

Installation NPS

Objectif :

Installation et configuration d'un serveur RADIUS

Réalisation :

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

Assistant Ajout de rôles et de fonctionnalités

Sélectionner des rôles de serveurs

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 un ou plusieurs rôles à installer sur le serveur sélectionné.

Rôles

☐ Contrôleur de réseau
☐ Hyper-V
☐ Serveur de télécopie
☐ Serveur DHCP
☒ Serveur DNS (Installé)
☒ Serveur Web (IIS) (19 sur 42 installé(s))
☐ Service Guardian hôte
☐ Services AD LDS (Active Directory Lightweight Dire
☐ Services AD RMS (Active Directory Rights Manager
☒ Services Bureau à distance (3 sur 6 installé(s))
☐ Services d'activation en volume
☐ Services d'impression et de numérisation de docur
☐ Services de certificats Active Directory
☐ Services de déploiement Windows
☒ Services de domaine Active Directory (Installé)
☐ Services de fédération Active Directory (AD FS)
☒ Services de fichiers et de stockage (2 sur 12 install
☒ Services de stratégie et d'accès réseau
☐ Services WSUS (Windows Server Update Services)

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

< Précédent

Suivant >

Installer

Annuler

Assistant Ajout de rôles et de fonctionnalités

Sélectionner des fonctionnalités

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 une ou plusieurs fonctionnalités à installer sur le serveur sélectionné.

Fonctionnalités

☒ .NET Framework 4.8 Features (3 sur 7 installé(s))
☒ Antivirus Microsoft Defender (Installé)
☐ Assistance à distance
☒ Background Intelligent Transfer Service (BITS)
☒ Base de données interne Windows (Installé)
☐ BranchCache
☐ Chiffrement de lecteur BitLocker
☐ Client d'impression Internet
☐ Client pour NFS
☐ Clustering de basculement
☐ Collection des événements de configuration et de
☐ Conteneurs
☐ Data Center Bridging
☐ Déverrouillage réseau BitLocker
☐ Direct Play
☐ Équilibrage de la charge réseau
☐ Équilibreur de charge logiciel
☐ Expérience audio-vidéo haute qualité Windows
☐ Extension ISS Management OData

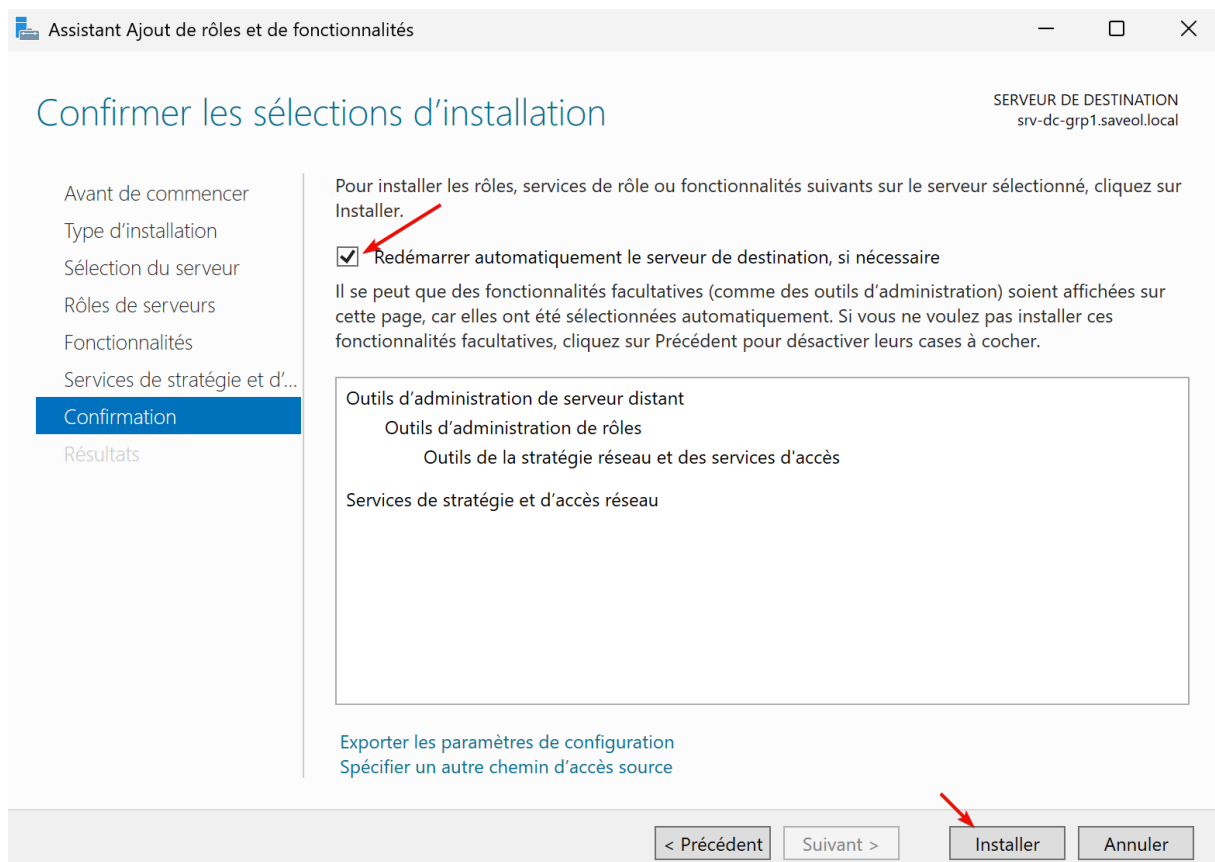
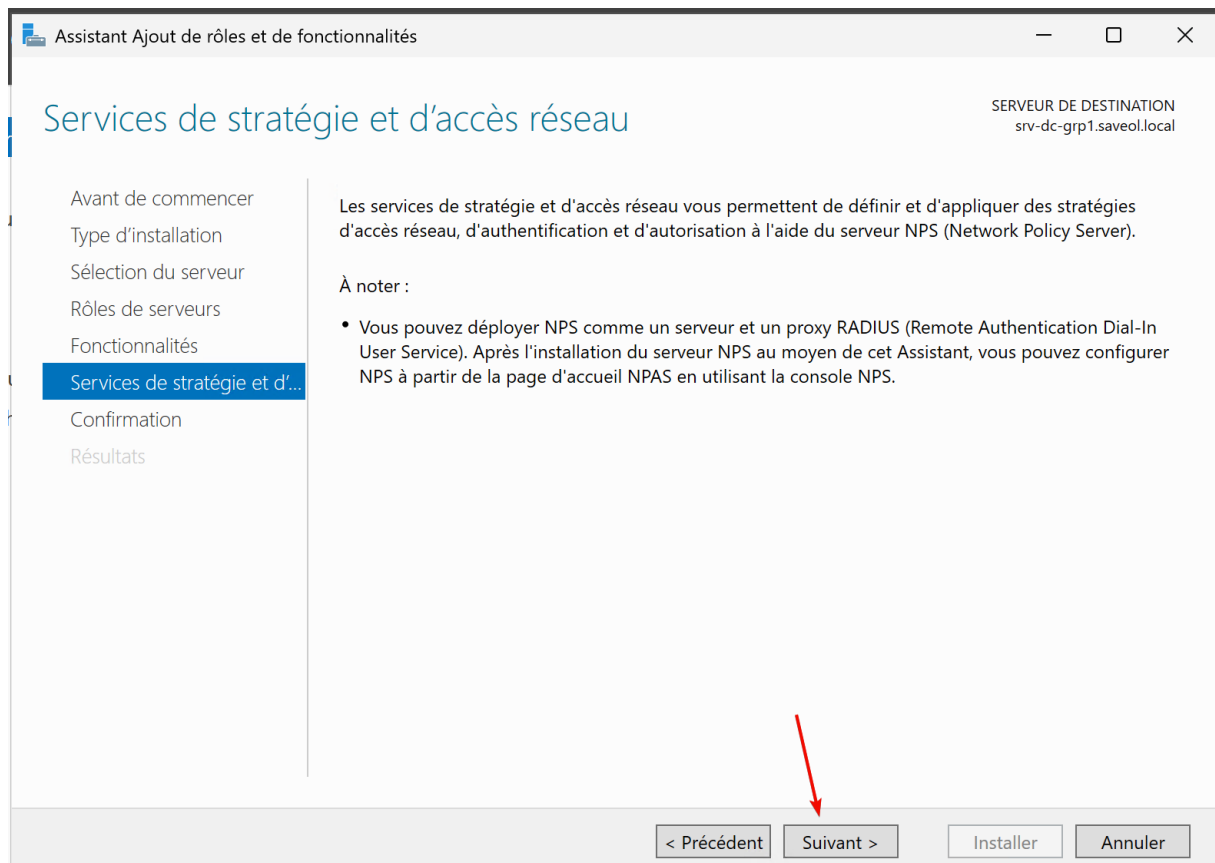
Description
.NET Framework 4.8 provides a comprehensive and consistent programming model for quickly and easily building and running applications that are built for various platforms including desktop PCs, Servers, smart phones and the public and private cloud.

< Précédent

Suivant >

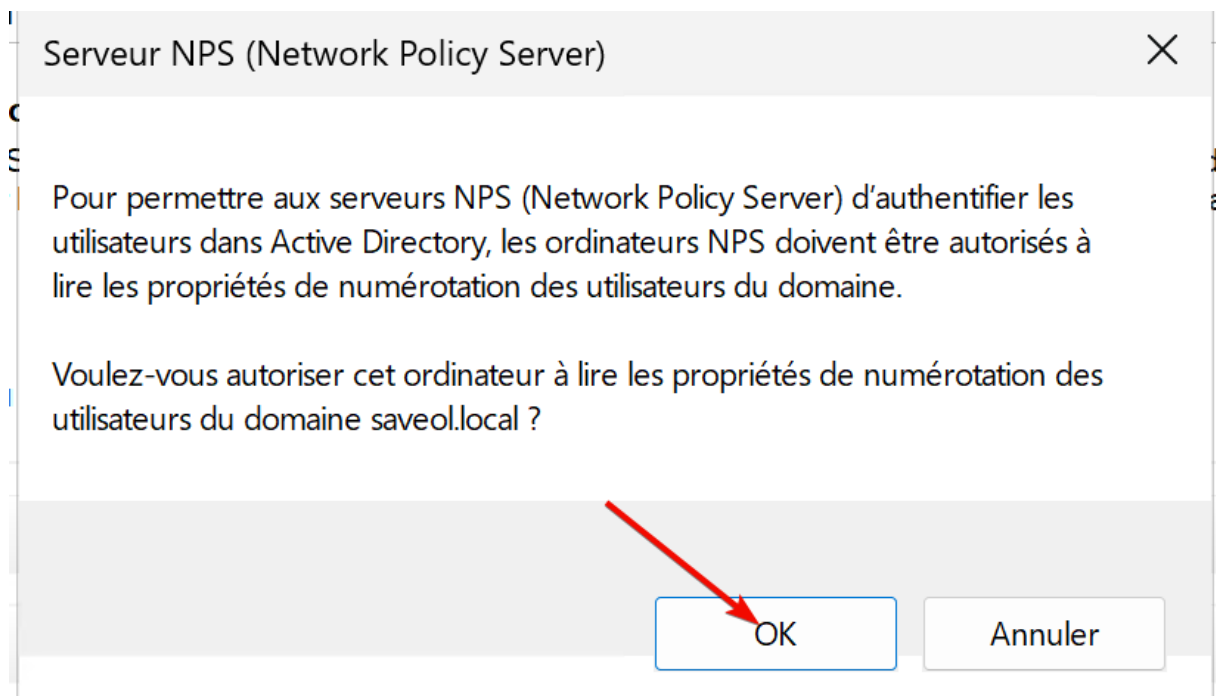
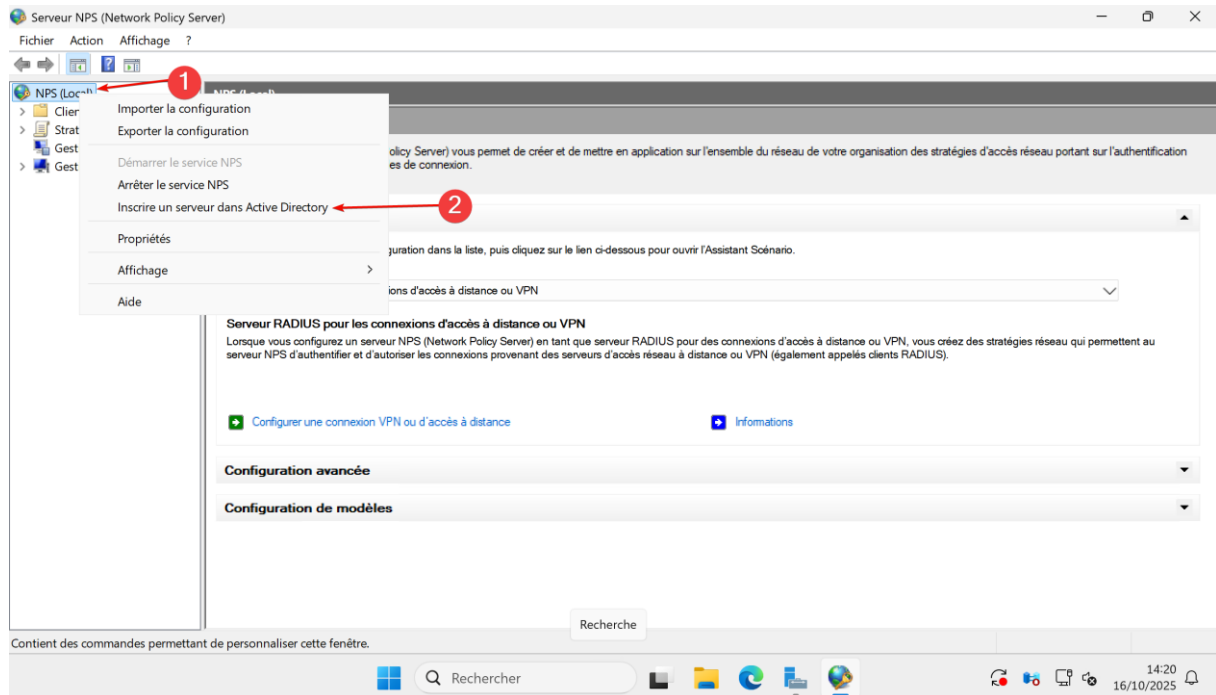
Installer

Annuler



Enregistrer NPS dans Active Directory

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



Serveur NPS (Network Policy Server)

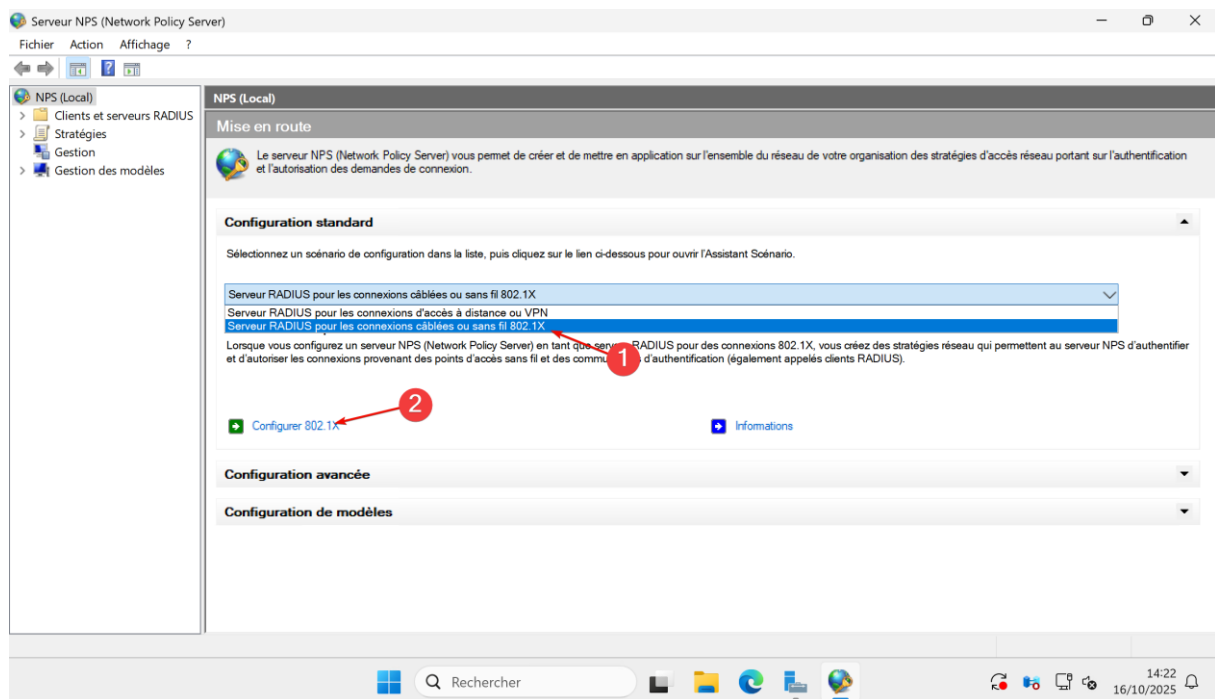
Cet ordinateur est désormais autorisé à lire les propriétés de numérotation des utilisateurs du domaine saveol.local.

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
- définir le mot de passe

Nouveau client RADIUS



Paramètres

☐ Sélectionner un modèle existant :

Nom et adresse

Nom convivial :

Adresse (IP ou DNS) :

Vérifier...

Secret partagé

Sélectionnez un modèle de secrets partagés existant :

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

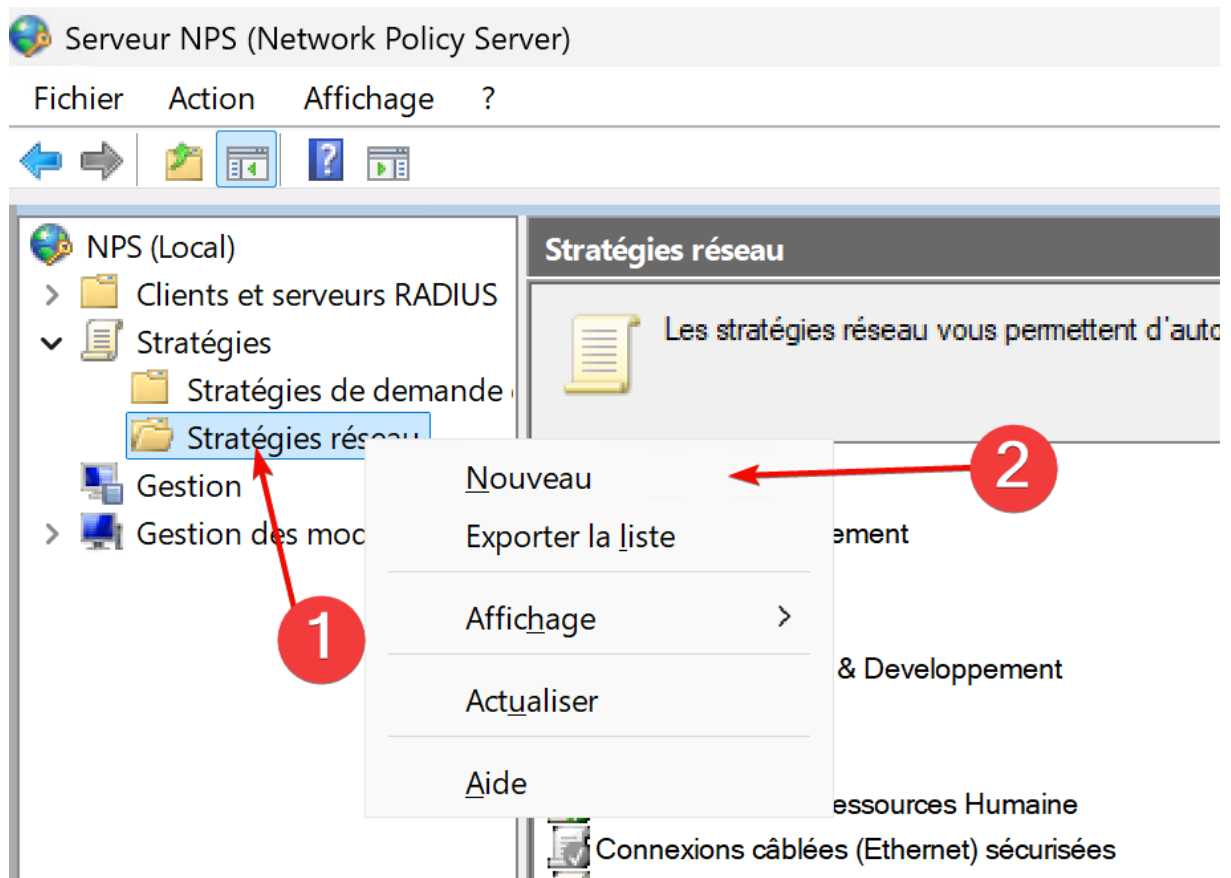
Suivant

Terminer

Annuler

Configuration des Stratégies réseaux

Faite un clique 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

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

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

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 auxquelles les tentatives de connexion sont autorisées ou non. Ces restrictions sont basées sur le fuseau horaire du serveur NPS (Network Policy Server).

Ajouter...

Annuler

1

Ajouter...

Modifier...

Supprimer

Précédent

Suivant

Terminer

Annuler

Groupes d'utilisateurs



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

Groupes

SAVEOL\Admins du domaine

2

1

Ajouter des groupes...

Supprimer

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.

☒ Accès accordé

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

☐ Accès refusé

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

☐ L'accès est déterminé par les propriétés de numérotation des utilisateurs (qui remplacent la stratégie NPS)

Choisissez selon les propriétés de numérotation utilisateur si les tentatives de connexion des clients répondent aux conditions de la stratégie

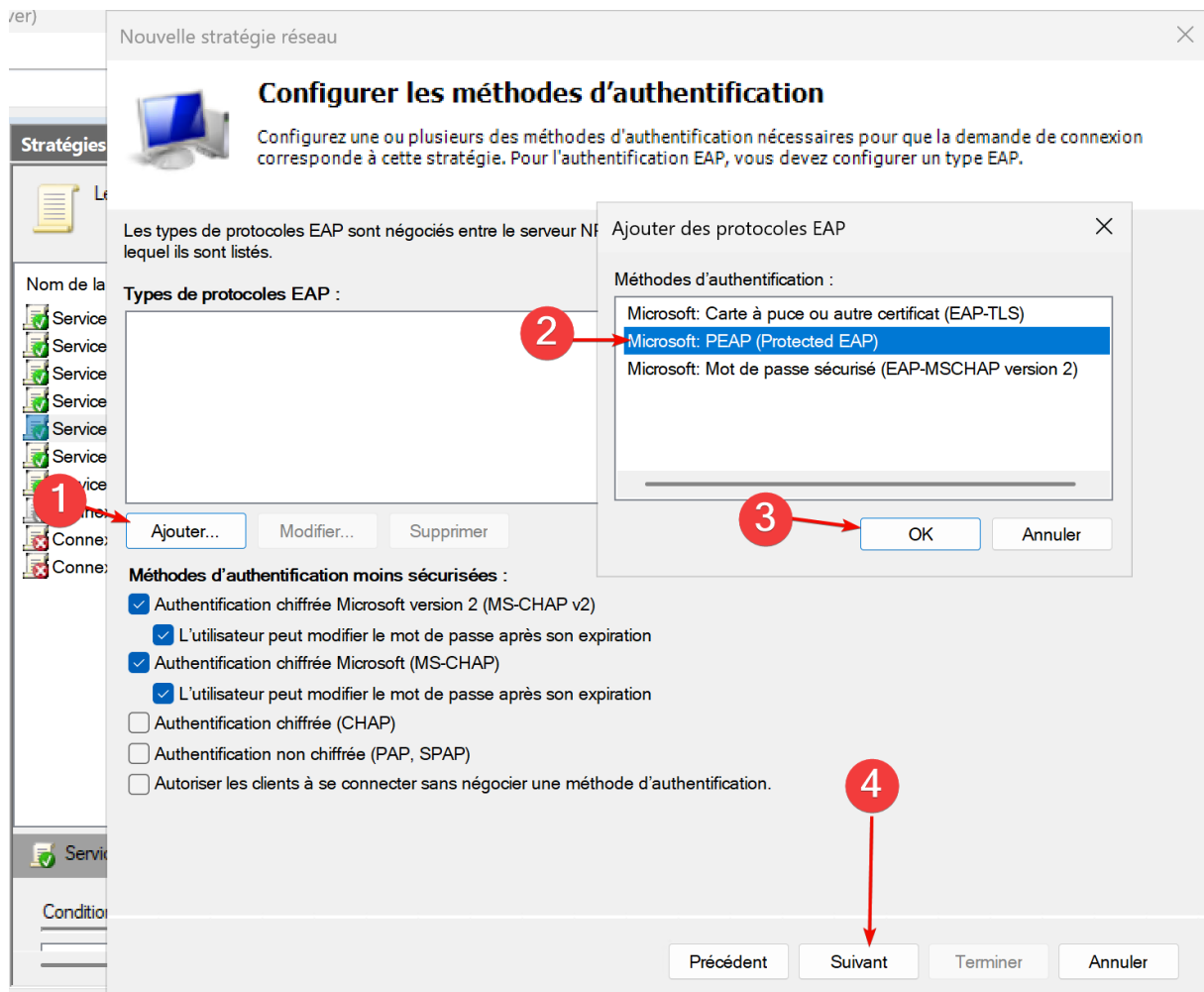
Précédent

Suivant

Terminer

Annuler

Sélectionne Ajouter -> sélectionner 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
- Restrictions relatives aux jours et aux heures
- 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
- ☐ 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

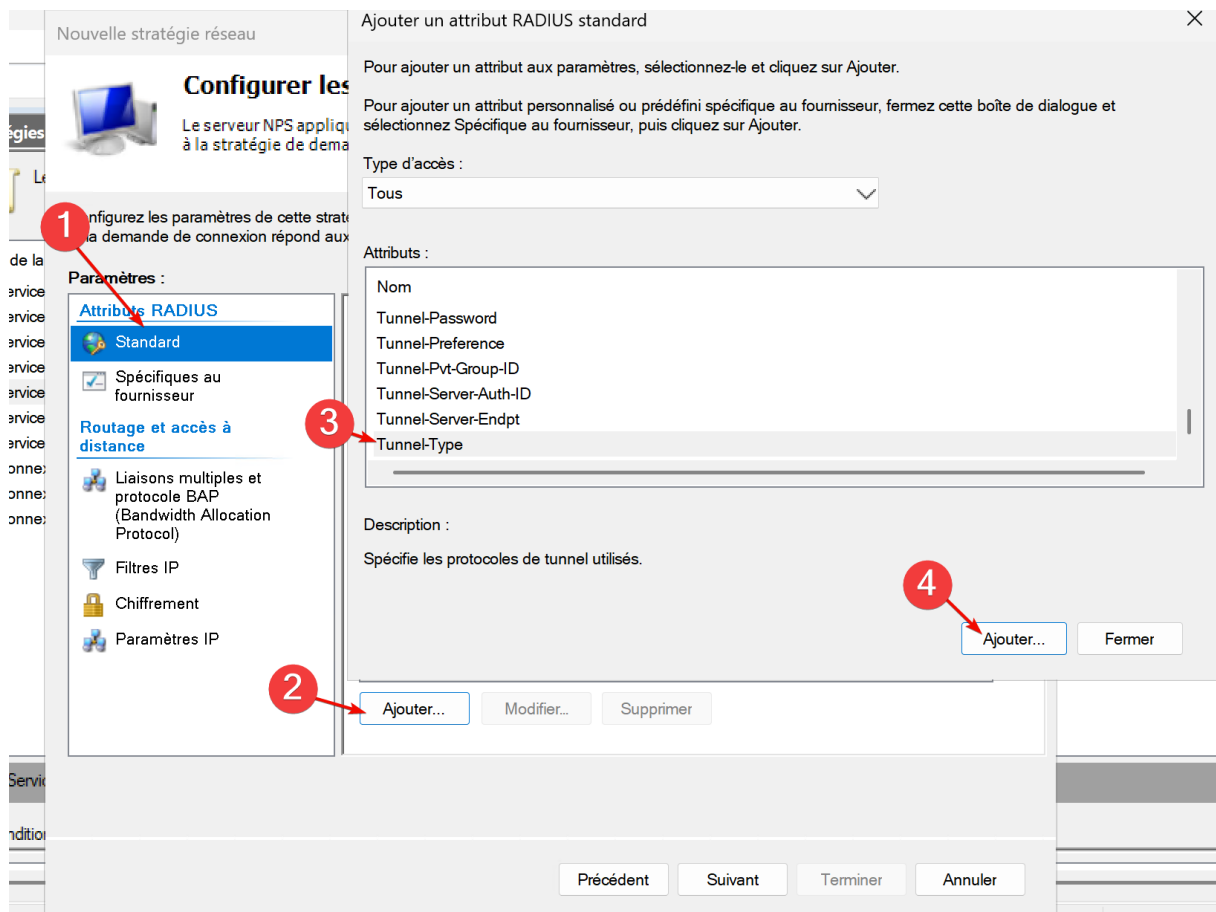
Précédent

Suivant

Terminer

Annuler

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



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

☒ Communément utilisé pour les connexions 802.1x

☐ Autres

1 2 3

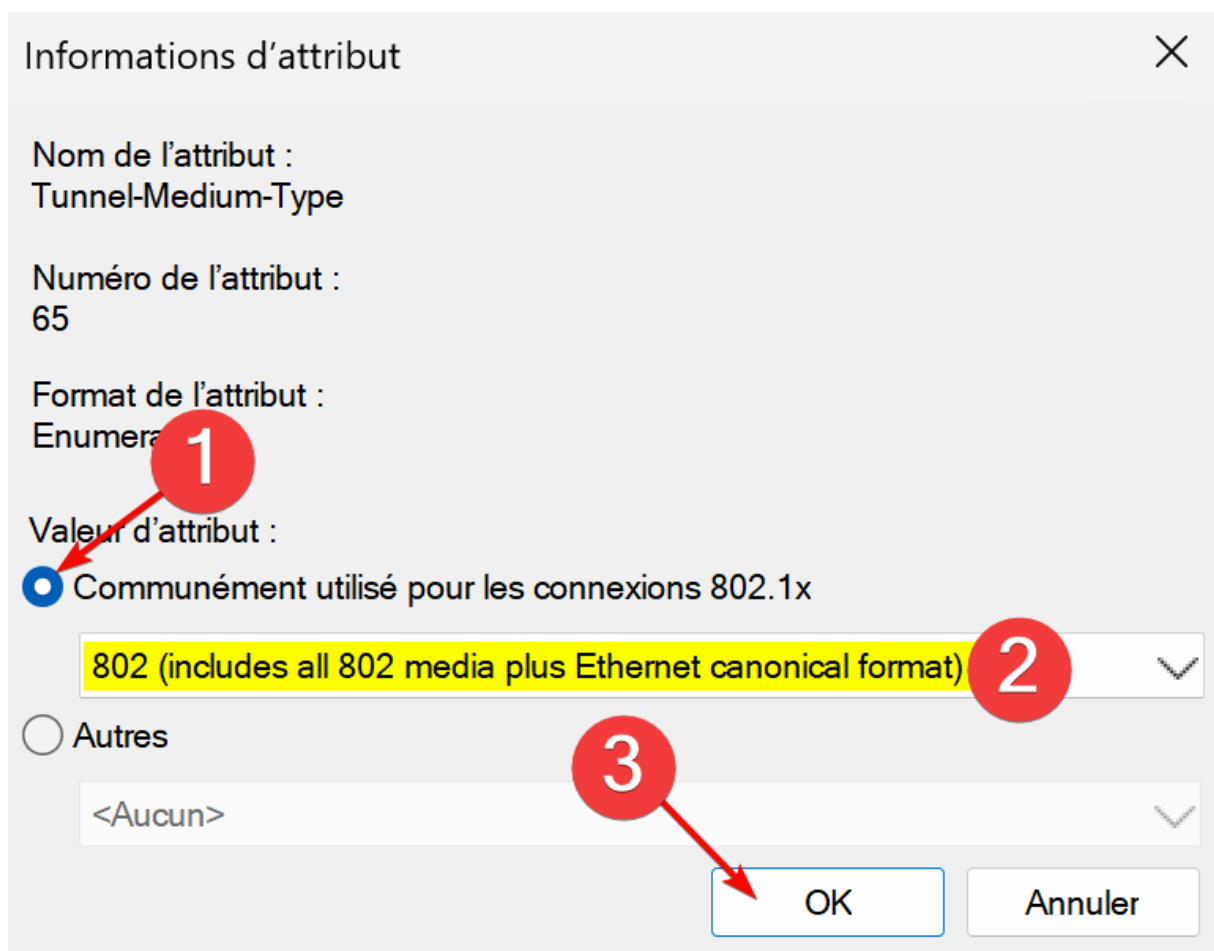
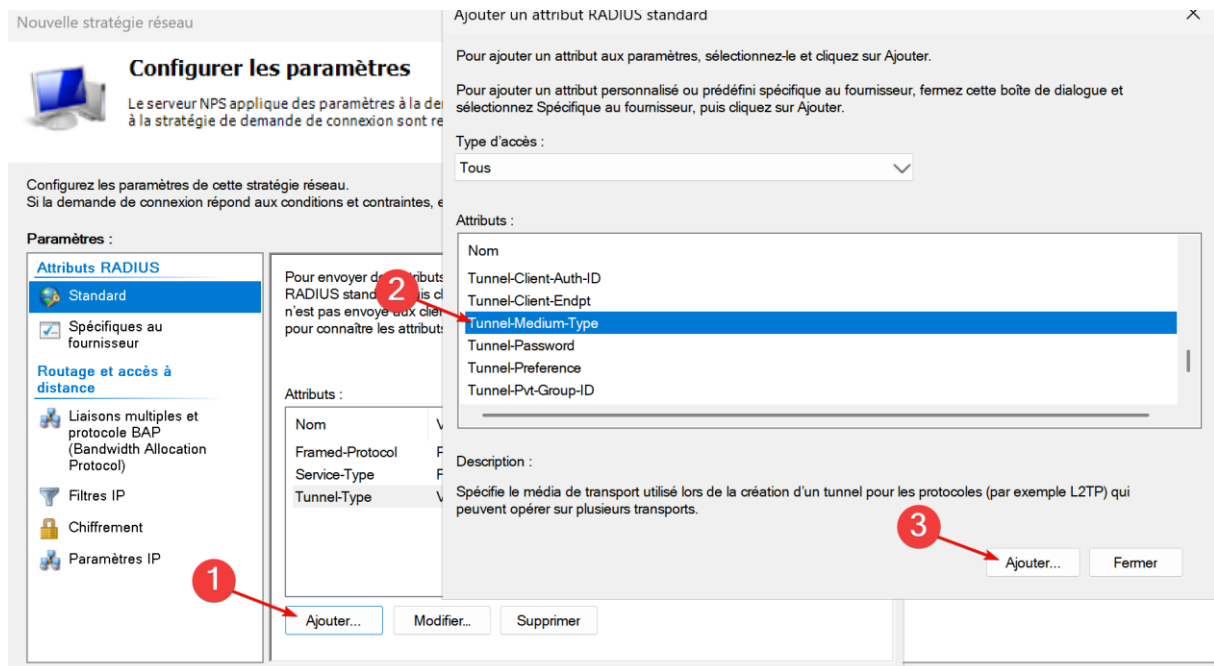
<Aucun>

Virtual LANs (VLAN)

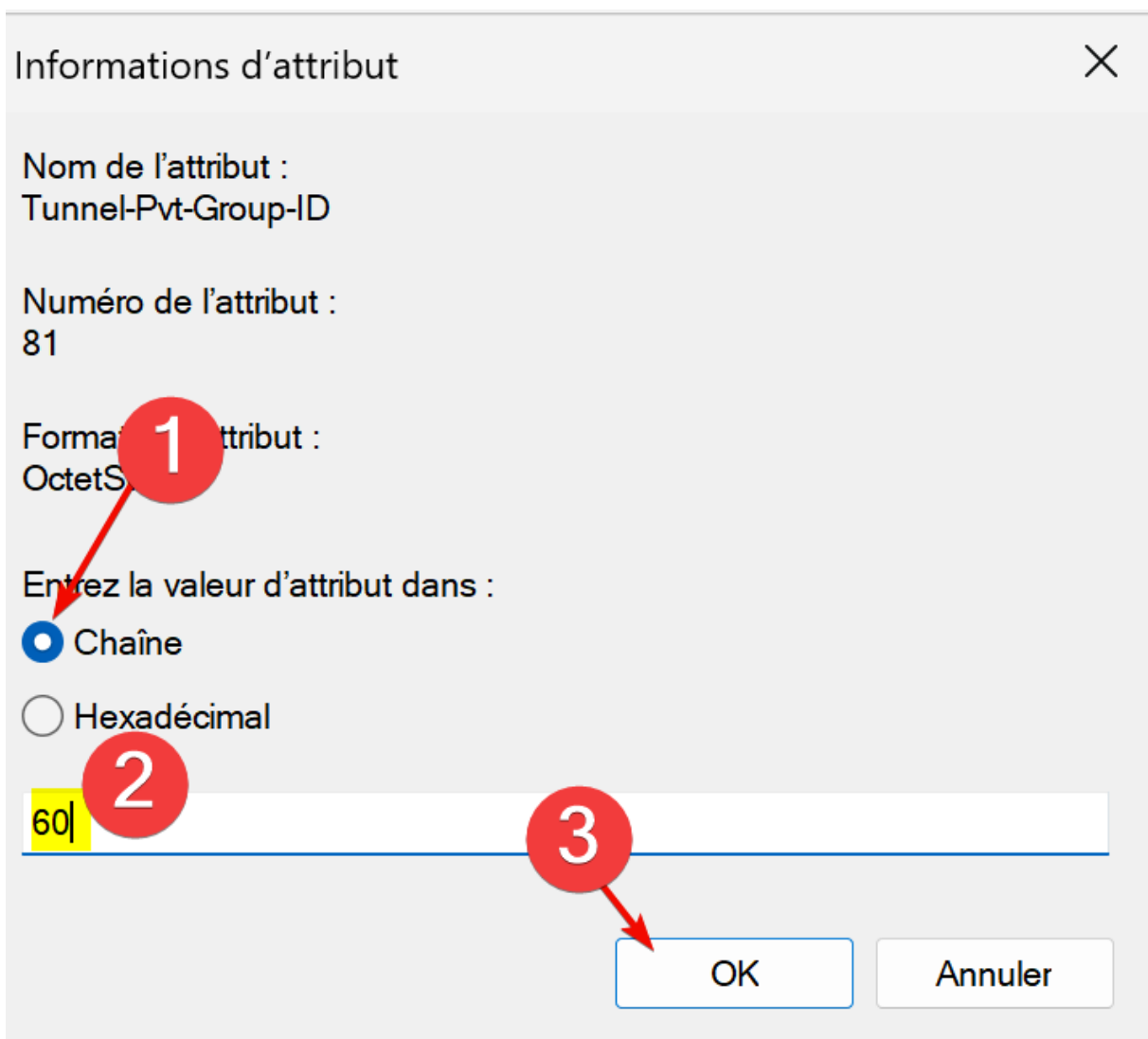
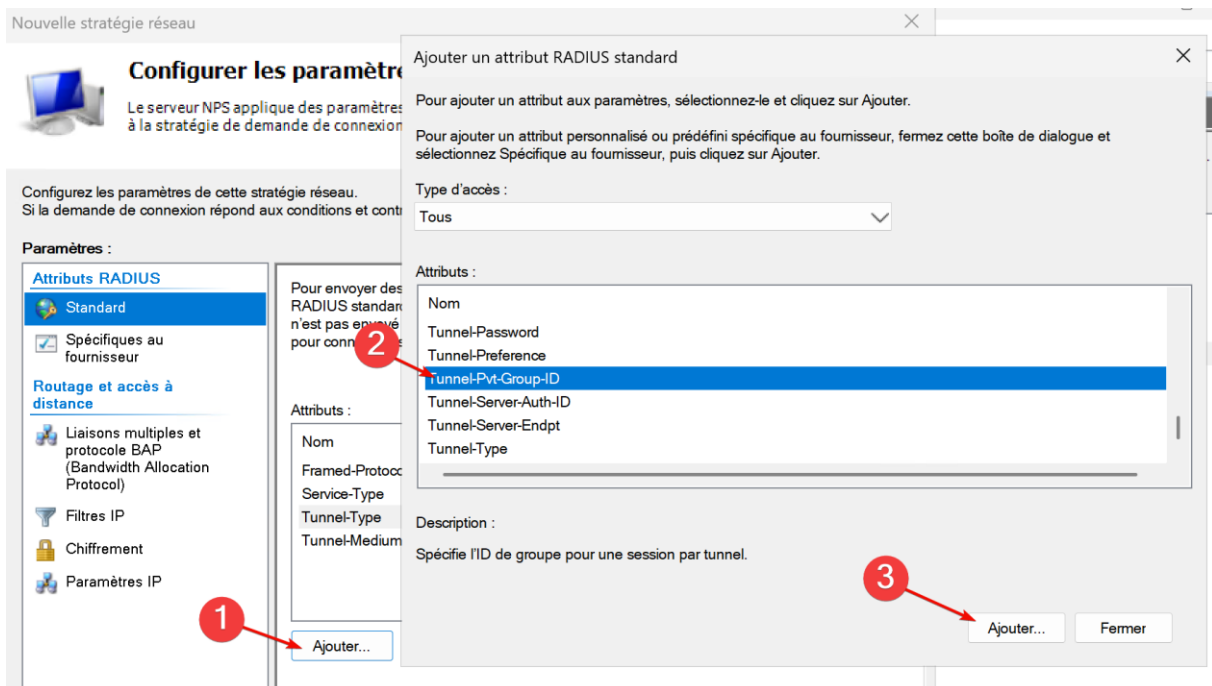
<Aucun>

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 -> Tunnel-Pvt-Groupe-ID -> Ajouter -> Sélectionner « chaîne » -> rentré le numéro du vlan -> OK





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	60

Ajouter...

Modifier...

Supprimer

2

Précédent

Suivant

Terminer

Annuler

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 :

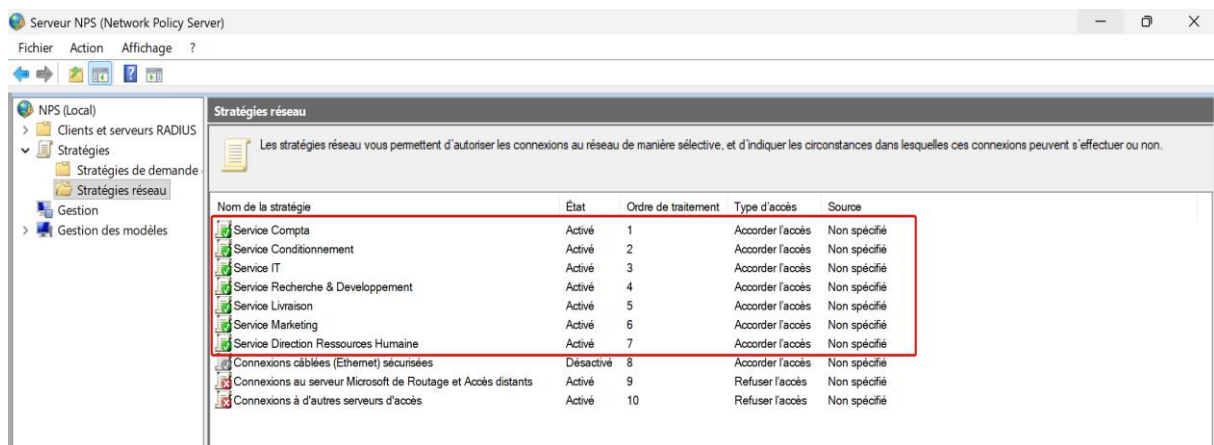
Condition	Valeur
Type de port NAS	Ethernet
Tunnel-Type	Virtual LANs (VLAN)
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical format)
Tunnel-Pvt-Group-ID	60
Pourcentage de capacité du protocole BAP	Réduisez les liaisons multiples si le serveur atteint 50% pour 2 minutes

Pour fermer cet Assistant, cliquez sur Terminer.

Précédent
Suivant
Terminer
Annuler

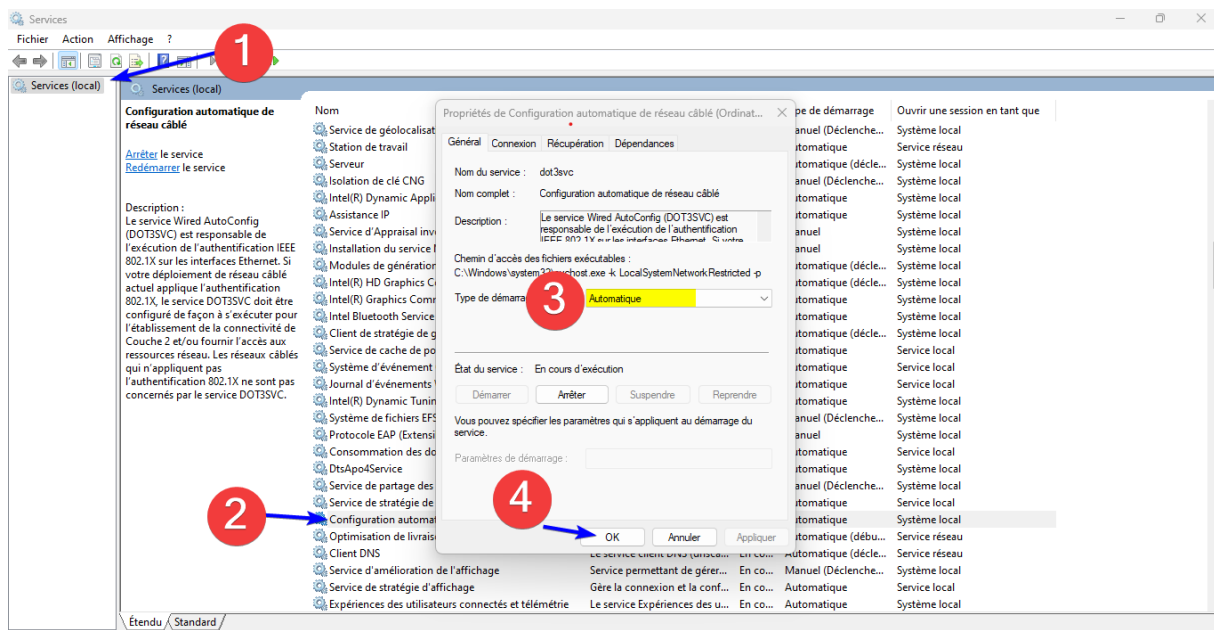
Reproduisez la stratégie réseau en ajustant les paramètres du groupe et le numéro du VLAN pour chaque stratégie, en vous basant sur les informations du tableau.

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 :

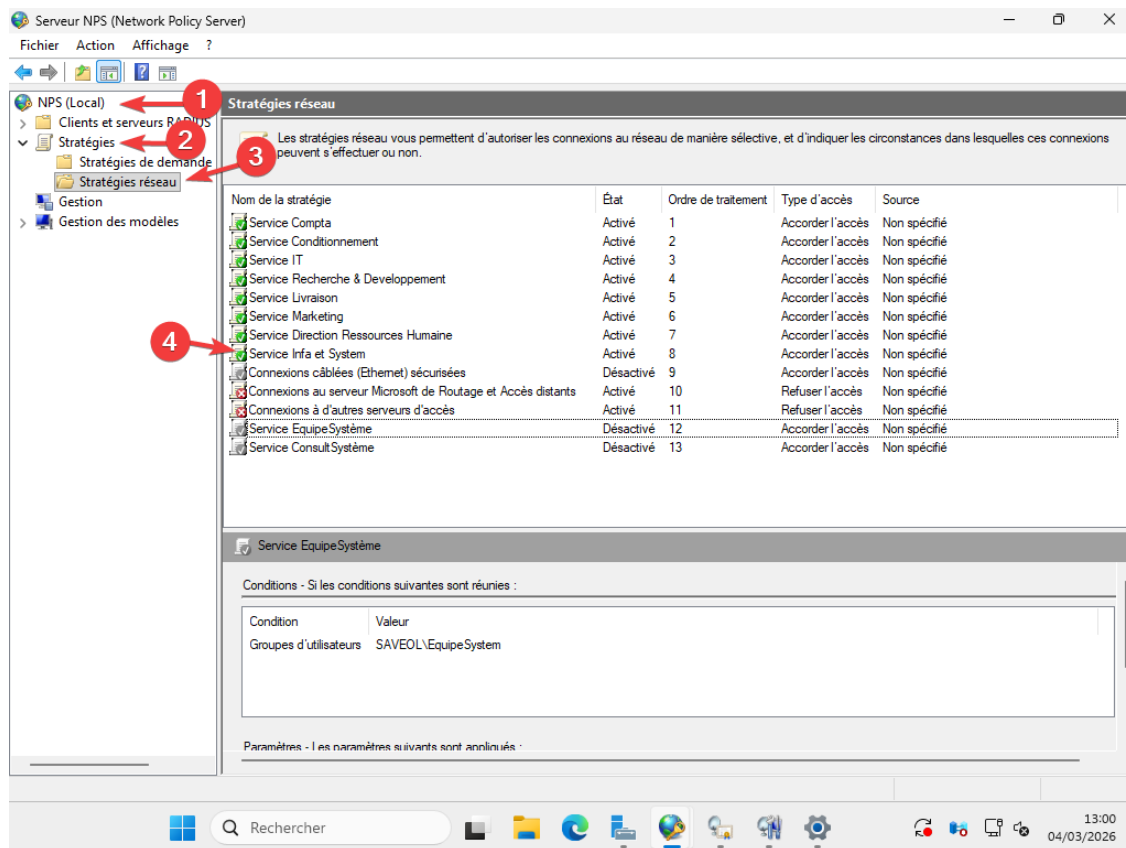
```
aaa new-model
aaa group server radius DC1

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

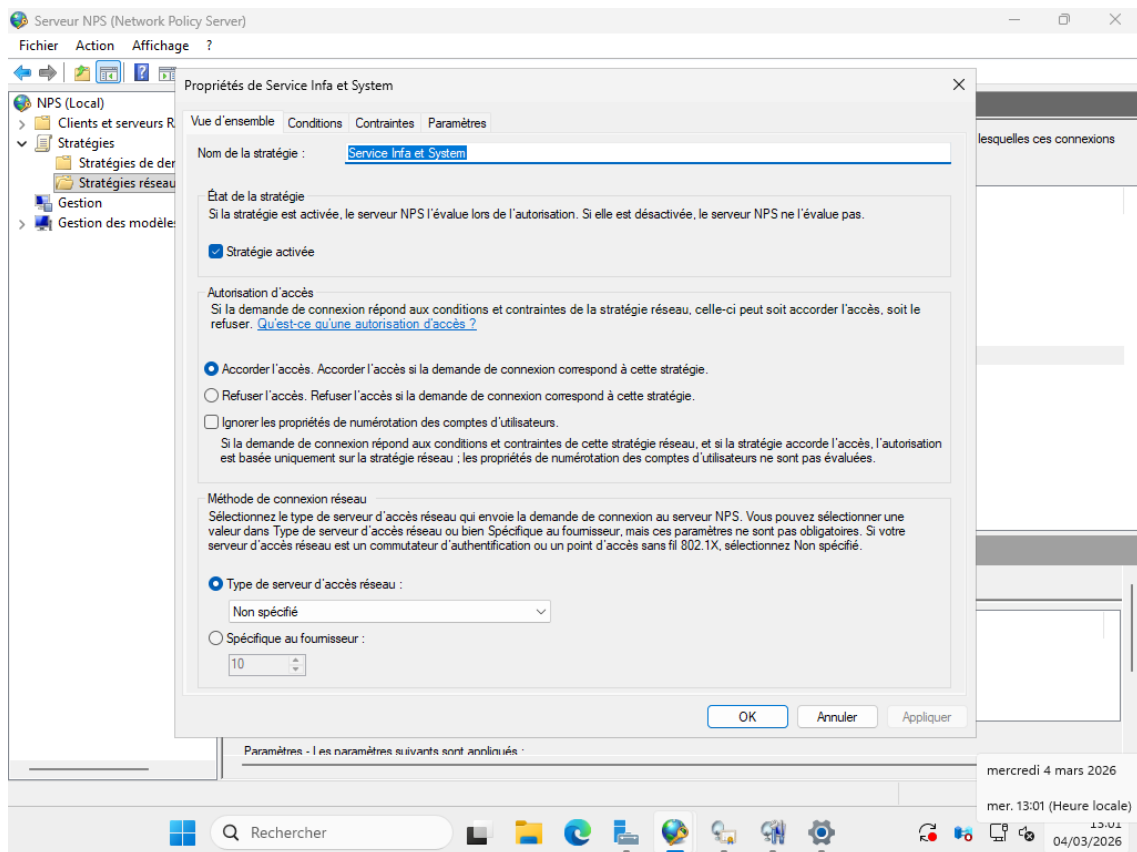
aaa authorization network default group radius
dot1x system-auth-control
radius-server host 172.16.100.2 auth-port 1645 acct-port 1646 key admin
radius-server host 172.16.100.2 auth-port 1812 acct-port 1813 key admin
```

Creation de la strategies réseau pour le login SSH:

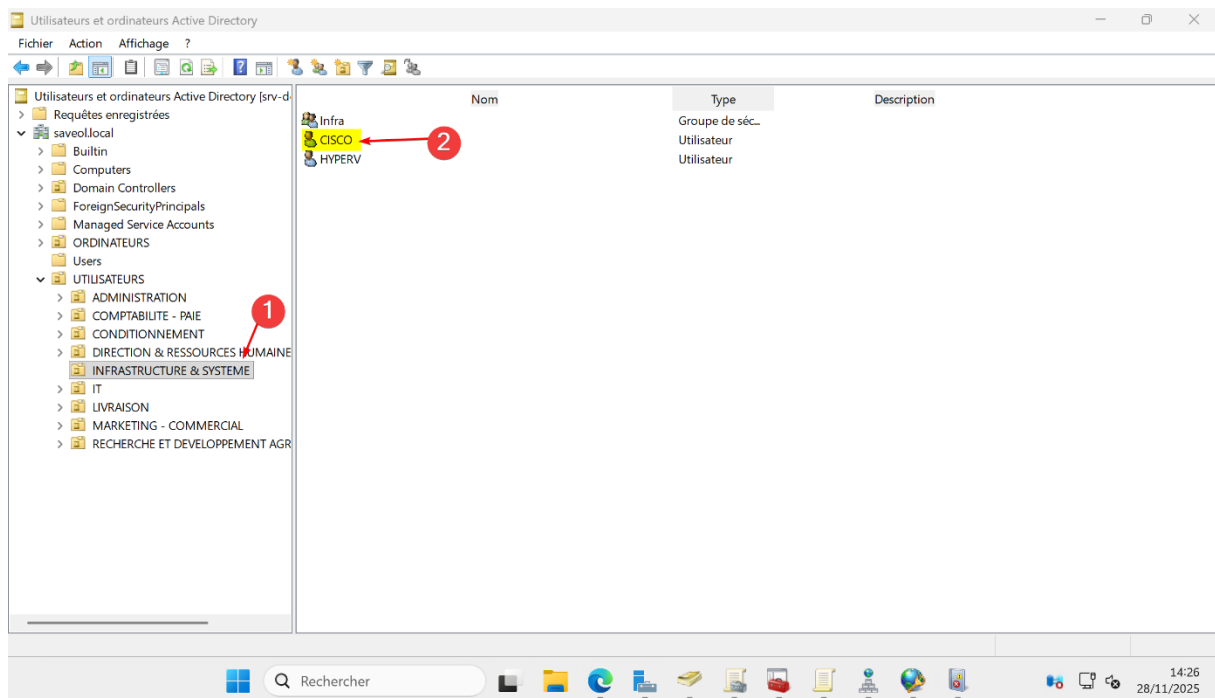
Dans la console NPS, naviguer dans Stratégies → Stratégies réseau. On retrouve ici l'ensemble des stratégies configurées. La stratégie « Service Infa et System » est activé, avec le type d'accès Accorder l'accès.

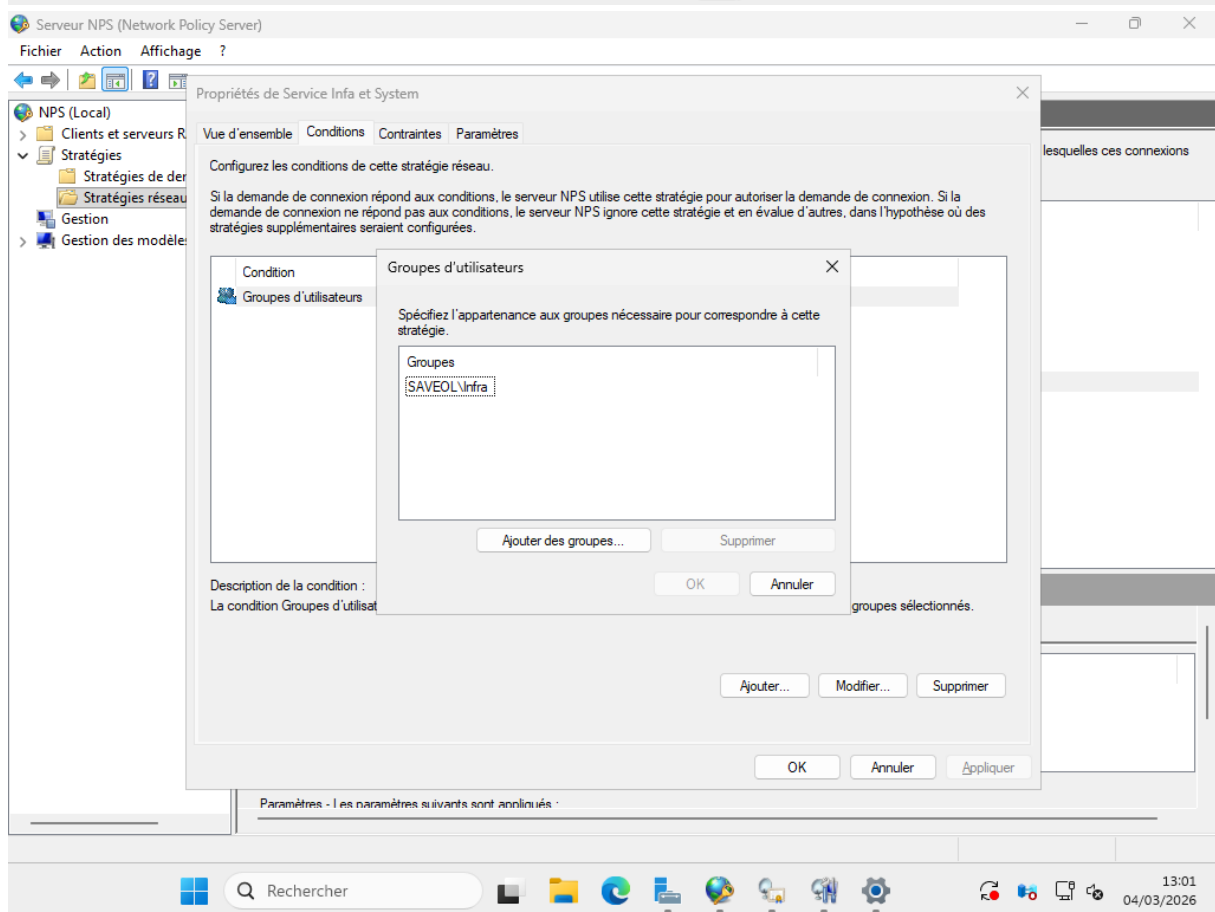
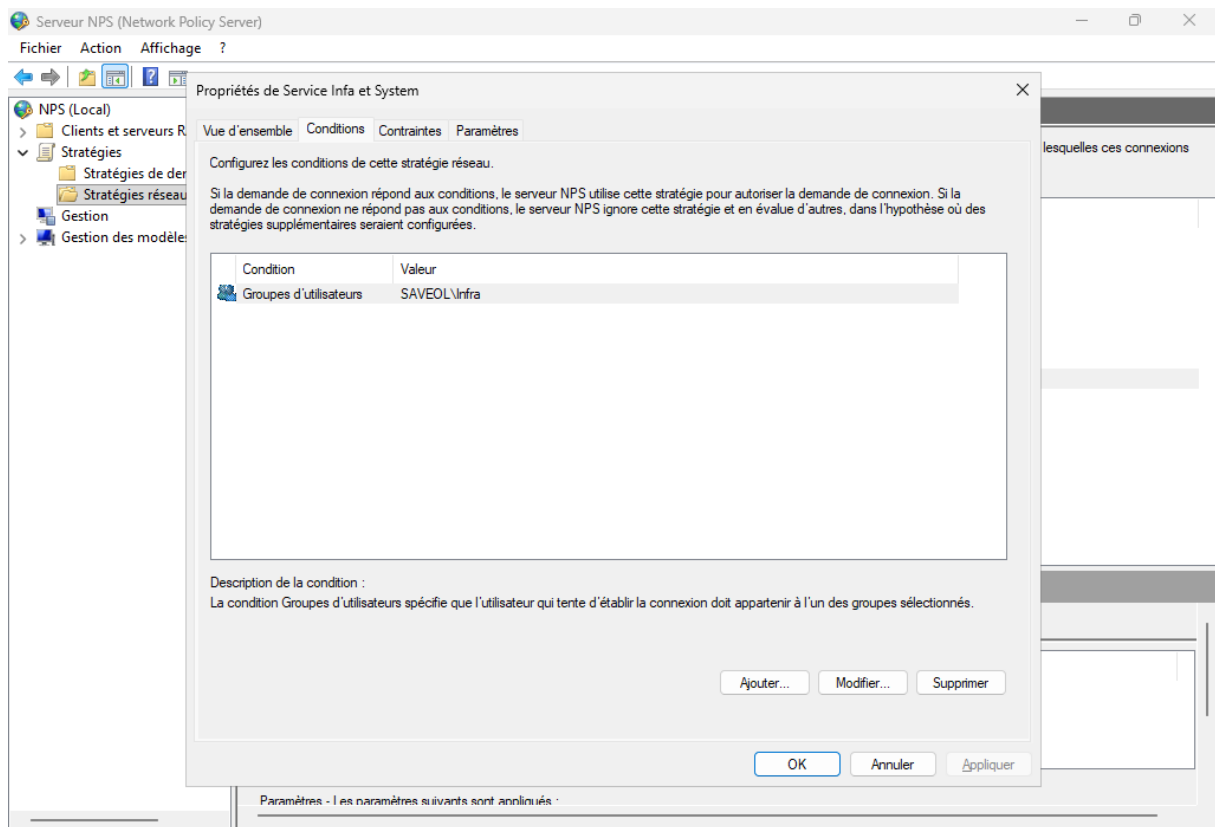


Nommer la stratégie « Service Infa et System », laisser le type de serveur d'accès réseau sur Non spécifié, cocher Stratégie activée et sélectionner Accorder l'accès.

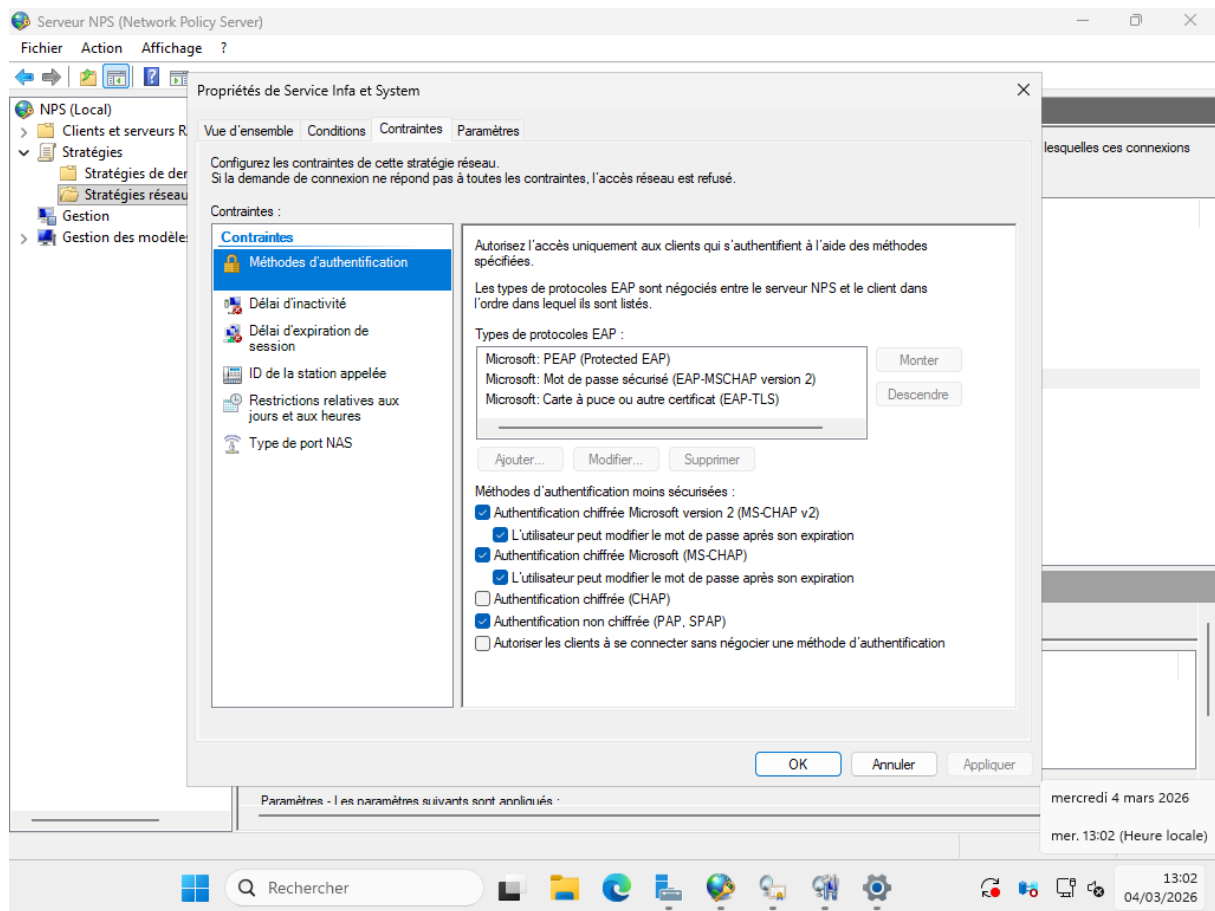


Dans l'onglet Conditions, ajouter le groupe SAVEOL\Infra comme condition d'appartenance. Seuls les membres de ce groupe seront concernés par cette stratégie en l'occurrence le membre CISCO.

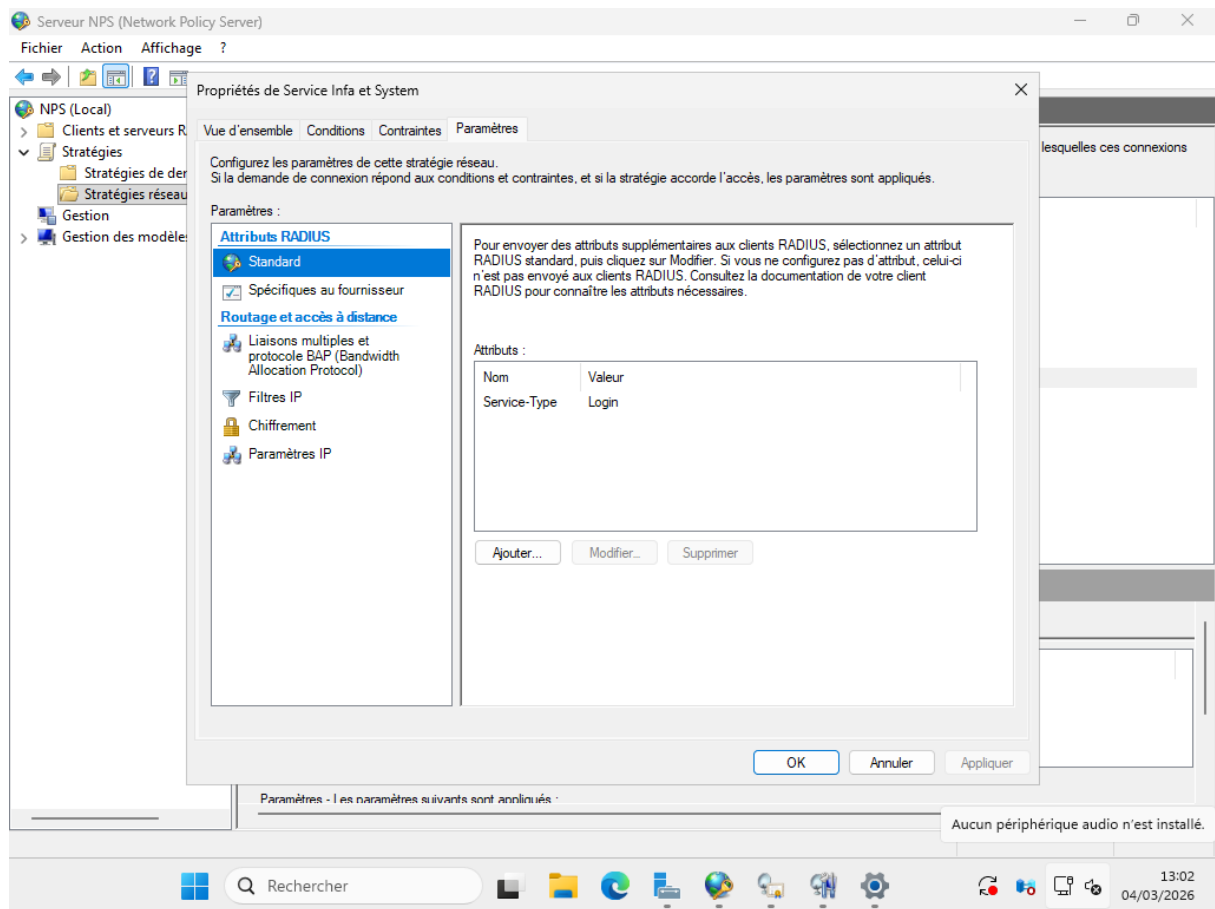




Dans l'onglet Contraintes, ajouter les protocoles EAP : PEAP, EAP-MSCHAP v2 et EAP-TLS. Activer également MS-CHAP v2 et MS-CHAP pour la compatibilité avec les switchs et Router.



Dans l'onglet Paramètres → Attributs RADIUS Standard, ajouter l'attribut Service-Type avec la valeur "Login"



Aller dans Attributs RADIUS → Spécifiques au fournisseur, ajouter l'attribut Cisco-AV-Pair avec la valeur shell:priv-lvl=15. Cela accorde le niveau de privilège maximum sur les équipement Cisco pour les membres du groupe Infra.

