

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

Table des matières

2.2 Ajout du rôle Services de certificats Active Directory.....	5
2.3 Installation du service NPS.....	16
2.4 Configuration du serveur RADIUS NPS.....	21

Configuration du routeur :

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface G0/0
Router(config-if)# no shutdown
Router(config-if)#
Router(config-if)#interface G0/0.1
Router(config-subif)# encapsulation dot1Q 1
Router(config-subif)# ip address 192.168.0.1 255.255.255.248
Router(config-subif)#
Router(config-subif)#interface G0/0.2
Router(config-subif)# encapsulation dot1Q 2
Router(config-subif)# ip address 192.168.1.1 255.255.255.240
Router(config-subif)#
Router(config-subif)#interface G0/0.3
Router(config-subif)# encapsulation dot1Q 3
Router(config-subif)# ip address 192.168.1.17 255.255.255.240
Router(config-subif)#
Router(config-subif)#interface G0/0.99
Router(config-subif)# encapsulation dot1Q 99
Router(config-subif)# ip address 192.168.1.33 255.255.255.240
Router(config-subif)#
Router(config-subif)#interface G0/0.4
Router(config-subif)# encapsulation dot1Q 4
Router(config-subif)# ip address 192.168.1.49 255.255.255.248
Mar 5 09:56:05.427: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to down
Mar 5 09:56:08.727: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
Mar 5 09:56:09.727: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
```

```
Router(config-subif)#exit
Router(config)#ip dhcp excluded-address 192.168.1.1
Router(config)#ip dhcp excluded-address 192.168.1.17
Router(config)#ip dhcp excluded-address 192.168.1.33
Router(config)#
Router(config)#
Router(config)#ip dhcp pool VLAN2_PEDAGO
Router(dhcp-config)# network 192.168.1.0 255.255.255.240
Router(dhcp-config)# default-router 192.168.1.1
Router(dhcp-config)# dns-server 192.168.1.50
Router(dhcp-config)#
Router(dhcp-config)#ip dhcp pool VLAN3_ADMIN
Router(dhcp-config)# network 192.168.1.16 255.255.255.240
Router(dhcp-config)# default-router 192.168.1.17
Router(dhcp-config)# dns-server 192.168.1.50
Router(dhcp-config)#
Router(dhcp-config)#ip dhcp pool VLAN99_GUEST
Router(dhcp-config)# network 192.168.1.32 255.255.255.240
Router(dhcp-config)# default-router 192.168.1.33
Router(dhcp-config)# dns-server 192.168.1.50
```

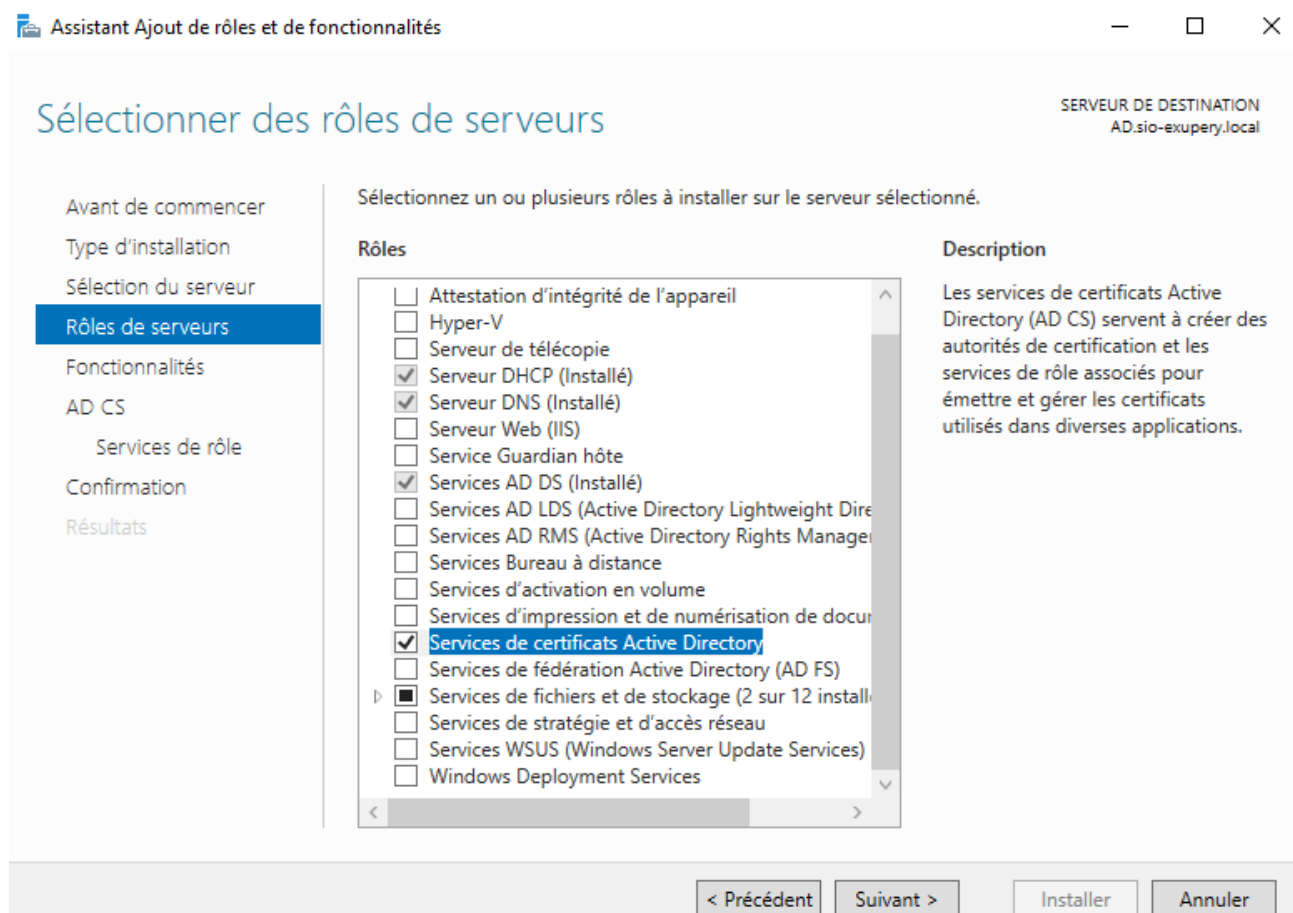
Configuration de base du switch

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

2.2 Ajout du rôle Services de certificats Active Directory

Ajoutez le rôle Service de certificats Active Directory.

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



Assistant Ajout de rôles et de fonctionnalités

SÉLECTIONNER DES RÔLES DE SERVEURS

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

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

Rôles	Description
<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 Directory Services)	
<input type="checkbox"/> Services AD RMS (Active Directory Rights Management Services)	
<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 documents	
<input checked="" type="checkbox"/> Services de certificats Active Directory	Les services de certificats Active Directory (AD CS) servent à créer des autorités de certification et les services de rôle associés pour émettre et gérer les certificats utilisés dans diverses applications.
<input type="checkbox"/> Services de fédération Active Directory (AD FS)	
<input checked="" type="checkbox"/> Services de fichiers et de stockage (2 sur 12 installés)	
<input 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 > Installer Annuler

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

The screenshot shows the 'Assistant Ajout de rôles et de fonctionnalités' (Server Manager) window. The title bar reads 'Assistant Ajout de rôles et de fonctionnalités'. The main content area is titled 'Services de certificats Active Directory' and indicates the 'SERVEUR DE DESTINATION' as 'AD.sio-exuperly.local'. On the left, a navigation pane lists the following steps: 'Avant de commencer', 'Type d'installation', 'Sélection du serveur', 'Rôles de serveurs', 'Fonctionnalités', 'AD CS' (highlighted in blue), 'Services de rôle', 'Confirmation', and 'Résultats'. The main pane contains the following text: 'Les services de certificats Active Directory (AD CS) fournissent l'infrastructure de certificats pour prendre en charge des scénarios tels que les réseaux sans fil sécurisés, les réseaux privés virtuels, la sécurité IPSec (Internet Protocol Security), la protection d'accès réseau (NAP), le système de fichiers EFS (Encrypting File System) et la connexion par carte à puce.' Below this, under 'À noter :', there is a bullet point: '• Les paramètres de nom et de domaine de cet ordinateur ne sont pas modifiables après l'installation d'une autorité de certification. Si vous voulez changer le nom de l'ordinateur, joindre un domaine ou promouvoir ce serveur en contrôleur de domaine, effectuez ces modifications avant d'installer l'autorité de certification. Pour plus d'informations, consultez Attribution d'un nom à une autorité de certification.' At the bottom of the window, there are four buttons: '< Précédent', 'Suivant >', 'Installer', and 'Annuler'.

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

The screenshot shows the 'Assistant Ajout de rôles et de fonctionnalités' window. The title bar includes the window name and standard minimize, maximize, and close buttons. The main content area is titled 'Confirmer les sélections d'installation' and shows the target server as 'SERVEUR DE DESTINATION AD.sio-exupery.local'. A left-hand 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 area contains instructions to click 'Installer' and a checked checkbox for 'Redémarrer automatiquement le serveur de destination, si nécessaire'. Below this, 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', and a set of navigation buttons: '< Précédent', 'Suivant >', 'Installer', and 'Annuler'.

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.

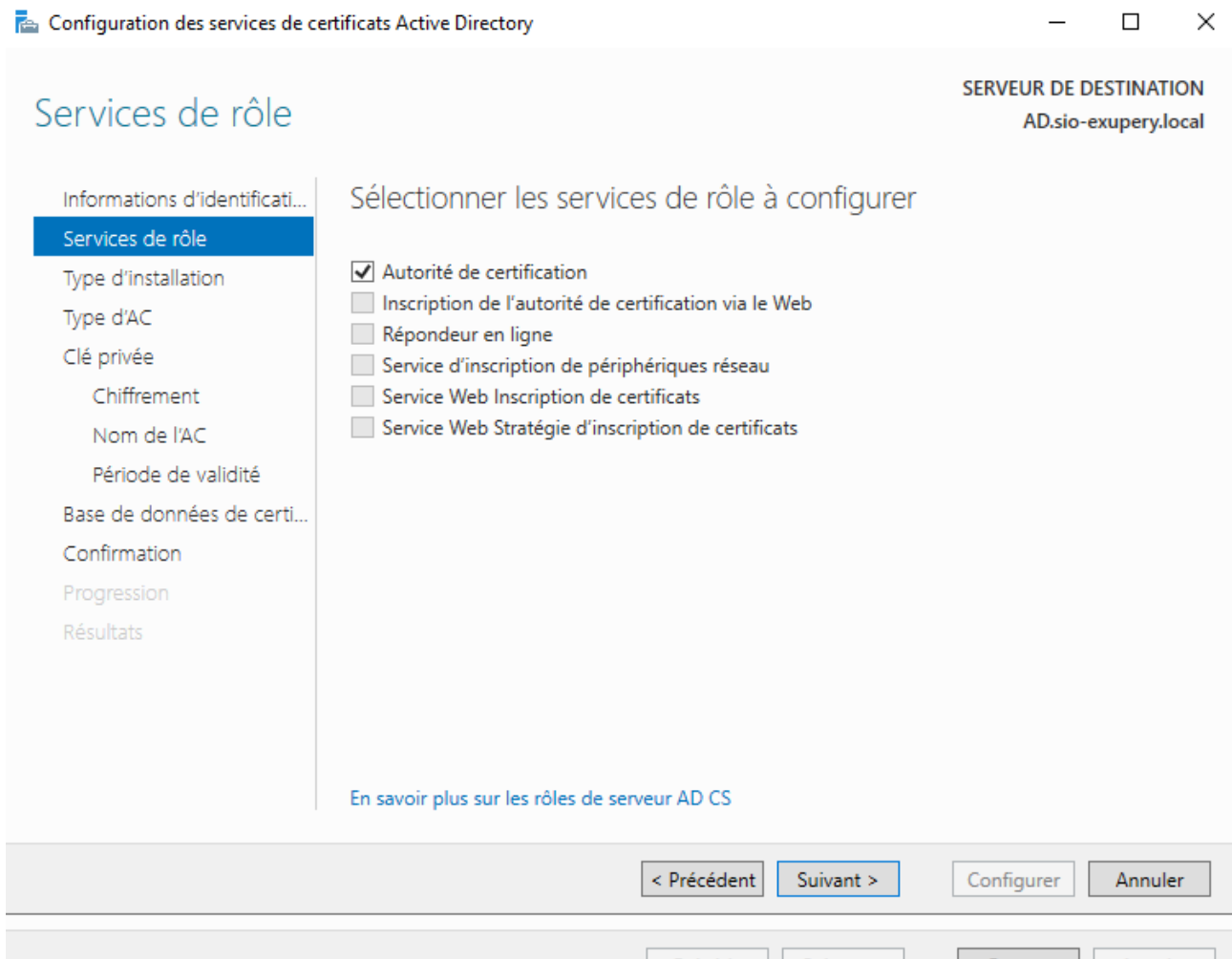
Outils d'administration de serveur distant
Outils d'administration de rôles
Outils des services de certificats Active Directory
Outils de gestion de l'autorité de certification

Services de certificats Active Directory
Autorité de certification

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

< Précédent Suivant > Installer Annuler

Je coche la case Autorité de certification pour configurer ce rôle



Je sélectionne l'autorité de certification d'entreprise

The screenshot shows the 'Configuration des services de certificats Active Directory' wizard. The title bar includes the application name and standard window controls. The main window has a left-hand navigation pane with the following items: 'Informations d'identificati...', 'Services de rôle', 'Type d'installation' (highlighted in blue), 'Type d'AC', 'Clé privée', 'Chiffrement', 'Nom de l'AC', 'Période de validité', 'Base de données de certi...', 'Confirmation', 'Progression', and 'Résultats'. The main content area is titled 'Type d'installation' and 'Spécifier le type d'installation de l'AC'. It contains a paragraph explaining that enterprise CAs can use Active Directory (AD DS) for certificate management, while autonomous CAs do not. Below this are two radio button options: 'Autorité de certification d'entreprise' (selected) and 'Autorité de certification autonome'. Each option has a descriptive paragraph. At the bottom of the main area is a link: 'En savoir plus sur le type d'installation'. The bottom of the window features a navigation bar with buttons: '< Précédent', 'Suivant >', 'Configurer', and 'Annuler'. The top right corner of the window displays 'SERVEUR DE DESTINATION' and 'AD.sio-exupery.local'.

Configuration des services de certificats Active Directory

SERVEUR DE DESTINATION
AD.sio-exupery.local

Type d'installation

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

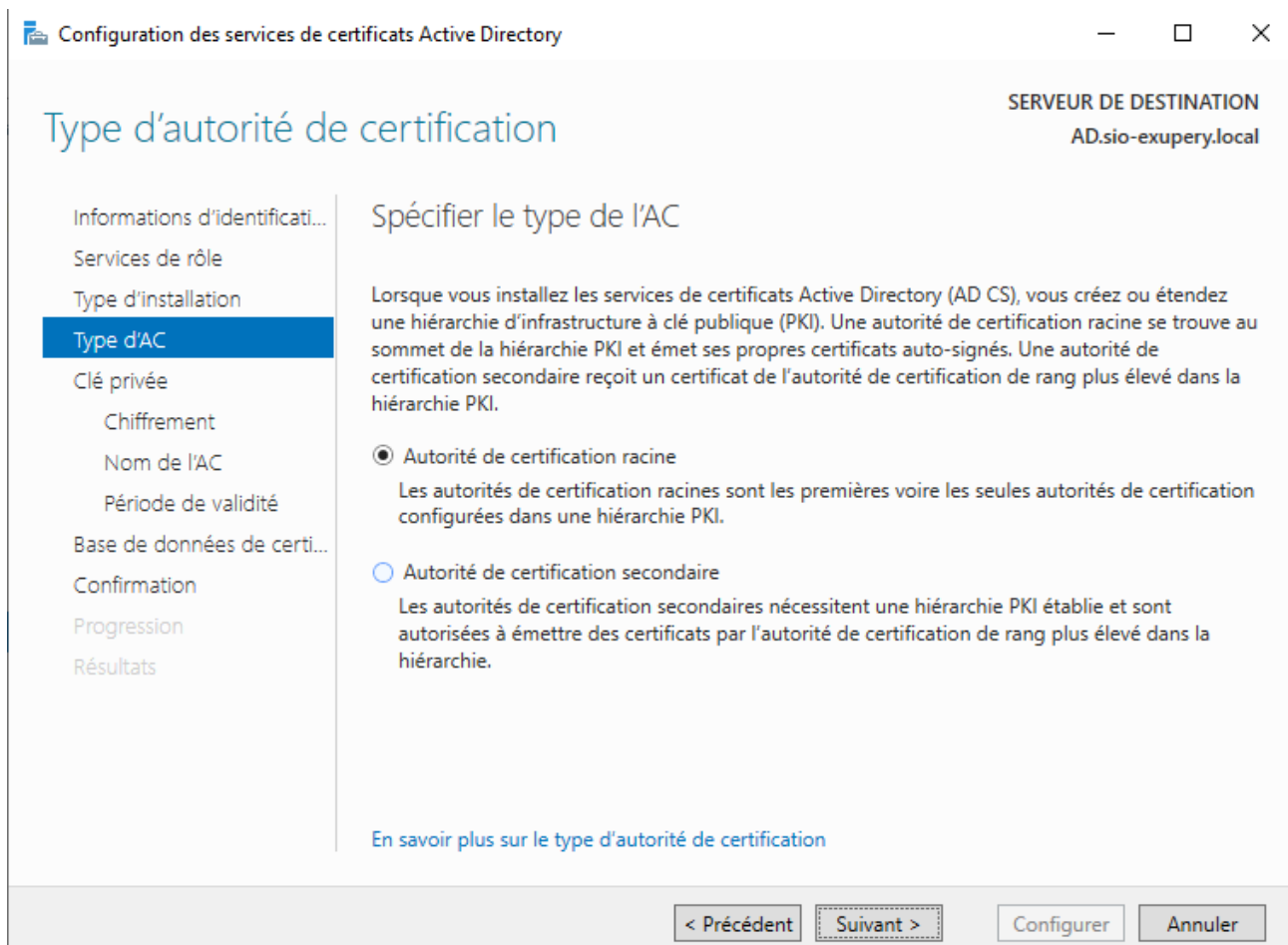
Les autorités de certification d'entreprise peuvent utiliser les services de domaine Active Directory (AD DS) pour simplifier la gestion des certificats. Les autorités de certification autonomes n'utilisent pas AD DS pour émettre ou gérer des certificats.

- 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).

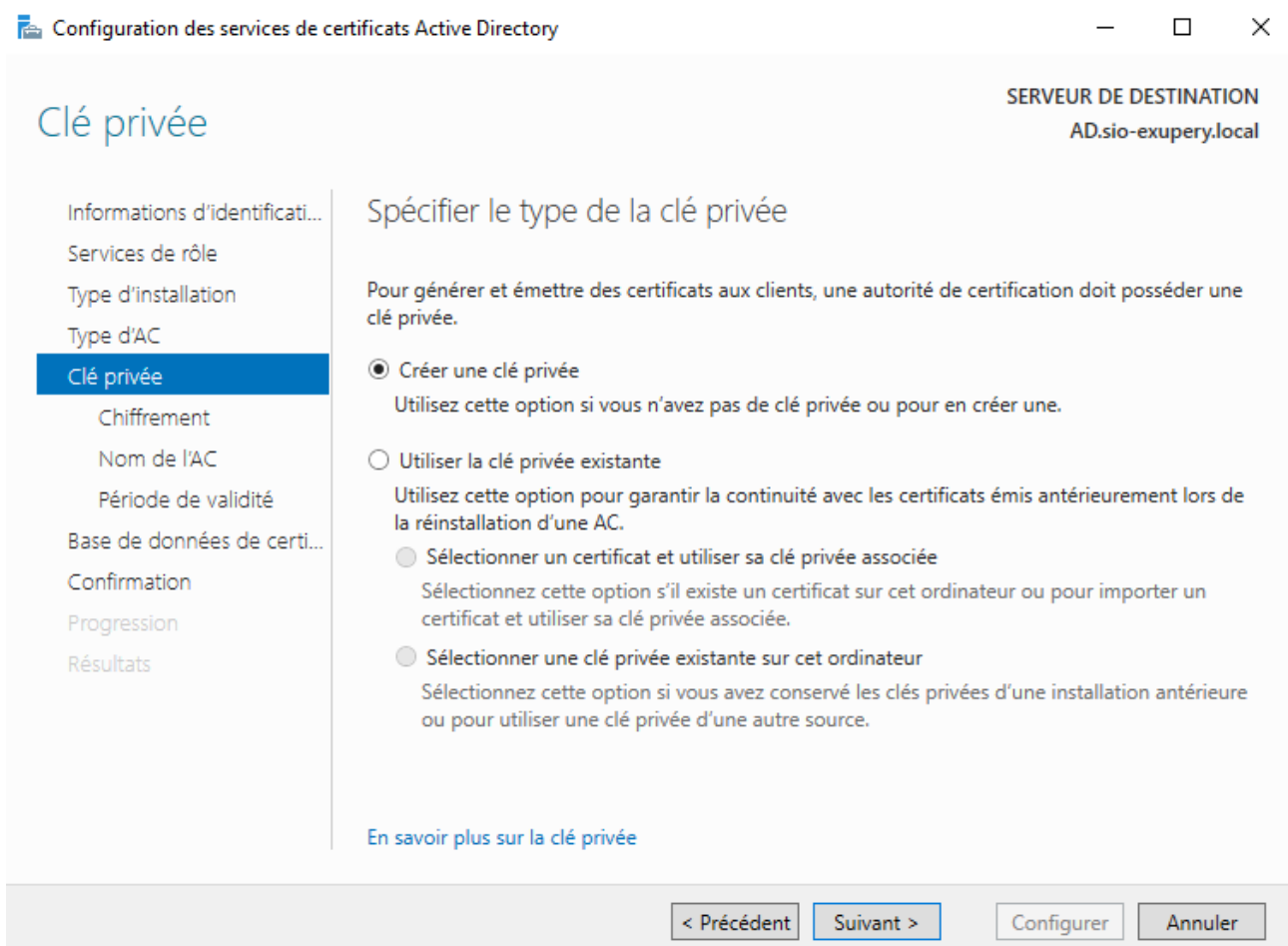
[En savoir plus sur le type d'installation](#)

< Précédent Suivant > Configurer Annuler

Je sélectionne l'autorité de certification racine



Je sélectionne Créer une nouvelle clé privée



Je choisis l'algorithme de chiffrement ainsi que le 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 :

RSA#Microsoft Software Key Storage Provider

Longueur de la clé :

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

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 :

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 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 :

Années

Date d'expiration de l'AC : 12/03/2031 10:33:00

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](#)

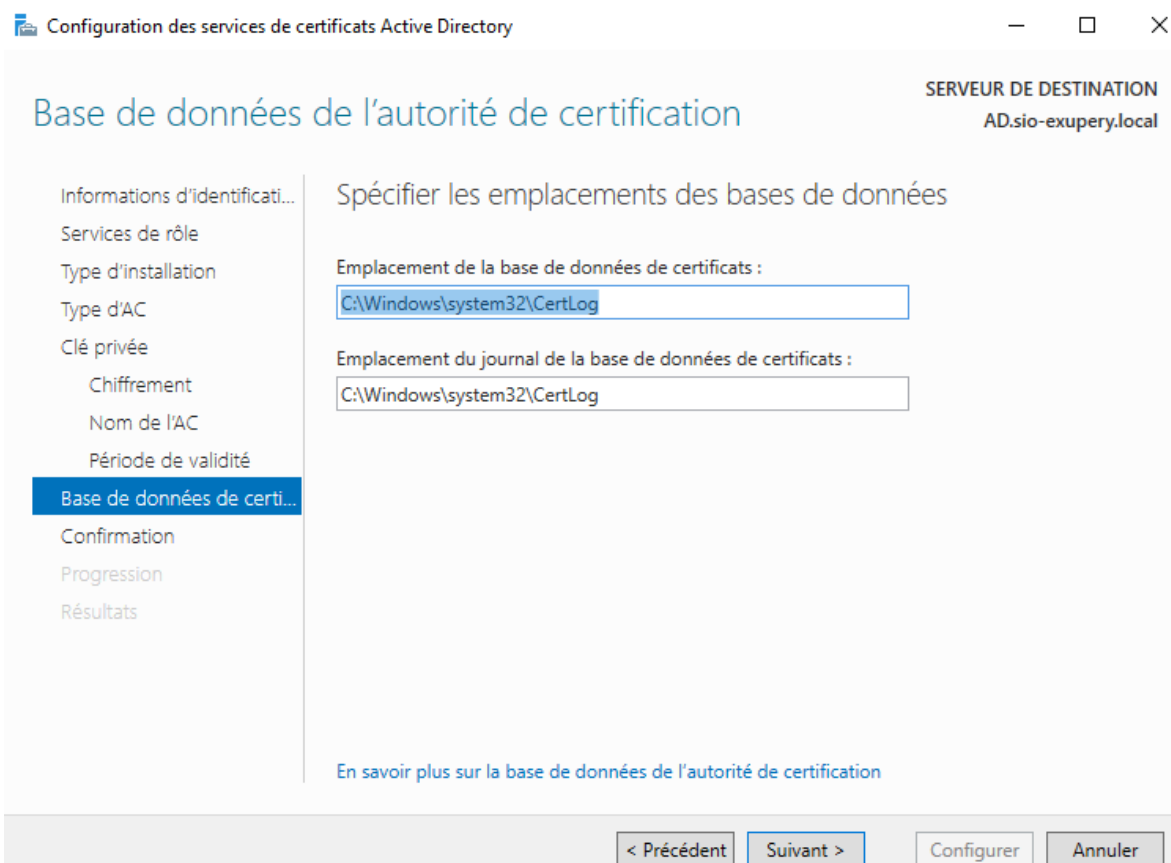
< Précédent

Suivant >

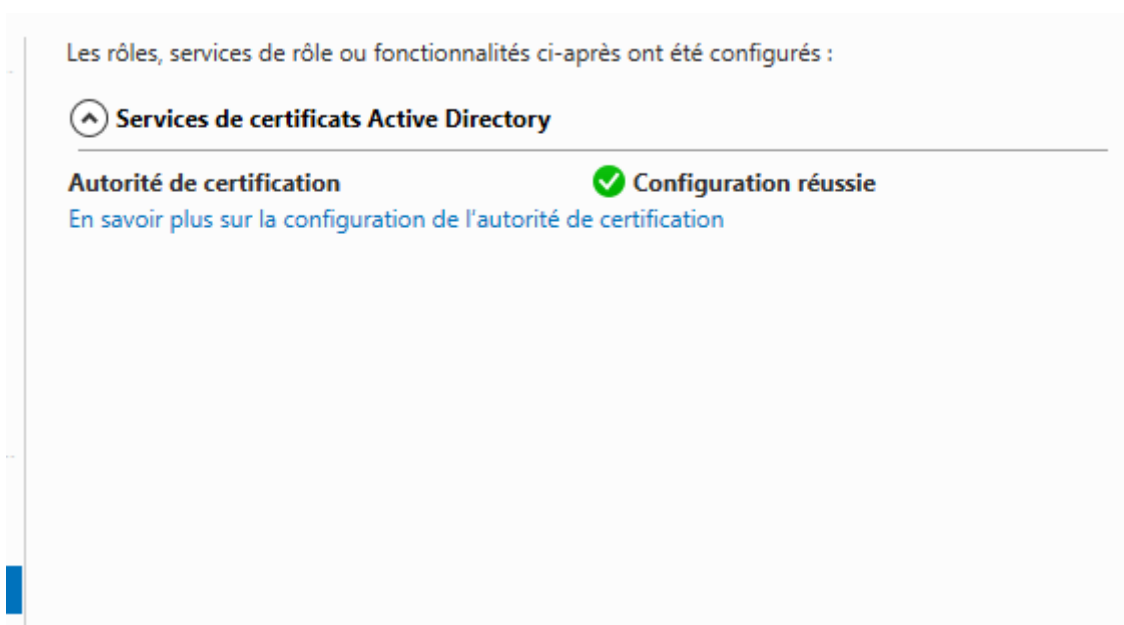
Configurer

Annuler

Laissez les dossiers des bases de données, par défaut

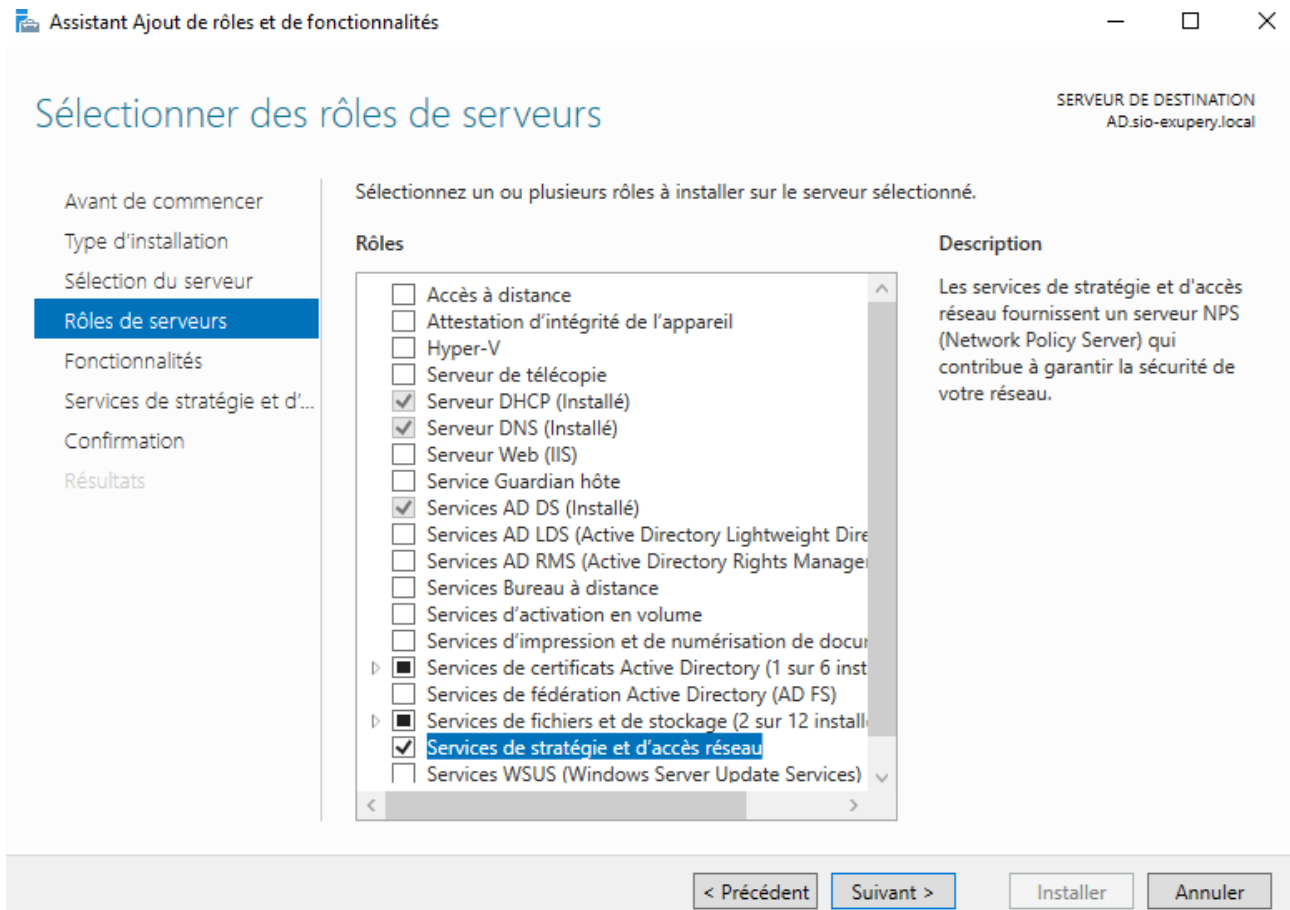


Votre autorité de certification est maintenant installée et configurée. Cliquez sur Fermer



2.3 Installation du service NPS

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



Je clique sur suivant

Sélectionnez une ou plusieurs fonctionnalités à installer sur le serveur sélectionné.

Fonctionnalités

<input type="checkbox"/>	Extension WinRM IIS
▷ <input type="checkbox"/>	Fonctionnalités de .NET Framework 3.5
<input checked="" type="checkbox"/>	Gestion de stratégie de groupe (Installé)
<input type="checkbox"/>	Gestion du stockage Windows basé sur des norme
<input type="checkbox"/>	IFilter TIFF Windows
<input type="checkbox"/>	IIS Hostable Web Core
<input type="checkbox"/>	Insights système
<input type="checkbox"/>	Kit d'administration du Gestionnaire des connexion
<input type="checkbox"/>	Limite de bande passante SMB
<input type="checkbox"/>	Media Foundation
▷ <input type="checkbox"/>	Message Queuing
<input type="checkbox"/>	Moniteur de port LPR
<input type="checkbox"/>	MPIO (Multipath I/O)
▷ <input type="checkbox"/>	MultiPoint Connector
▲ <input checked="" type="checkbox"/>	Outils d'administration de serveur distant (6 sur 43
▷ <input type="checkbox"/>	Outils d'administration de fonctionnalités
▷ <input checked="" type="checkbox"/>	Outils d'administration de rôles (6 sur 26 instal
<input type="checkbox"/>	Outils de protection d'ordinateur virtuel pour la ge
<input checked="" type="checkbox"/>	Prise en charge WoW64 (Installé)

Description

Les Outils d'administration de serveur distant comprennent des composants logiciels enfichables et des outils en ligne de commande pour la gestion à distance des rôles et des fonctionnalités.

< Précédent

Suivant >

Installer

Annuler

Je clique sur suivant

Services de stratégie et d'accès réseau

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

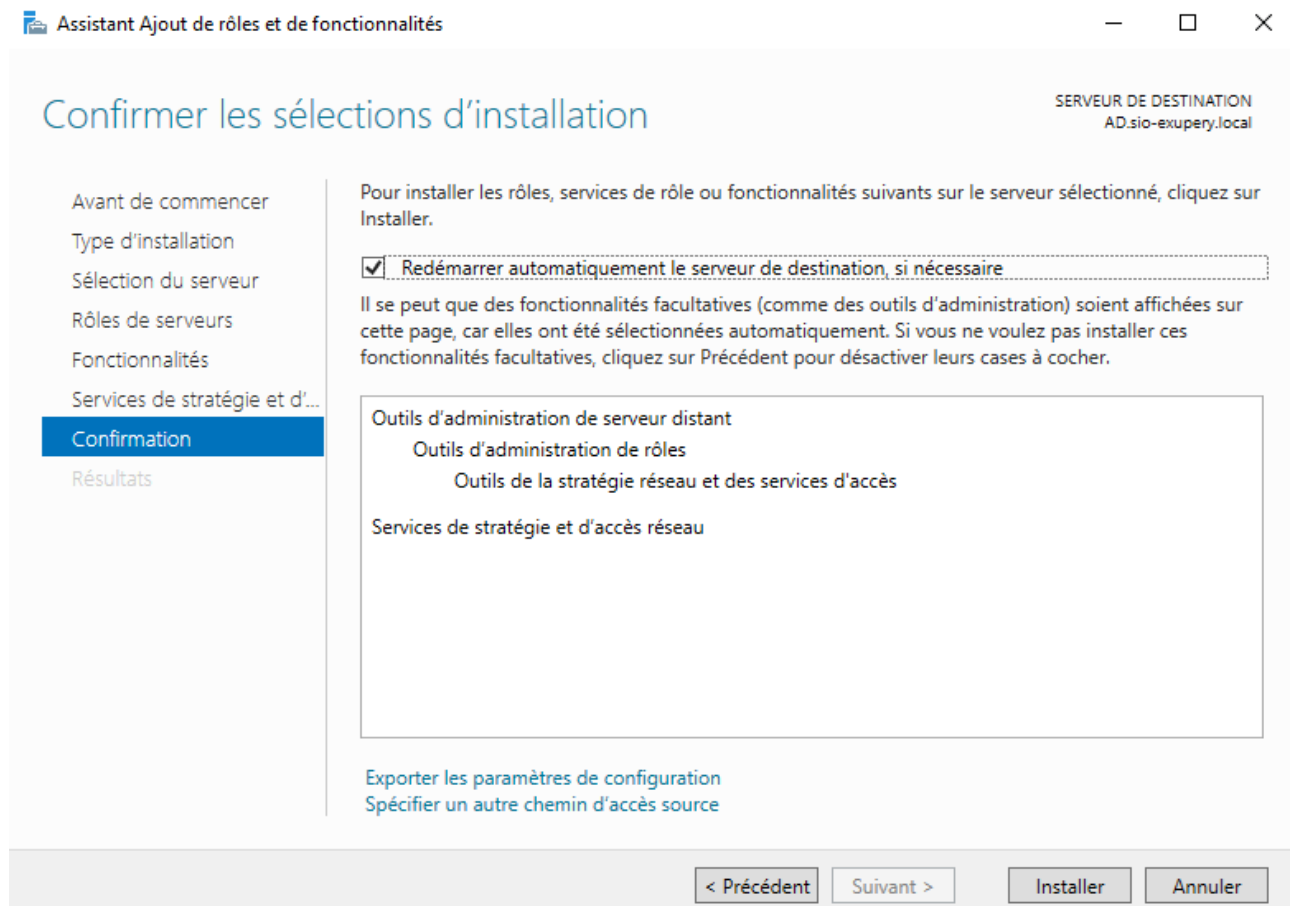
Résultats

Les services de stratégie et d'accès réseau vous permettent de définir et d'appliquer des stratégies d'accès réseau, d'authentification et d'autorisation à l'aide du serveur NPS (Network Policy Server).

À noter :

- Vous pouvez déployer NPS comme un serveur et un proxy RADIUS (Remote Authentication Dial-In User Service). Après l'installation du serveur NPS au moyen de cet Assistant, vous pouvez configurer NPS à partir de la page d'accueil NPAS en utilisant la console NPS.

Je coche le redémarrage automatique du serveur



Puis j'installe et je ferme

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

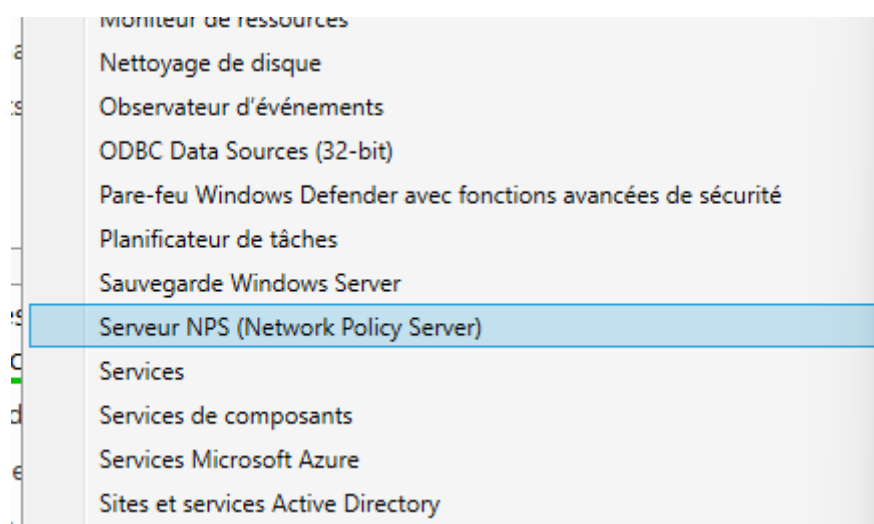
Services de stratégie et d'accès réseau

i 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

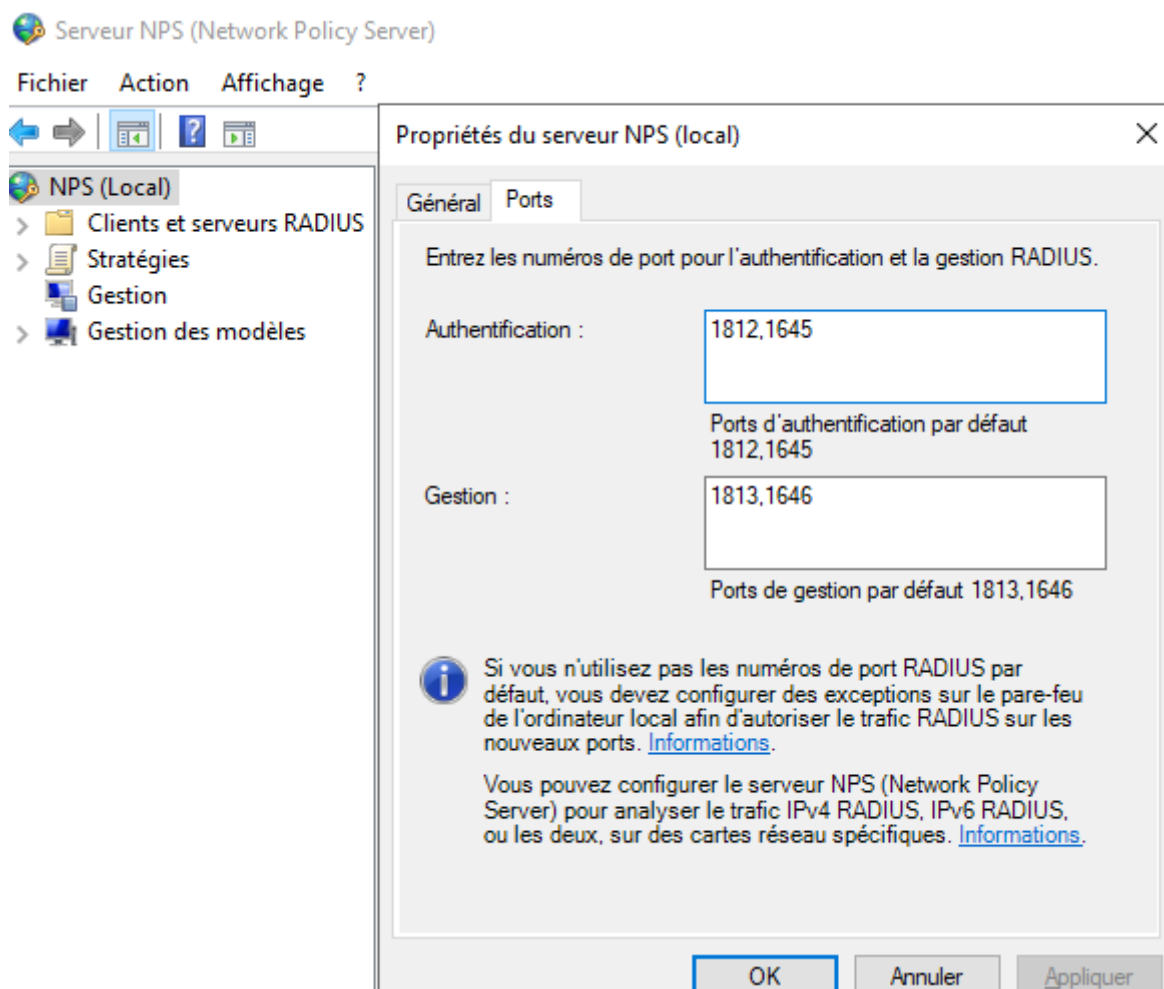
Constatez la présence de la console Serveur NPS



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

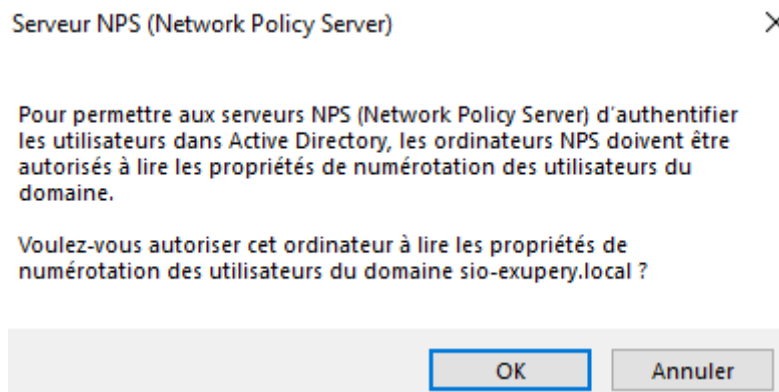
```
UDP 192.168.1.50:88 *:*
UDP 192.168.1.50:137 *:*
UDP 192.168.1.50:138 *:*
UDP 192.168.1.50:464 *:*
UDP 192.168.1.50:1645 *:*
UDP 192.168.1.50:1646 *:*
UDP 192.168.1.50:1812 *:*
UDP 192.168.1.50:1813 *:*
UDP 192.168.1.50:2535 *:*
C:\Users\Administrateur>
```

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

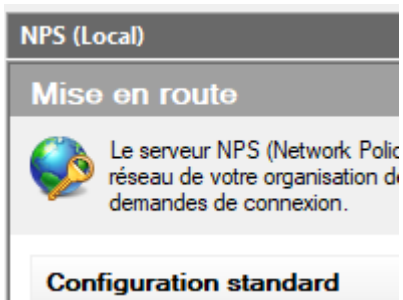


2.4 Configuration du serveur RADIUS NPS

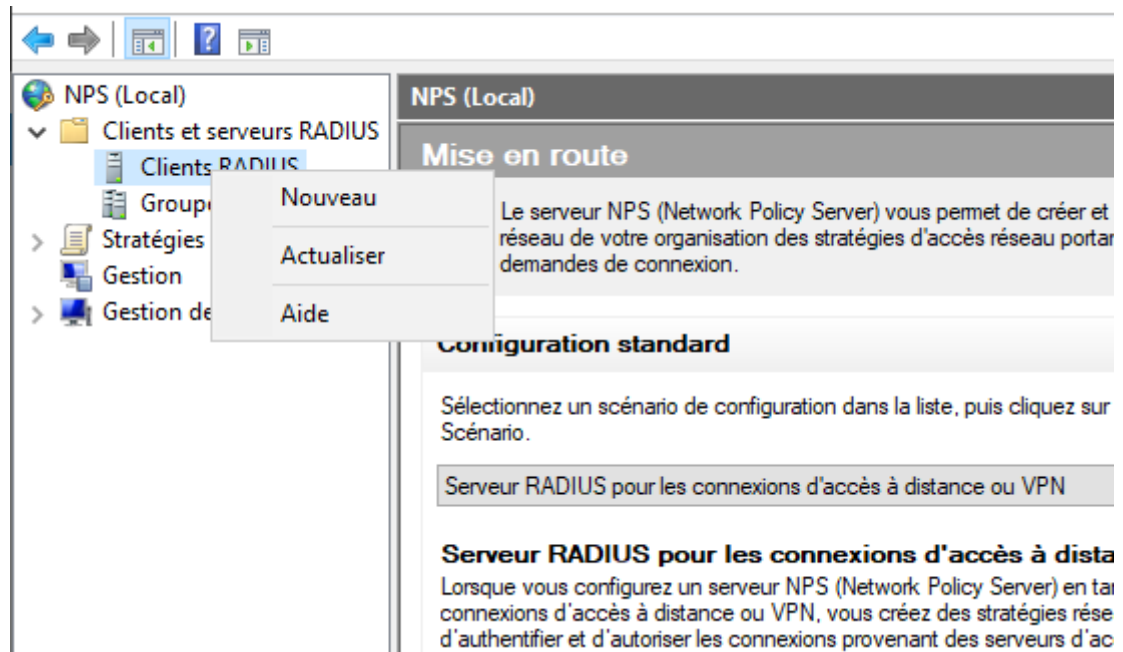
Afin d'inscrire NPS dans Active Directory pour lui permettre d'interroger la base des utilisateurs, cliquez depuis le menu Action sur Inscrire un serveur dans Active Directory puis OK



Un agent s'est mis en route



Ensuite clic droit sur client radius puis nouveau



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

Nouveau client RADIUS ✕

Paramètres **Avancé**

Activer ce client RADIUS

Sélectionner un modèle existant :

[Menu déroulant vide]

Nom et adresse

Nom convivial :
Client-Cisco2960

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 :
[Champ masqué]

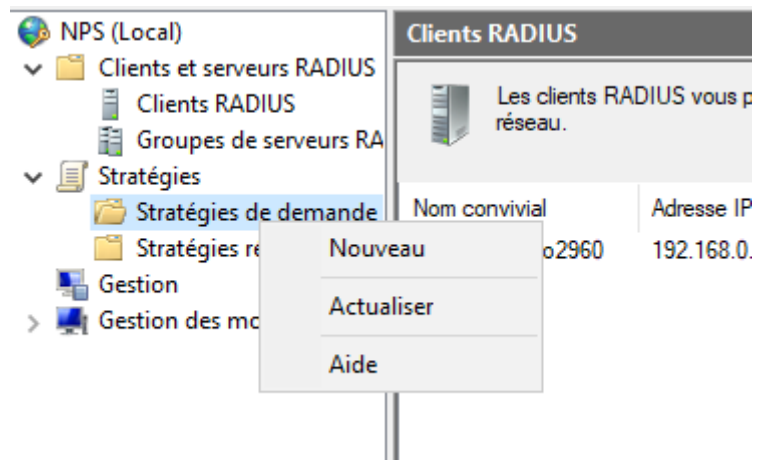
Confirmez le secret partagé :
[Champ masqué]

OK Annuler

Le client est bien ajouté

Clients RADIUS			
 Les clients RADIUS vous permettent de spécifier les serveurs d'accès réseau qui fournissent l'accès à réseau.			
Nom convivial	Adresse IP	Fabricant du périphérique	État
 Client-Cisco2960	192.168.0.2	RADIUS Standard	Activé

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



Je la nomme :

Nom de la stratégie :
Connexion câblée

Méthode de connexion réseau
Sélectionnez le type de serveur d'accès réseau qui envoie la demande de valeur dans Type de serveur d'accès réseau ou bien Spécifique au fournisseur. Un serveur d'accès réseau est un commutateur d'authentification ou un point d'accès.

Type de serveur d'accès réseau :
Non spécifié

Spécifique au fournisseur :
10



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

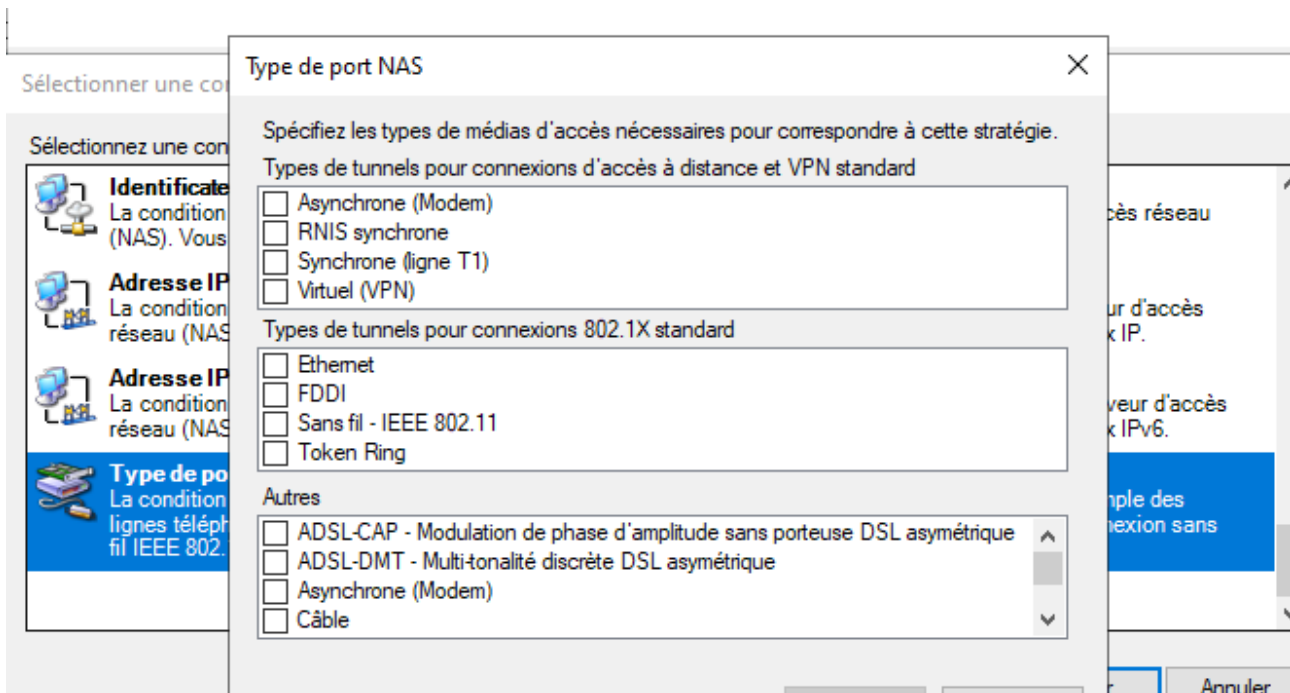
Description de la condition :

Ajouter...

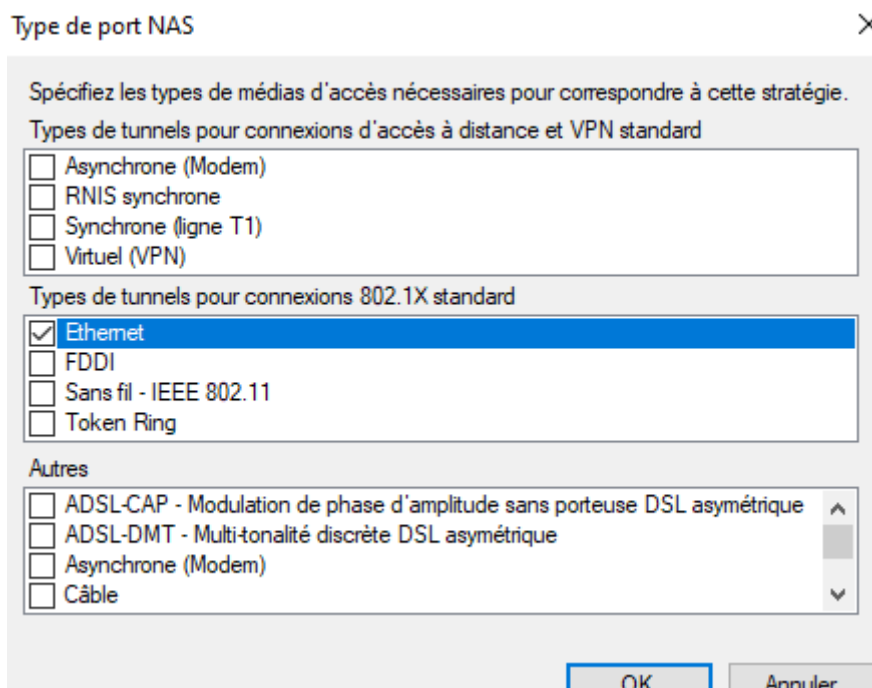
Modifier...

Supprimer


Ensuite je clique sur ajouter puis type de port NAS



Je coche ethernet






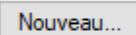
Puis je valide et il apparaît dans les conditions

Conditions :	
Condition	Valeur
 Type de port NAS	Ethernet

Je clique sur suivant

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

Paramètres :

<p>Transfert de la demande de connexion</p> <ul style="list-style-type: none"> Authentification Gestion	<p>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.</p> <p><input checked="" type="radio"/> Authentifier les demandes sur ce serveur</p> <p><input type="radio"/> Transférer les demandes au groupe de serveurs RADIUS distants suivant pour authentification :</p> <p><input type="text" value="<non configurée>"/>  </p> <p><input type="radio"/> Accepter les utilisateurs sans validation des informations d'identification</p>
--	---

et encore sur suivant J'apparaît sur cet page et on clique encore sur suivant

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.

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 :

<p>Spécifier un nom de domaine</p> <p>Attribut</p> <p>Attributs RADIUS</p> <p>Standard</p> <p><input checked="" type="checkbox"/> Spécifiques au fournisseur</p>	<p>Sélectionnez les attributs auxquels les règles suivantes seront appliquées. Les règles sont traitées selon leur ordre d'apparition dans la liste.</p> <p>Attribut : <input type="text" value="ID de la station appelée"/></p> <p>Règles :</p> <table border="1"><thead><tr><th>Rechercher</th><th>Remplacer par</th></tr></thead><tbody><tr><td> </td><td> </td></tr></tbody></table> <p>Ajouter Modifier Supprimer Monter Descendre</p>	Rechercher	Remplacer par		
Rechercher	Remplacer par				

Précédent **Suivant** Terminer Annuler

On clique maintenant sur valider



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.

La stratégie a été rajouter

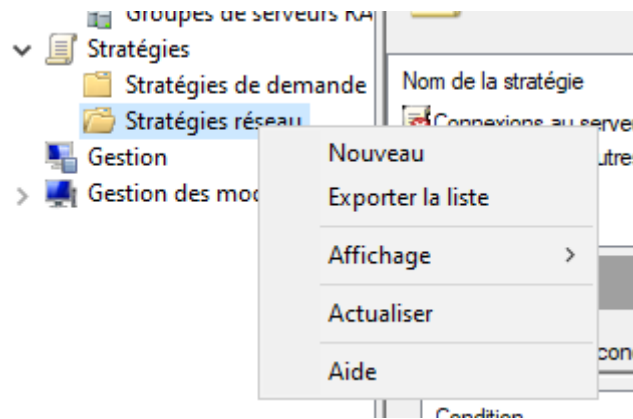
Stratégies de demande de connexion



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

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



Nom de la stratégie :
Strategie pour clients câbles 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

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

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).

Ajouter Annuler

J'ajoute le groupe prof

Groupes Windows

Spécifiez l'appartenance aux groupes nécessaire pour correspondre à cette stratégie.

Groupes
SIO-EXUPERY\PROF

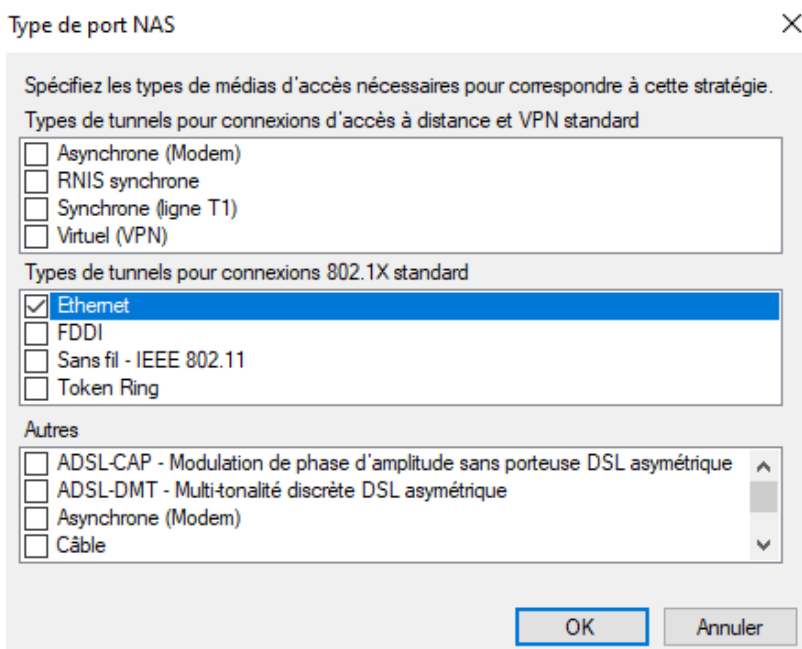
Ajouter des groupes... Supprimer

OK Annuler



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



Je coche ethernet



Les deux conditions ont bien été ajoutées

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

on clique sur suivant on garde accès accordé

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

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)
- Authentification non chiffrée (PAP, SPAP)
- Autoriser les clients à se connecter sans négocier une méthode d'authentification.

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








Configurer des contraintes

Les contraintes sont des paramètres supplémentaires de la stratégie réseau, auxquels les demandes de connexion doivent se conformer. Si une demande de connexion ne répond pas à une contrainte, le serveur NPS (Network Policy Server) rejette automatiquement cette demande. Les contraintes sont facultatives ; si vous ne souhaitez pas configurer de contraintes, cliquez sur Suivant.

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

Contraintes :

Contraintes	
 Délai d'inactivité	<p>Spécifiez le délai maximal d'inactivité du serveur en minutes avant déconnexion</p> <p><input type="checkbox"/> Déconnecter au-delà de la durée d'inactivité maximale</p> <p><input type="text" value="1"/></p>
 Délai d'expiration de session	
 ID de la station appelée	
 Restrictions relatives aux jours et aux heures	
 Type de port NAS	

Précédent

Suivant

Terminer

Annuler

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

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 :
Tous ▼

Attributs :

Nom	▲
Acct-Interim-Interval	
Callback-Number	
Class	
Filter-Id	
Framed-AppleTalk-Link	
Framed-AppleTalk-Network	▼
<	>

Description :
Spécifie la durée de l'intervalle (en secondes) entre chaque mise à niveau intermédiaire envoyée par le serveur NAS.

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

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 les protocoles de tunnel utilisés.

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

On clique encore sur ajouter

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 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 :

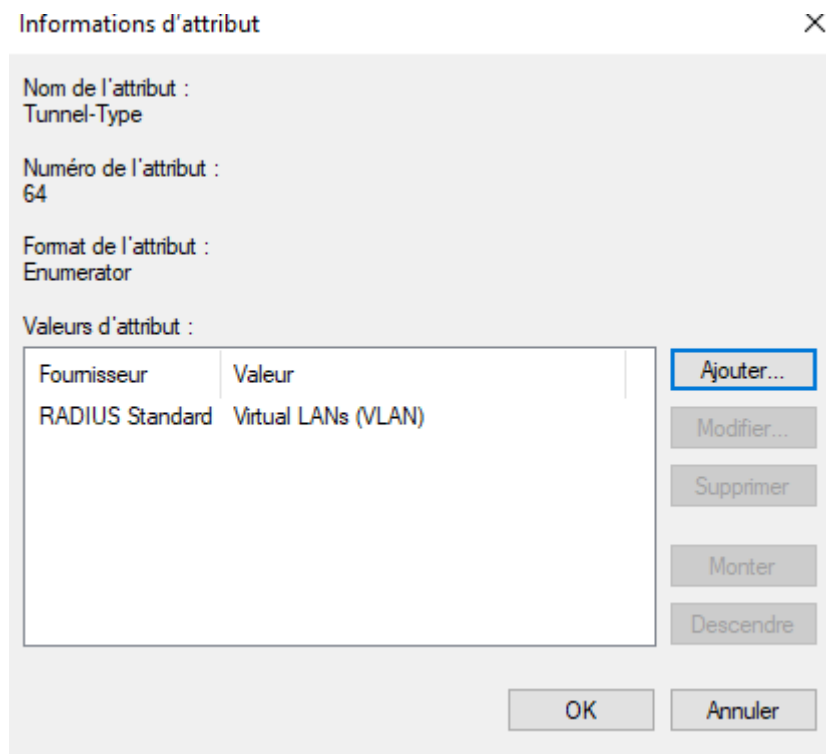
Communément utilisé pour les connexions d'accès à distance ou VPN
<Aucun>

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

Autres
<Aucun>

OK Annuler

Je clique sur OK



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

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

Je sélectionne 802,,,

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

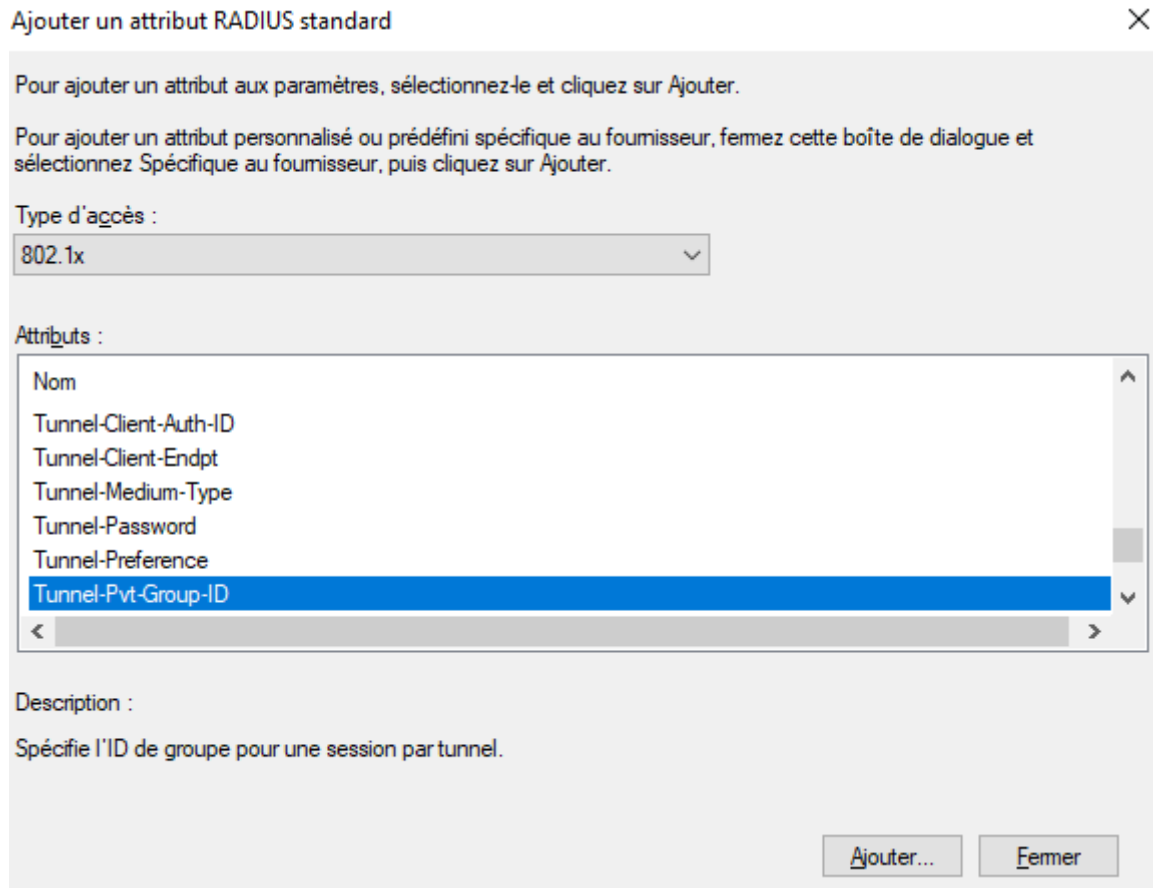
802 (includes all 802 media plus Ethernet canonical format)

Autres

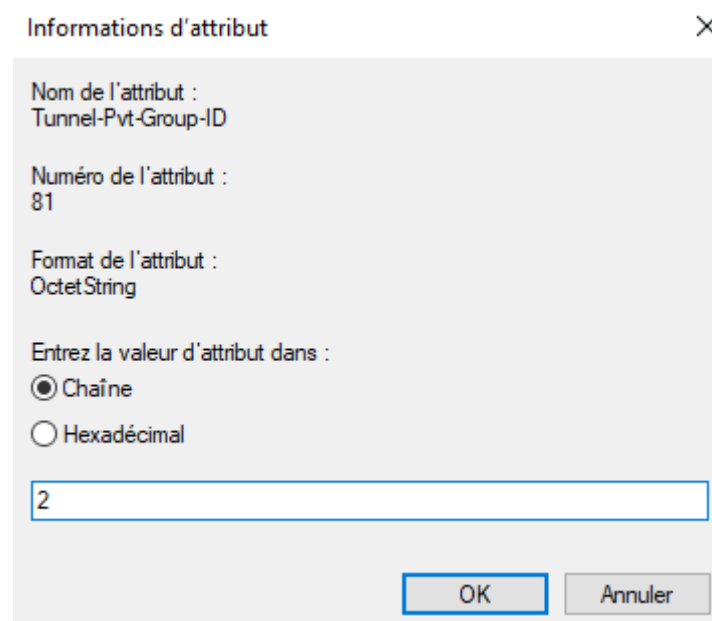
<Aucun>

OK Annuler

Je sélectionne ensuite tunnel-PVT-GROUP-ID



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



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

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 Ethemet canonical for...
Tunnel-Pvt-Group-ID	2

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 câbles 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 modifie...
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

J'ai mis en place sur le serveur NPS :

Une stratégie de demande de connexion associée aux connexions filaire Ethernet ;

Une stratégie d'accès réseau Ethernet 802.1x plaçant dans le VLAN2 les membres authentifiés comme faisant partie du groupe Prof

Précisant le groupe autorisé (Prof) ainsi que la stratégie de demande de connexion (NAS Ethernet) : notion de condition ;

Précisant la méthode d'authentification (PEAP/MSCHAPV2) : notion de contrainte ;

Précisant les paramètres renvoyés au client radius (VLAN) : notion d'attribut.

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

Propriétés de Strategie pour clients câbles 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

Propriétés de Strategie pour clients câbles 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


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


Contraintes :


Contraintes


 Méthodes d'authentification

 Délai d'inactivité

 Délai d'expiration de session

 ID de la station appelée

 Restrictions relatives aux jours et aux heures

 Type de port NAS

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

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

Types de protocoles EAP :

Microsoft: PEAP (Protected EAP)

Monter

Descendre

< >

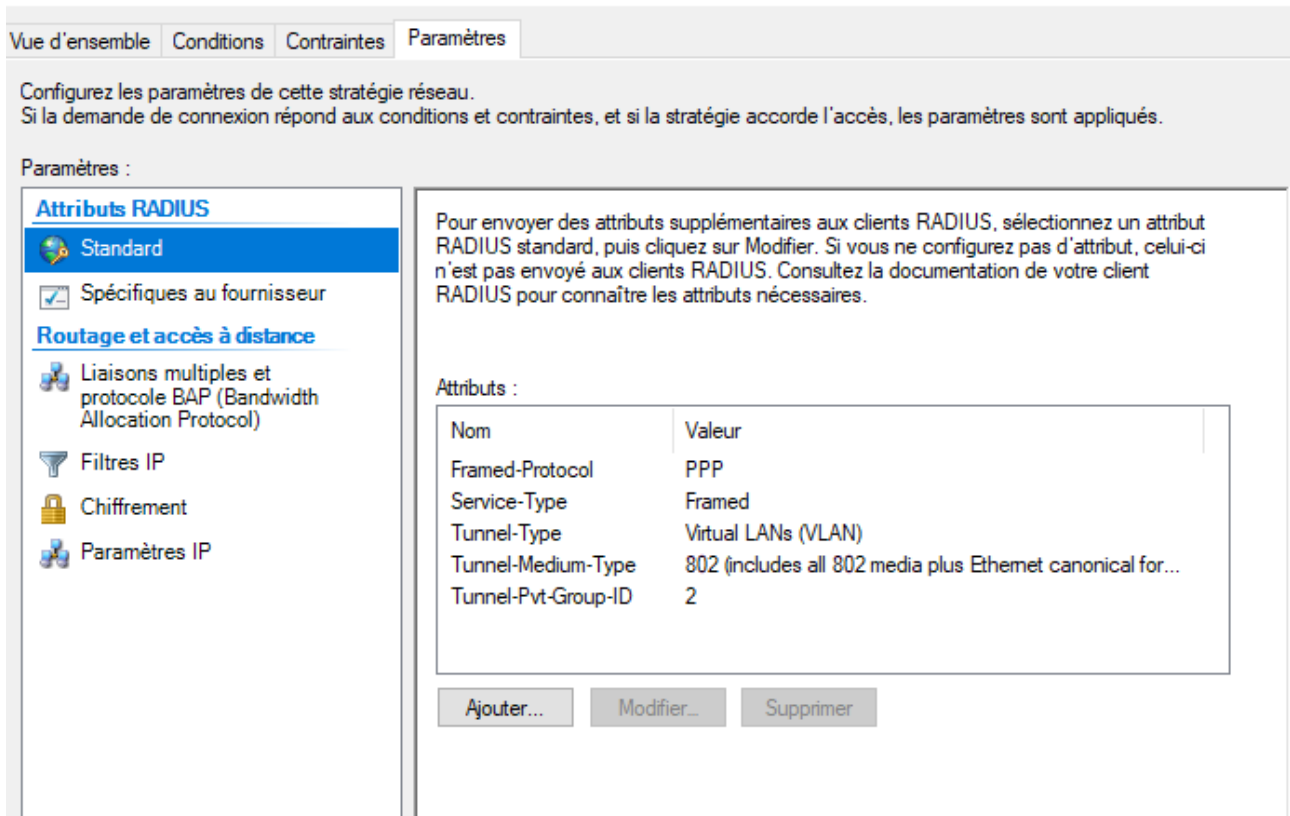
Ajouter...

Modifier...

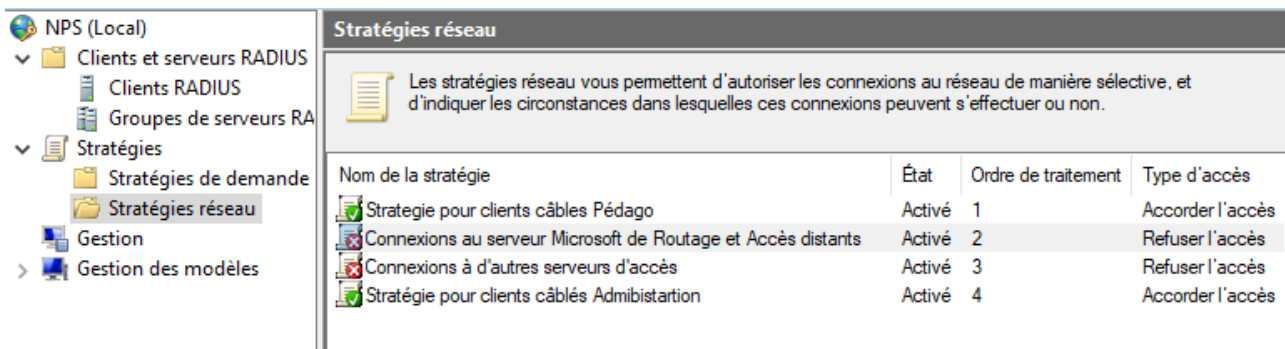
Supprimer

Méthodes d'authentification moins sécurisées :

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



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



REVOIR L'ORDRE DES SCREEN

Commutateur client Radius

```
S1>sh dot1x all summary
```

Interface	PAE	Client	Status
Fa0/7	AUTH	503e.aa03.6d5c	AUTHORIZED
Fa0/8	AUTH	none	UNAUTHORIZED

```
S1>
```

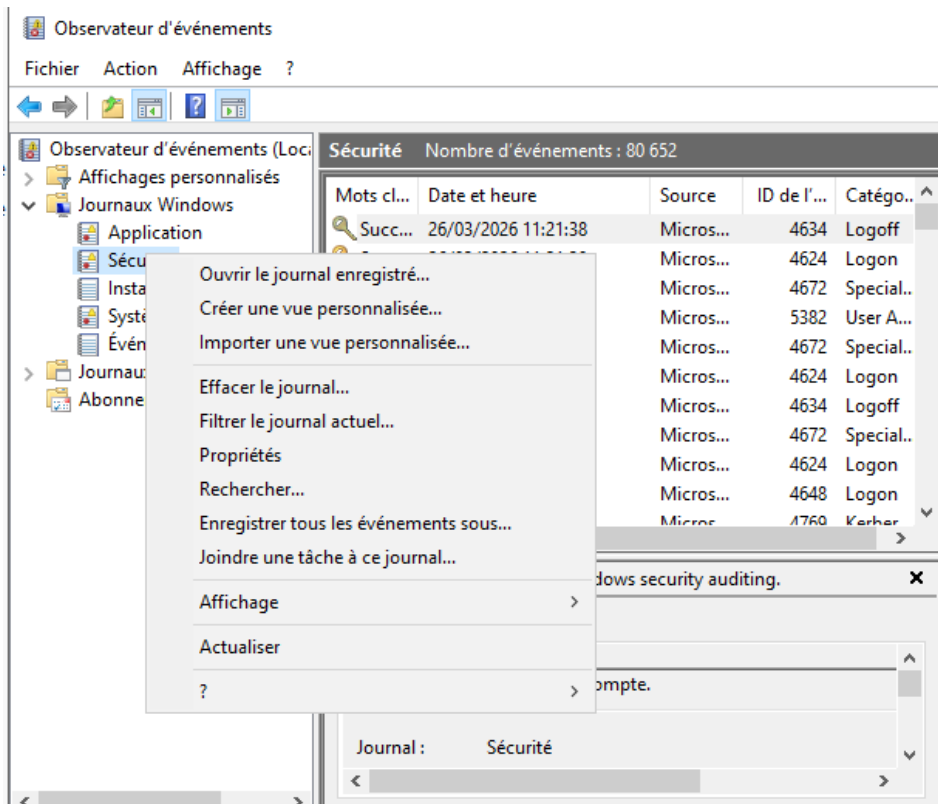
```

COM7 - PuTTY
-----
VLAN Name                Status    Ports
-----
1    default                active   Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                   Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                   Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                   Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                   Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                   Fa0/24, Gi0/1, Gi0/2
2    Pedagogie              active   Fa0/7
3    Administration          active
4    Serveurs                 active   Fa0/2
99   Gestion                  active
1002 fddi-default            act/unsup
1003 token-ring-default    act/unsup
1004 fddinet-default        act/unsup
1005 trnet-default          act/unsup

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

```

Exportation du fichier XML depuis l'AD



Filterer le journal actuel



XML

Connecté :

Niveau d'événement :
 Critique
 Avertissement
 Commentaires

 Erreur
 Information

Par journal
 Par source

Journaux d'événements :

Sources d'événements :

Inclut/exclut des ID d'événements : entrez les numéros ou les plages d'identificateurs en les séparant par des virgules. Pour exclure des critères, faites-les précéder du signe « moins ». Par exemple 1,3,5-99,-76

Catégorie de la tâche :

Mots clés :

Utilisateur :

Ordinateur(s) :

Mots cl...	Date et heure	Source	ID de l'...	Catégo...
Succ...	26/03/2026 11:04:06	Micros...	6272	Networ
Éche...	12/03/2026 11:26:41	Micros...	6273	
Éche...	12/03/2026 11:26:41	Micros...	6273	
Éche...	12/03/2026 11:26:41	Micros...	6273	

Ouvrir le journal ...

Créer une vue pe...

Propriétés de l'événement

Joindre une tâche à cet événement...

Copier >

Enregistrer les événements sélectionnés...

Actualiser

? >

Copier le tableau

Copier les détails au format texte

Enregistrer le fich...

Nom du journal :Security
Source : Microsoft-Windows-Security-Auditing
Date : 26/03/2026 11:04:06
ID de l'événement :6272
Catégorie de la tâche :Network Policy Server
Niveau : Information
Mots clés : Succès de l'audit
Utilisateur : N/A
Ordinateur : AD.sio-exupery.local
Description :
Le serveur NPS a accordé l'accès à un utilisateur.

Utilisateur :

ID de sécurité : SIO-EXUPERY\rveau
Nom de compte : rveau
Domaine de compte : SIO-EXUPERY
Nom de compte complet : sio-exupery.local/Professeurs/PROF/Régis Veau

Ordinateur client :

ID de sécurité : NULL SID
Nom de compte : -
Nom de compte complet : -
Identificateur de la station appelée : 00-08-2F-F7-8C-87
Identificateur de la station appelante : 50-3E-AA-03-6D-5C

Serveur NAS :

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

Client RADIUS :

Nom convivial du client : Client-Cisco2960
Adresse IP du client : 192.168.0.2

Informations détaillées sur l'authentification :

Nom de stratégie de demande de connexion : Connexion câblée
Nom de stratégie réseau : Strategie pour clients câbles Pédago
Fournisseur d'authentification : Windows
Serveur d'authentification : AD.sio-exupery.local
Type d'authentification : PEAP
Type EAP : Microsoft: Mot de passe sécurisé (EAP-MSCHAP version 2)
Identificateur de la session du compte : -

Résultats de la journalisation :
inscrites dans le fichier journal local.

Les informations de suivi ont été

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

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

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

Capture en cours de Ethernet

Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

radius

No.	Time	Source	Destination	Protocol	Length	Info
75	48.616877	192.168.0.2	192.168.1.50	RADIUS	282	Access-Request id=31
76	48.619412	192.168.1.50	192.168.0.2	RADIUS	132	Access-Challenge id=31
77	48.626054	192.168.0.2	192.168.1.50	RADIUS	514	Access-Request id=32
78	48.626464	192.168.1.50	192.168.0.2	RADIUS	277	Access-Challenge id=32
79	48.635258	192.168.0.2	192.168.1.50	RADIUS	371	Access-Request id=33

> Frame 75: 282 bytes on wire (2256 bits), 282 bytes captured (2256 bits) on interface \Device\NPF_{03A08334-0770} < >

> Ethernet II, Src: Cisco_08:08:07:50 (44:03:a7:08:07:50), Dst: PCSSystemtec_f7:4e:f7 (08:00:27:f7:4e:f7)

> Internet Protocol Version 4, Src: 192.168.0.2, Dst: 192.168.1.50

> User Datagram Protocol, Src Port: 1645, Dst Port: 1812

▼ RADIUS Protocol

- Code: Access-Request (1)
- Packet identifier: 0x1f (31)
- Length: 240
- Authenticator: 589874dd8afdd7b6ecd702a8314c4ad6
- ▼ Attribute Value Pairs
 - > AVP: t=User-Name(1) l=7 val=rveau
 - > 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-F7-8C-87
 - > AVP: t=Calling-Station-Id(31) l=19 val=50-3E-AA-03-6D-5C
 - ▼ AVP: t=EAP-Message(79) l=12 Last Segment[1]
 - Type: 79
 - Length: 12
 - EAP fragment: 0201000a017276656175
 - ▼ Extensible Authentication Protocol
 - Code: Response (2)
 - Id: 1
 - Length: 10
 - Type: Identity (1)
 - Identity: rveau
 - > AVP: t=Message-Authenticator(80) l=18 val=5f7c7555dcfba2a3e6555131dc114d40
 - > AVP: t=EAP-Key-Name(102) l=2 val=[wrong length]
 - > AVP: t=Vendor-Specific(26) l=49 vnd=ciscoSystems(9)
 - > AVP: t=Vendor-Specific(26) l=20 vnd=ciscoSystems(9)
 - > AVP: t=NAS-IP-Address(4) l=6 val=192.168.0.2
 - > AVP: t=NAS-Port-Id(87) l=17 val=FastEthernet0/7
 - > AVP: t=NAS-Port-Type(61) l=6 val=Ethernet(15)
 - > AVP: t=NAS-Port(5) l=6 val=50107

