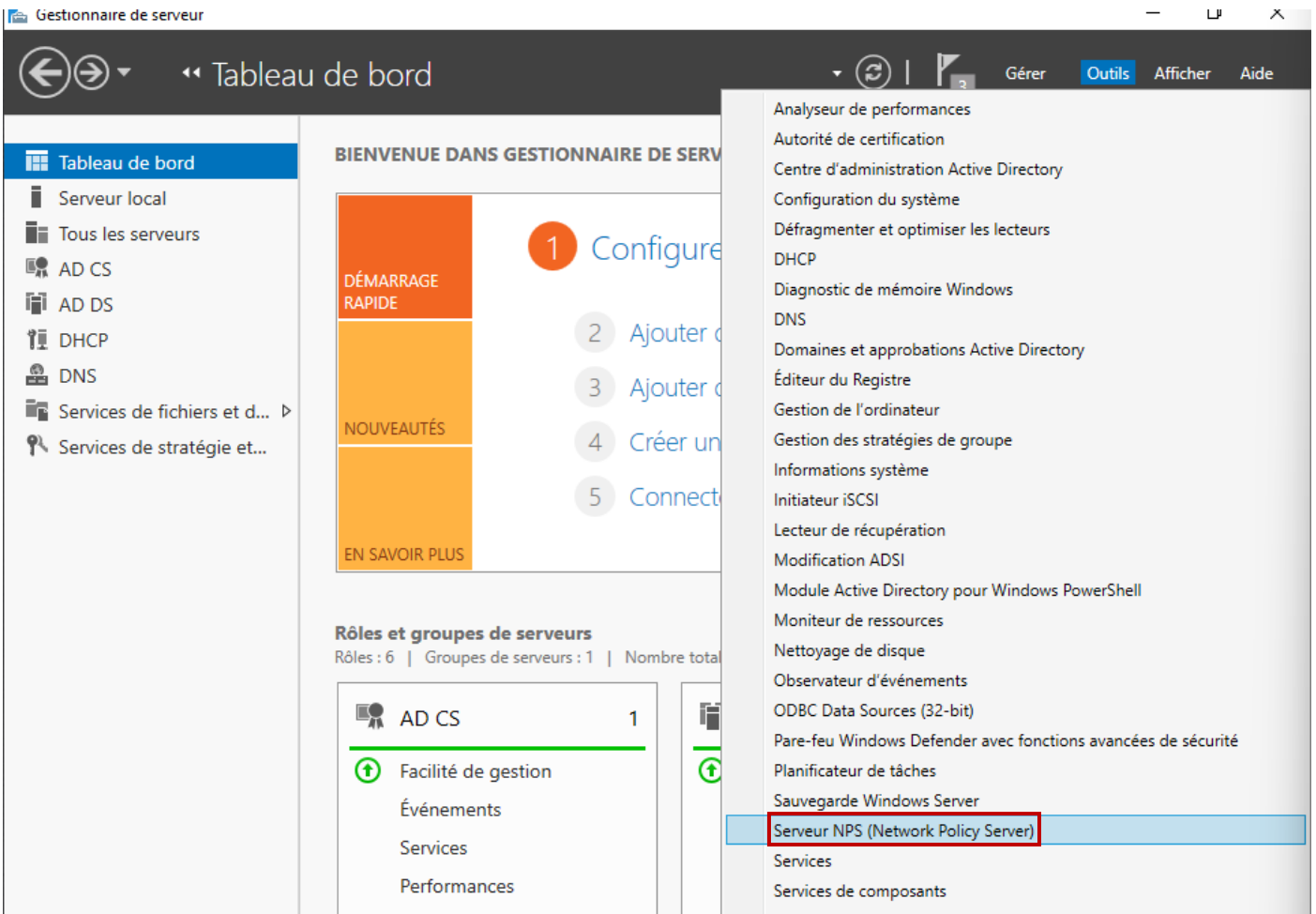
Services de stratégie et d'accès réseau

1 Vous pouvez fermer cet Assistant sans interrompre les tâches en cours d'exécution. Examinez leur progression ou rouvrez cette page en cliquant sur Notifications dans la barre de commandes, puis sur Détails de la tâche.

[Exporter les paramètres de configuration](#)

< Précédent Suivant > Fermer Annuler

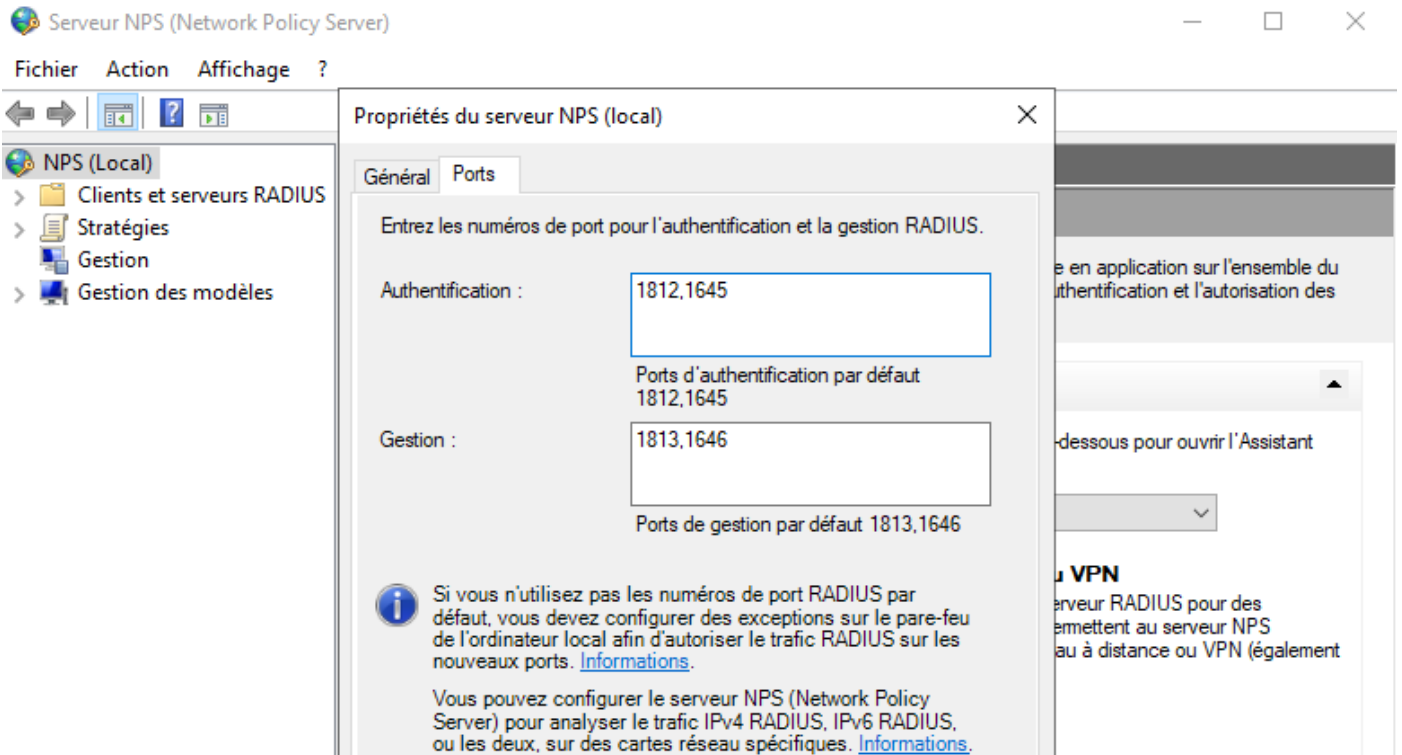
➤ Dans les outils je peux apercevoir la console Serveur NPS :



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

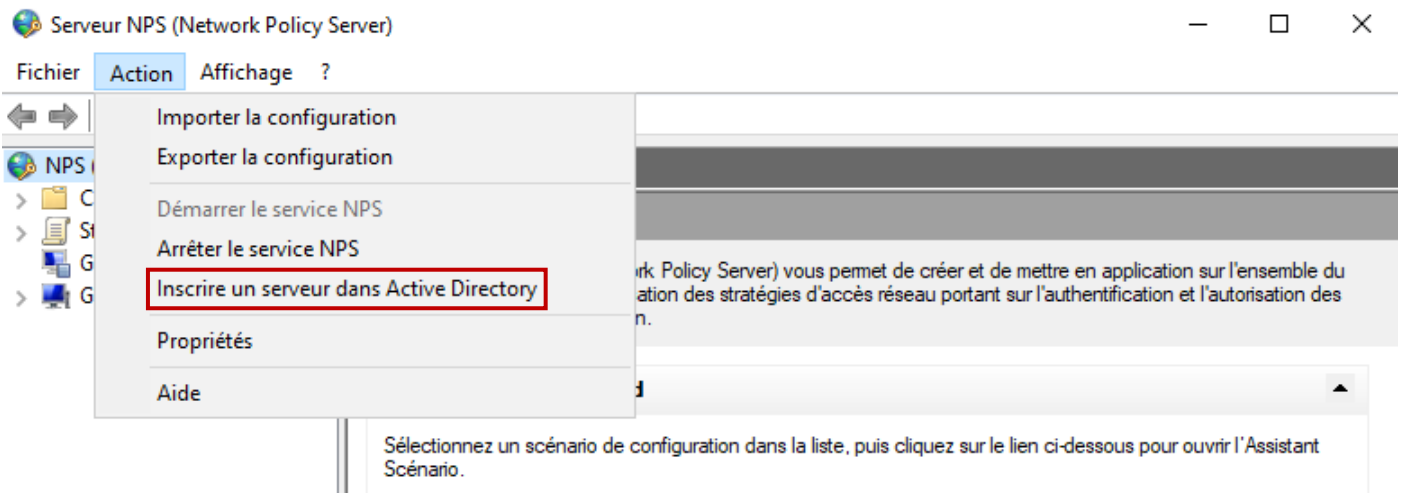


- J'ouvre la console Serveur NPS et je retrouve ces ports dans les propriétés du serveur NPS :

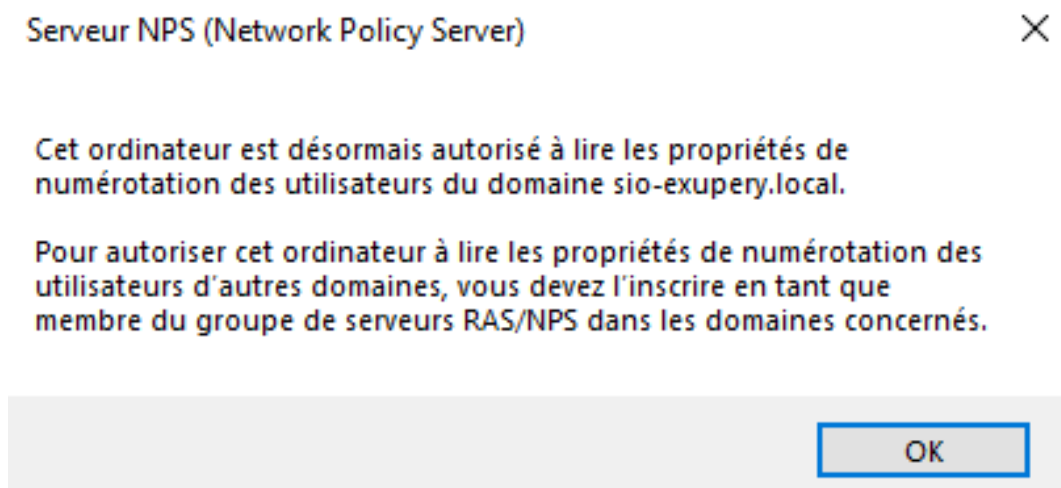
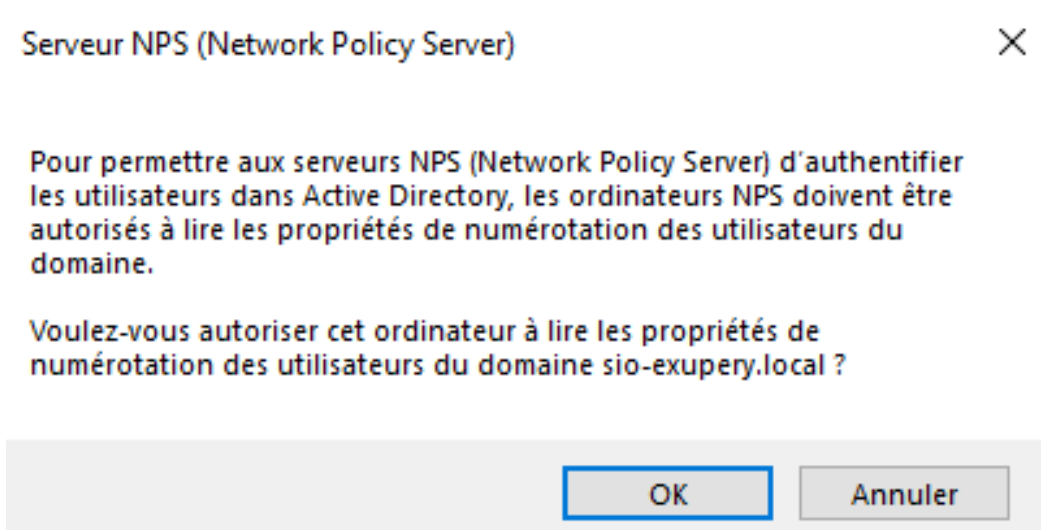


2.4 Configuration du serveur RADIUS NPS

- 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) :

Nouveau client RADIUS

Paramètres Avancé

Activer ce client RADIUS

Sélectionner un modèle existant :

Nom et adresse

Nom convivial : Client-Cisco-2960

Adresse (IP ou DNS) : 192.168.0.2 Vérifier...

Secret partagé

Sélectionnez un modèle de secrets partagés existant : Aucun

Pour taper manuellement un secret partagé, cliquez sur Manuel. Pour générer automatiquement un secret partagé, cliquez sur Générer. Vous devez configurer le client RADIUS avec le même secret partagé entré ici. Les secrets partagés respectent la casse.

Manuel Générer

Secret partagé :

Confirmez le secret partagé :

OK Annuler

Serveur NPS (Network Policy Server)

Fichier Action Affichage ?

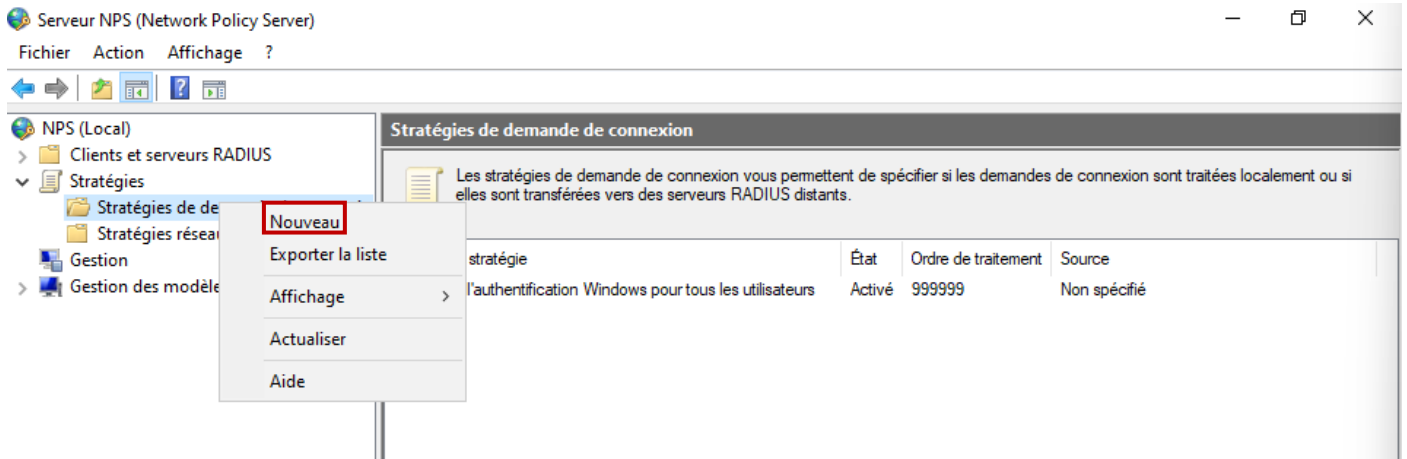
NPS (Local)

- Clients et serveurs RADIUS
 - Clients RADIUS**
 - Groupes de serveurs RA
- Stratégies
- Gestion
- Gestion des modèles

Les clients RADIUS vous permettent de spécifier les serveurs d'accès réseau qui fournissent l'accès à votre réseau.

Nom convivial	Adresse IP	Fabricant du périphérique	État
Client-Cisco-2960	192.168.0.2	RADIUS Standard	Activé

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



➤ Je clique sur suivant :

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 :

Connexion câblée

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

- Sur cette fenêtre je clique sur Ajouter :

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
-----------	--------

Description de la condition :





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

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.

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

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

- Je clique 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 :

➤ Je laisse par défaut et je clique sur 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

➤ Idem pour cette fenêtre :

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 :

MonterDescendre

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

- Je clique sur le bouton 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

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

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 :

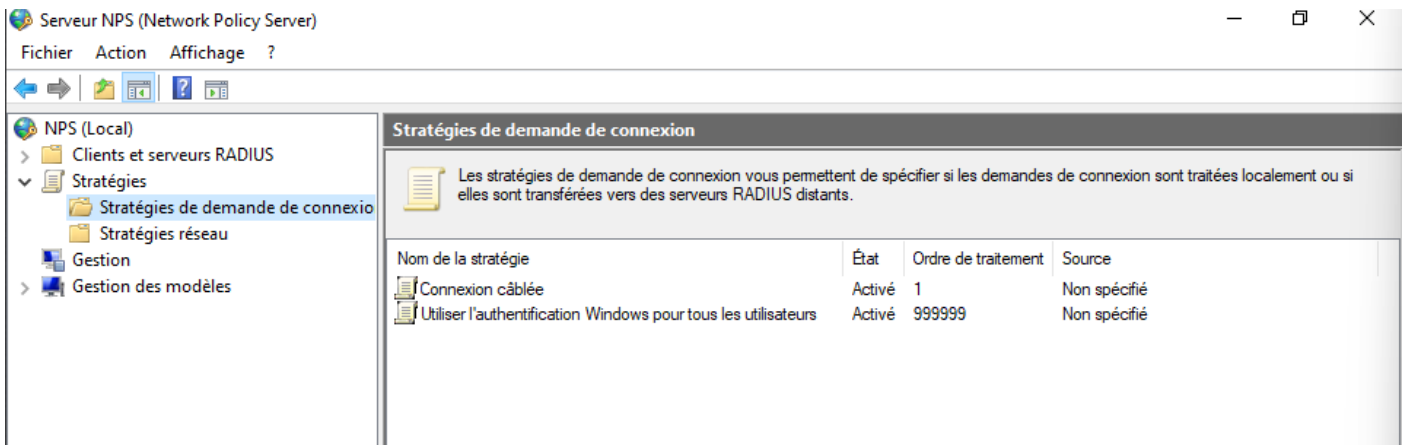
Condition	Valeur
Type de port NAS	Ethemet

Paramètres de la stratégie :

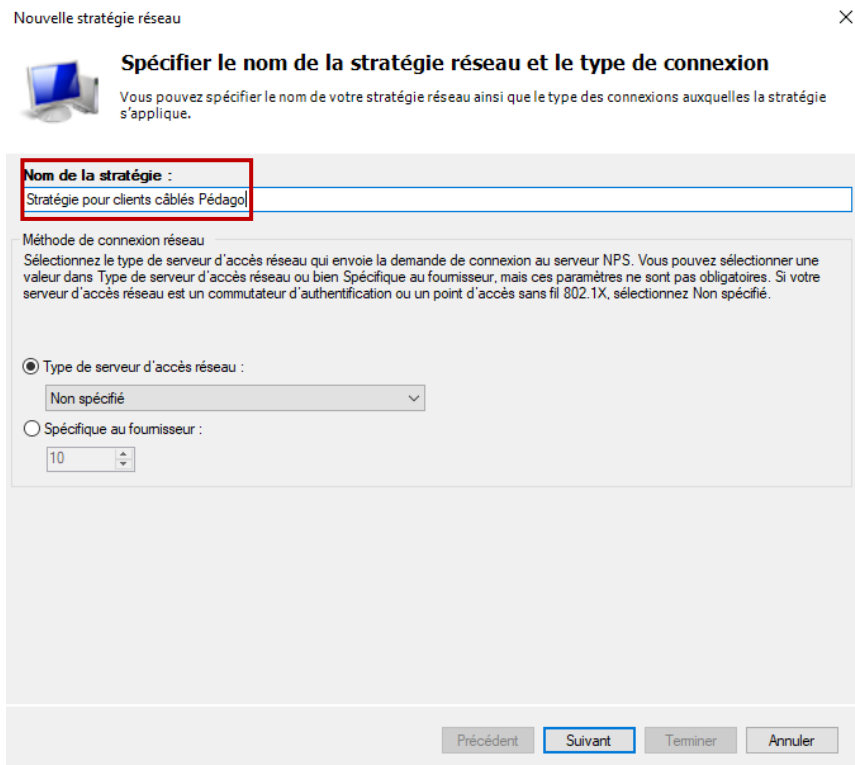
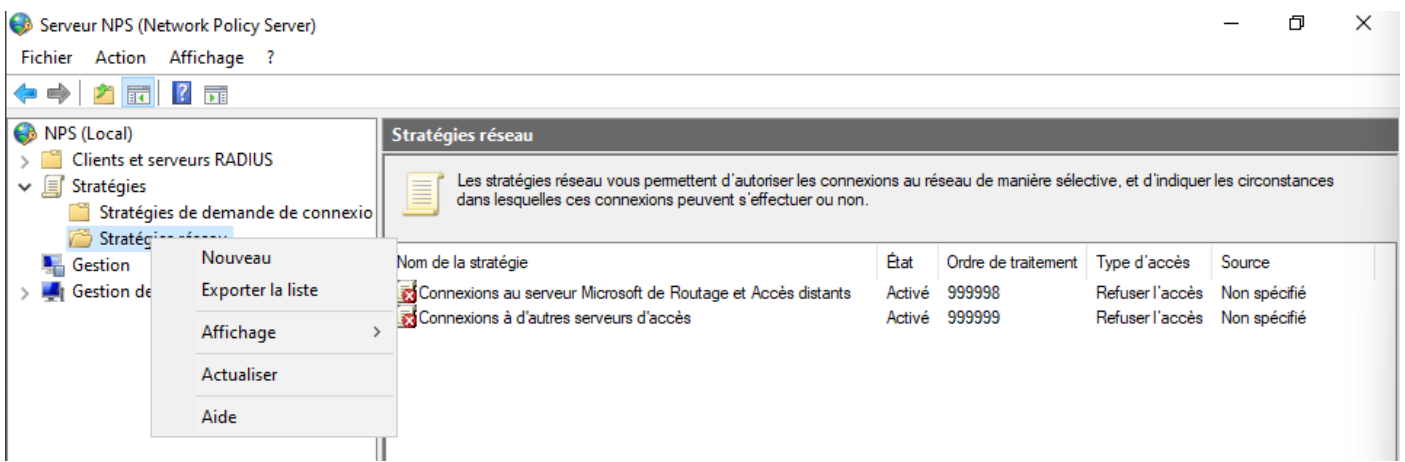
Condition	Valeur
Fournisseur d'authentification	Ordinateur local

Pour fermer cet Assistant, cliquez sur Terminer.

Précédent Suivant **Terminer** Annuler




➤ 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 :

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
-----------	--------

Description de la 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 :




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

-  **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).

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

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.



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

- Je coche 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

➤ Je clique 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\Pröf
 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.

➤ J'accorde 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.

- Dans l'écran Configurer les méthodes d'authentification, je déclare 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

- Dans l'écran Configurer des contraintes, je clique 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

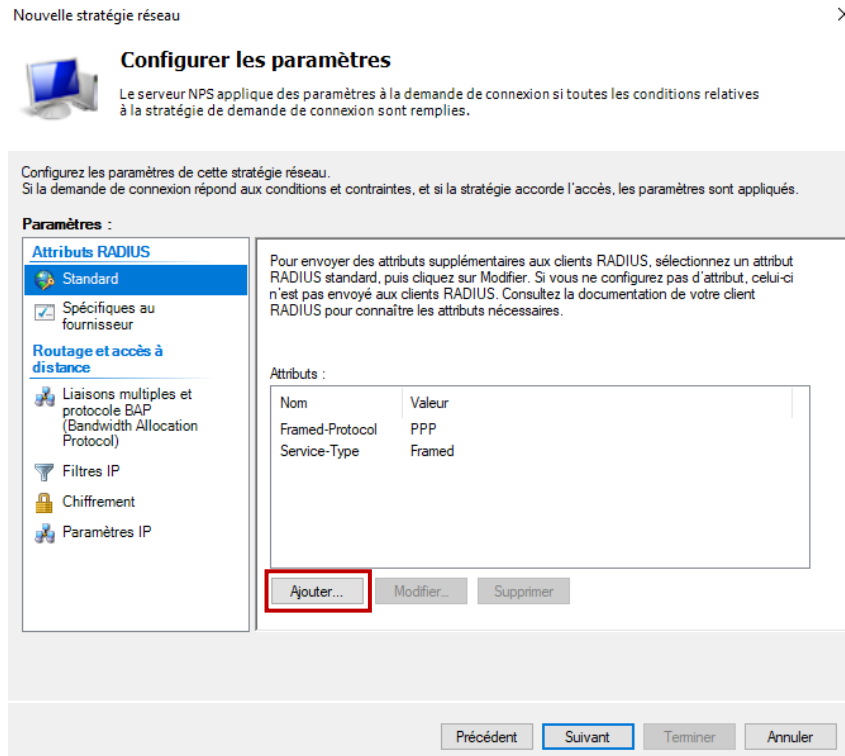
Spécifiez le délai maximal d'inactivité du serveur en minutes avant déconnexion

Déconnecter au-delà de la durée d'inactivité maximale

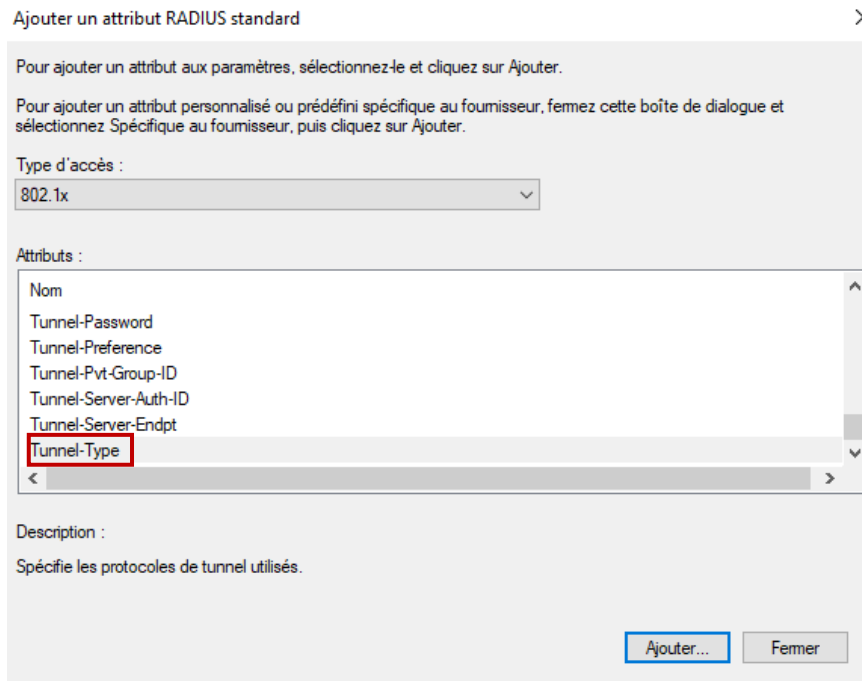
1

Précédent Suivant Terminer Annuler

- Dans l'écran Configurer les paramètres, 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 :

Informations d'attribut

Nom de l'attribut :
Tunnel-Type

Numéro de l'attribut :
64

Format de l'attribut :
Enumerator

Valeurs d'attribut :

Fournisseur	Valeur
-------------	--------

Ajouter...
Modifier...
Supprimer
Monter
Descendre

OK Annuler

- Je sélectionne Virtual LANs :

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

- Je clique sur OK :

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

➤ Je 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

- Je spécifie le numéro de VLAN dans lequel je veux 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

2

OK Annuler

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

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

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

Nouvelle stratégie réseau ×

 **Fin de la configuration de la nouvelle stratégie réseau**

Vous avez correctement créé la stratégie réseau suivante :

Stratégie pour clients câblés 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

- Je recréer une nouvelle stratégie pour les clients câblés :

Propriétés de Stratégie pour clients câblés Pédago ×

Vue d'ensemble **Conditions** Contraintes Paramètres

Nom de la stratégie :

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.

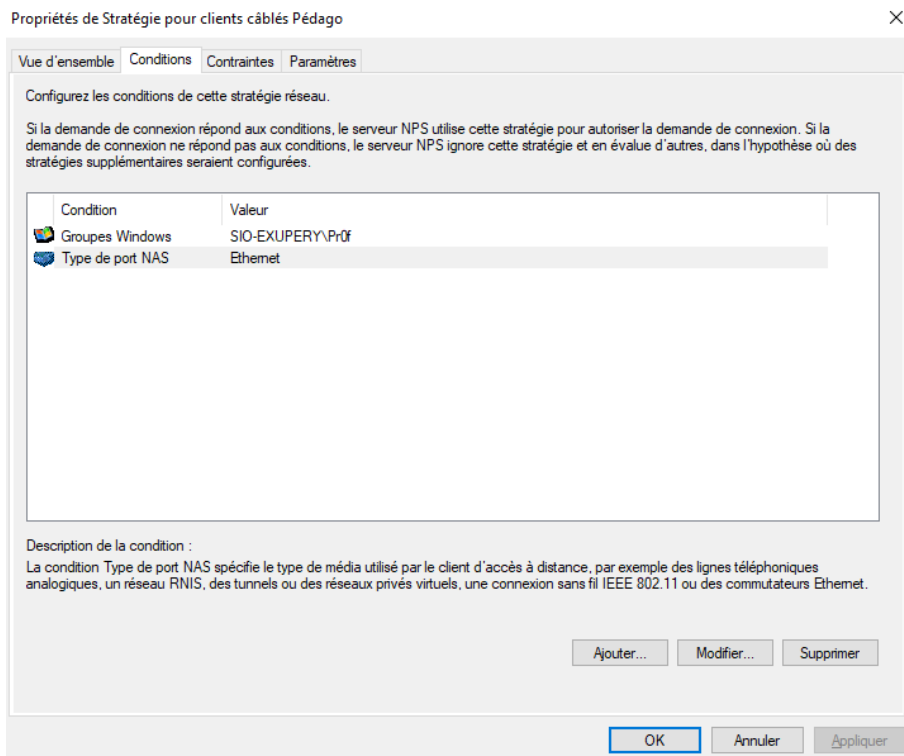
Méthode de connexion réseau
Sélectionnez le type de serveur d'accès réseau qui envoie la demande de connexion au serveur NPS. Vous pouvez sélectionner une valeur dans Type de serveur d'accès réseau ou bien Spécifique au fournisseur, mais ces paramètres ne sont pas obligatoires. Si votre serveur d'accès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

Type de serveur d'accès réseau :

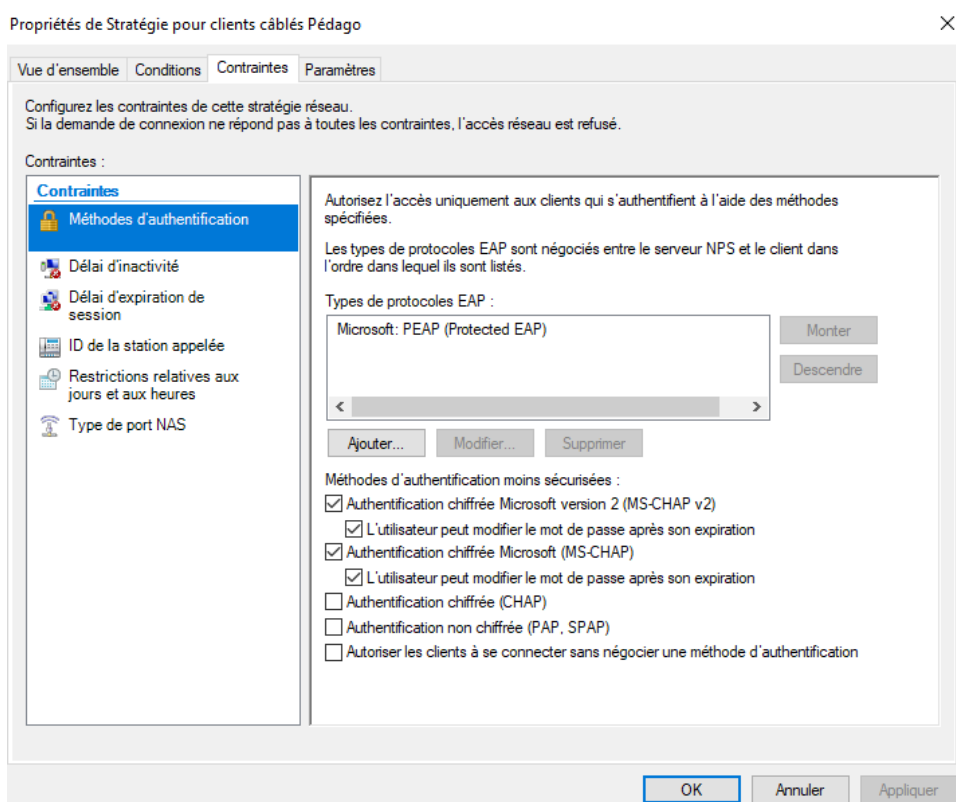
Spécifique au fournisseur :

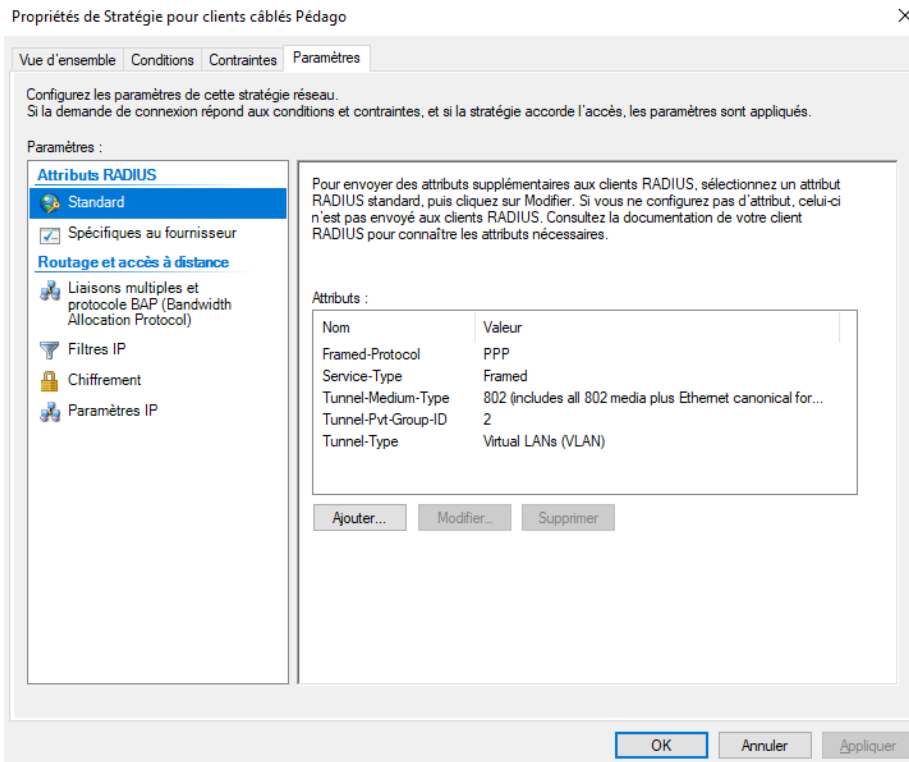
OK Annuler Appliquer

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

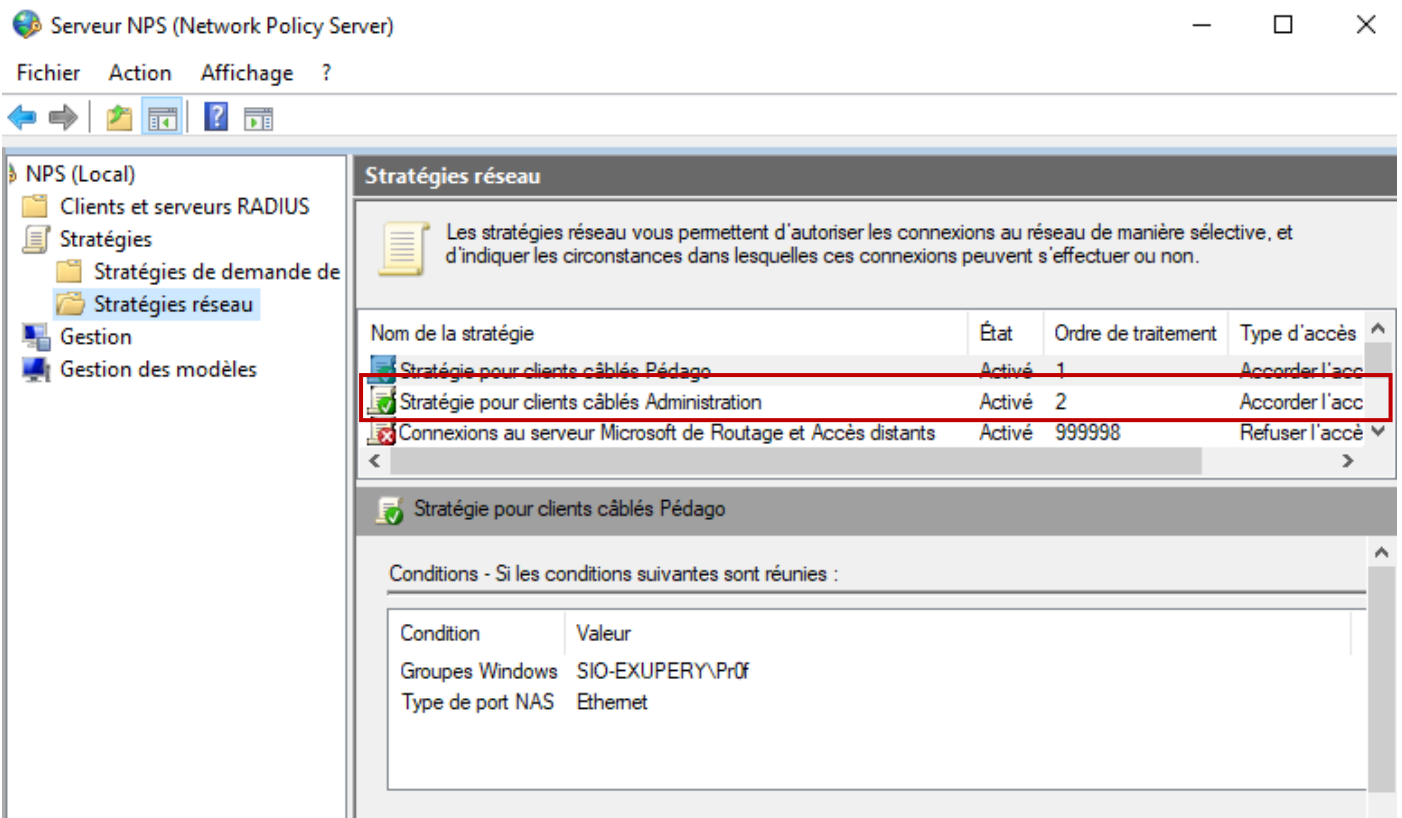


➤ J'ajoute la méthode d'authentification PEAP :






- En suivant le même procédé 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 :

Nouvelle stratégie réseau X

 **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\Direction
 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.

➤ J'ajoute la méthode d'authentification PEAP :

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

-  Liens 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-Medium-Type	802 (includes all 802 media plus Ethernet canonical for...
Tunnel-Pvt-Group-ID	3
Tunnel-Type	Virtual LANs (VLAN)

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

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-Medium-Type	802 (includes all 802 media plus Ethernet canonical for...
Tunnel-Pvt-Group-ID	3
Tunnel-Type	Virtual LANs (VLAN)

Ajouter...

Modifier...

Supprimer

Précédent

Suivant

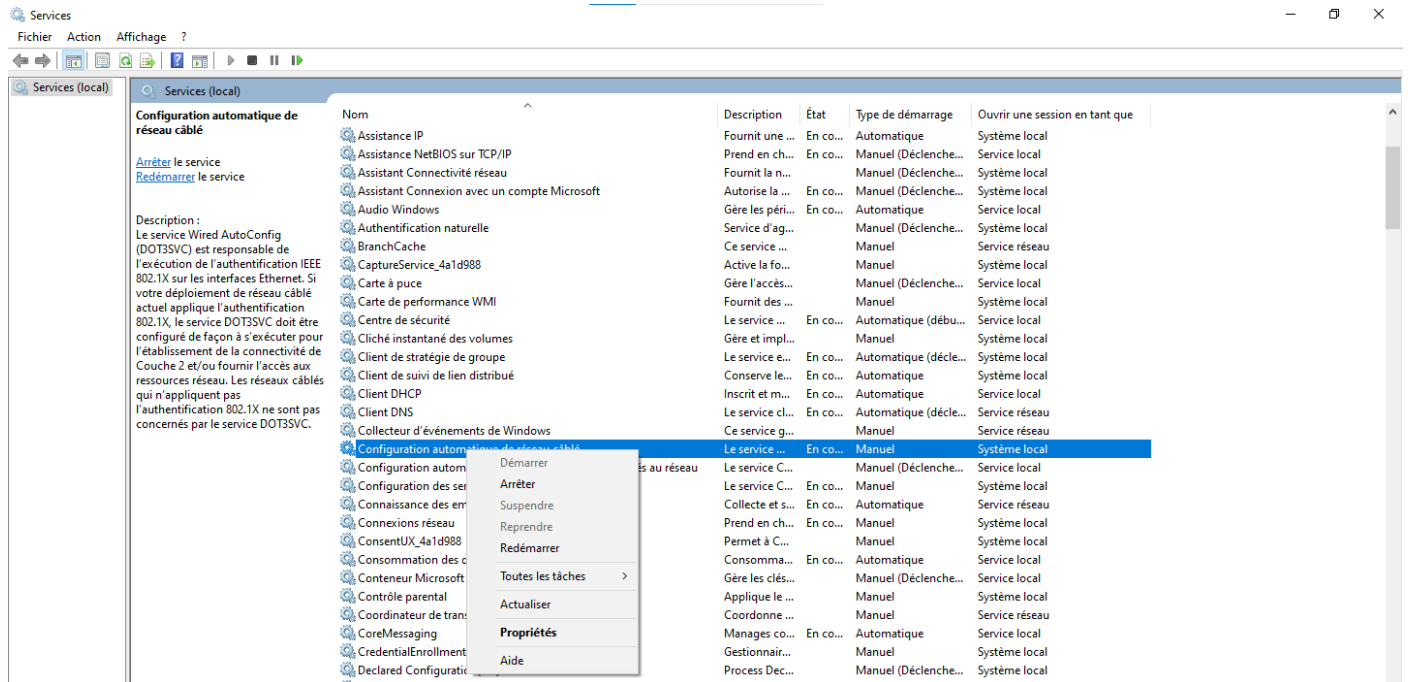
Terminer

Annuler

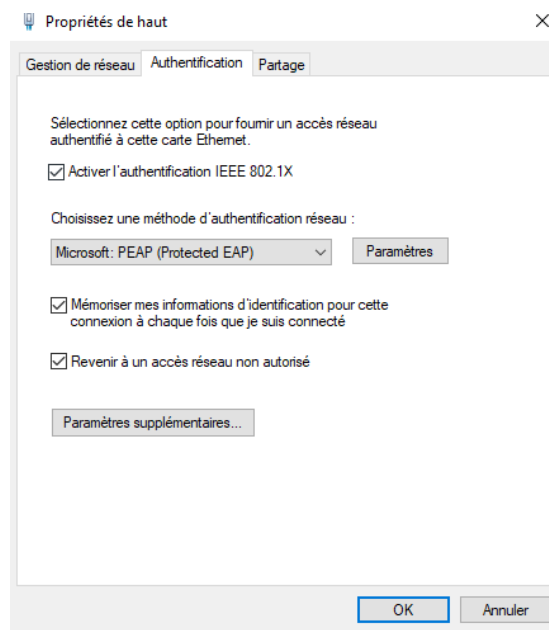
Annexe 3 : Demande de connexion des utilisateurs rveau et cgeley

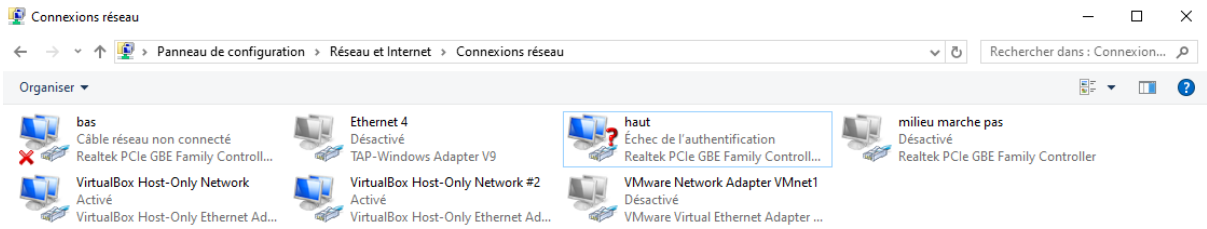
Sur le PC2 qui est un poste hors domaine

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

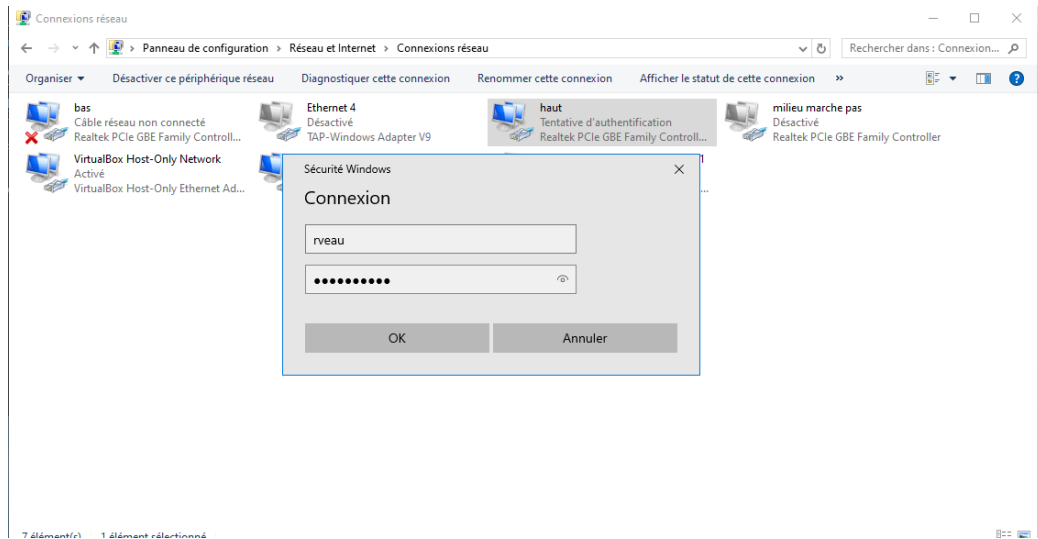


- Et puis dans les propriétés de la carte réseau du PC2 : je coche Activer et désactive l'authentification IEEE 802.1x pour faire apparaître le menu d'authentification :





➤ 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 :

```
C:\> Invite de commandes

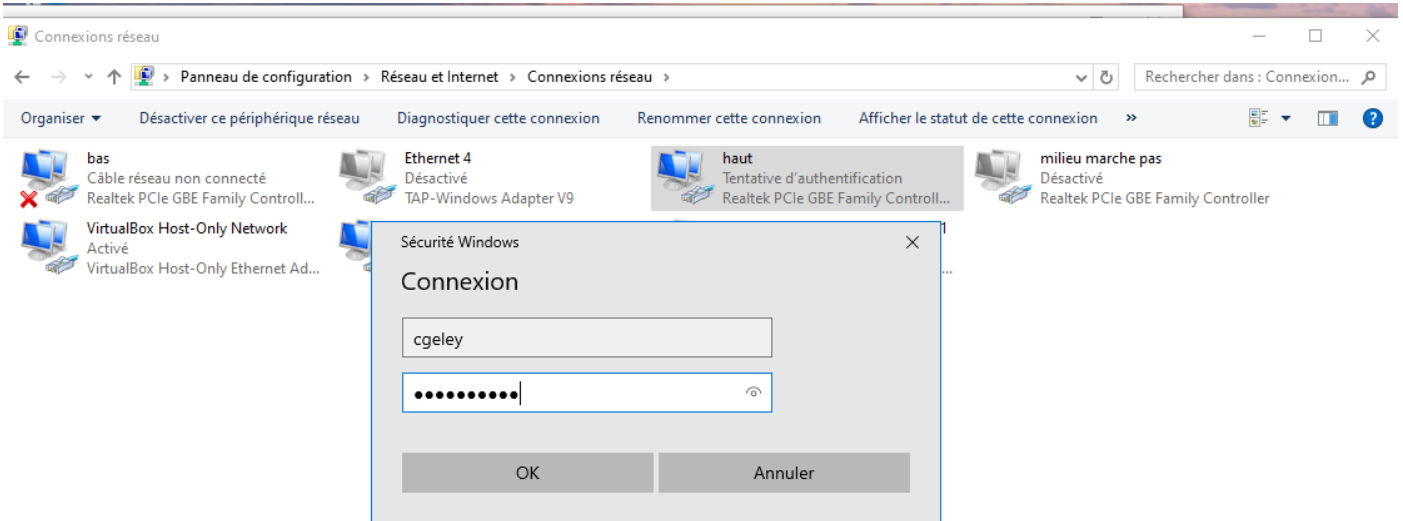
Adresse d'autoconfiguration IPv4 . . . : 169.254.254.215(préféré)
Masque de sous-réseau . . . . . : 255.255.0.0
Passerelle par défaut . . . . . :
IAID DHCPv6 . . . . . : 872546380
DUID de client DHCPv6 . . . . . : 00-01-00-01-23-49-30-2B-50-3E-AA-03-A2-0B
Serveurs DNS . . . . . : fec0:0:0:ffff::1%1
                          fec0:0:0:ffff::2%1
                          fec0:0:0:ffff::3%1
NetBIOS sur Tcpip . . . . . : Activé

Carte Ethernet haut :

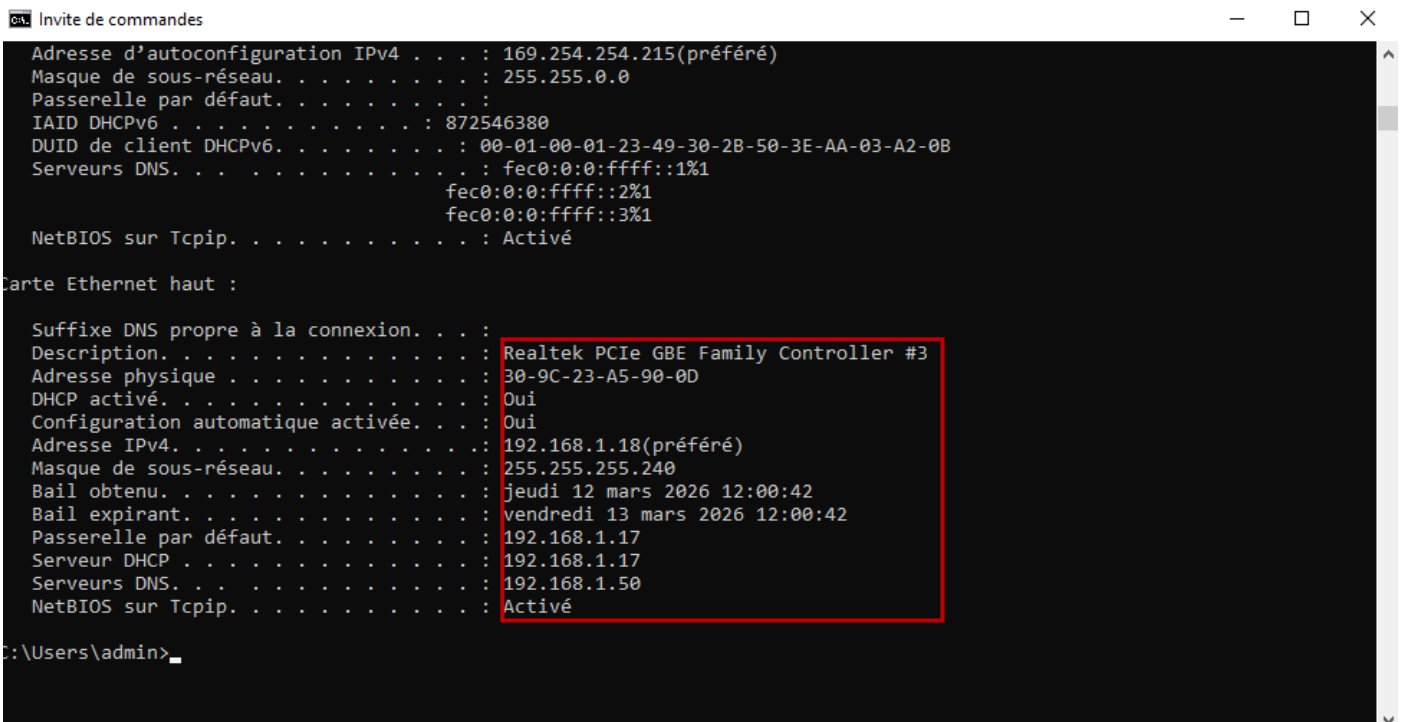
Suffixe DNS propre à la connexion . . . :
Description . . . . . : Realtek PCIe GBE Family Controller #3
Adresse physique . . . . . : 30-9C-23-A5-90-0D
DHCP activé . . . . . : Oui
Configuration automatique activée . . . : Oui
Adresse IPv4 . . . . . : 192.168.1.2(préféré)
Masque de sous-réseau . . . . . : 255.255.255.240
Bail obtenu . . . . . : jeudi 12 mars 2026 11:59:16
Bail expirant . . . . . : vendredi 13 mars 2026 11:59:15
Passerelle par défaut . . . . . : 192.168.1.1
Serveur DHCP . . . . . : 192.168.1.1
Serveurs DNS . . . . . : 192.168.1.50
NetBIOS sur Tcpip . . . . . : Activé

C:\Users\admin>
```

➤ 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 AuditSessionID
*Mar 3 00:06:28.679: %AUTHMGR-7-RESULT: Authentication result 'timeout' from 'dot1x' for client (309c.23a5.900d) on
Interface Fa0/8 AuditSessionID COA80002000000110A4CFFFB
*Mar 3 00:07:26.409: %AUTHMGR-5-START: Starting 'dot1x' for client (309c.23a5.900d) on Interface Fa0/8 AuditSessionID
COA80002000000120A52A715
*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 COA80002000000120A52A715
*Mar 3 00:07:36.702: %AUTHMGR-5-VLANASSIGN: VLAN 2 assigned to Interface Fa0/8 AuditSessionID COA80002000000120A52A7
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 COA80002000000120A52A715
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>

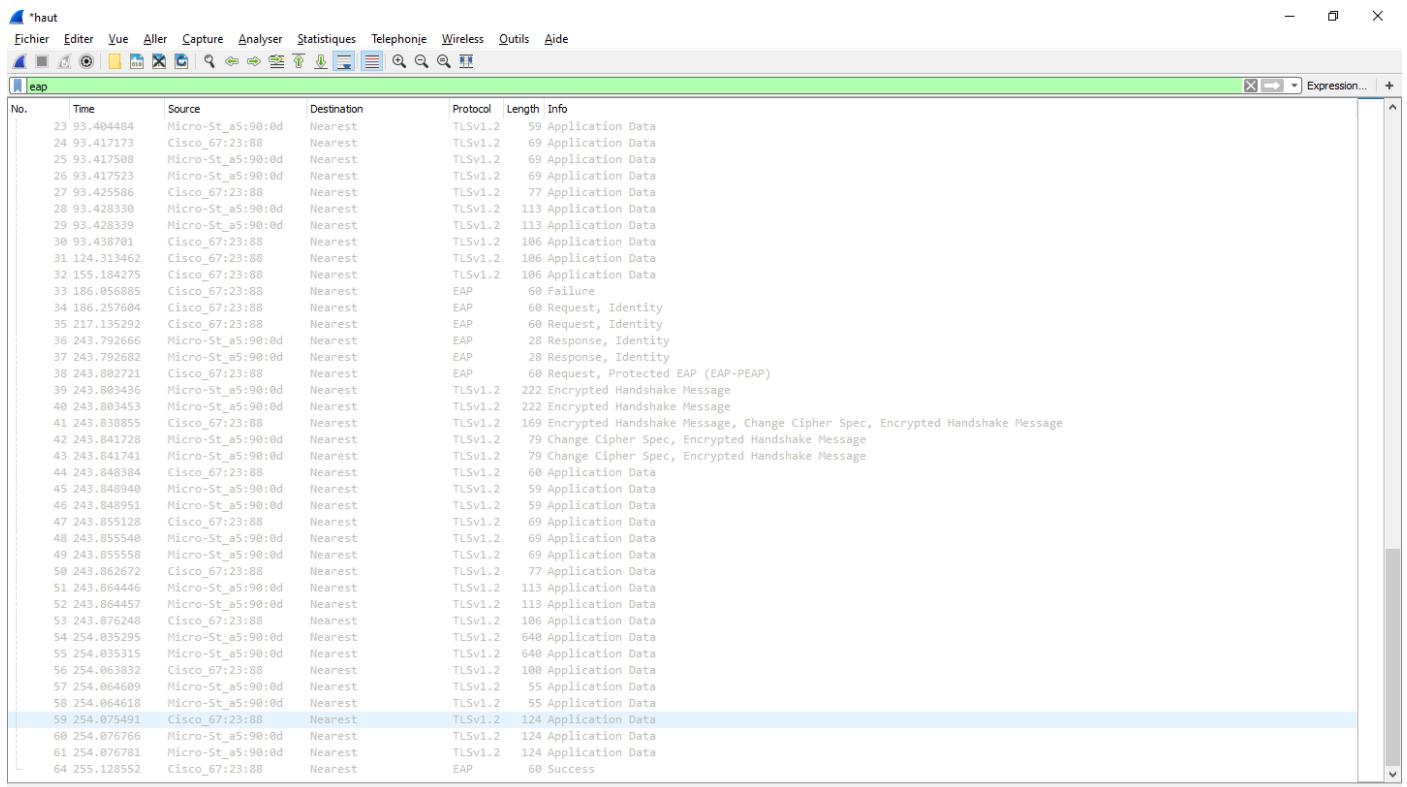
</EventData>

</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 :



No.	Time	Source	Destination	Protocol	Length	Info
23	93.404484	Micro-St_a5:90:0d	Nearest	TLSPv1.2	59	Application Data
24	93.417173	Cisco_67:23:88	Nearest	TLSPv1.2	69	Application Data
25	93.417508	Micro-St_a5:90:0d	Nearest	TLSPv1.2	69	Application Data
26	93.417523	Micro-St_a5:90:0d	Nearest	TLSPv1.2	69	Application Data
27	93.425586	Cisco_67:23:88	Nearest	TLSPv1.2	77	Application Data
28	93.428330	Micro-St_a5:90:0d	Nearest	TLSPv1.2	113	Application Data
29	93.428339	Micro-St_a5:90:0d	Nearest	TLSPv1.2	113	Application Data
30	93.438701	Cisco_67:23:88	Nearest	TLSPv1.2	106	Application Data
31	124.313462	Cisco_67:23:88	Nearest	TLSPv1.2	106	Application Data
32	155.184275	Cisco_67:23:88	Nearest	TLSPv1.2	106	Application Data
33	186.056885	Cisco_67:23:88	Nearest	EAP	60	Failure
34	186.257604	Cisco_67:23:88	Nearest	EAP	60	Request, Identity
35	217.135292	Cisco_67:23:88	Nearest	EAP	60	Request, Identity
36	243.792666	Micro-St_a5:90:0d	Nearest	EAP	28	Response, Identity
37	243.792682	Micro-St_a5:90:0d	Nearest	EAP	28	Response, Identity
38	243.802721	Cisco_67:23:88	Nearest	EAP	60	Request, Protected EAP (EAP-PEAP)
39	243.803436	Micro-St_a5:90:0d	Nearest	TLSPv1.2	222	Encrypted Handshake Message
40	243.803453	Micro-St_a5:90:0d	Nearest	TLSPv1.2	222	Encrypted Handshake Message
41	243.838855	Cisco_67:23:88	Nearest	TLSPv1.2	169	Encrypted Handshake Message, Change Cipher Spec, Encrypted Handshake Message
42	243.841728	Micro-St_a5:90:0d	Nearest	TLSPv1.2	79	Change Cipher Spec, Encrypted Handshake Message
43	243.841741	Micro-St_a5:90:0d	Nearest	TLSPv1.2	79	Change Cipher Spec, Encrypted Handshake Message
44	243.848384	Cisco_67:23:88	Nearest	TLSPv1.2	60	Application Data
45	243.848940	Micro-St_a5:90:0d	Nearest	TLSPv1.2	59	Application Data
46	243.848951	Micro-St_a5:90:0d	Nearest	TLSPv1.2	59	Application Data
47	243.855128	Cisco_67:23:88	Nearest	TLSPv1.2	69	Application Data
48	243.855540	Micro-St_a5:90:0d	Nearest	TLSPv1.2	69	Application Data
49	243.855558	Micro-St_a5:90:0d	Nearest	TLSPv1.2	69	Application Data
50	243.862672	Cisco_67:23:88	Nearest	TLSPv1.2	77	Application Data
51	243.864446	Micro-St_a5:90:0d	Nearest	TLSPv1.2	113	Application Data
52	243.864457	Micro-St_a5:90:0d	Nearest	TLSPv1.2	113	Application Data
53	243.876248	Cisco_67:23:88	Nearest	TLSPv1.2	106	Application Data
54	254.035295	Micro-St_a5:90:0d	Nearest	TLSPv1.2	640	Application Data
55	254.035315	Micro-St_a5:90:0d	Nearest	TLSPv1.2	640	Application Data
56	254.063832	Cisco_67:23:88	Nearest	TLSPv1.2	100	Application Data
57	254.064609	Micro-St_a5:90:0d	Nearest	TLSPv1.2	55	Application Data
58	254.064618	Micro-St_a5:90:0d	Nearest	TLSPv1.2	55	Application Data
59	254.075491	Cisco_67:23:88	Nearest	TLSPv1.2	124	Application Data
60	254.076766	Micro-St_a5:90:0d	Nearest	TLSPv1.2	124	Application Data
61	254.076781	Micro-St_a5:90:0d	Nearest	TLSPv1.2	124	Application Data
64	255.128552	Cisco_67:23:88	Nearest	EAP	60	Success

➤ Sur le serveur Radius :

No.	Time	Source	Destination	Protocol	Length	Info
114	33.636621	192.168.0.2	192.168.1.50	RADIUS	186	Access-Request id=80
115	33.715589	192.168.1.50	192.168.0.2	RADIUS	132	Access-Challenge id=80
116	33.725623	192.168.0.2	192.168.1.50	RADIUS	418	Access-Request id=81
118	33.734913	192.168.1.50	192.168.0.2	RADIUS	152	Access-Challenge id=81
119	33.743449	192.168.0.2	192.168.1.50	RADIUS	220	Access-Request id=82
120	33.743721	192.168.1.50	192.168.0.2	RADIUS	772	Access-Challenge id=82
121	33.754958	192.168.0.2	192.168.1.50	RADIUS	389	Access-Request id=83
122	33.756520	192.168.1.50	192.168.0.2	RADIUS	187	Access-Challenge id=83
123	33.769054	192.168.0.2	192.168.1.50	RADIUS	220	Access-Request id=84
124	33.769381	192.168.1.50	192.168.0.2	RADIUS	162	Access-Challenge id=84
125	33.775762	192.168.0.2	192.168.1.50	RADIUS	255	Access-Request id=85
126	33.776016	192.168.1.50	192.168.0.2	RADIUS	177	Access-Challenge id=85
127	33.783720	192.168.0.2	192.168.1.50	RADIUS	265	Access-Request id=86
128	33.784482	192.168.1.50	192.168.0.2	RADIUS	185	Access-Challenge id=86
129	33.793893	192.168.0.2	192.168.1.50	RADIUS	309	Access-Request id=87
130	33.796776	192.168.1.50	192.168.0.2	RADIUS	208	Access-Challenge id=87
131	33.808860	192.168.0.2	192.168.1.50	RADIUS	251	Access-Request id=88
132	33.809246	192.168.1.50	192.168.0.2	RADIUS	232	Access-Challenge id=88
133	33.817111	192.168.0.2	192.168.1.50	RADIUS	320	Access-Request id=89
134	33.819446	192.168.1.50	192.168.0.2	RADIUS	346	Access-Accept id=89

Frame 114: 186 bytes on wire (1488 bits), 186 bytes captured (1488 bits) on interface 0
 Ethernet II, Src: Cisco_ee:f6:a8 (e0:2f:6d:ee:f6:a8), Dst: PCSSys_08:00:27:74:eb:de (08:00:27:74:eb:de)
 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

RADIUS Protocol

- Code: Access-Accept (1)
- Packet Identifier: 0x50 (80)
- Length: 144
- Authenticator: 2ae6739e4134d10b6f22f58ac27ae49b4
- [The response to this request is in frame 113]
- Attribute Value Pairs
 - AVP: t=User-Name(1) i=7 val=rveau
 - AVP: t=Service-Type(6) i=6 val=Framed(2)
 - AVP: t=Framed-MTU(12) i=6 val=1500
 - AVP: t=Called-Station-ID(30) i=19 val=24-01-C7-67-23-88
 - AVP: t=Calling-Station-ID(31) i=19 val=24-01-C7-67-23-88
 - AVP: t=NAS-IP-Address(79) i=12 last segment=11
 - Type: 79
 - Length: 12
 - IP-Address: 192.168.0.172
 - Extensible Authentication Protocol
 - Code: Response (2)
 - Length: 72
 - Type: Identity (1)
 - Identity: rveau