

Installation NPS

Installer le rôle NPS en vous référant aux captures d'écran.

Assistant Ajout de rôles et de fonctionnalités

Sélectionner le serveur de destination

SERVEUR DE DESTINATION
srv-dc-grp1.saveol.local

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

Services de stratégie et d'...

Confirmation

Résultats

Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et des fonctionnalités.

Sélectionner un serveur du pool de serveurs

Sélectionner un disque dur virtuel

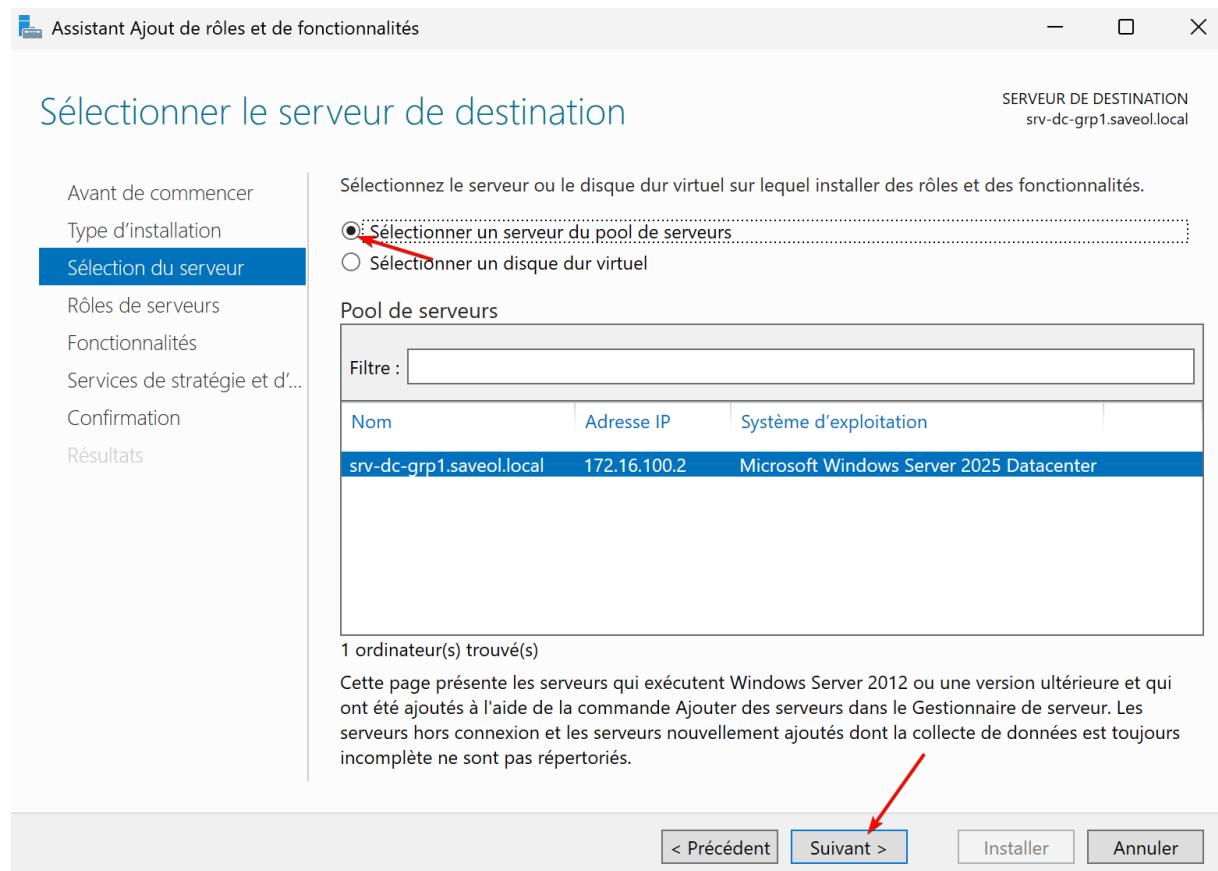
Pool de serveurs

Filtre :		
Nom	Adresse IP	Système d'exploitation
srv-dc-grp1.saveol.local	172.16.100.2	Microsoft Windows Server 2025 Datacenter

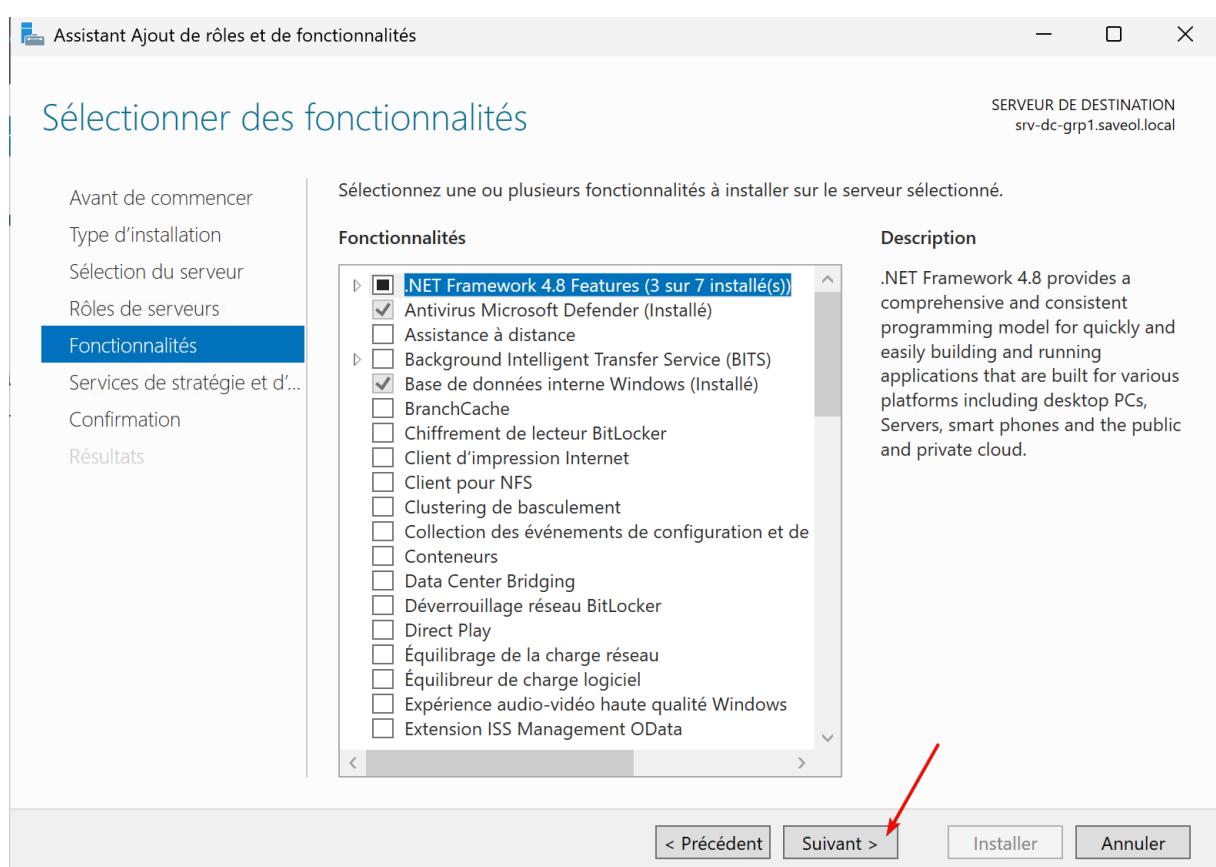
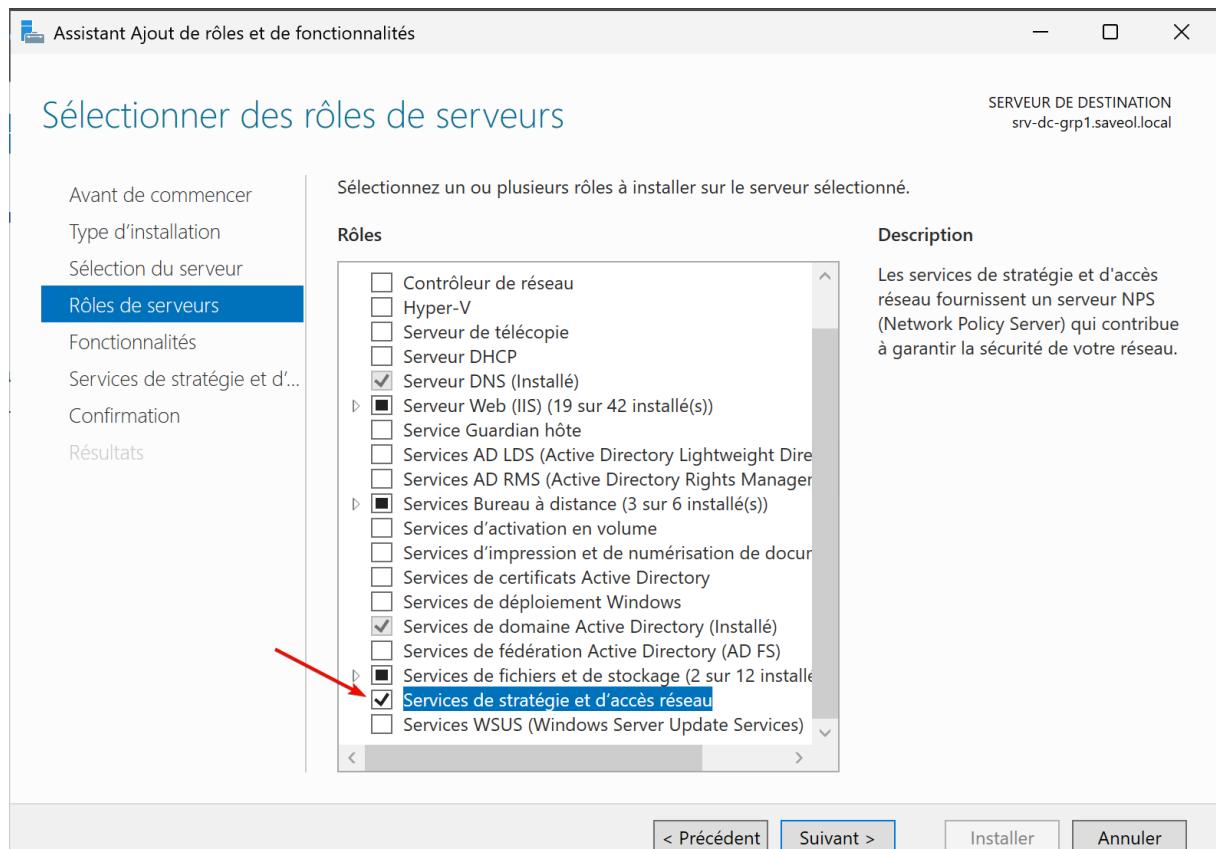
1 ordinateur(s) trouvé(s)

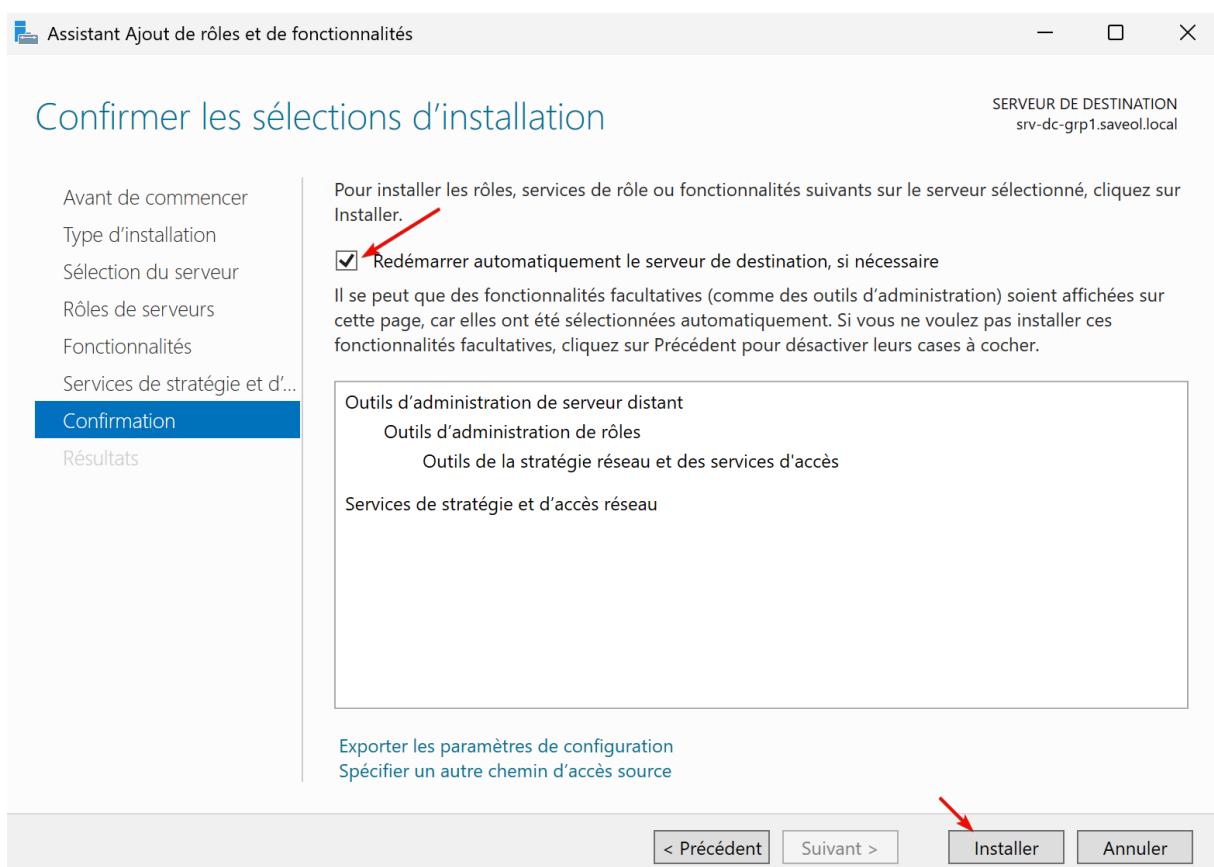
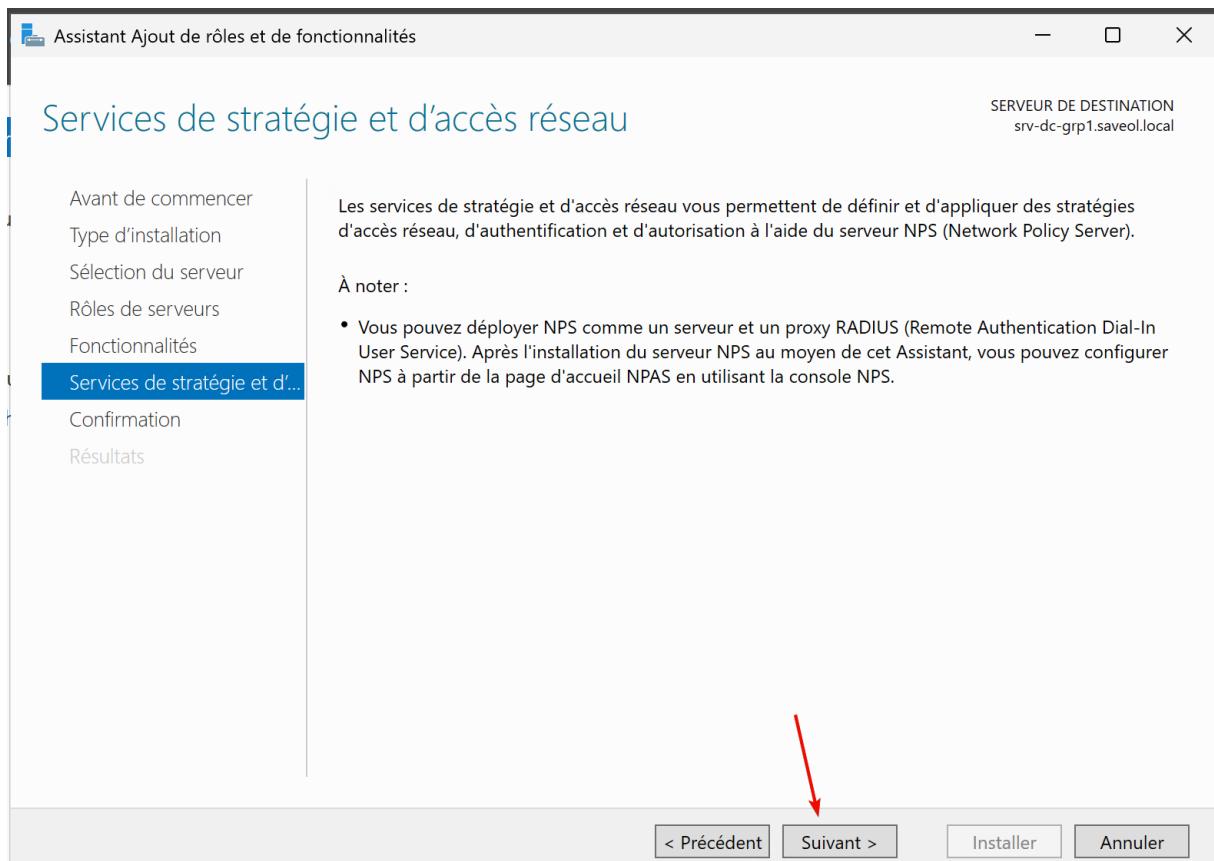
Cette page présente les serveurs qui exécutent Windows Server 2012 ou une version ultérieure et qui ont été ajoutés à l'aide de la commande Ajouter des serveurs dans le Gestionnaire de serveur. Les serveurs hors connexion et les serveurs nouvellement ajoutés dont la collecte de données est toujours incomplète ne sont pas répertoriés.

< Précédent **Suivant >** Installer Annuler



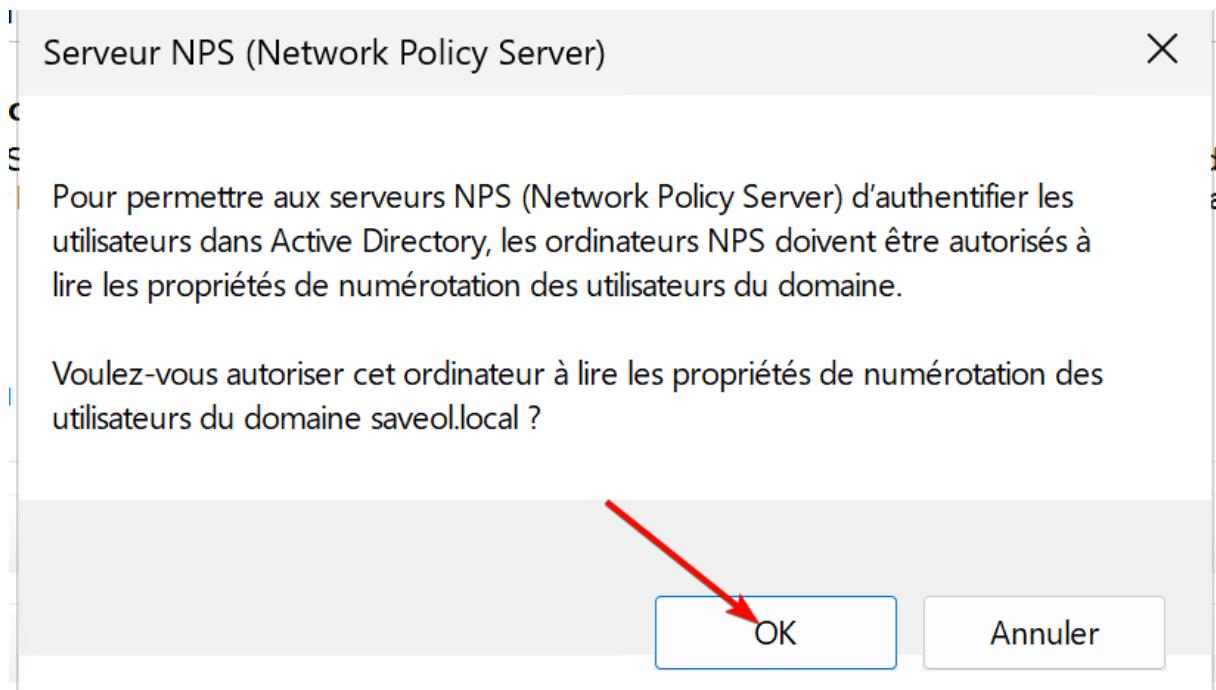
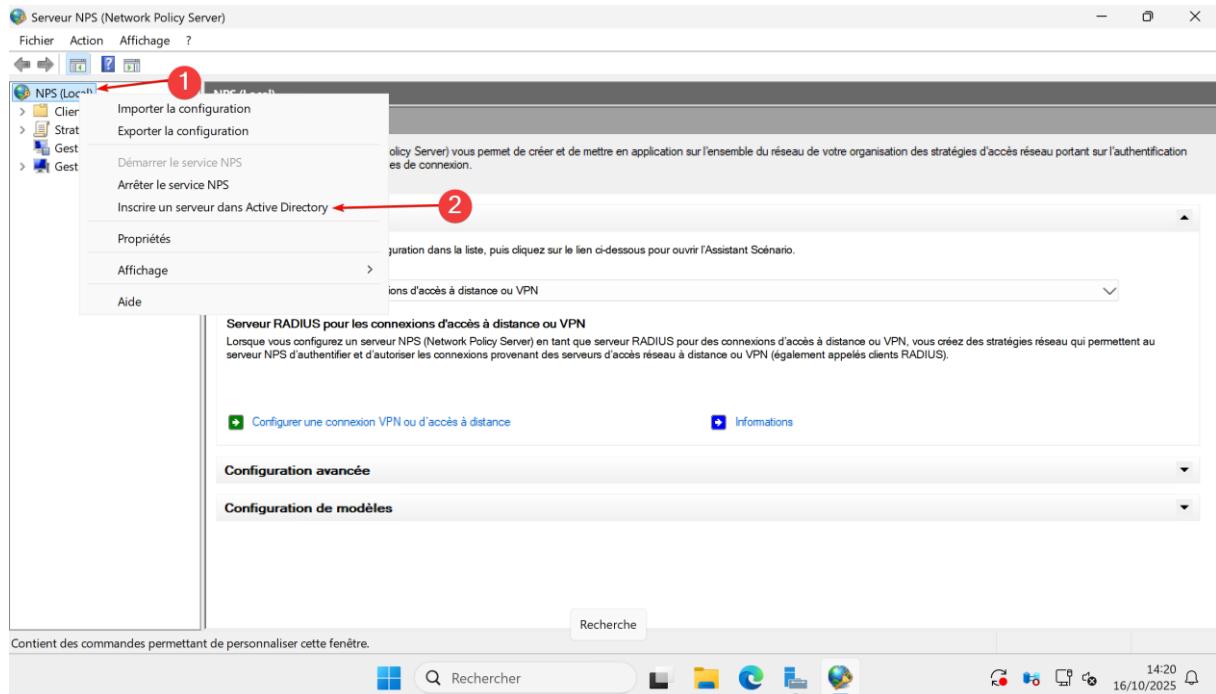
Nom	Adresse IP	Système d'exploitation
srv-dc-grp1.saveol.local	172.16.100.2	Microsoft Windows Server 2025 Datacenter





Enregistrer NPS dans Active Directory

Une fois cela fait lier le serveur NPS a l'active directory



Serveur NPS (Network Policy Server)

X

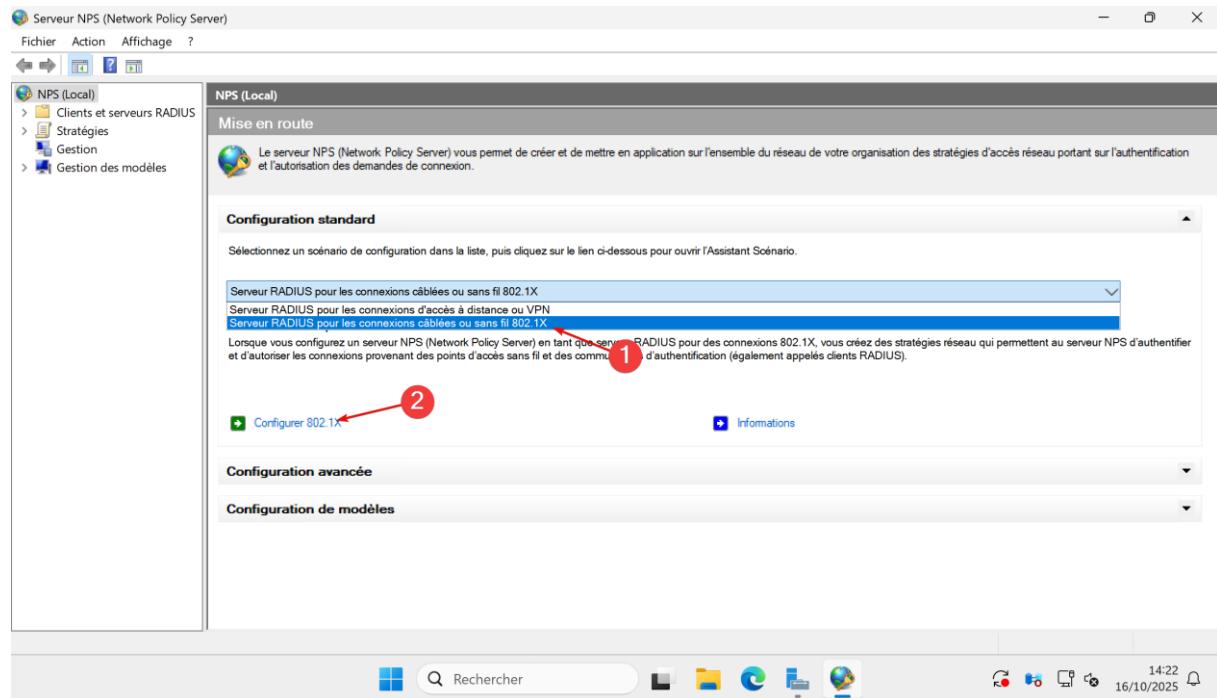
Cet ordinateur est désormais autorisé à lire les propriétés de numérotation des utilisateurs du domaine saveol.local.

Pour autoriser cet ordinateur à lire les propriétés de numérotation des utilisateurs d'autres domaines, vous devez l'inscrire en tant que membre du groupe de serveurs RAS/NPS dans les domaines concernés.

OK

Création des clients RADIUS

Une fois cela fait il faut créer une configuration pour que les équipements puissent se connecter



Faire comme la configuration du switch SW_2^E pour tous les équipements de l'infra
En définissant :

- le nom de l'appareil
- l'adresse IP de l'équipement
- defnir le mot de passe

Nouveau client RADIUS



Paramètres

Sélectionner un modèle existant :

Nom et adresse

Nom convivial :

SW_2E

Adresse (IP ou DNS) :

172.16.70.251

Vérifier...

Secret partagé

Sélectionnez un modèle de secrets partagés existant :

Aucun



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

Manuel

Générer

Secret partagé :

Confirmez le secret partagé :

*****|

OK

Annuler



Spécifier les commutateurs 802.1X

Spécifiez les commutateurs ou points d'accès sans fil 802.1X (clients RADIUS)

Les clients RADIUS sont des serveurs d'accès réseau, à l'image des commutateurs d'authentification. Les clients RADIUS ne sont pas des ordinateurs clients.

Pour spécifier un client RADIUS, cliquez sur Ajouter.

Clients RADIUS :

SWRC	RNET1
SW_1E	RNET2
SW_2E	
SWCOEUR	
ZYXEL	
SW_DMZ_INTERMEDIAIRE	
SW_DMZ_INTERNE	
SWNET	

Ajouter...

Modifier...

Supprimer

Précédent

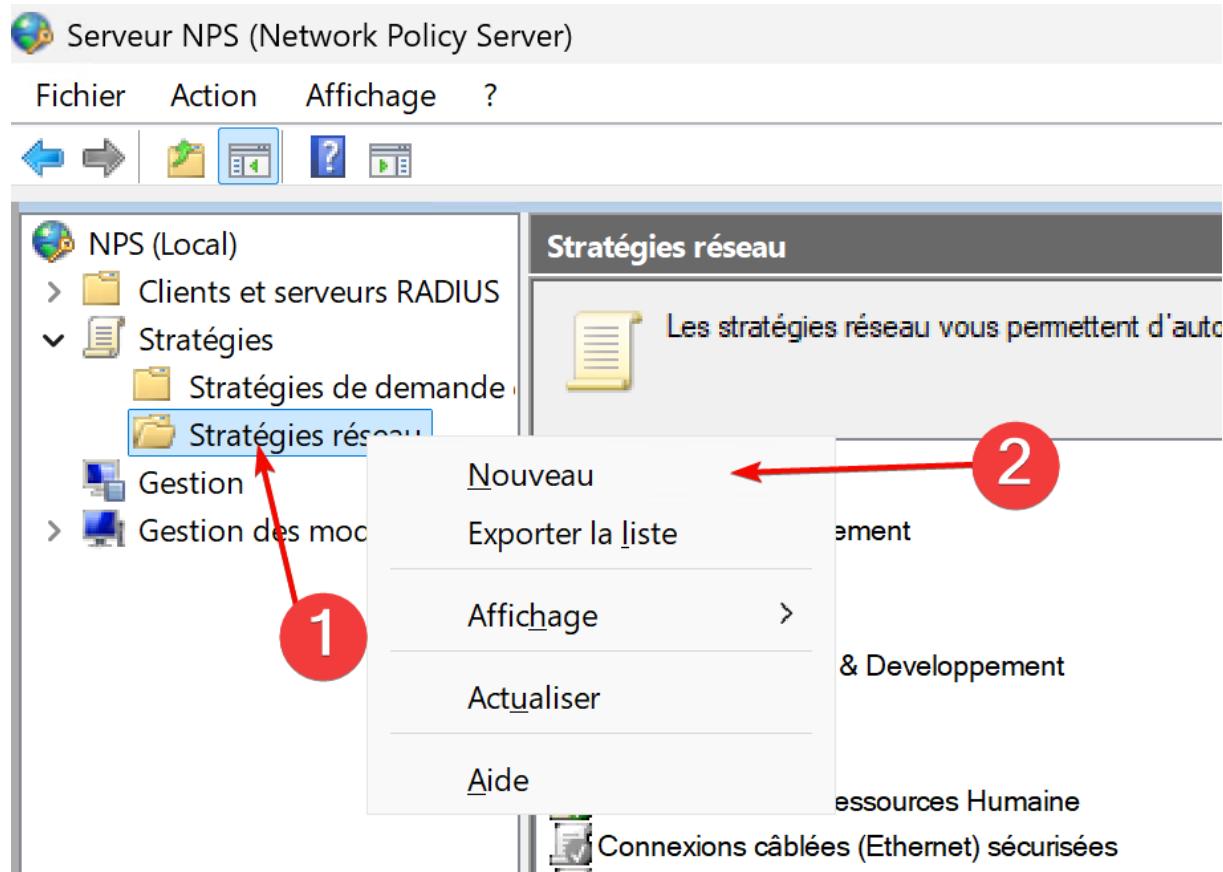
Suivant

Terminer

Annuler

Configuration des Stratégies réseaux

Faites un clic droit sur : Stratégies réseau -> Nouveau



Nommé la stratégie en fonction du VLAN à assigner pour ma part « Service IT », puis laisser le type de serveur d'accès réseau dans « non spécifier », cliquer sur suivant

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 :

Service IT

1

Méthode de connexion réseau

Selectionnez 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

2

 Spécifique au fournisseur :

10

3

Précédent

Suivant

Terminer

Annuler

Sélectionne le groupe d'utilisateur -> Ajouter -> sélectionner le groupe des user -> ok
-> suivant

Spécifier les conditions

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

Selectionner une condition X

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).

2

Ajouter...

Annuler

1

Ajouter...

Modifier...

Supprimer

Précédent

Suivant

Terminer

Annuler

Groupes d'utilisateurs

X

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

Groupes

SAVEOL\Admins du domaine

2

1

Ajouter des groupes...

Supprim

3

OK

Annuler

Sélectionner « accès accordé » -> Suivant

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.

1

 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.

2

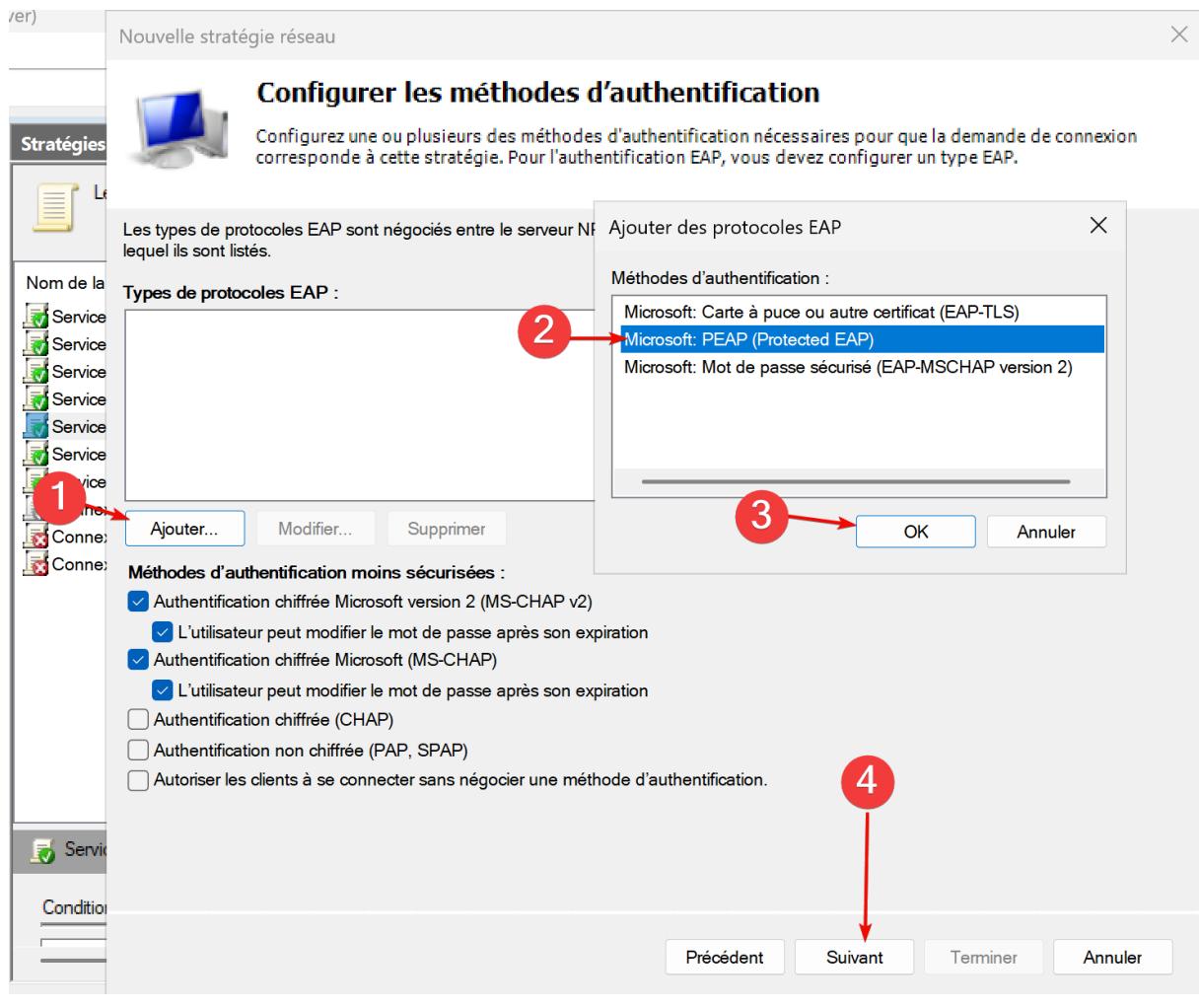
Précédent

Suivant

Terminer

Annuler

Sélectionnez Ajouter -> sélectionnez le protocole PEAP -> ok -> suivant



Aller dans « Type de port NAS » -> Cocher la case « Ethernet » -> 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
- Délai d'expiration de session
- ID de la station appelée
- Rest. de temps relatives aux jours et aux heures 1
- Type de port NAS

Spécifier 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 2
- 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

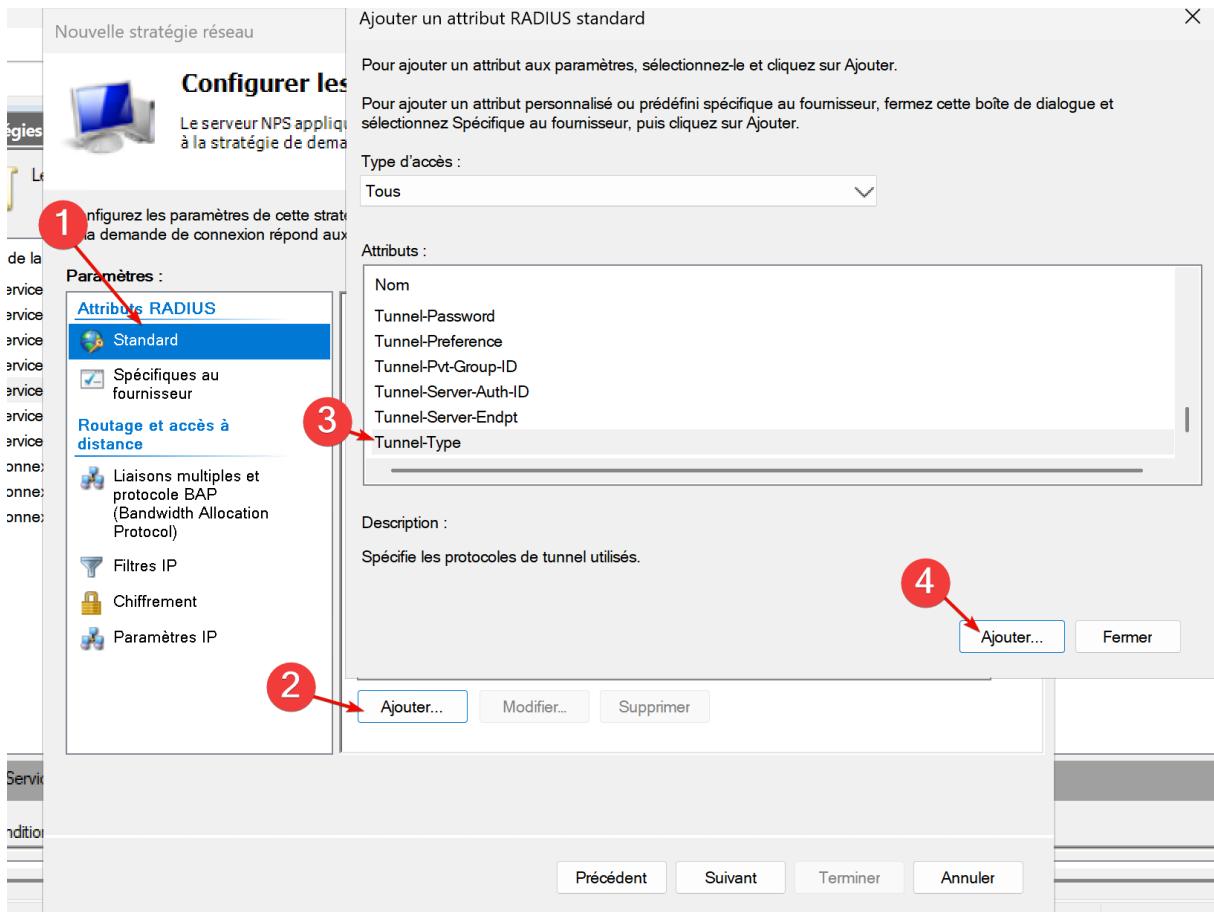
Précédent

Suivant 3

Terminer

Annuler

Cliquer sur attributs radius -> Ajouter -> Tunnel-Type -> Ajouter -> Sélectionner « communément utilisé pour les connexions 802.1X » -> Selectionner « VLAN » -> OK



Informations d'attribut

X

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>

1

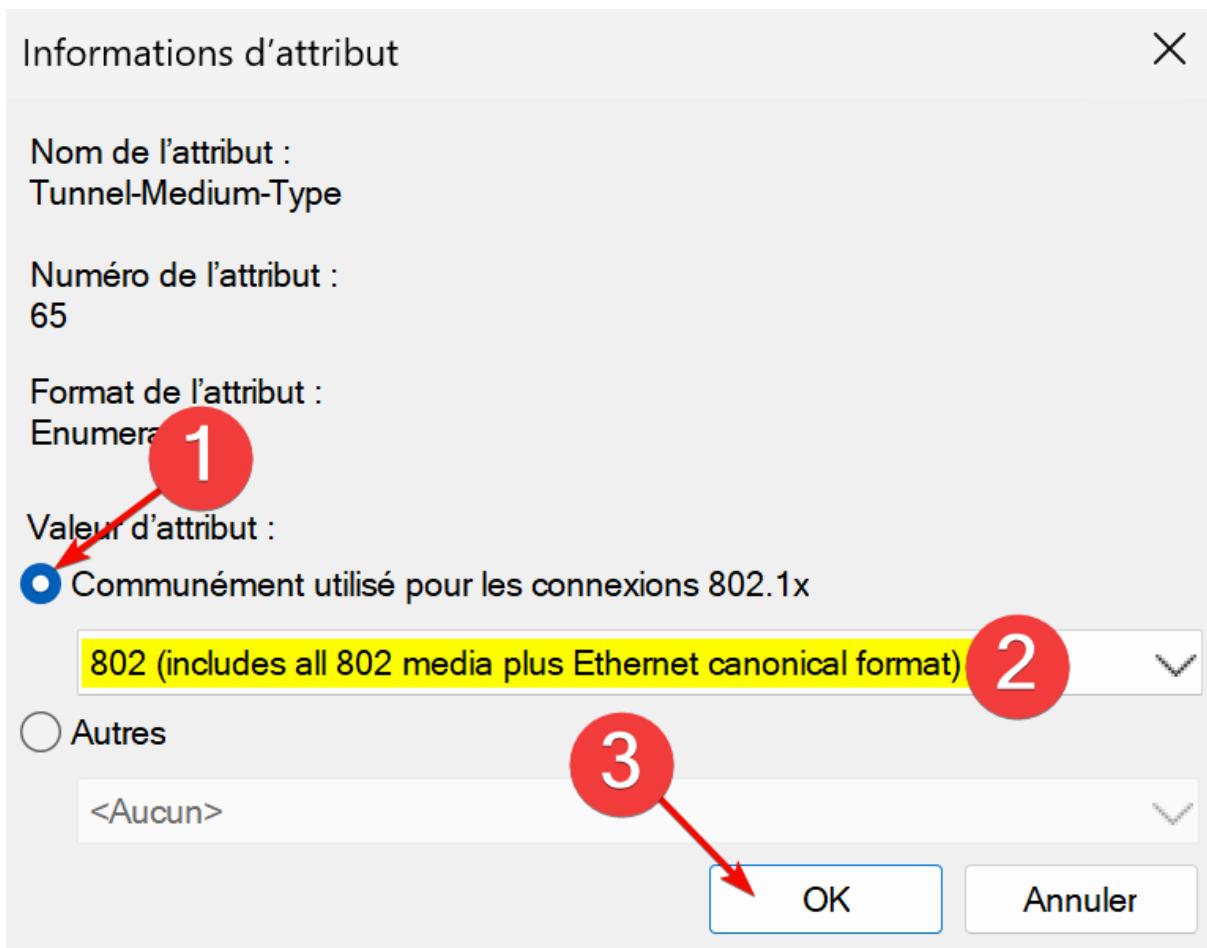
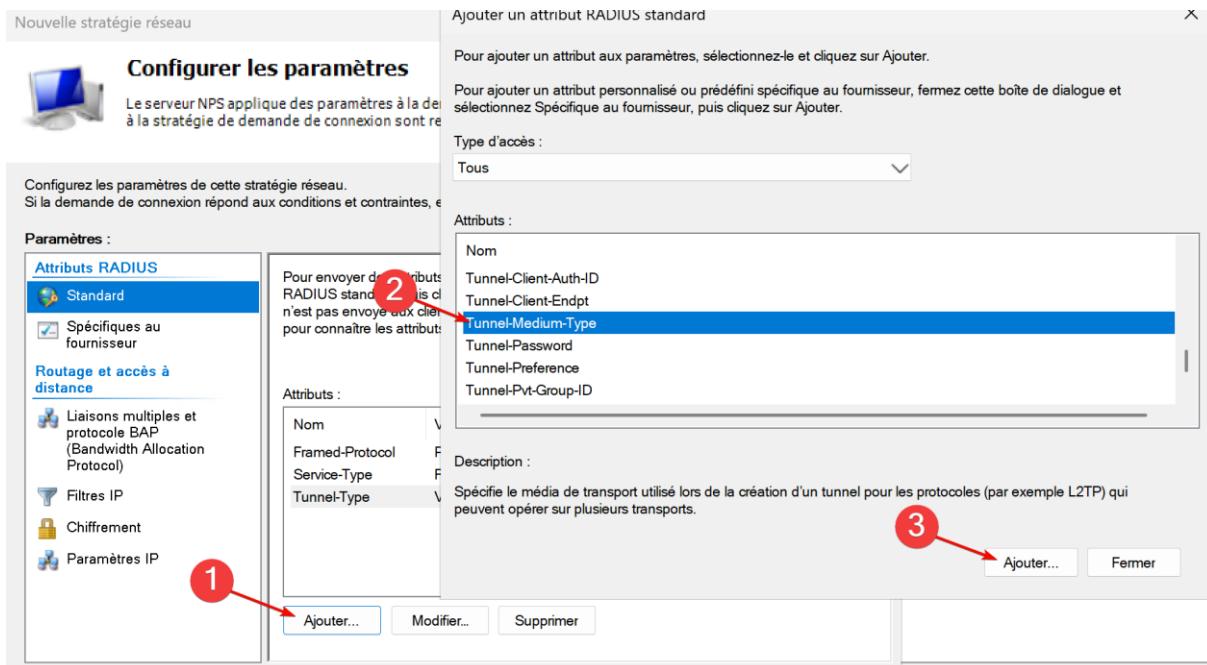
2

3

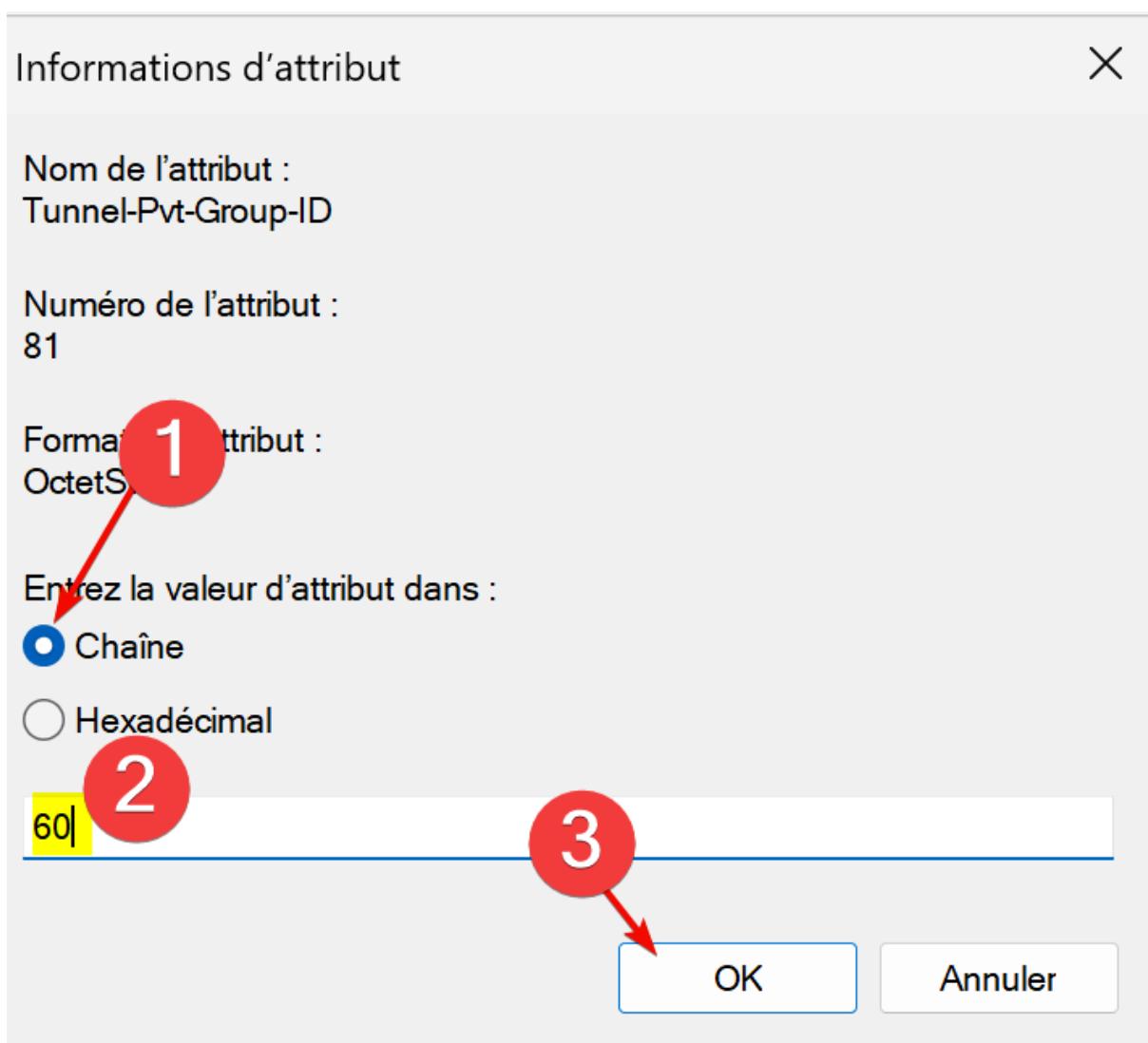
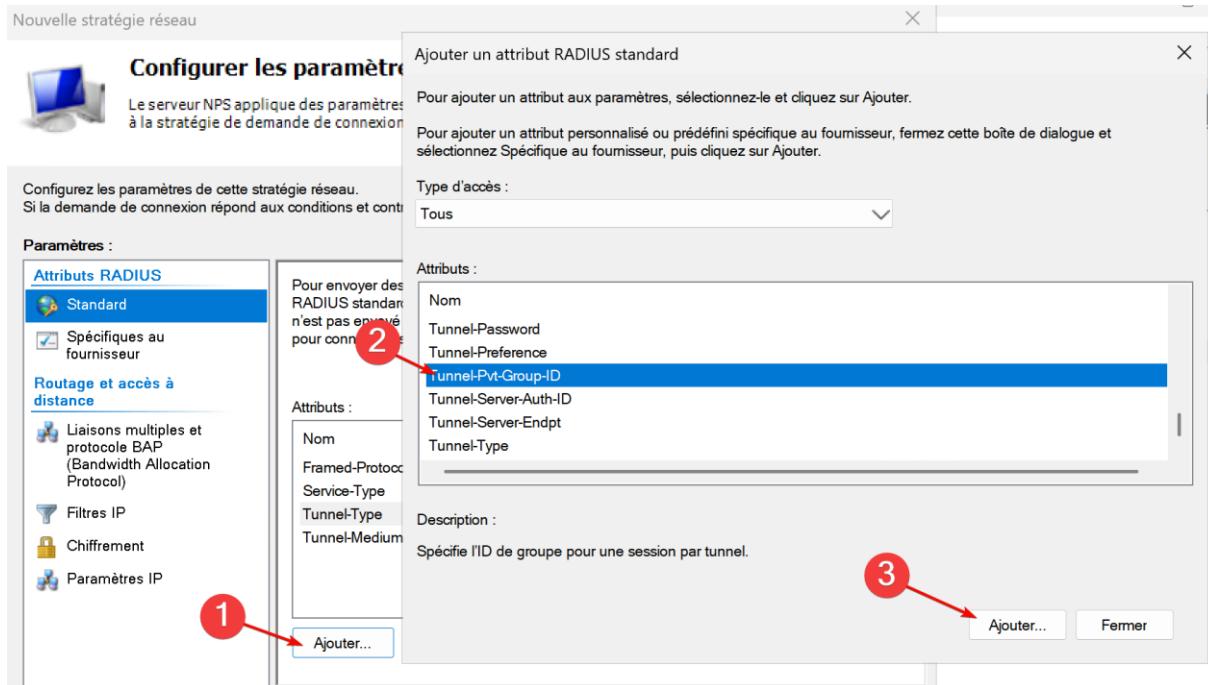
OK

Annuler

Cliquer sur attributs radius -> Ajouter -> Tunnel-Medium-Type -> Ajouter -> Sélectionner « communément utilisé pour les connexions 802.1X » -> Sélectionner « 802 » -> OK



Cliquer sur attributs radius -> Ajouter -> Tunel-Pvt-Groupe-ID -> Ajouter -> Sélectionner « chaîne » -> rentré le numéro du vlan -> OK



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** (Sélectionné)
- 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	60

1

Ajouter... Modifier... Supprimer

Précédent **Suivant** Terminer Annuler

2

Cliquer sur attributs radius -> Vérifier que la configuration soit identique au screen -> Suivant -> Terminer

Nouvelle stratégie réseau

Fin de la configuration de la nouvelle stratégie réseau



Vous avez correctement créé la stratégie réseau suivante :

Service IT.

Conditions de la stratégie :

Condition	Valeur
Groupes d'utilisateurs	SAVEOL\Admins du domaine

Paramètres de la stratégie :

Condition	Valeur
Type de port NAS	Ethernet
Tunnel-Type	Virtual LANs (VLAN)
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical format)
Tunnel-Pvt-Group-ID	60
Pourcentage de capacité du protocole BAP	Réduisez les liaisons multiples si le serveur atteint 50% pour 2 minutes

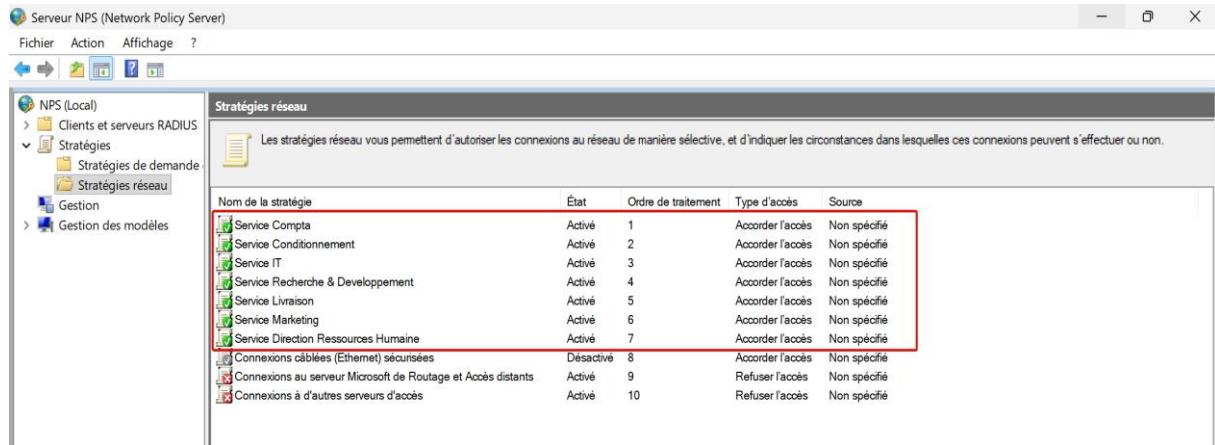
Pour fermer cet Assistant, cliquez sur Terminer.



Précédent Suivant **Terminer** Annuler

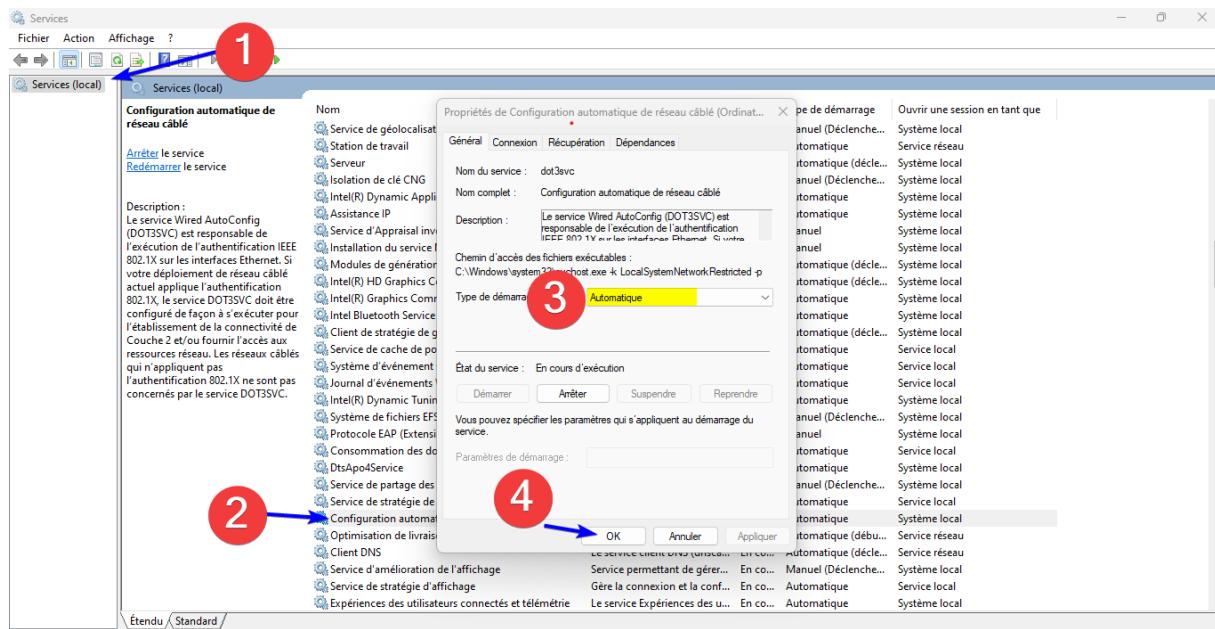
Reproduisez la stratégie réseau en ajustant les paramètres du groupe et le numéro du VLAN pour chaque stratégie, en vous basant sur les informations du tableau.

Nom de la stratégie	Nom du groupe	Numéro du vlan
Service Compta	Comptabilité	10
Service Marketing	Marketing	20
Service Conditionnement	Conditionnement	30
Service Livraison	Livraison	40
Service R&D	Recherche	50
Service IT	Admins du domaine	60
Service Direction RH	Direction	80



Paramétrage du 802.1X sur le PC client

Ouvrir « Service » -> cliquer sur « Configuration de configuration automatique de réseau câblé » -> sélectionner comme type de démarrage « Automatique » -> cliquer sur « ok »



Configuration des switches

Configuration des switches :

```
(config)#aaa new-model
(config)#aaa authentication dot1x default group RADIUS
(config)#aaa authorization network default group RADIUS
(config)#dot1x system-auth-control
```

```
(config)#RADIUS-server host 172.16.100.2 auth-port 1645 acct-port 1646 key admin
(config)#RADIUS-server host 172.16.100.2 auth-port 1812 acct-port 1813 key admin
```

```
aaa group server radius DC1
  server 172.16.100.2 auth-port 1645 acct-port 1646
!
aaa authentication dot1x default group radius
aaa authorization network default group radius
!
```

Configuration des ports du switch :

```
interface FastEthernet0/1
  switchport mode access
  authentication host-mode multi-host
  authentication port-control auto
  dot1x pae authenticator
  spanning-tree portfast trunk
!
interface FastEthernet0/2
  switchport mode access
  authentication host-mode multi-host
  authentication port-control auto
  dot1x pae authenticator
  spanning-tree portfast trunk
!
interface FastEthernet0/3
  switchport mode access
  authentication host-mode multi-host
  authentication port-control auto
  dot1x pae authenticator
  spanning-tree portfast trunk
!
```

Configuration des switches pour mettre en place l'authentification en mode radius :

```
aaa new-model
aaa group server radius DC1

server 172.16.100.2 auth-port 1645 acct-port 1646
aaa authentication login default group radius local
aaa authentication dot1x default group radius
aaa authorization exec default group radius local

aaa authorization network default group radius
dot1x system-auth-control
radius-server host 172.16.100.2 auth-port 1645 acct-port 1646 key admin
radius-server host 172.16.100.2 auth-port 1812 acct-port 1813 key admin
```