

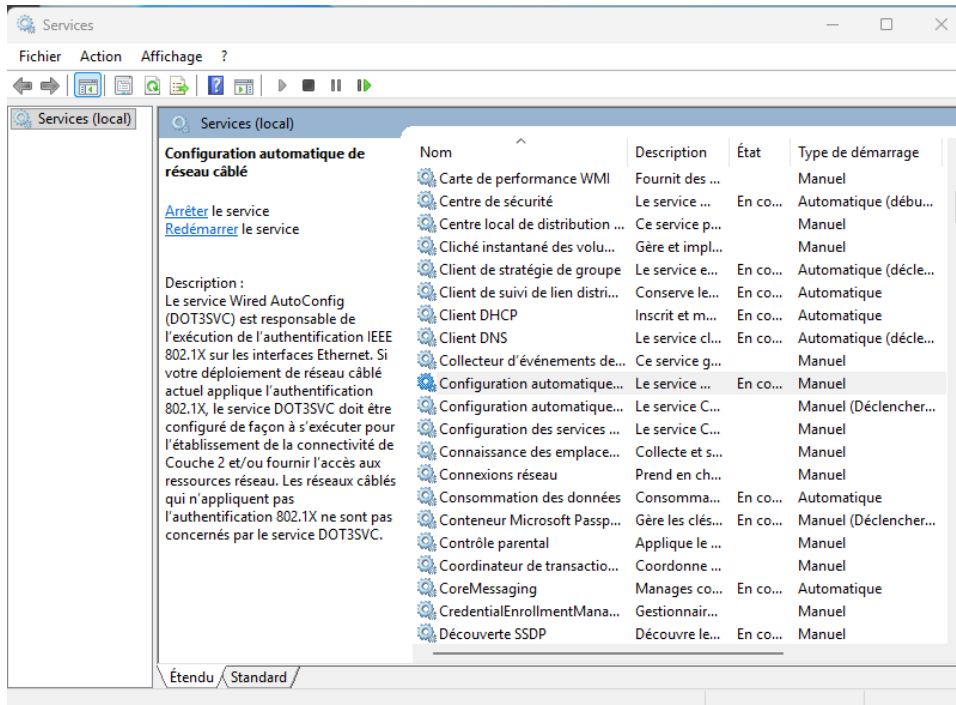
TP1 : Radius

Sommaire

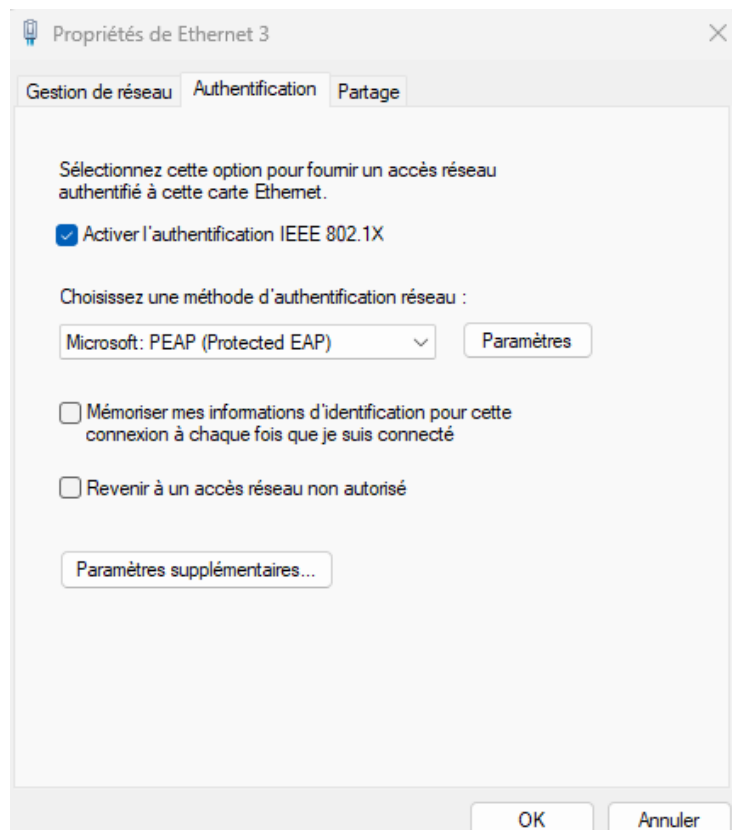
1 – Préparation client	2
2 – Annexe 1 : Commutateur et Routeur	4
3 – Annexe 2 : Mise en place du serveur RADIUS (service NPS)	7
3.2 - Ajout du rôle Services de certificats Active Directory	8
3-3 - Installation du service NPS :	15
3.4 - Configuration du serveur RADIUS NPS :	19
4 - Annexe 3 : Demande de connexion des utilisateurs rveau et cgeley :	42
5 - Annexe 4 : Capture de trames : messages RADIUS :	45

1 – Préparation client

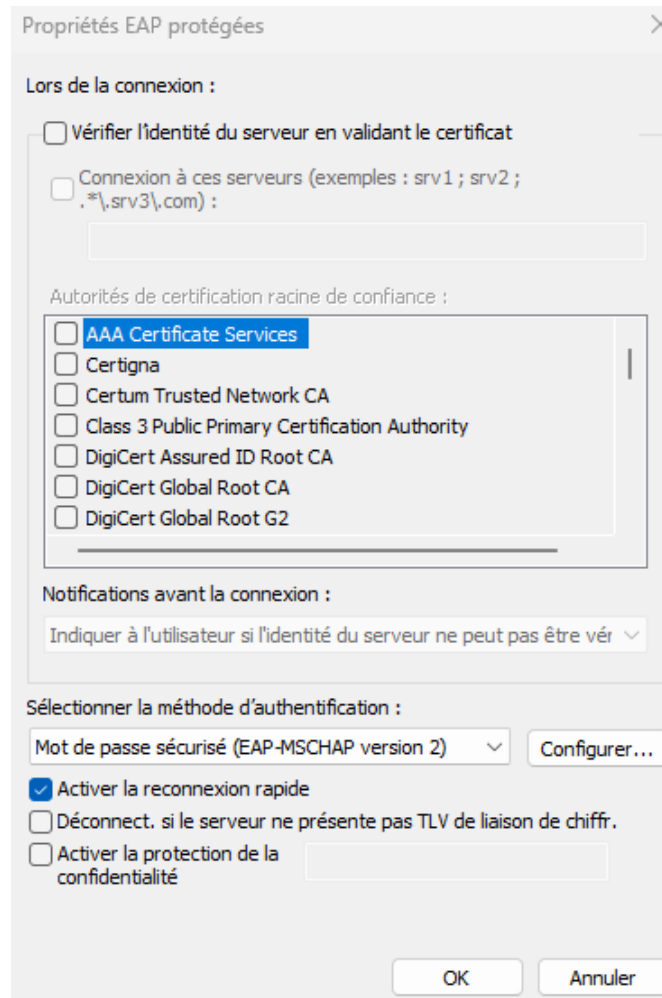
- Dans Windows, pour activer cette couche logicielle, il faut lancer le service Configuration automatique de réseau câblé :



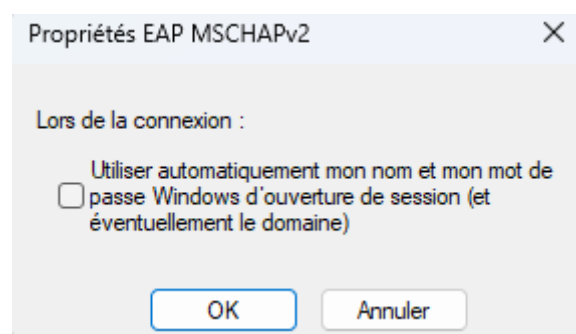
- La mise en route du service provoque l'apparition de l'onglet Authentification dans les propriétés de la carte réseau.



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



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



2 – Annexe 1 : Commutateur et Routeur

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

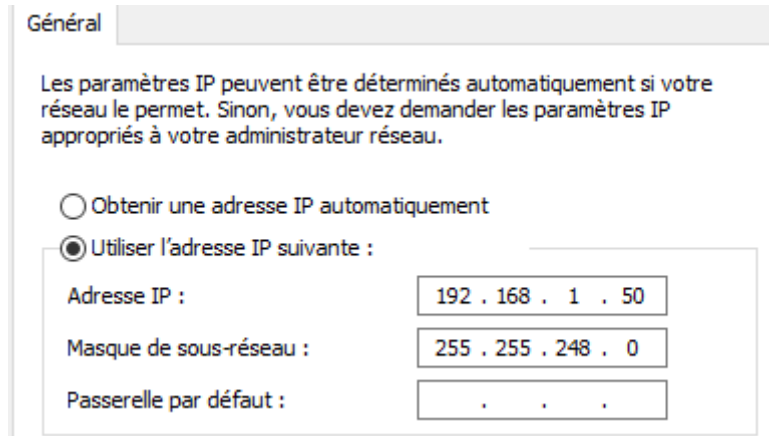
```
Current configuration : 3416 bytes
!
! Last configuration change at 21:49:34 UTC Tue Mar 2 1993
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Switch
!
boot-start-marker
boot-end-marker
!
!
aaa new-model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


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

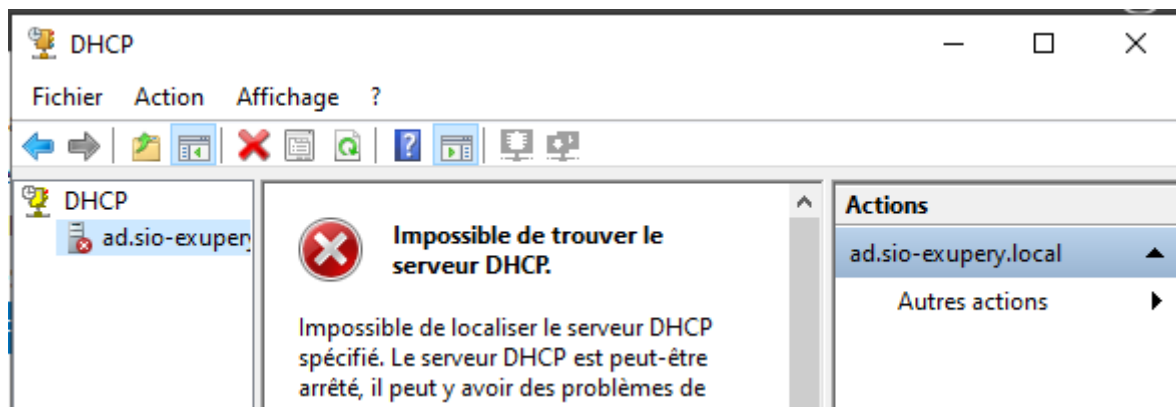
```
ip dhcp excluded-address 192.168.1.1
ip dhcp excluded-address 192.168.1.17
!
ip dhcp pool vlan2
 network 192.168.1.0 255.255.255.240
!
ip dhcp pool vlan3
 network 192.168.1.16 255.255.255.240
 default-router 192.168.1.17
 dns-server 192.168.1.50
!
ip dhcp pool vlan 2
 default-router 192.168.1.1
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

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

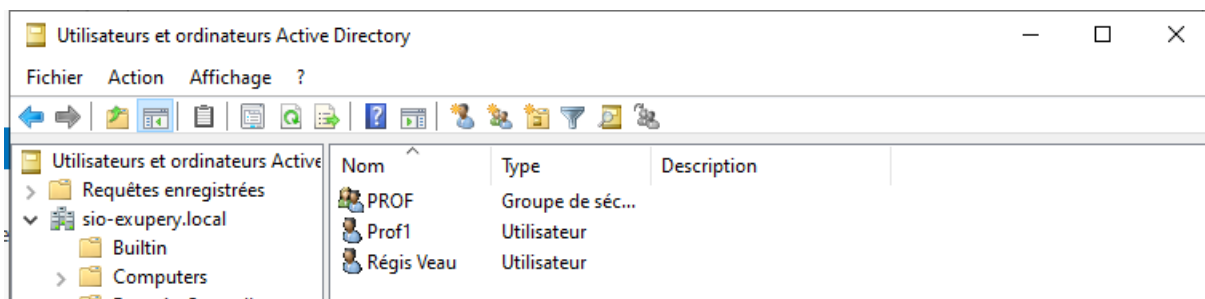
- J'applique une configuration IP au serveur AD :



- Je désactive le serveur DHCP :

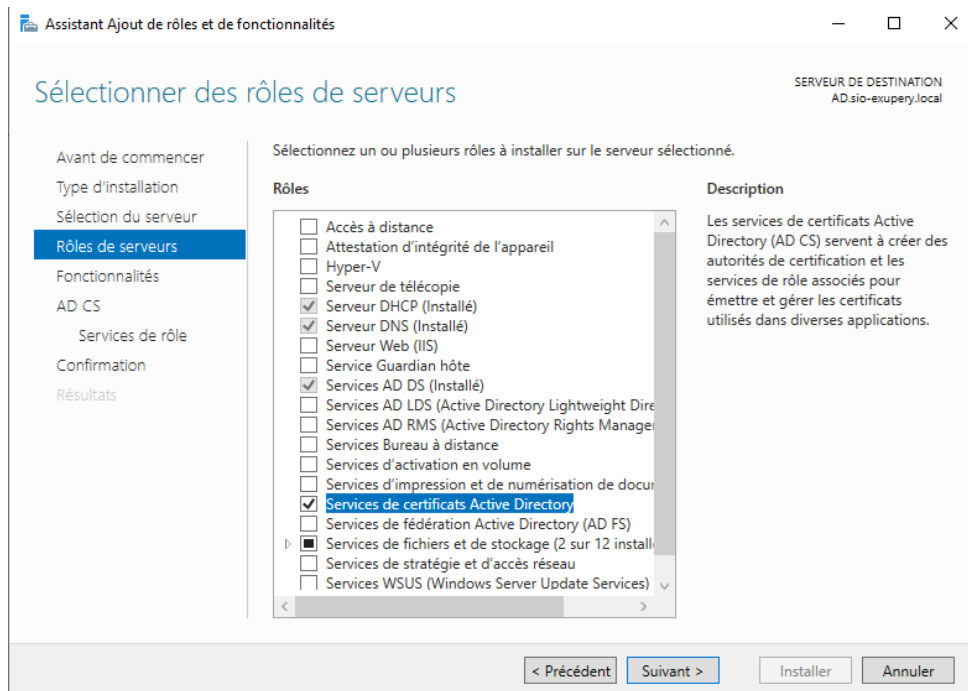


- Je crée deux UO :

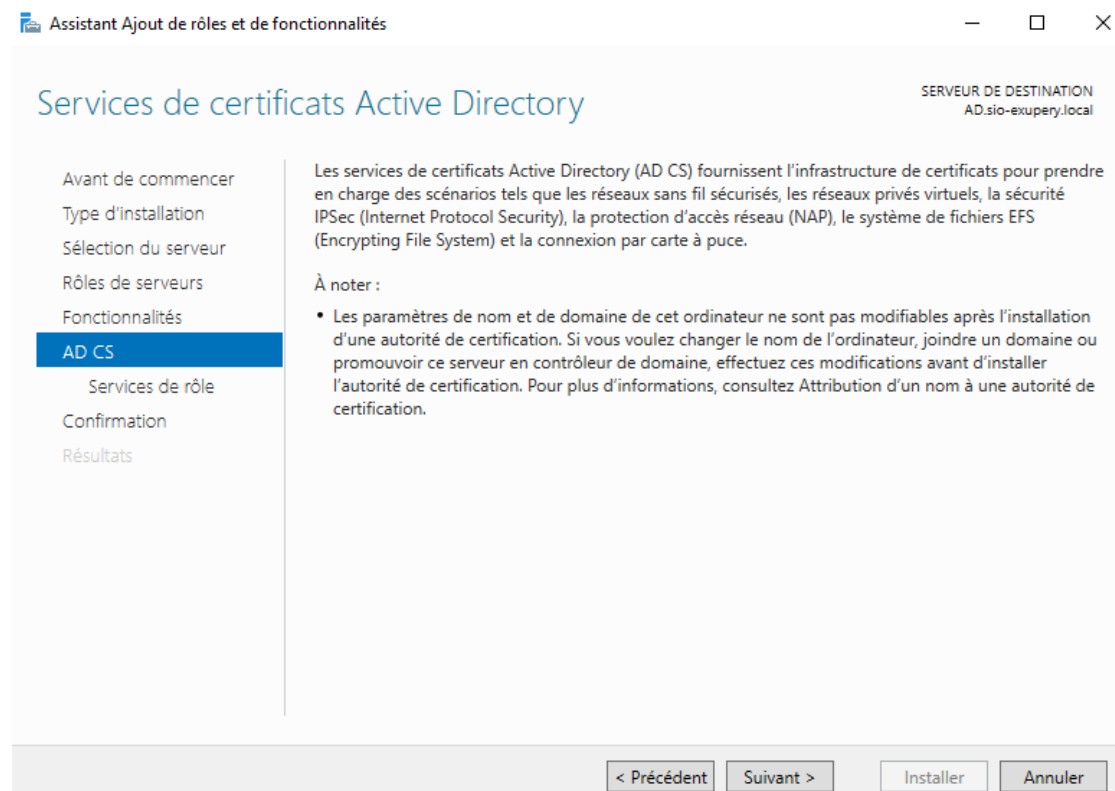


3.2- Ajout du rôle Services de certificats Active Directory

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



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



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

The screenshot shows the 'Assistant Ajout de rôles et de fonctionnalités' window. The title bar reads 'Assistant Ajout de rôles et de fonctionnalités'. The main heading is 'Confirmer les sélections d'installation'. In the top right corner, it says 'SERVEUR DE DESTINATION AD.sio-exupery.local'. On the left, a navigation pane lists steps: 'Avant de commencer', 'Type d'installation', 'Sélection du serveur', 'Rôles de serveurs', 'Fonctionnalités', 'AD CS', 'Services de rôle', 'Confirmation' (highlighted), and 'Résultats'. The main content area contains the text: 'Pour installer les rôles, services de rôle ou fonctionnalités suivants sur le serveur sélectionné, cliquez sur Installer.' Below this, a checkbox labeled 'Redémarrer automatiquement le serveur de destination, si nécessaire' is checked and highlighted with a red box. A note follows: '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.' A list of roles and features is shown: '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', and 'Autorité de certification'. At the bottom, there are links for 'Exporter les paramètres de configuration' and 'Spécifier un autre chemin d'accès source'. At the very bottom, there are buttons for '< Précédent', 'Suivant >', 'Installer', and 'Annuler'.

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

The screenshot shows the 'Assistant Ajout de rôles et de fonctionnalités' window at the 'Progression de l'installation' step. The title bar is the same. The main heading is 'Progression de l'installation'. The top right corner still shows 'SERVEUR DE DESTINATION AD.sio-exupery.local'. The left navigation pane is the same, but 'Résultats' is now highlighted. The main content area has the heading 'Afficher la progression de l'installation'. Below it, an information icon (i) is followed by 'Installation de fonctionnalité' and a progress bar. Below the bar, it says 'Configuration requise. Installation réussie sur AD.sio-exupery.local.' A box contains the following text: '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' (highlighted with a red box), and 'Autorité de certification'. Below this box, it lists 'Outils d'administration de serveur distant', 'Outils d'administration de rôles', 'Outils des services de certificats Active Directory', and 'Outils de gestion de l'autorité de certification'. At the bottom, there is a notification icon (1) and a message: '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.' Below this is a link for 'Exporter les paramètres de configuration'.

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

Services de rôle 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

Sélectionner les services de rôle à configurer

- Autorité de certification
- Inscription de l'autorité de certification via le Web
- Répondeur en ligne
- Service d'inscription de périphériques réseau
- Service Web Inscription de certificats
- Service Web Stratégie d'inscription de certificats

[En savoir plus sur les rôles de serveur AD CS](#)

- Je sélectionne Autorité de certification d'entreprise.

Type d'installation 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 d'installation de l'AC

Les autorités de certification d'entreprise peuvent utiliser les services de domaine Active Directory (AD DS) pour simplifier la gestion des certificats. Les autorités de certification autonomes n'utilisent pas AD DS pour émettre ou gérer des certificats.

- Autorité de certification d'entreprise
 Les autorités de certification d'entreprise doivent être membres d'un domaine et sont généralement en ligne pour émettre des certificats ou des stratégies de certificat.
- Autorité de certification autonome
 Les autorités de certification autonomes peuvent être membres d'un groupe de travail ou d'un domaine. Les autorités de certification autonomes ne nécessitent pas AD DS et peuvent être utilisées sans connexion réseau (hors connexion).

[En savoir plus sur le type d'installation](#)

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

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

- Je sélectionne Créer une nouvelle clé privée :

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

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

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](#)

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

Nom 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 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 :

sio-exupery-AD-CA

Suffixe du nom unique :

DC=sio-exupery,DC=local

Aperçu du nom unique :

CN=sio-exupery-AD-CA,DC=sio-exupery,DC=local

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

- Je laisse la période de validité par défaut :

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 :

Date d'expiration de l'AC : 12/03/2031 10:54:00

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](#)

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

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 certi...
Confirmation
Progression
Résultats

Spécifier les emplacements des bases de données

Emplacement de la base de données de certificats :

Emplacement du journal de la base de données de certificats :

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

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

The screenshot shows the 'Confirmation' step of the Active Directory Certificate Services (AD CS) configuration wizard. The title bar indicates the destination server is 'AD.sio-exupery.local'. The left sidebar lists various configuration steps, with 'Confirmation' selected. The main area displays the following configuration details:

- Services de certificats Active Directory**
- Autorité de certification**
- Type d'AC : Racine d'entreprise
- Fournisseur de services de chiffrement : RSA#Microsoft Software Key Storage Provider
- Algorithme de hachage : SHA256
- Longueur de la clé : 2048
- Autoriser l'interaction de l'administrateur : Désactivé
- Période de validité du certificat : 12/03/2031 10:54:00
- Nom unique : CN=sio-exupery-AD-CA,DC=sio-exupery,DC=local
- 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

At the bottom, there are navigation buttons: '< Précédent', 'Suivant >', 'Configurer' (highlighted with a red box), and 'Annuler'.

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


The screenshot shows the 'Résultats' (Results) step of the Active Directory Certificate Services (AD CS) configuration wizard. The title bar indicates the destination server is 'AD.sio-exupery.local'. The left sidebar lists various configuration steps, with 'Résultats' selected. The main area displays the following configuration details:

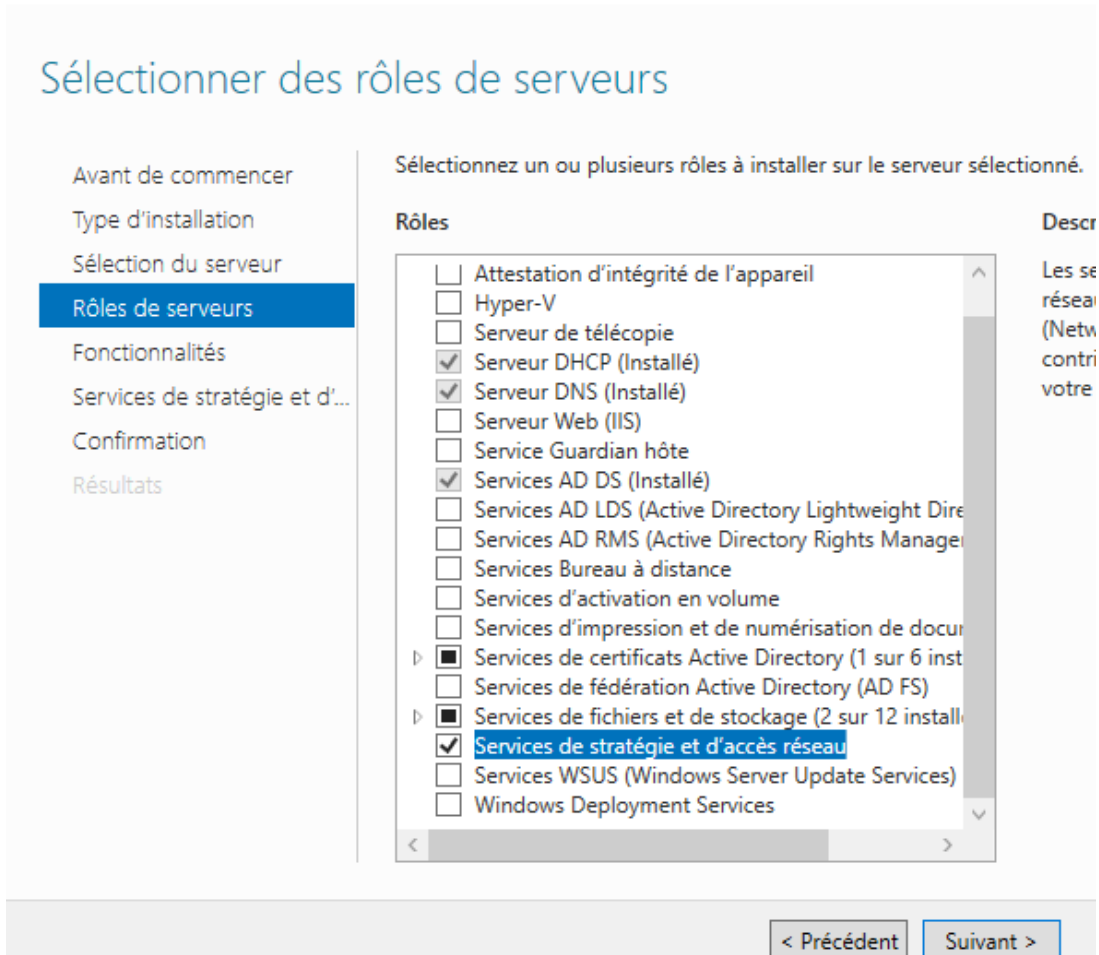
- Services de certificats Active Directory**
- Autorité de certification** ✔ **Configuration réussie**
- [En savoir plus sur la configuration de l'autorité de certification](#)

At the bottom, there are navigation buttons: '< Précédent', 'Suivant >', 'Fermer', and 'Annuler'.

3-3- Installation du service NPS :

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

 Assistant Ajout de rôles et de fonctionnalités



Sélectionner des rôles de serveurs

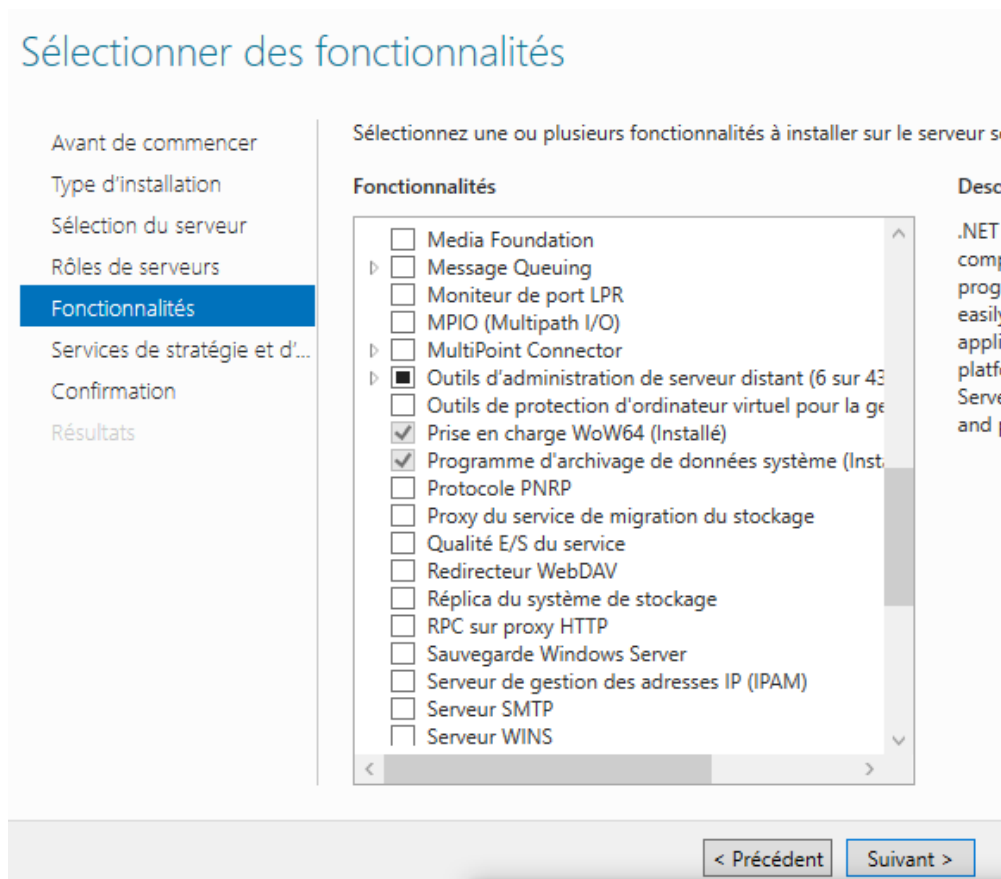
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Services de stratégie et d'...
Confirmation
Résultats

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

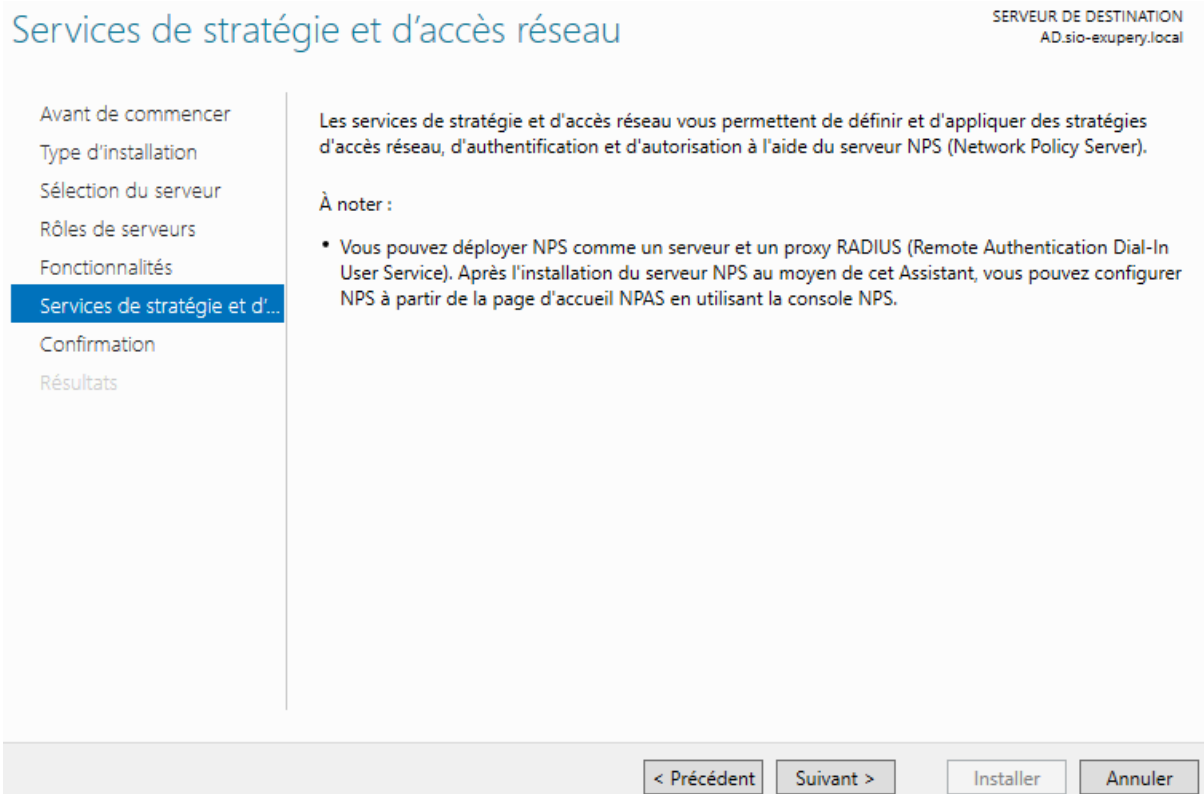
Rôles	Descr
<input type="checkbox"/> Attestation d'intégrité de l'appareil	
<input type="checkbox"/> Hyper-V	
<input type="checkbox"/> Serveur de télécopie	
<input checked="" type="checkbox"/> Serveur DHCP (Installé)	
<input checked="" type="checkbox"/> Serveur DNS (Installé)	
<input type="checkbox"/> Serveur Web (IIS)	
<input type="checkbox"/> Service Guardian hôte	
<input checked="" type="checkbox"/> Services AD DS (Installé)	
<input type="checkbox"/> Services AD LDS (Active Directory Lightweight Dire	
<input type="checkbox"/> Services AD RMS (Active Directory Rights Manage	
<input type="checkbox"/> Services Bureau à distance	
<input type="checkbox"/> Services d'activation en volume	
<input type="checkbox"/> Services d'impression et de numérisation de docu	
▾ <input checked="" type="checkbox"/> Services de certificats Active Directory (1 sur 6 inst	
<input type="checkbox"/> Services de fédération Active Directory (AD FS)	
▾ <input checked="" type="checkbox"/> Services de fichiers et de stockage (2 sur 12 install	
<input checked="" type="checkbox"/> Services de stratégie et d'accès réseau	
<input type="checkbox"/> Services WSUS (Windows Server Update Services)	
<input type="checkbox"/> Windows Deployment Services	

< Précédent Suivant >

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



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



- Je clique sur le bouton Installer :

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
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

- Je clique sur le bouton Fermer :

Progression de l'installation

SERVEUR DE DESTINATION
AD.sio-exupery.local

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

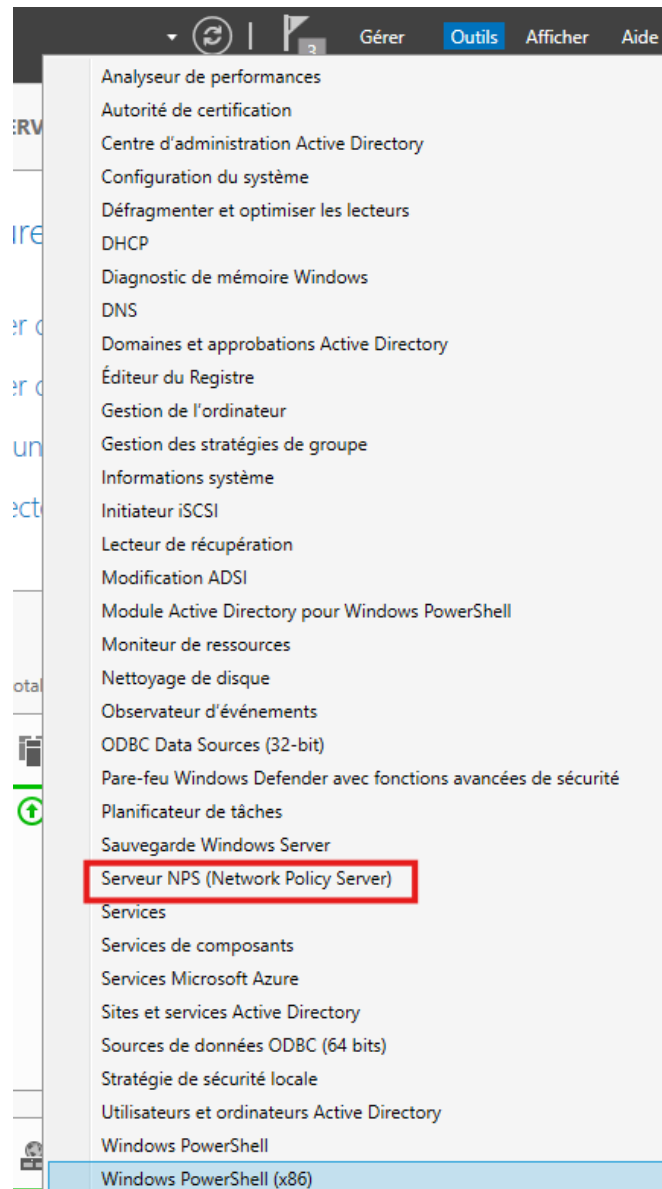
Services de stratégie et d'accès réseau

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.

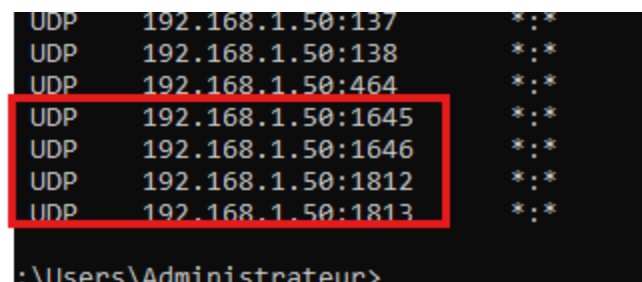
Exporter les paramètres de configuration

< Précédent Suivant > **Fermer** Annuler

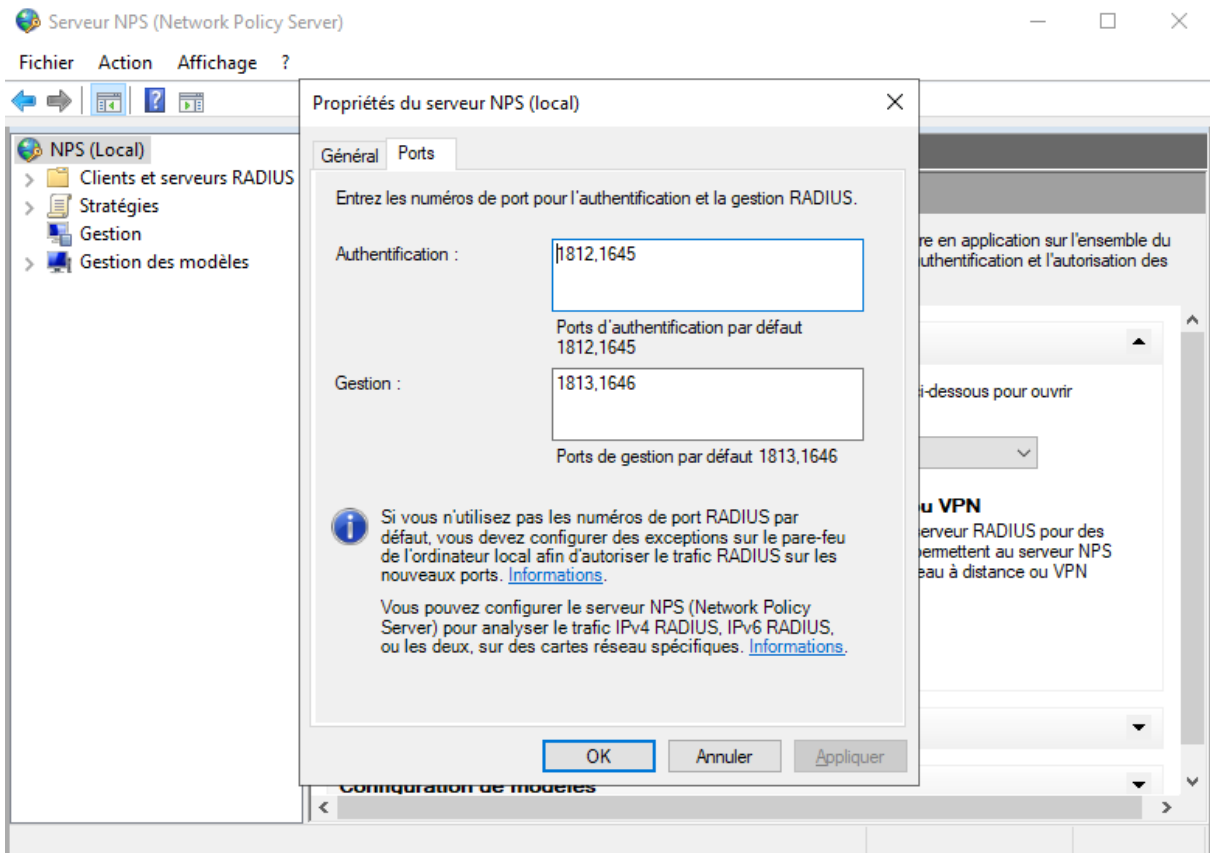
- Je constate la présence de la console Serveur NPS :



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

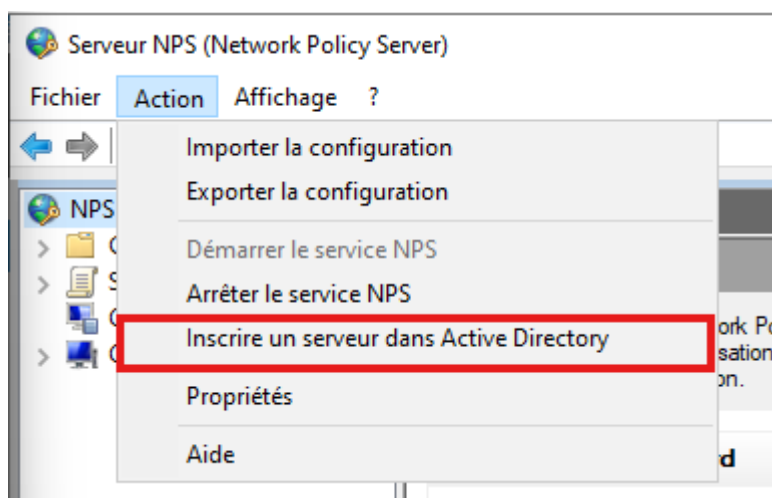


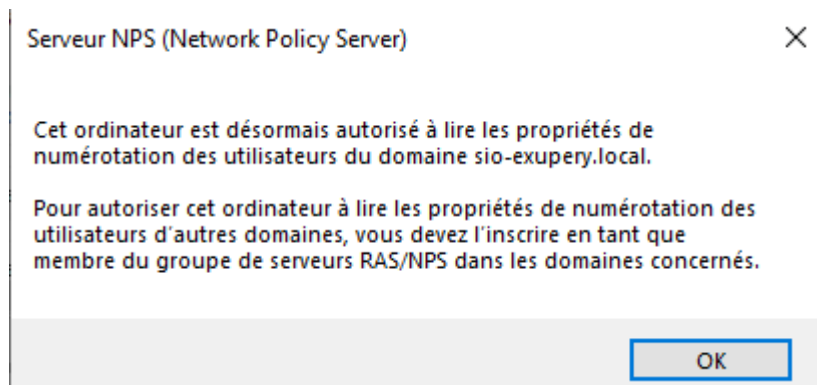
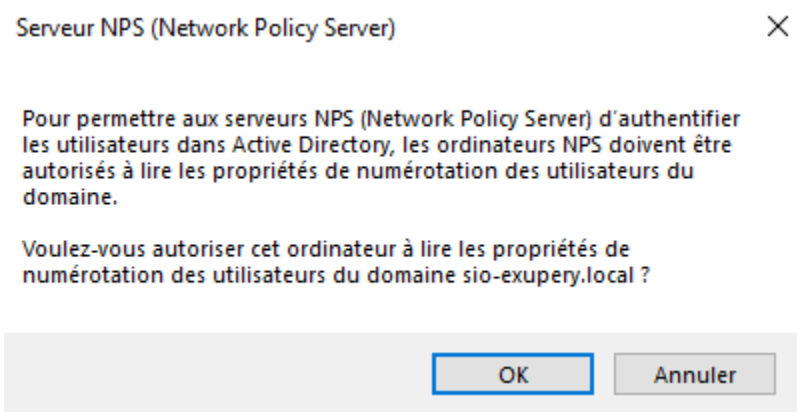
- J'ouvre la console Serveur NPS (Network Policy Server) et je retrouve ces ports dans les propriétés du serveur NPS :



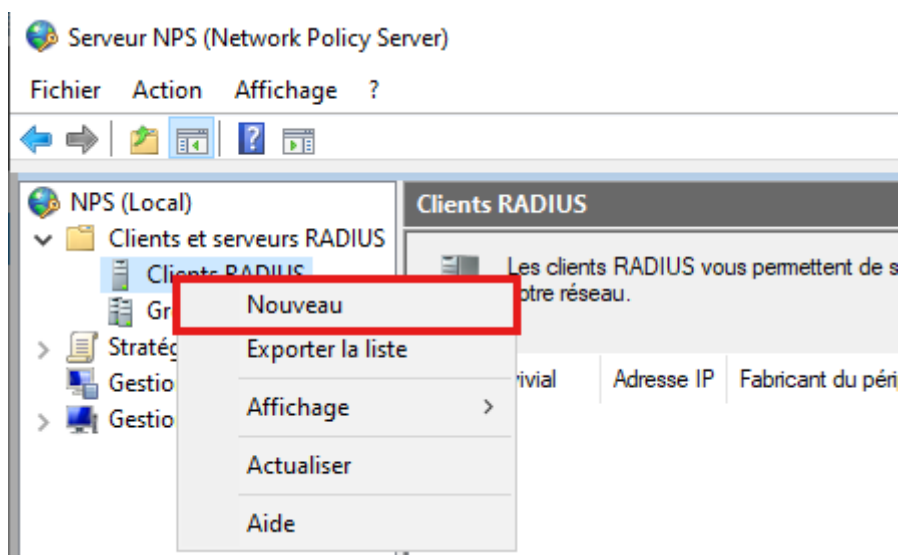
3.4- Configuration du serveur RADIUS NPS :

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





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



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

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 Vérier...

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

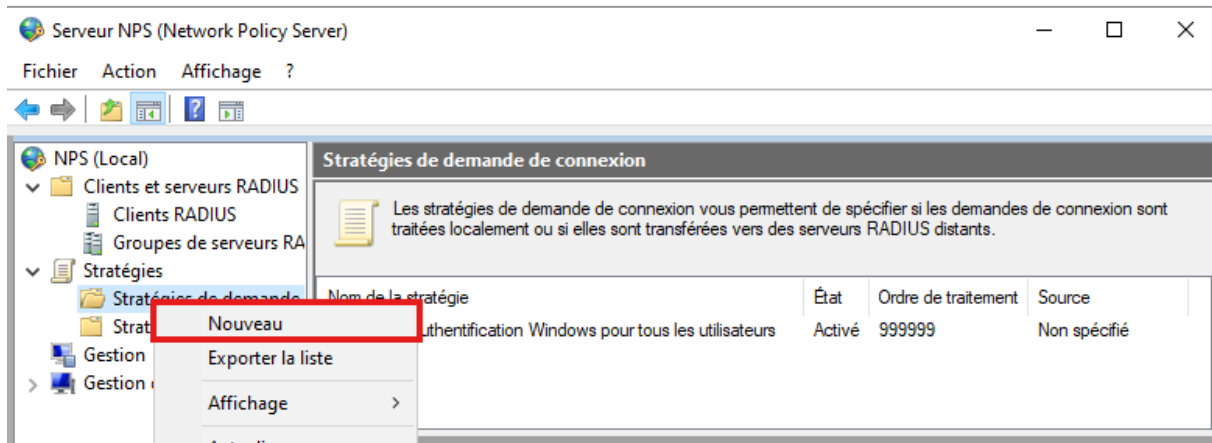
Clients RADIUS

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

Déclaration d'une stratégie de demande de connexion :

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



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

- Je clique sur le bouton 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 puis cliquez sur le bouton Ajouter :

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


OK Annuler

- Je clique sur le bouton Suivant :

 **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

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



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 :

<non configurée>

Nouveau...

Accepter les utilisateurs sans validation des informations d'identification

Précédent

Suivant

Terminer

Annuler

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

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 :

Méthodes d'authentification moins sécurisées :

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

- Je clique de nouveau sur le bouton Suivant :



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 :

Règles :

Rechercher	Remplacer par

- Je clique sur le bouton Terminer dans l'écran récapitulatif de la 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
 - Clients RADIUS
 - Groupes de serveurs RA
- Stratégies
 - Stratégies de demande**
 - Stratégies réseau
- Gestion
- Gestion des modèles

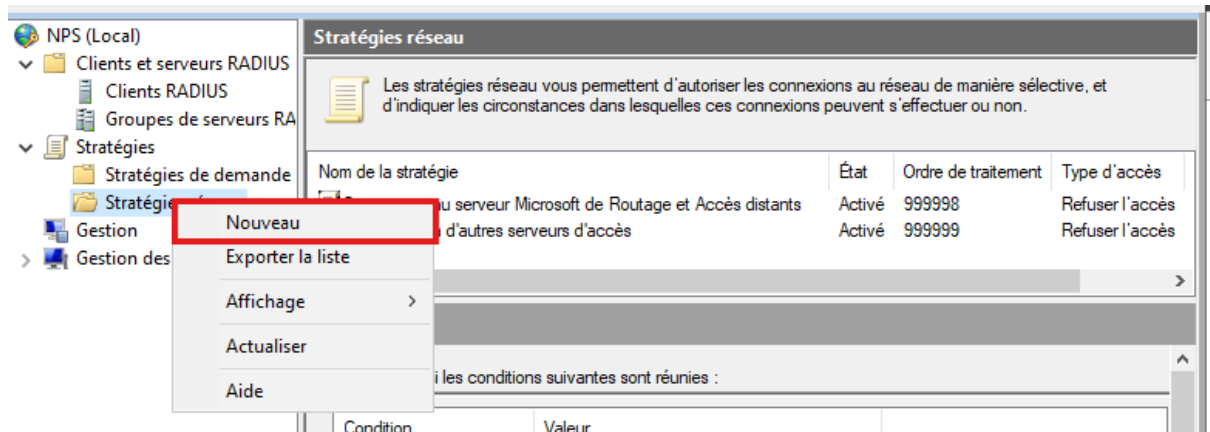
Stratégies de demande de connexion

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

Déclaration d'une stratégie d'accès au réseau :

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



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 clients câblés 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

- 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 :

Ajouter...

Modifier...

Supprimer

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

Groupes

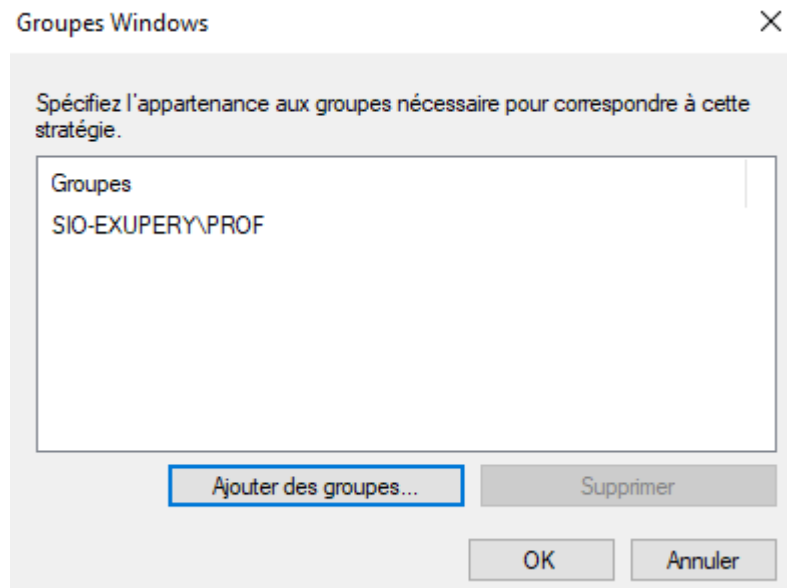
- Groupes Windows**
La condition Groupes Windows spécifie que l'utilisateur ou l'ordinateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.
- Groupes d'ordinateurs**
La condition Groupes d'ordinateurs spécifie que l'ordinateur qui tente d'établir la connexion doit appartenir 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](#)

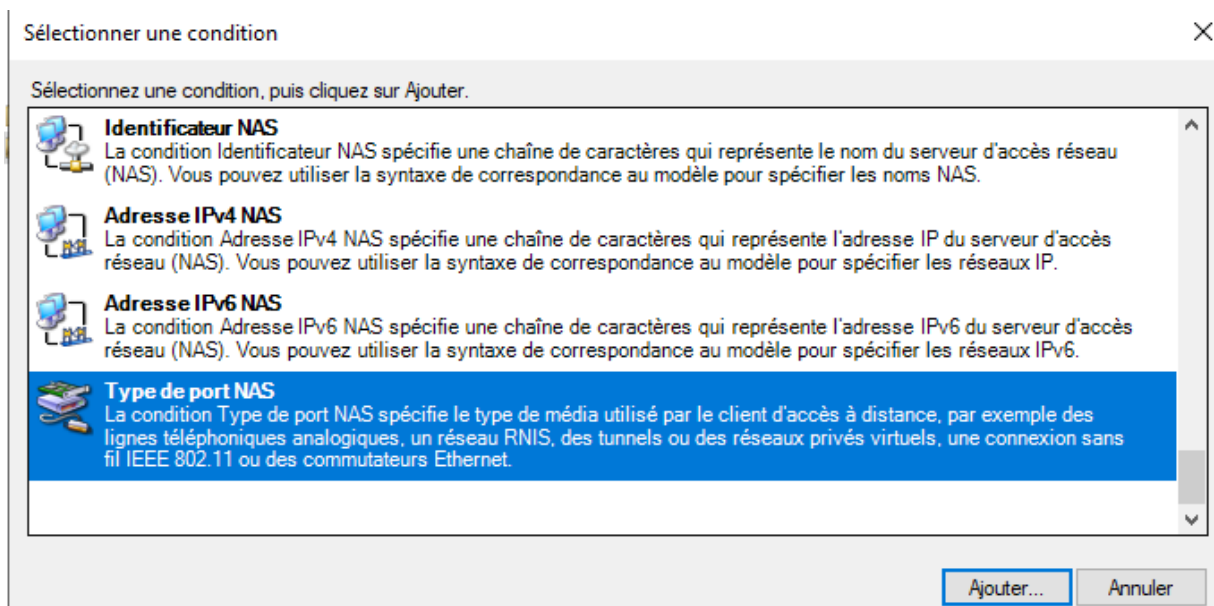
- Restrictions relatives aux jours et aux heures**
Les restrictions relatives aux jours et aux heures indiquent les jours et les heures auxquels les tentatives de connexion sont autorisées ou non. Ces restrictions sont basées sur le fuseau horaire du serveur NPS (Network Policy Server).

Ajouter... Annuler

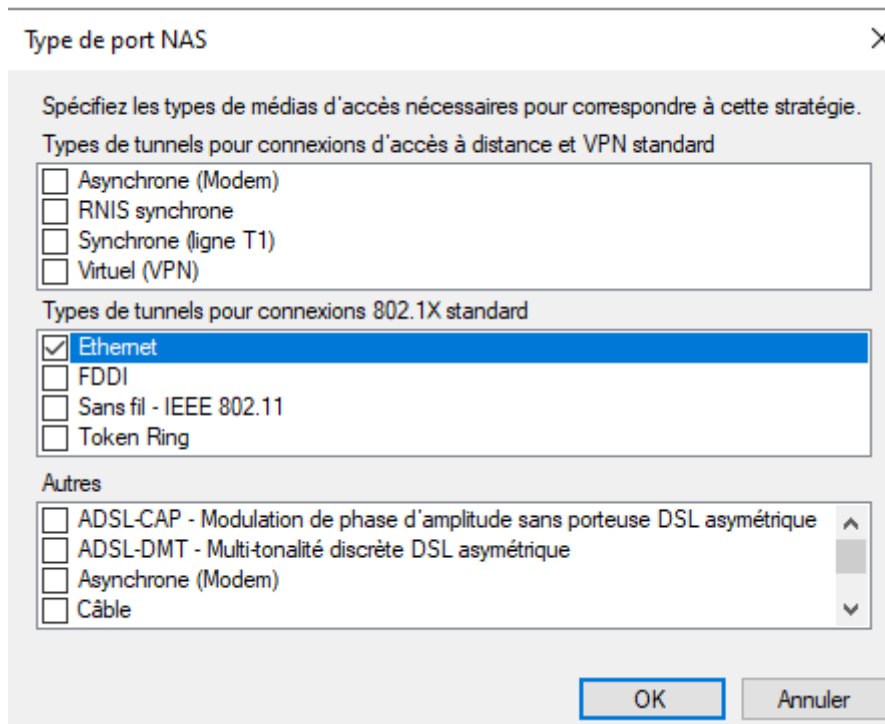
- J'ajoute le groupe Prof :



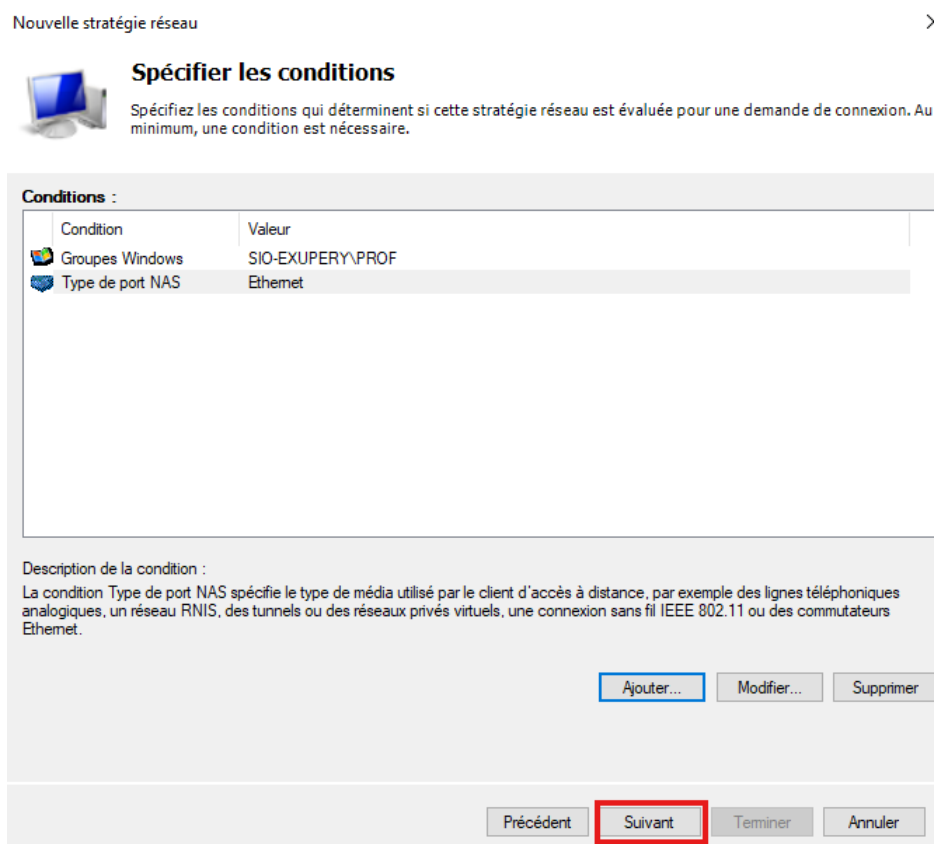
- J'ajoute une deuxième condition pour spécifier le type de port NAS :



- Je coche Ethernet :




- Je clique sur Suivant :



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

Nouvelle stratégie réseau X

 **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)

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)

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

Nouvelle stratégie réseau X








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

- Dans l'écran Configurer les paramètres, je clique sur Ajouter pour 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

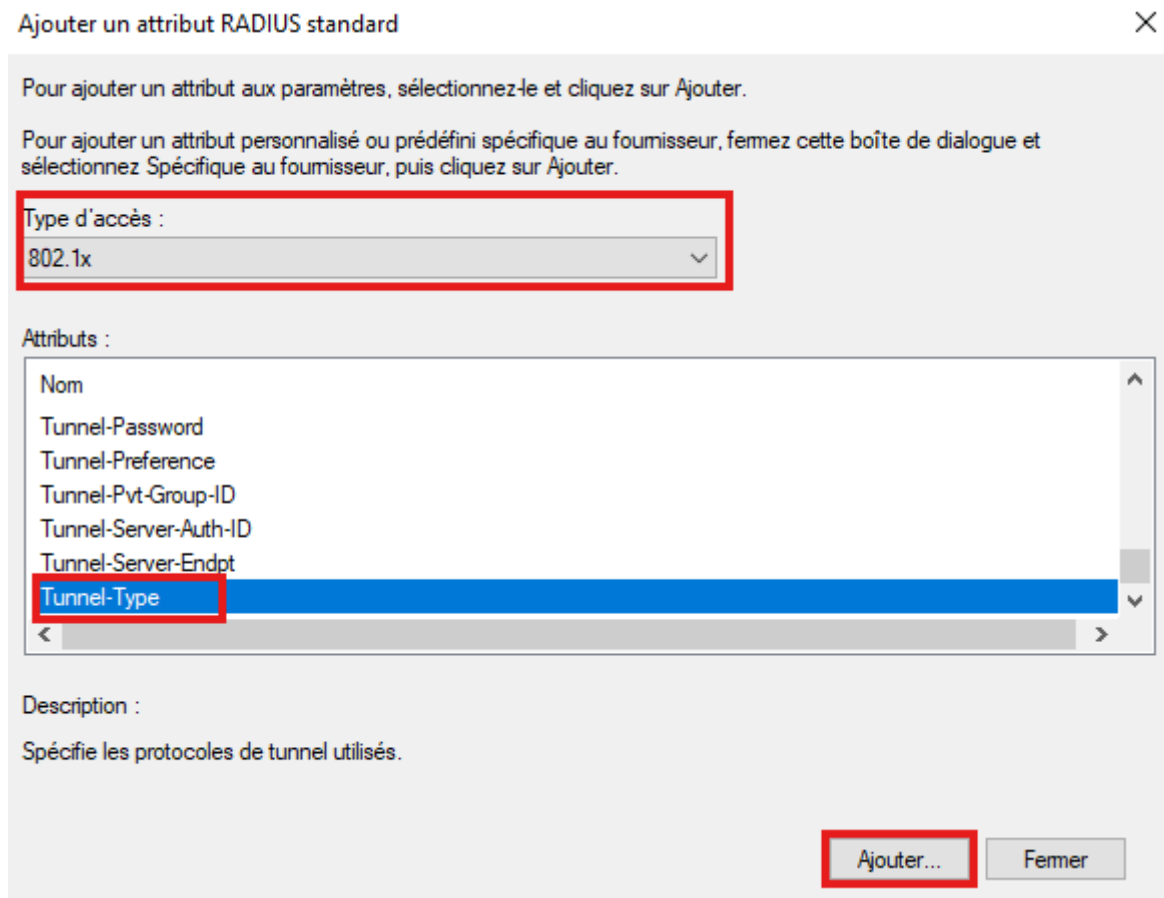
-  Liaisons multiples et protocole BAP (Bandwidth Allocation Protocol)
-  Filtres IP
-  Chiffrement
-  Paramètres IP

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.

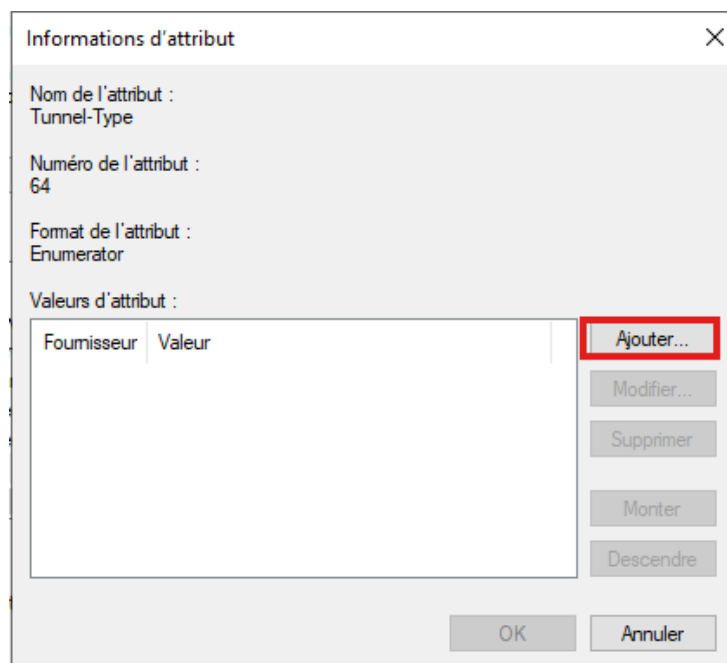
Attributs :

Nom	Valeur
Framed-Protocol	PPP
Service-Type	Framed

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



- Je clique sur Ajouter :



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

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 procède 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
- Termination-Action
- Tunnel-Assignment-ID
- Tunnel-Client-Auth-ID
- Tunnel-Client-Endpt
- Tunnel-Medium-Type**
- Tunnel-Password

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

- Enfin, j'ajoute 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

- Je spécifie 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

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.

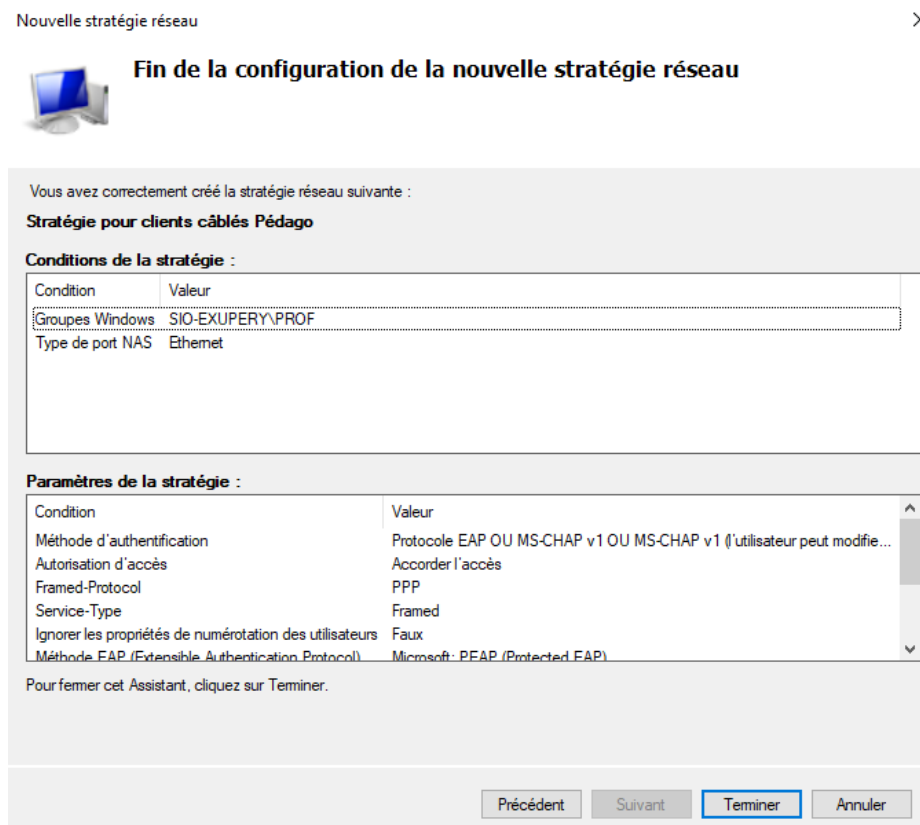
Attributs :

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

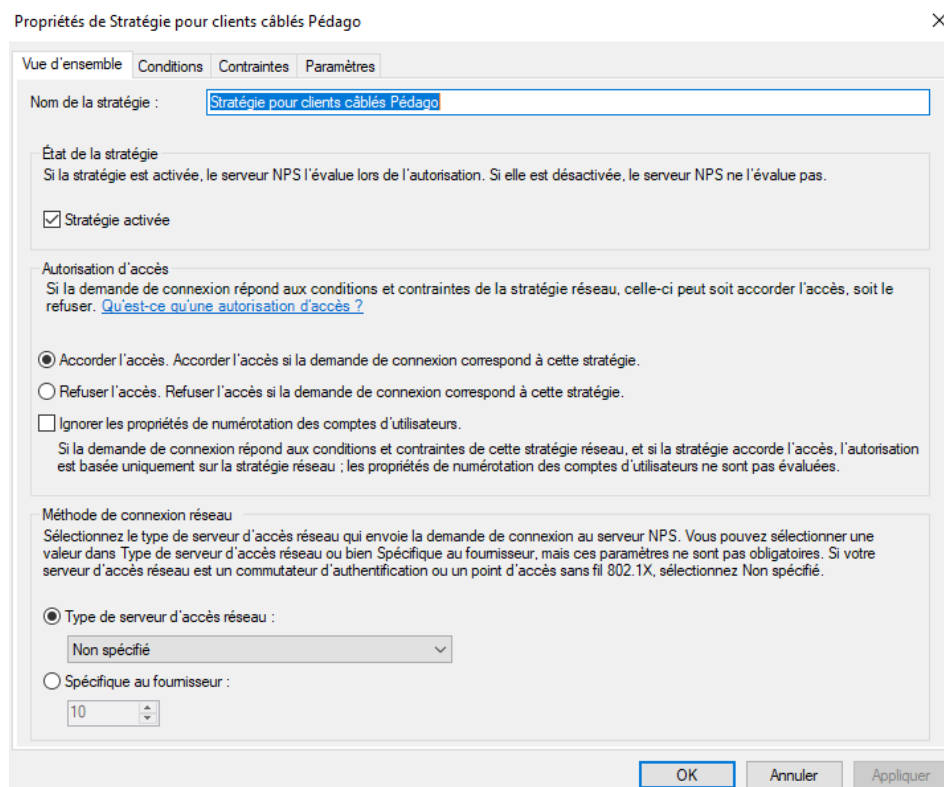
Ajouter... Modifier... Supprimer

Précédent **Suivant** Terminer Annuler

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



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



Propriétés de Stratégie pour clients câblés Pédago



Vue d'ensemble Conditions **Contraintes** Paramètres

Configurez les conditions de cette stratégie réseau.

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

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

Description de la condition :

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

Ajouter... Modifier... Supprimer

OK Annuler Appliquer

Propriétés de Stratégie pour clients câblés Pédago



Vue d'ensemble Conditions Contraintes **Paramètres**

Configurez les contraintes de cette stratégie réseau.

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

Contraintes :

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

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

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

Types de protocoles EAP :

Microsoft: PEAP (Protected EAP) Monter Descendre

Ajouter... Modifier... Supprimer

Méthodes d'authentification moins sécurisées :

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

OK Annuler Appliquer

Vue d'ensemble Conditions Contraintes Paramètres

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

Paramètres :

Attributs RADIUS

Standard

Spécifiques au fournisseur

Routage et accès à distance

Liaisons multiples et protocole BAP (Bandwidth Allocation Protocol)

Filtres IP

Chiffrement

Paramètres IP

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

Attributs :

Nom	Valeur
Framed-Protocol	PPP
Service-Type	Framed
Tunnel-Type	Virtual LANs (VLAN)
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical for...
Tunnel-Pvt-Group-ID	2

Ajouter... Modifier... Supprimer

OK Annuler Appliquer

Vue d'ensemble Conditions Contraintes Paramètres

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

Contraintes :

Contraintes

Méthodes d'authentification

Délai d'inactivité

Délai d'expiration de session

ID de la station appelée

Restrictions relatives aux jours et aux heures

Type de port NAS

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

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

Types de protocoles EAP :

<
Microsoft: PEAP (Protected EAP)
>

Monter
Descendre

Ajouter... Modifier... Supprimer

Méthodes d'authentification moins sécurisées :

Authentification chiffrée Microsoft version 2 (MS-CHAP v2)
 L'utilisateur peut modifier le mot de passe après son expiration

Authentification chiffrée Microsoft (MS-CHAP)
 L'utilisateur peut modifier le mot de passe après son expiration

Authentification chiffrée (CHAP)

Authentification non chiffrée (PAP, SPAP)

Autoriser les clients à se connecter sans négocier une méthode d'authentification

OK Annuler Appliquer

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

Propriétés de Stratégie pour les 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

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.

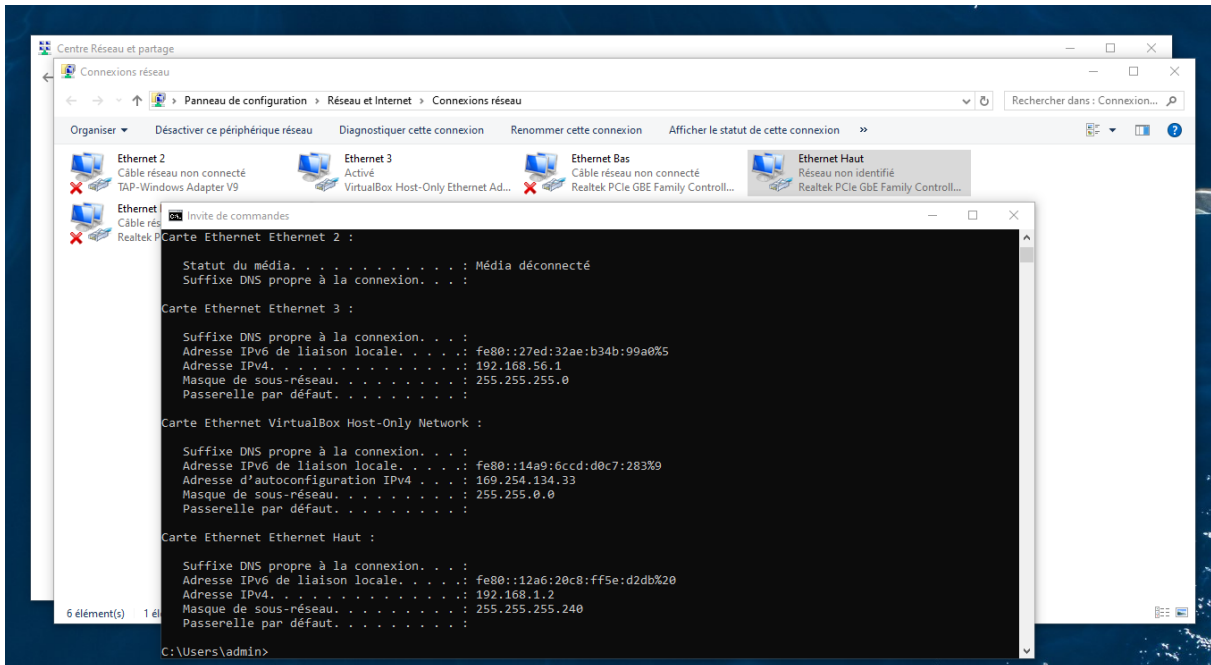
Attributs :

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	3

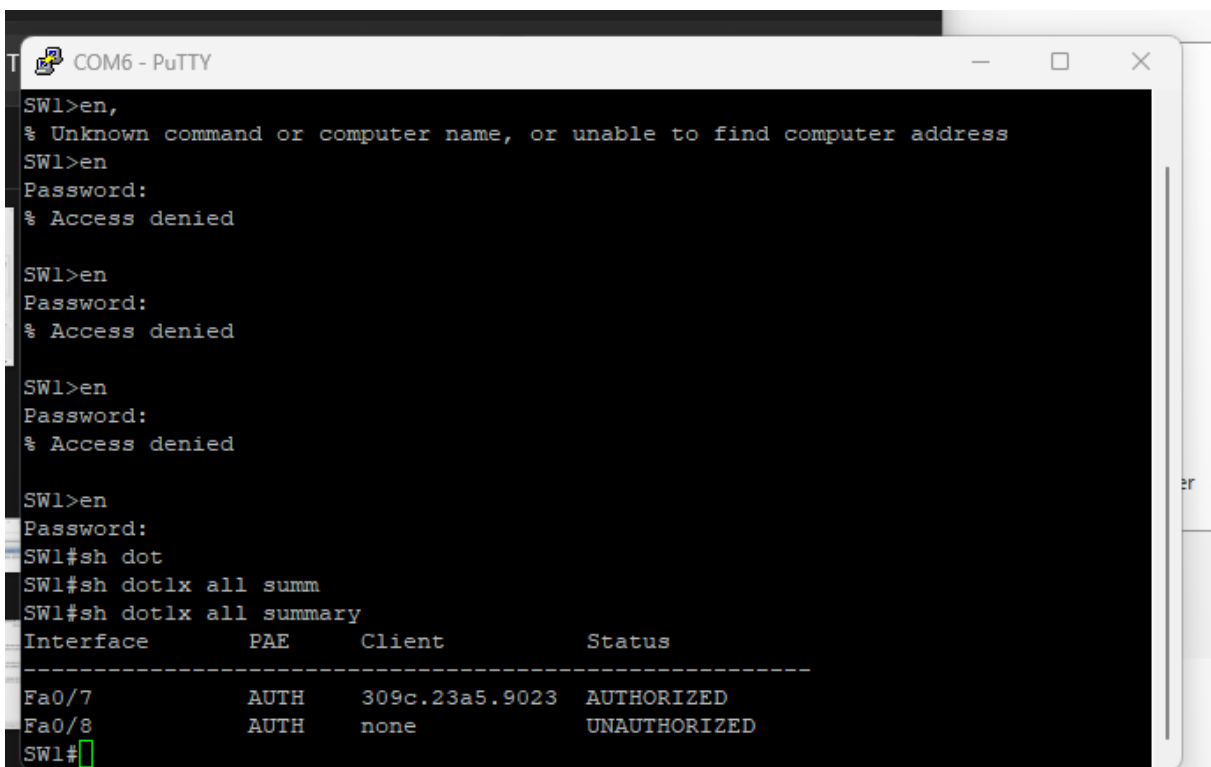
Ajouter... Modifier... Supprimer

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

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

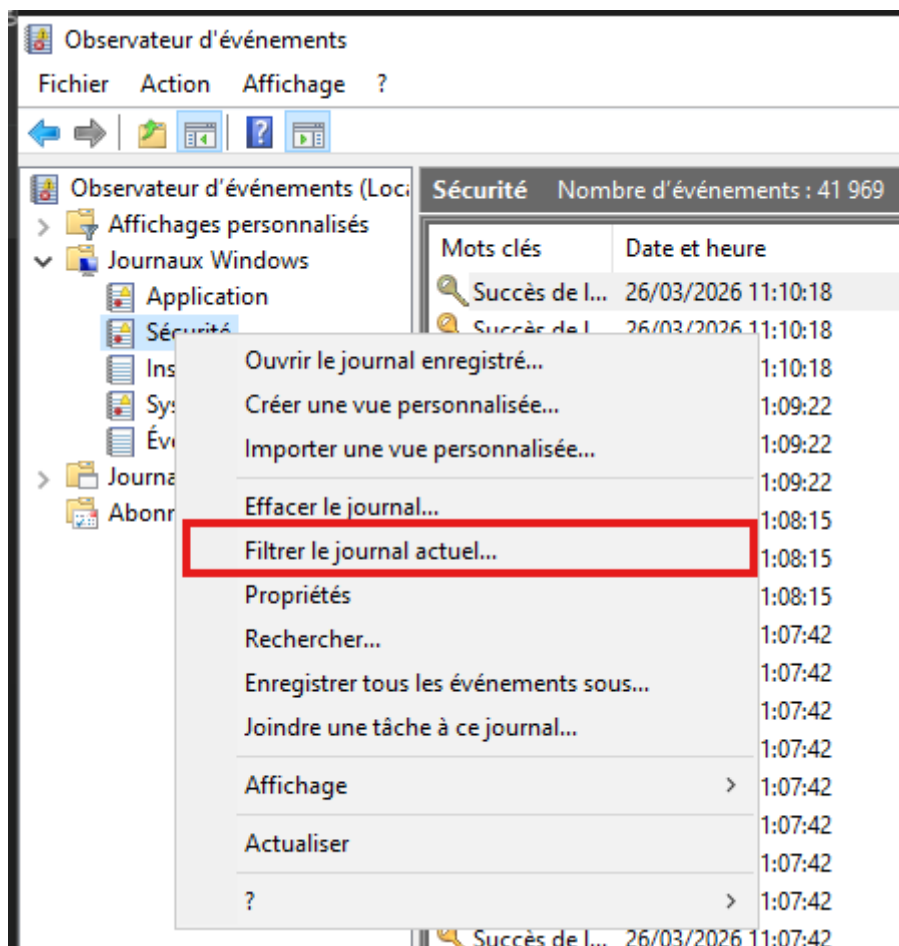


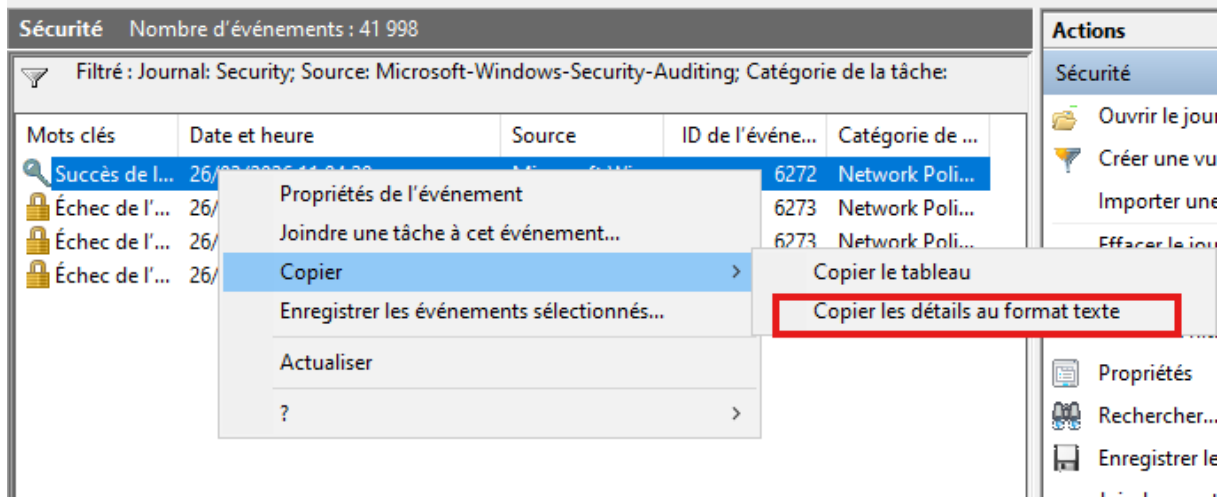
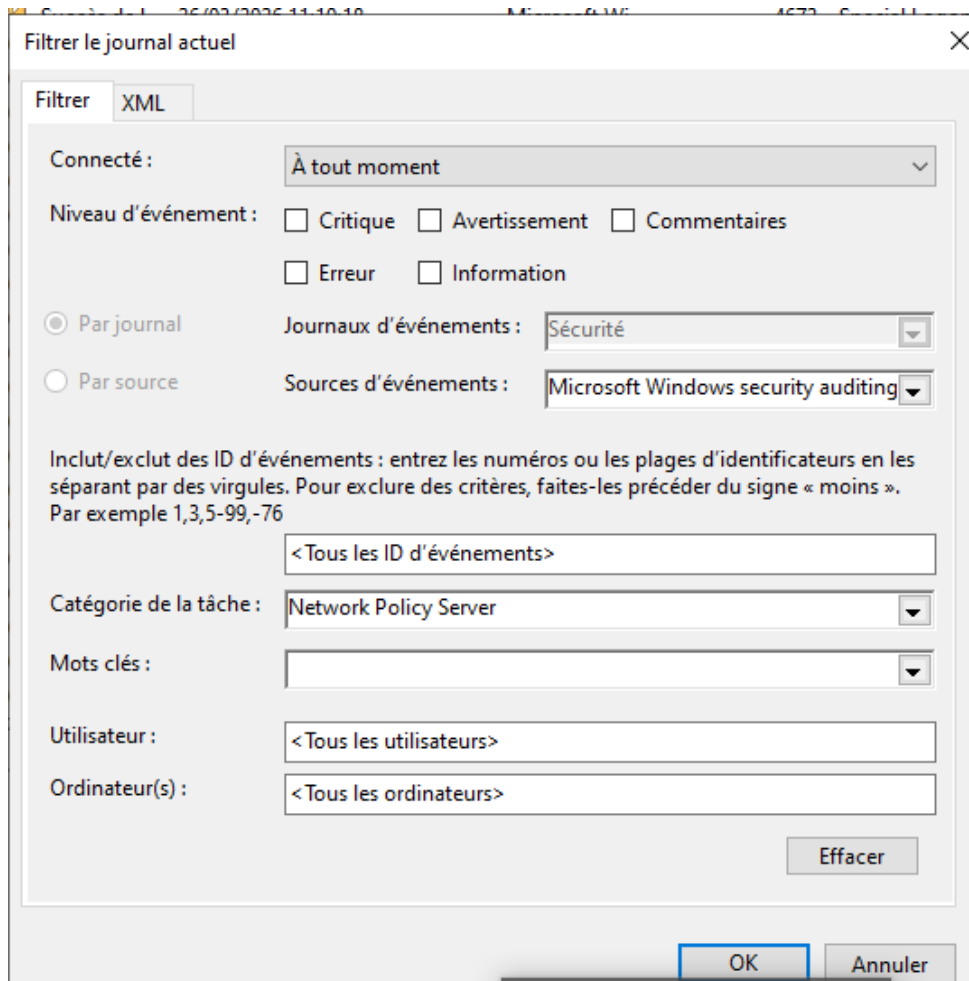
- Commutateur client Radius :



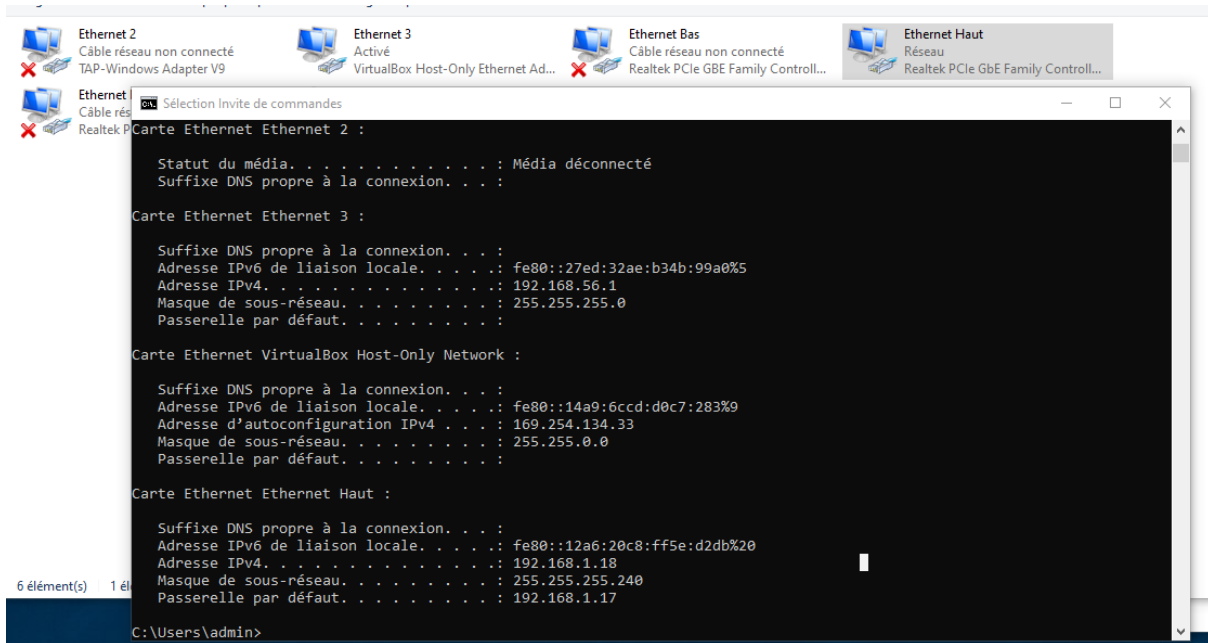
VLAN	Name	Status	Ports
1	default	active	Fa0/3, Fa0/4, Fa0/5, Fa0/6 Fa0/8, Fa0/9, Fa0/10, Fa0/11 Fa0/12, Fa0/13, Fa0/14, Fa0/15 Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/21, Fa0/22, Fa0/23 Fa0/24, Gi0/1, Gi0/2
2	Pedagogie	active	Fa0/7
3	Administration	active	
4	Serveurs	active	Fa0/2
99	Guest	active	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

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



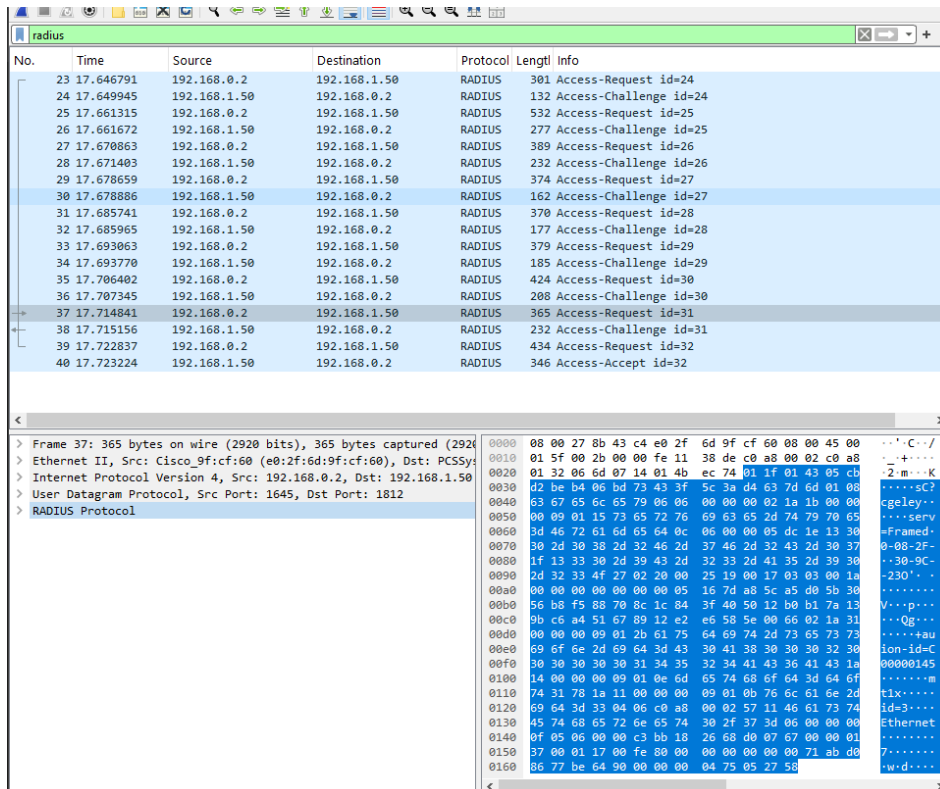


- PC2 et demande de connexion de l'utilisateur cgeley :



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

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



- Je développe la section RADIUS Protocol, comme ci-dessous, et je constate l'encapsulation RADIUS : lorsque le client RADIUS reçoit un paquet EAP du client final, il l'encapsule dans un attribut EAP-Message, lui-même encapsulé dans un message Access-Request. Il en est de même pour un message Access-Challenge provenant du serveur RADIUS :

29	17.678659	192.168.0.2	192.168.1.50	RADIUS	374 Access-Request id=27
30	17.678886	192.168.1.50	192.168.0.2	RADIUS	162 Access-Challenge id=27
31	17.685741	192.168.0.2	192.168.1.50	RADIUS	370 Access-Request id=28
32	17.685965	192.168.1.50	192.168.0.2	RADIUS	177 Access-Challenge id=28
33	17.693063	192.168.0.2	192.168.1.50	RADIUS	379 Access-Request id=29
34	17.693770	192.168.1.50	192.168.0.2	RADIUS	185 Access-Challenge id=29
35	17.706402	192.168.0.2	192.168.1.50	RADIUS	424 Access-Request id=30
36	17.707345	192.168.1.50	192.168.0.2	RADIUS	208 Access-Challenge id=30
37	17.714841	192.168.0.2	192.168.1.50	RADIUS	365 Access-Request id=31
38	17.715156	192.168.1.50	192.168.0.2	RADIUS	232 Access-Challenge id=31
39	17.722837	192.168.0.2	192.168.1.50	RADIUS	434 Access-Request id=32
40	17.723224	192.168.1.50	192.168.0.2	RADIUS	346 Access-Accept id=32

Packet identifier: 0x18 (24)
 Length: 259
 Authenticator: 51df2a72a78d07fd72d263c20c42cad0
[\[The response to this request is in frame 24\]](#)

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-7F-2C-07
- > AVP: t=Calling-Station-Id(31) l=19 val=30-9C-23-A5-90-23
- ▼ AVP: t=EAP-Message(79) l=13 Last Segment[1]
 - Type: 79
 - Length: 13
 - EAP fragment: 0217000b016367656c6579
 - ▼ Extensible Authentication Protocol
 - Code: Response (2)
 - Id: 23
 - Length: 11
 - Type: Identity (1)
 - Identity: cgeley
- > AVP: t=Message-Authenticator(80) l=18 val=4e7ef80b8210cc...