

MISE EN PLACE D'UN SERVEUR RADIUS POUR CONNEXION FILAIRE

StgInfo
RESE

Table des matières :

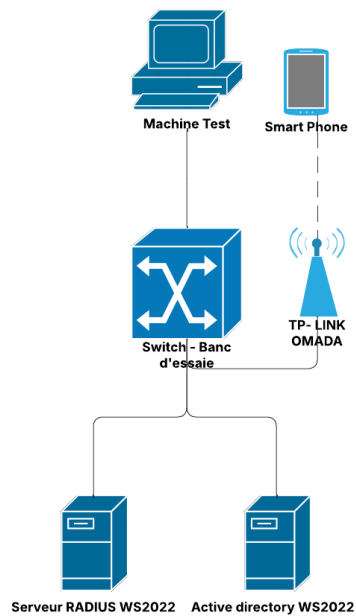
1. Matériel requis	2
Schéma réseau	2
2. Configuration du serveur Radius & NPS	3
3. Configuration de l'authentification filaire 802.1X	7
4. Configuration du switch	10
5. Dépannage	10
Problèmes courants et solutions	10

1. Matériel requis

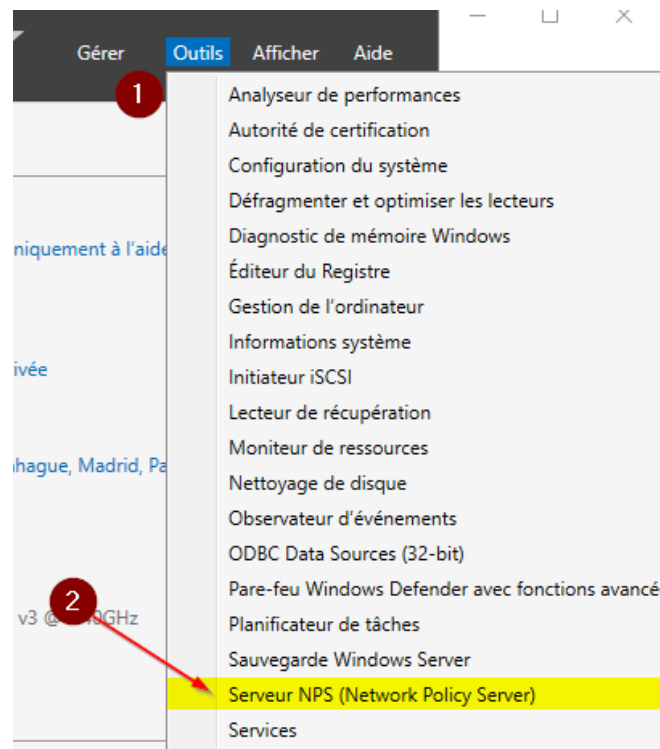
- **PC portable de test** (avec droits admin local)
- **Switch** (avec accès console/SSH)
- **Windows Server configuré en NPS**

Schéma réseau

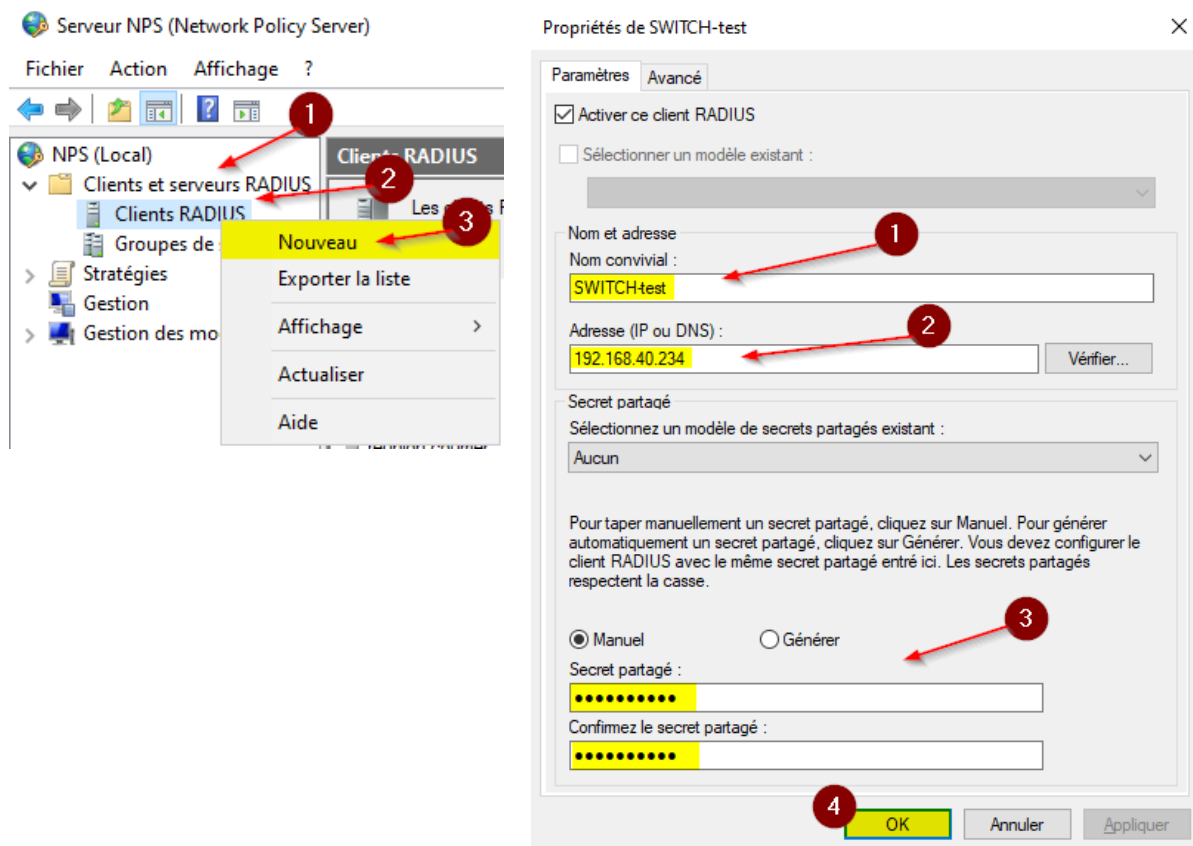
- **Port 48** : Connecté au serveur Windows 2022 / Réseau de la RESE
- **Port 5** : Connecté à la machine de test
- **Ports 5-10** : Authentification RADIUS EAP activée
- **Authentification 802.1X** : Mot de passe requis (peut être automatisé via GPO)



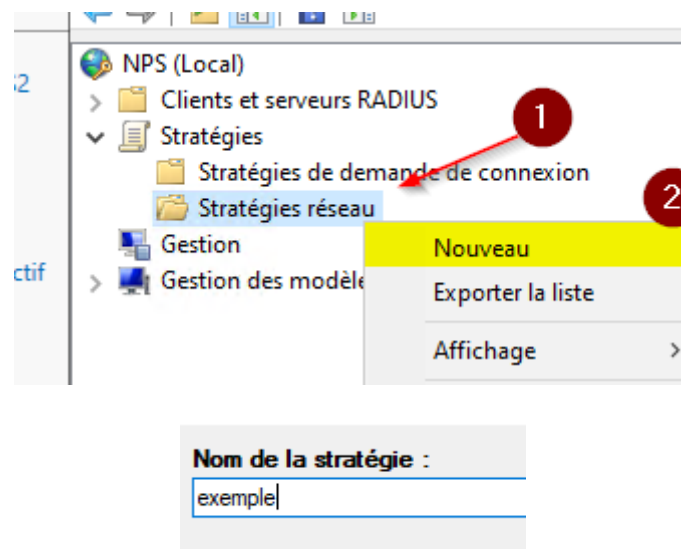
2. Configuration du serveur Radius & NPS



Le switch doit être ajouté en tant que client RADIUS sur le serveur NPS. Cela implique de spécifier son adresse IP et un mot de passe partagé, qui sera utilisé lors de la configuration du switch.



Ensuite, une règle de stratégie réseau est définie pour autoriser les connexions du groupe cible, en utilisant PEAP et un mot de passe pour l'authentification.



Donner un nom a la stratégie (sera visible dans les logs)



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

Précédent

Suivant

Terminer

Annuler

Ajoute une condition de connexion

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.



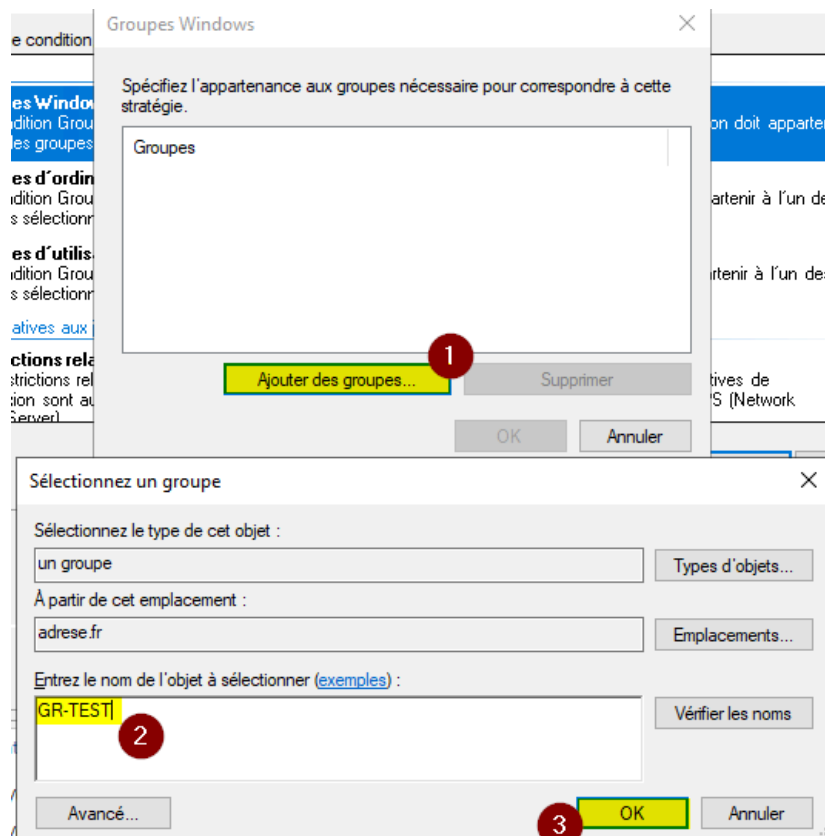
Restrictions relatives aux jours et aux heures

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...

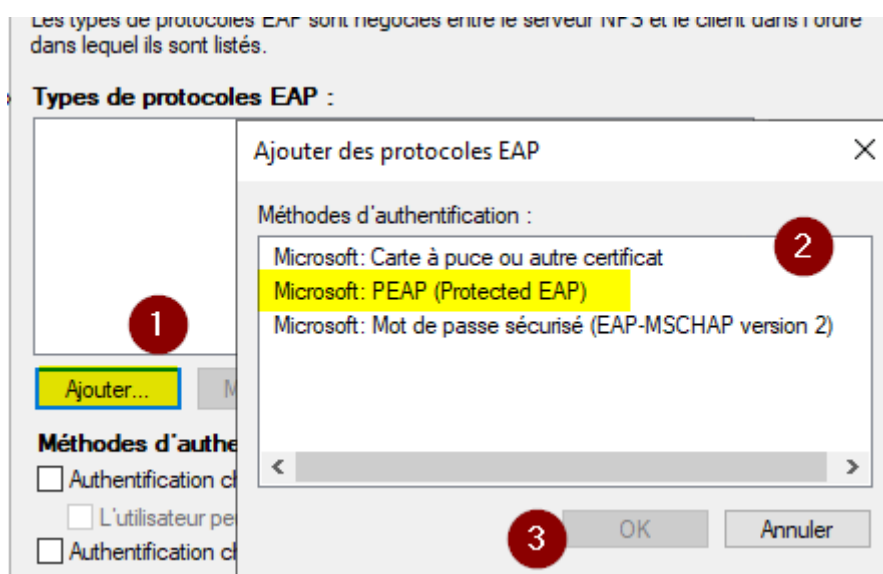
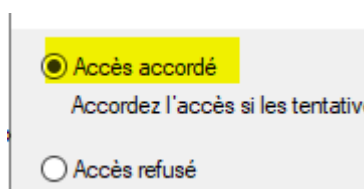
Annuler

Sélectionner
Groupe Windows afin que la stratégie fonctionne sur des utilisateurs et des ordinateurs. Pour que la stratégie ne soit effective uniquement sur des utilisateurs sélectionner groupe d'utilisateurs et ordinateurs pour que la stratégie soit effective sur des PC uniquement.



Sélectionner les groupes de personnes / ordinateurs pour qui la stratégie sera effective.

Ensuite, on **accorde l'accès** :



Puis, laissez coché seulement l'authentification non chiffré :

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

Une page apparaît, cliquer sur non, puis cliquer sur suivant sur la page de récapitulatif final.

Vous avez correctement créé la stratégie réseau suivante :

Test-SWitch

Conditions de la stratégie :

Condition	Valeur
Groupes Windows	ADRESE\GR-TEST

Paramètres de la stratégie :

Condition	Valeur
Méthode d'authentification	Protocole EAP OU Authentification non chiffrée (PAP, SPAP)
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)

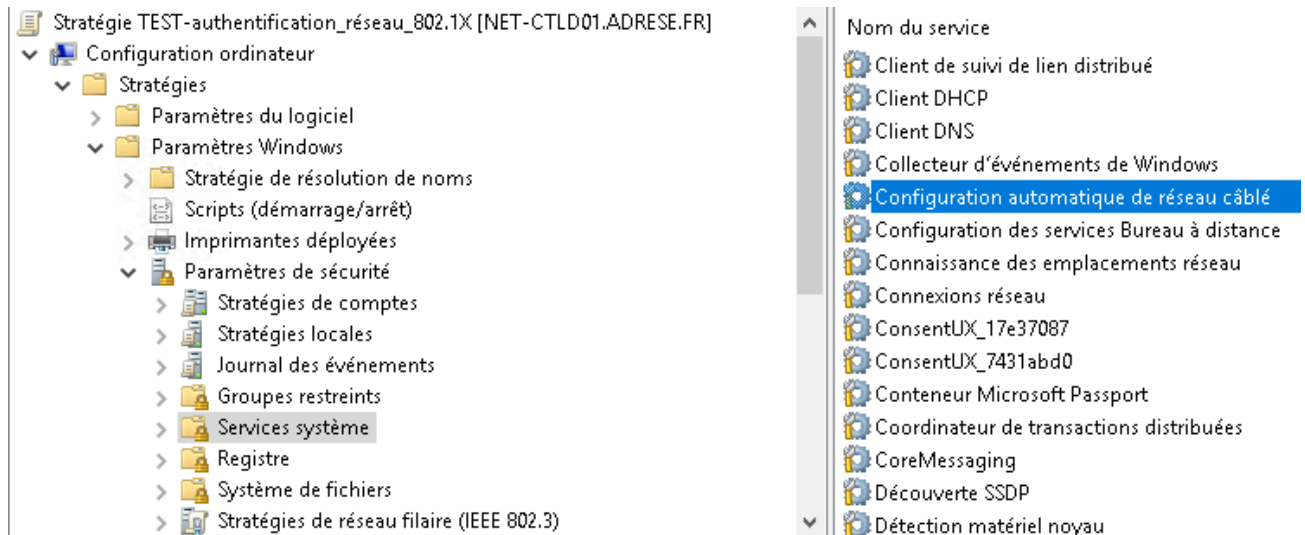
Pour fermer cet Assistant, cliquez sur Terminer.

Précédent Suivant **Terminer** Annuler

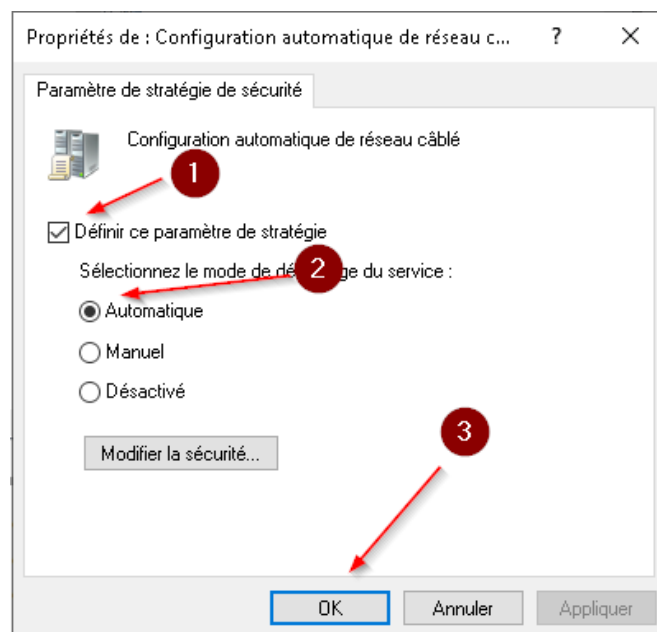
3. Configuration de l'authentification filaire 802.1X

L'authentification filaire repose sur la création d'une GPO dédiée.

Se rendre dans : **Configuration de l'ordinateur** > **stratégie** > **Paramètres Windows** > **Paramètres de sécurité** > **Services Systèmes** > **Configuration filaire automatique**

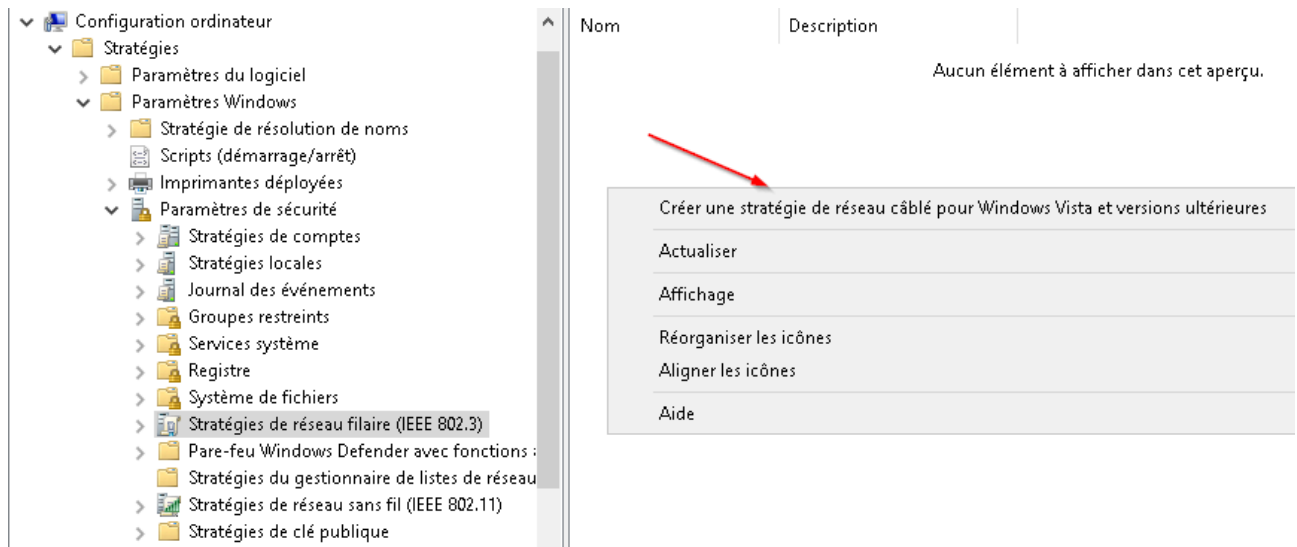


Puis, activer la configuration automatique :

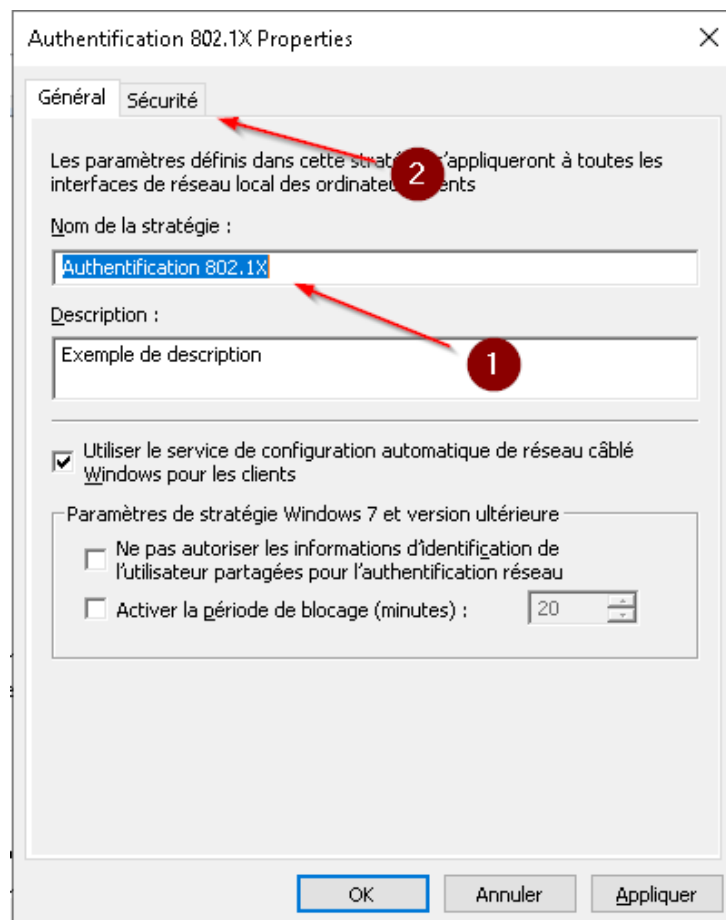


Ensuite dans : **Configuration de l'ordinateur** > **stratégie** > **Paramètres Windows** > **Paramètres de sécurité** > **Stratégie de Réseau Filaire (IEEE 802.3)**

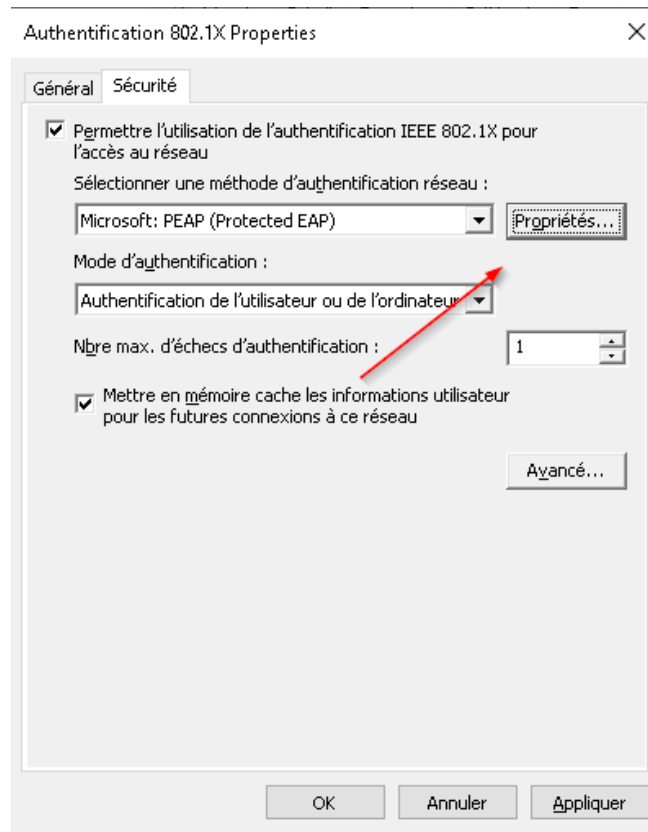
Clic droit pour créer une nouvelle stratégie :



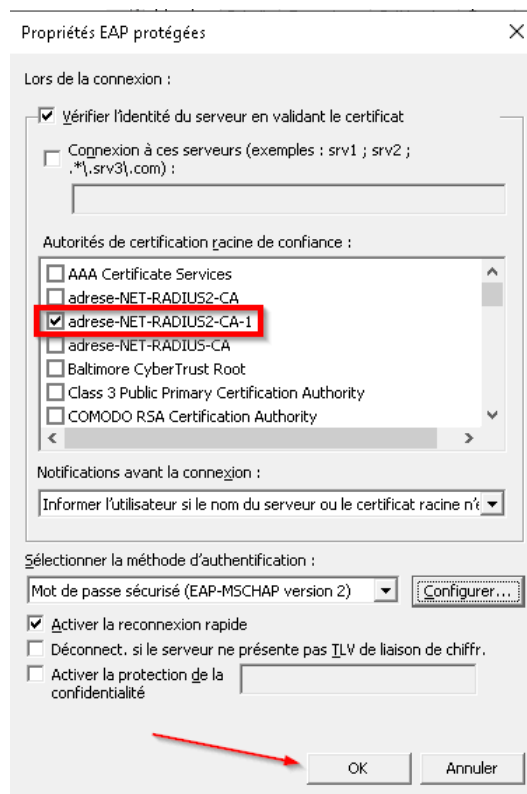
Lui donner un nom puis se rendre dans l'onglet sécurité :



Dans l'onglet sécurité, vérifier que la méthode d'authentification est bien PEAP Microsoft, puis se rendre dans les propriétés.



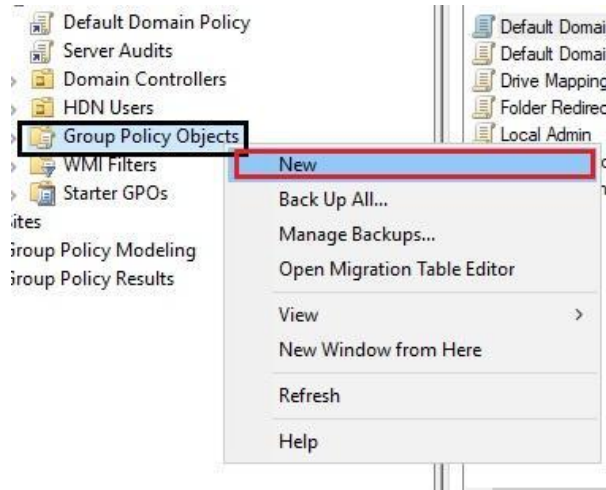
Enfin, sélectionner le certificat adrese-NET-RADIUS2-CA-1.



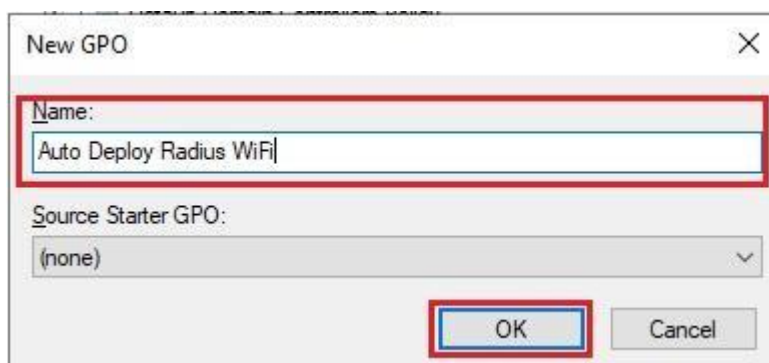
Valider et voilà.

Déployer wifi par GPO

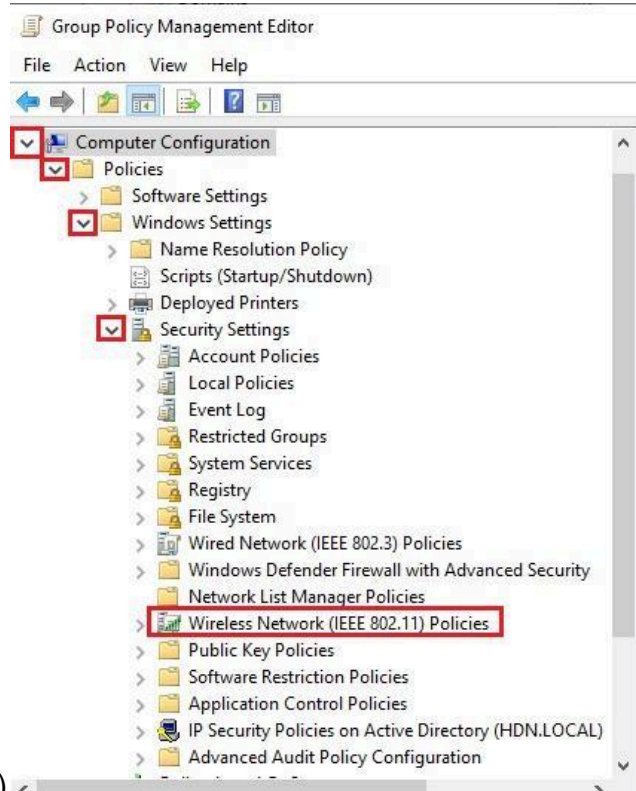
1. Créer une nouvelle GPO



2. Lui donner un nom

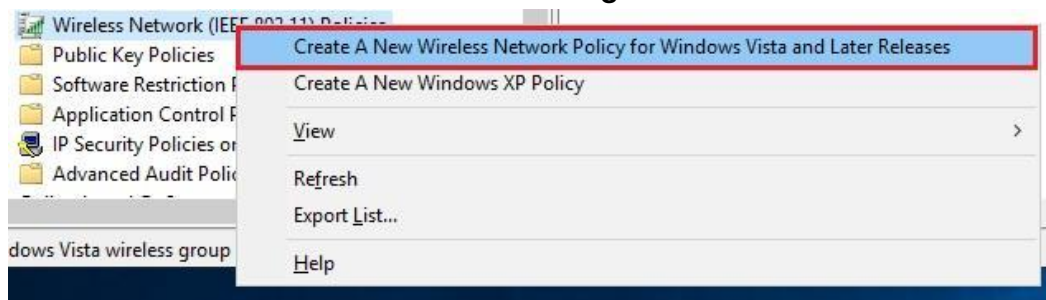


3. Dans Configuration de l'ordinateur > paramètres windows > paramètres de sécurité >

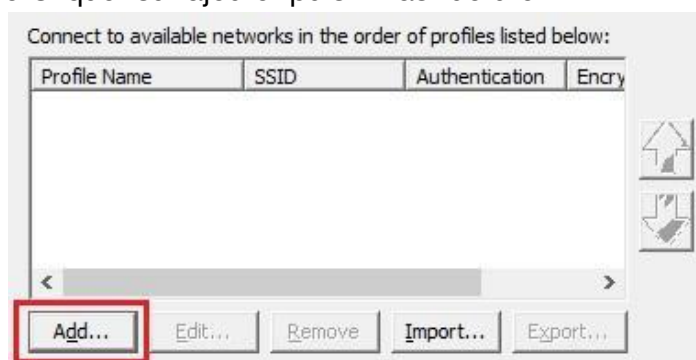


stratégie de réseau sans fils (IEEE 802.11) <

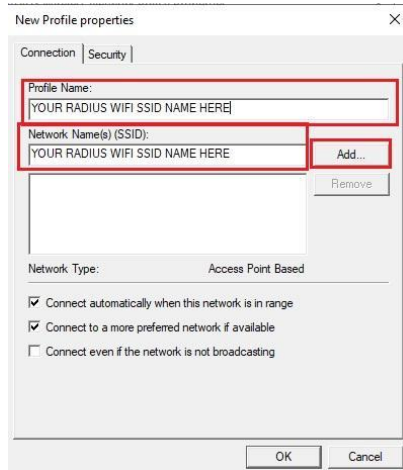
4. Clic droit sur **créer une nouvelle stratégie de réseau sans fils**.



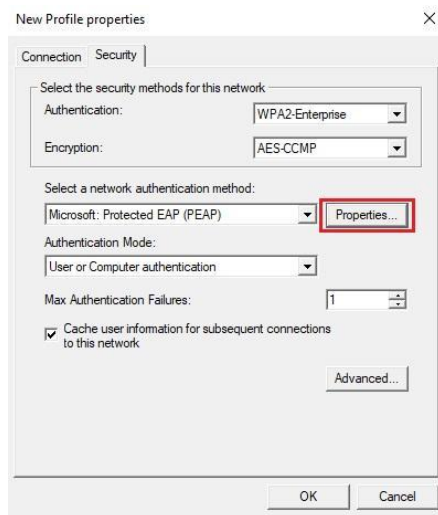
5. Cliquer sur ajouter puis infrastructure



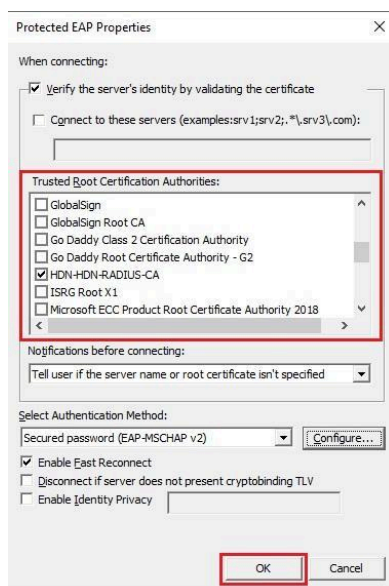
6. Donner un nom au WIFI (ce nom sera affiché dans la liste des wifi) puis le SSID



7. Dans l'onglet sécurité, aller dans les propriétés



8. Sélectionner le bon certificat puis valider.



9. Valider pour terminer la configuration

A la fin de la configuration, le panneau de récapitulation doit ressembler à ça :

Configuration ordinateur (activée)

1 Stratégies

2 Paramètres Windows

3 Paramètres de sécurité

4 Stratégies de réseau sans fil (802.11)

WIFI_RESE_TEST

Nom de la stratégie	WIFI_RESE_TEST
Description de stratégie	pour le 802.1X
Type de stratégie	Windows Vista et éditions ultérieures

Paramètres globaux

Filtres réseau

Profil réseau préférés

WIFI_RESE_TEST

Nom de profil	WIFI_RESE_TEST
Type de réseau	Infrastructure
Se connecter automatiquement à ce réseau	Activé
Basculer automatiquement vers un réseau préféré	Activé

Nom réseau (SSID)

RESE17_TEST	Le réseau diffuse son SSID.
	True

5

6

Paramètres de sécurité

Authentification	WPA2
Chiffrement	AES
Utiliser 802.1X	Activé
Mise en cache PMK (Pairwise Master Key)	Activé
Durée de vie PMK (minutes)	720
Nombre d'entrées dans le cache PMK	128
Nombre maximal d'échecs de pré-authentification	3

1

Paramètres IEEE 802.1X

Authentification de l'ordinateur	Nouvelle authentification de l'utilisateur
Nombre maximal d'échecs d'authentification	1
Nombre maximal de messages EAPOL-Start envoyés	
Période de maintien (secondes)	
Période de démarrage (secondes)	
Période d'authentification (secondes)	

Propriétés de la méthode d'authentification du réseau

Méthode d'authentification	PEAP (Protected EAP)
Valider le certificat du serveur	Activé
Connexion à ces serveurs	
Autorités de certification racines de confiance	adresse-NET-RADIUS2-CA-1
Ne pas demander à l'utilisateur d'autoriser de nouveaux serveurs ou des autorités de certification approuvées	Désactivé
Activer la reconnexion rapide	Activé
Déconnecter, si le serveur ne présente pas TLV de liaison de chiff.	Désactivé
Appliquer la protection d'accès réseau	Désactivé

2

Configuration de la méthode d'authentification

Méthode d'authentification	Mot de passe sécurisé (EAP-MSCHAP version 2)
Utiliser automatiquement mon nom et mon mot de passe Windows d'ouverture de session (et éventuellement le domaine)	Activé

3

Un simple gpupdate /force est nécessaire pour appliquer la stratégie.

4. Configuration du switch

Switch utilisé : **HP procureve-48G-PoEP-2530**

Mise en place de l'authentification RADIUS sur le switch :

```
3. radius-server host 192.168.40.111 key Password01
```

- Définit le serveur **RADIUS** avec l'adresse IP **192.168.40.111** et la clé partagée **Password01**

```
4. aaa accounting network start-stop radius
```

- Active la gestion des **logs de connexion** (accounting) pour le réseau, en envoyant un message "**start**" lors de l'authentification et un message "**stop**" à la déconnexion.

5. `aaa authentication port-access eap-radius`

- Configure l'authentification des utilisateurs via le **protocole EAP** en utilisant le serveur **RADIUS**.

6. `aaa port-access authenticator 5-10`

- Active la fonction **802.1X** sur les **ports 5 à 10** du switch, ce qui signifie que seuls les périphériques authentifiés via **RADIUS** pourront y accéder.

7. `aaa port-access authenticator active`

- Active globalement la fonctionnalité **802.1X** sur le switch, appliquant ainsi les règles d'authentification configurées précédemment.

Mise en place de l'authentification par adresse MAC sur le switch :

1. Port-security <port(s)> learn-mode static
2. Port-security <port(s)> address-limit <nombre d'adresses MAC (max 64)>
3. Port-security <port(s)> mac-address <adresse MAC>

Exemple :

```
port-security 1-4 learn-mode static
port-security 1-4 address-limit 64
port-security 1-4 mac-address 040e3c-229f54
port-security 1-4 mac-address 3c4a92-d0255e
```

Résultat sur l'interface web :

Name	Custom Name	Learn Mode	Address Limit	Violation Action
1		Static	64	None
2		Static	64	None
3		Static	64	None
4		Static	64	None

5. Dépannage

Problèmes courants et solutions

Problème	Cause possible	Solution
----------	----------------	----------

Erreur d'authentification	Certificat invalide ou non installé	Vérifier le certificat et sa validité
Impossible de se connecter	Mauvais mot de passe partagé	Vérifier la configuration côté switch
GPO non appliquée	Problème de réplication AD	Forcer la mise à jour avec <i>gpupdate /force</i>

Restant à faire :

- Améliorer l'authentification avec des certificats client <-> serveur
- Configuration sur les clients légers Windows 10