14/02/2024

Réalisation professionnelle

La mise en place d'une solution Wifi Sécurisée

Procédure d'installation et de configuration d'une solution Radius et d'un WPA2 Enterprise

ASSURMER

EVIEUX Lucas – COTTIN Elouan – BOUVIER Tristan
BTS SIO SISR A2

I. Procédure d'installation et de configuration d'une solution Radius et d'un WPA2 Enterprise

OBJET	DIFFUSION
Cette procédure a pour objet de décrire l'installation et la configuration d'un serveur Radius et d'un réseau Wifi WPA2 Enterprise	- En interne, DSI

Rédaction	**Relecteur**	**Approbation**
Lucas Evieux Technicien Informatique	**Elouan COTTIN** Technicien Informatique **Tristan Bouvier** Technicien Informatique	**Elouan COTTIN** Technicien Informatique **Tristan Bouvier** Technicien Informatique

Prérequis

La mise en place de la solution Wifi sécurisée nécessite :

- Un serveur Windows 2022 avec AD DS, DHCP et DNS.
- Une borne Cisco WAP271.
- Un appareil permettant de se connecter au Wi-Fi.

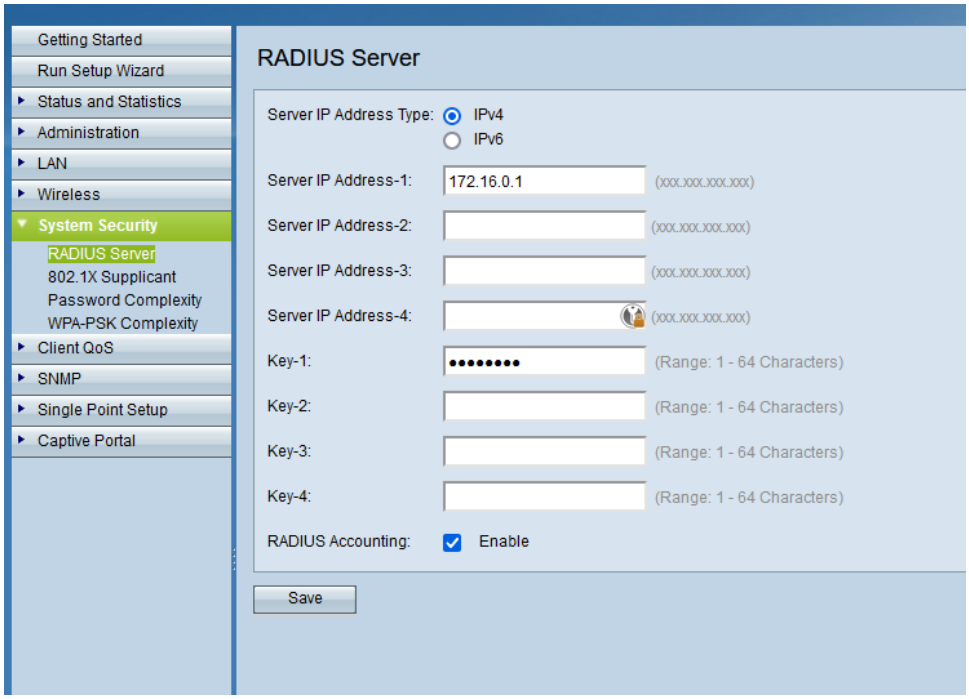
Lexique

1 : Action à réaliser

2 : L'action effectuée doit afficher

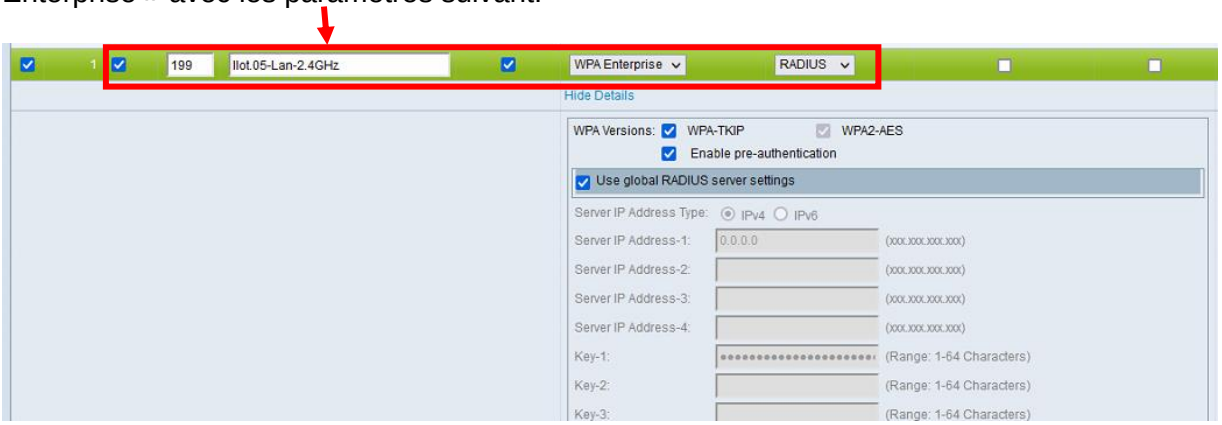
Mise en place du RADIUS sur la borne Cisco

Dans "System Security" puis "RADIUS Server" et entrer les informations suivantes :



L'adresse IP doit correspondre au future serveur RADIUS et la clé à la clé qui sera créer avec le serveur RADIUS.

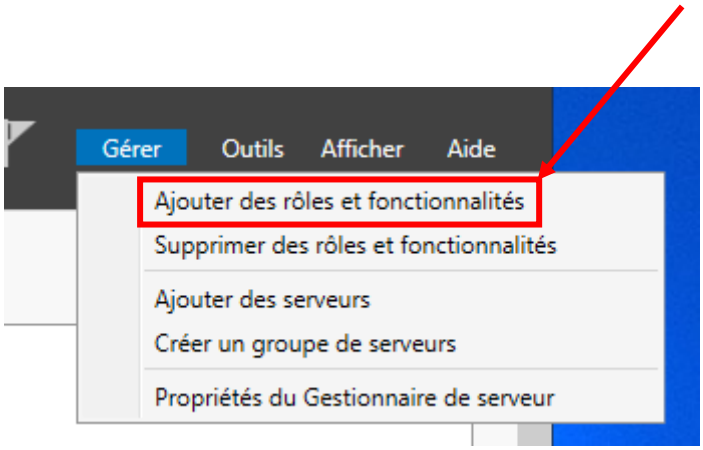
Ensuite dans « Wireless » et « Networks », et ajoutez un point d'accès en « WPA Enterprise » avec les paramètres suivant:



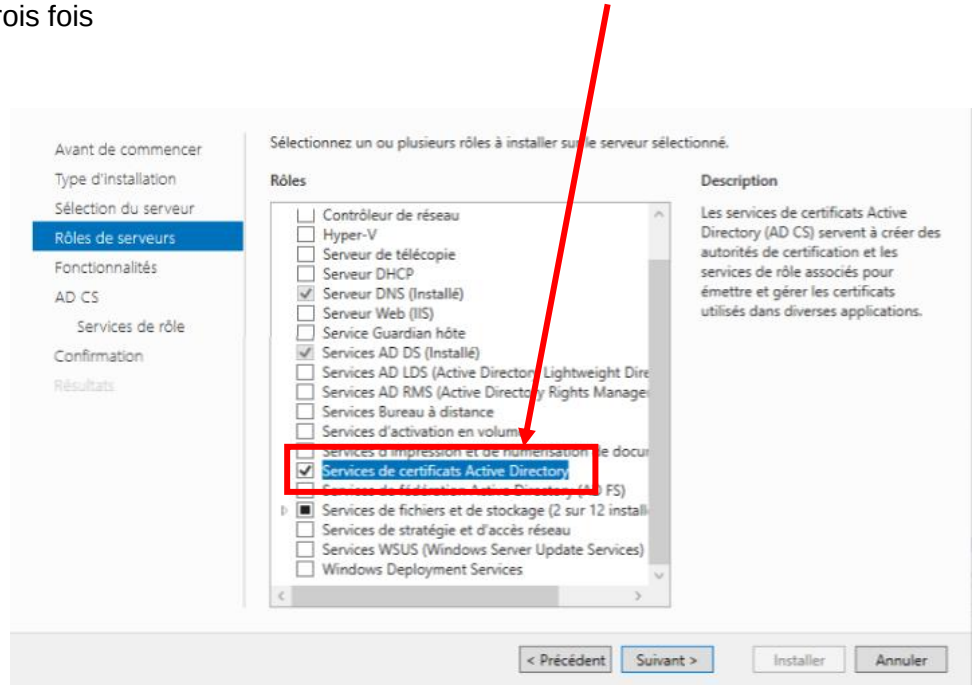
Installation et configuration du services AD CS

Pour commencer, installer le rôle AD CS qui permet de générer un certificat pour les postes client connectés en Wifi ainsi que pour le service NPS.

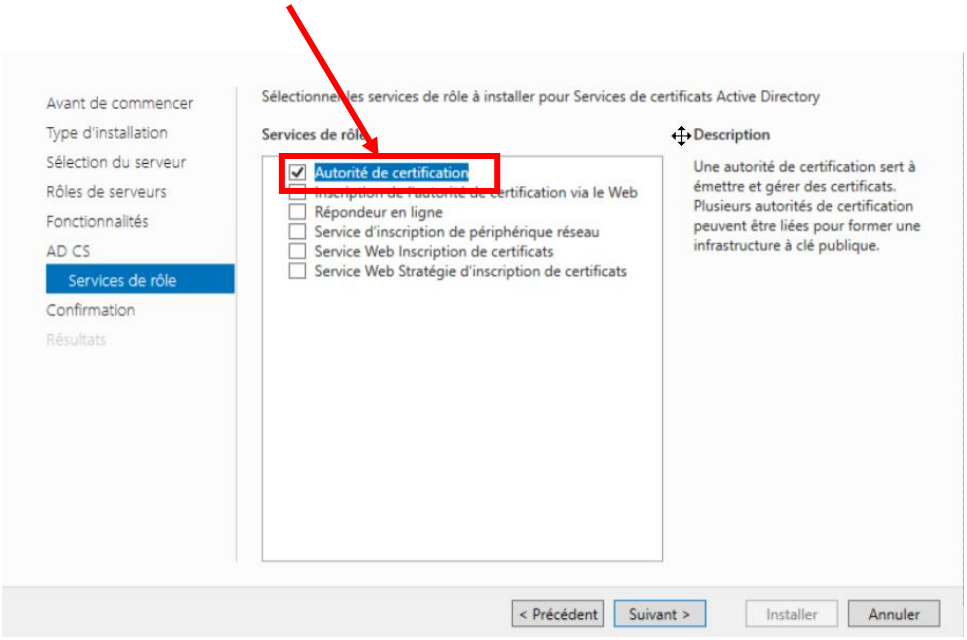
Dans le gestionnaire de serveur, appuyer sur « Gérer » puis « Ajouter des rôles et des fonctionnalités »



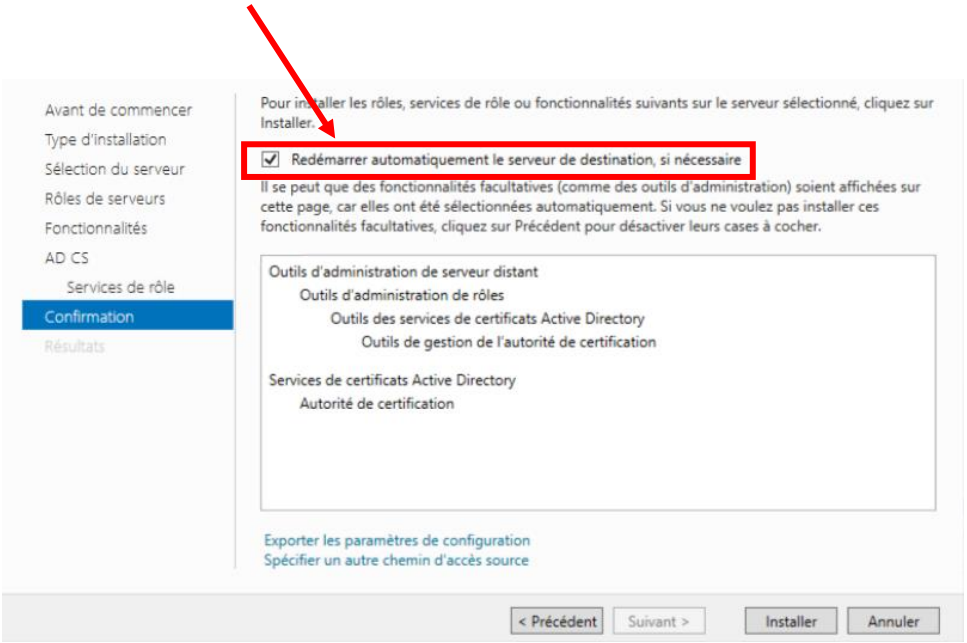
Faire “Suivant” deux fois, puis cocher “Services de certificats Active Directory” et faire “Suivant” encore trois fois



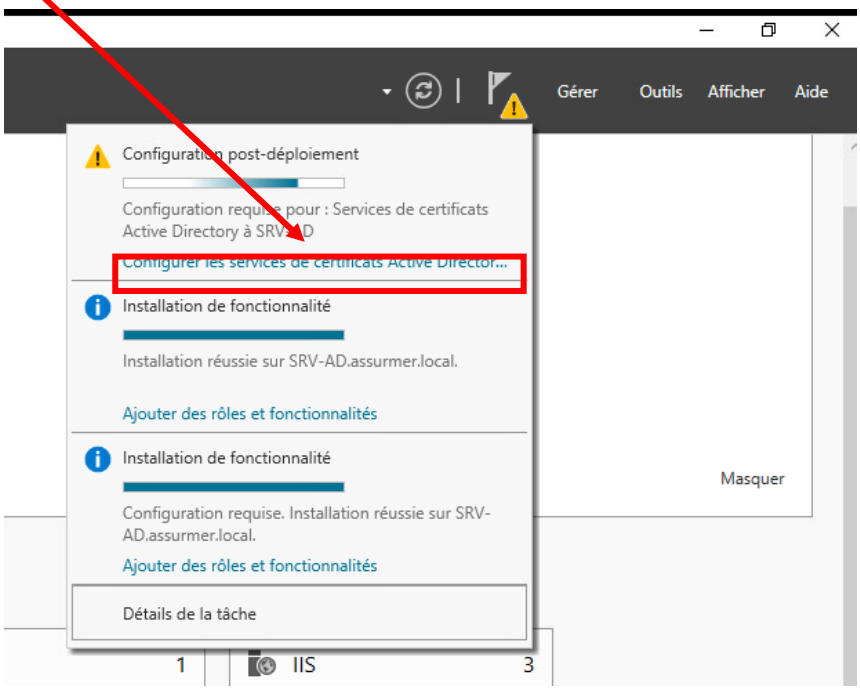
Cocher ensuite « Autorité de certification », et faites « Suivant »



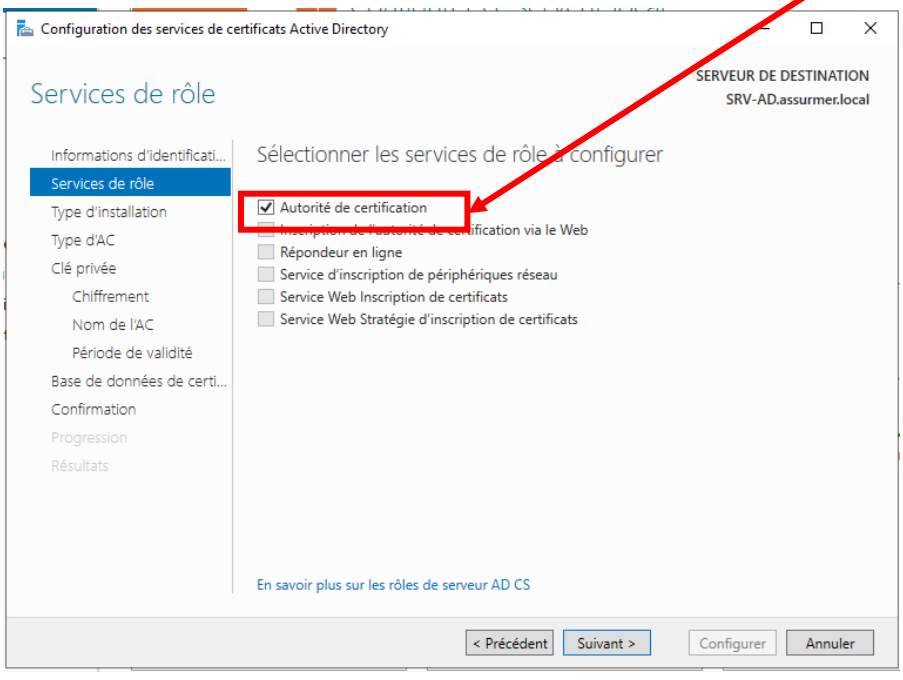
Cocher la case pour redémarrer automatiquement le serveur, puis faire “Installer”



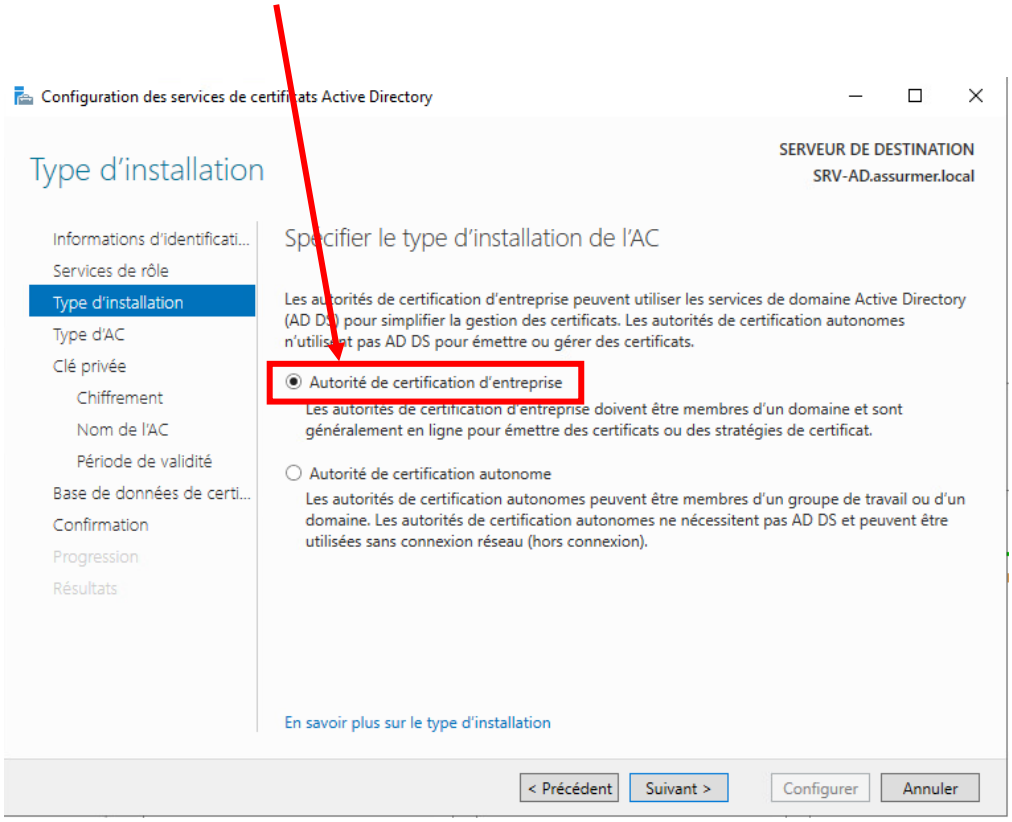
Une fois l'installation finie, retournez sur le Gestionnaire de serveur et cliquez sur « Configurer les services de certificats AD »



Faire "Suivant" une fois en laissant les paramètres par défaut, puis cocher "Autorité de certification" et continuer.

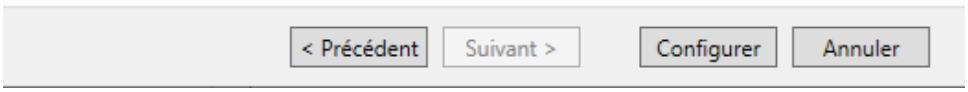


Cocher « Autorité de certification d'entreprise » puis faire « Suivant »



Faire « Suivant » en laissant les paramètres par défaut sur chaque étape.

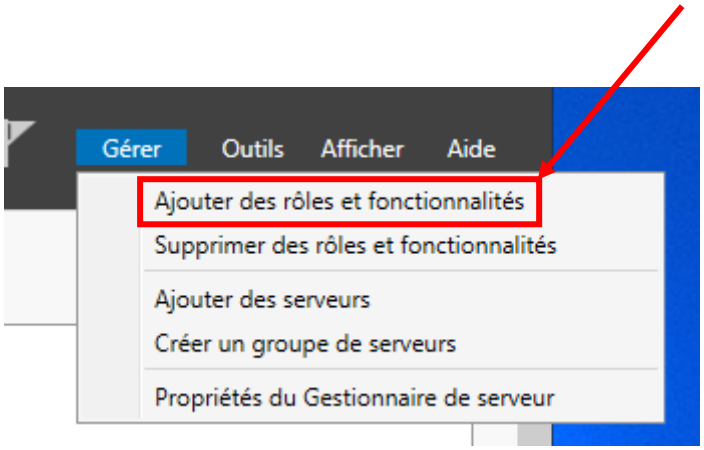
Une fois arrivé à l'étape « Confirmation », cliquez simplement sur « Configurer »



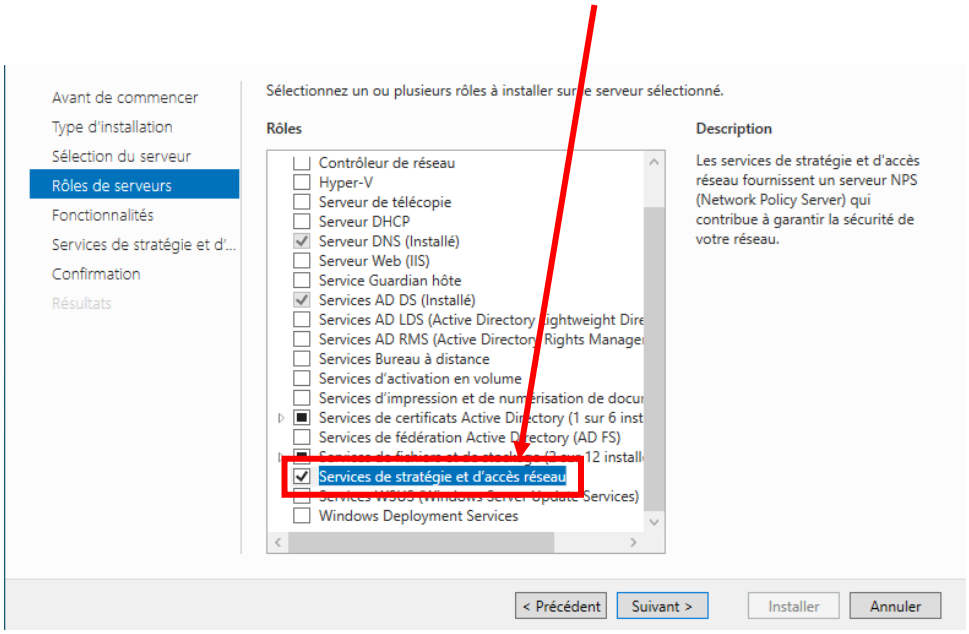
La configuration de l'ADCS est désormais finie.

Installation et configuration du service NPS (RADIUS)

Dans le gestionnaire de serveur, appuyer sur « Gérer » puis « Ajouter des rôles et des fonctionnalités »

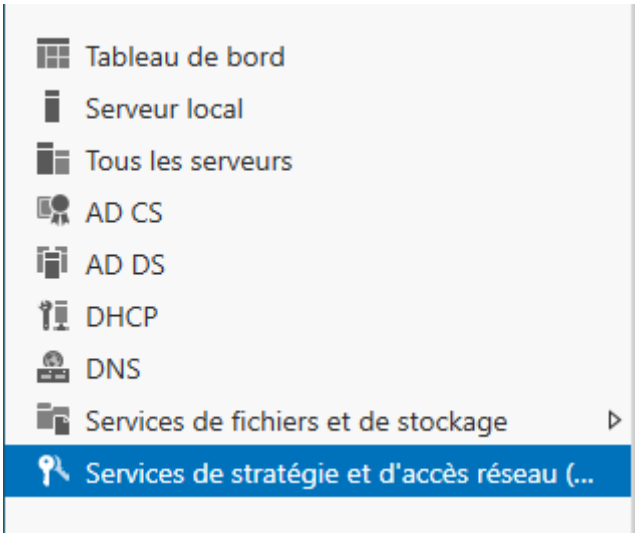


Faire « Suivant » deux fois, puis cocher « Services de stratégie et d'accès réseau »

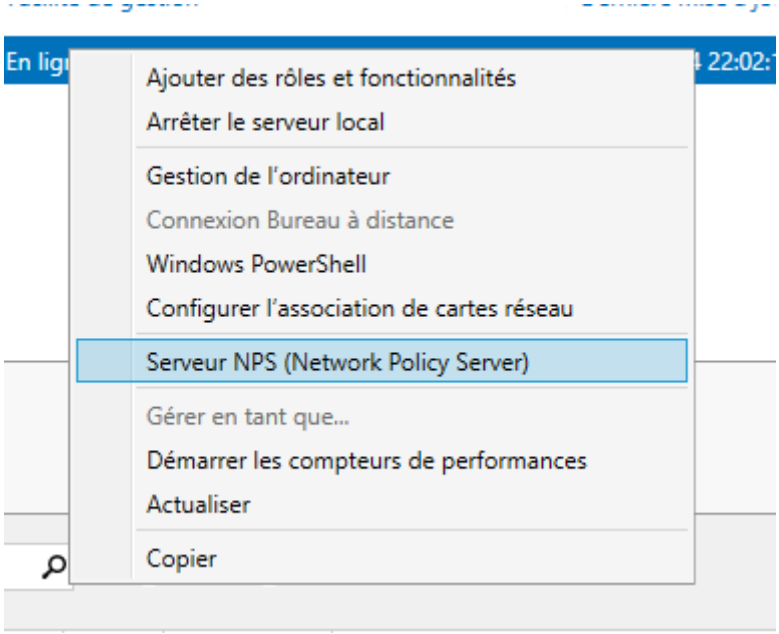


Faire « Suivant » jusqu'à l'installation du service.

Cliquer sur « Services de stratégie et d'accès réseau »



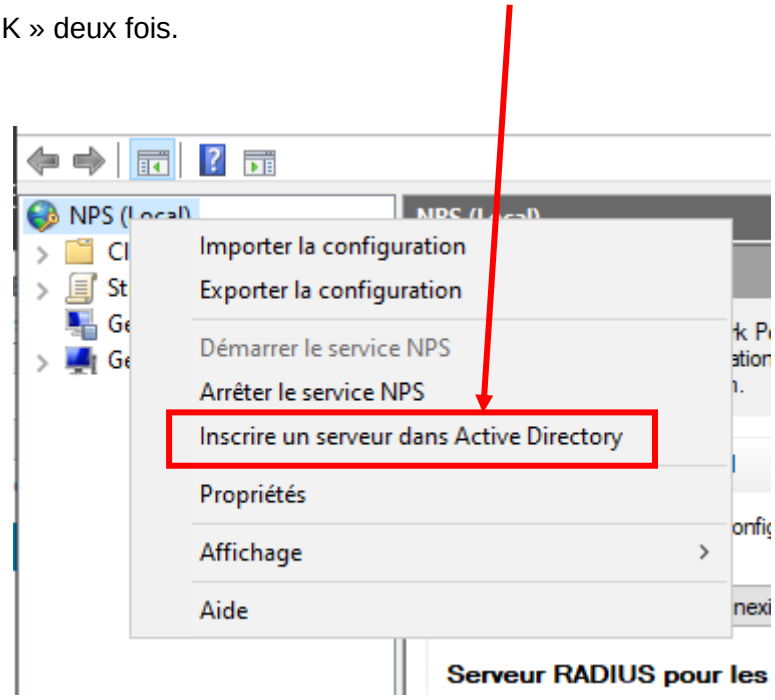
Faire un clic droit sur le serveur, puis cliquer sur « Serveur NPS »



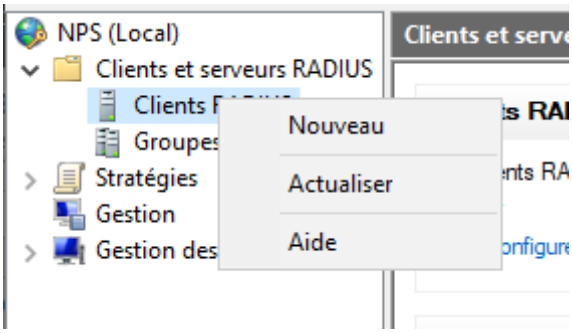
Une nouvelle fenêtre s'ouvre.

Faire clic droit sur « NPS (Local) », puis « Inscrire un serveur dans AD ».

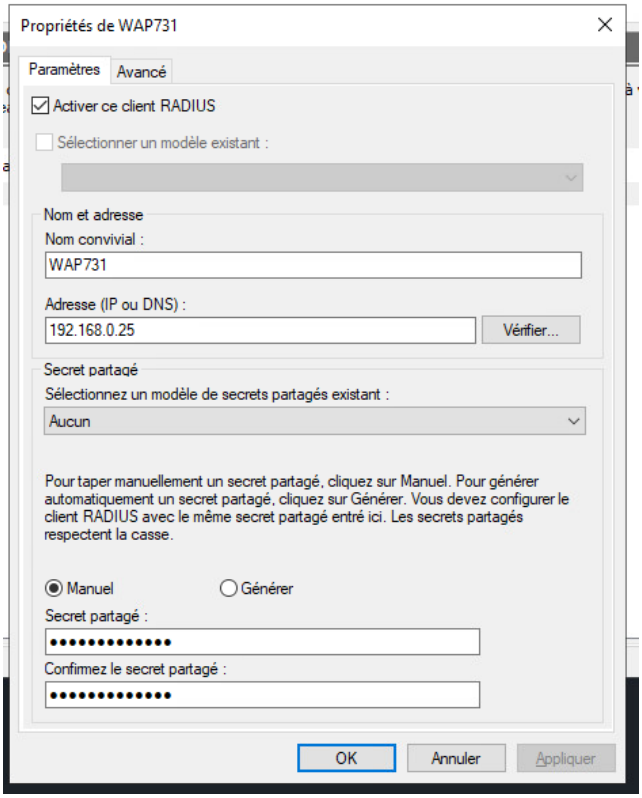
Appuyer sur « OK » deux fois.



Ensuite, aller dans le dossier "Clients et serveurs RADIUS", faire un clic droit sur "Clients RADIUS" puis "Nouveau"

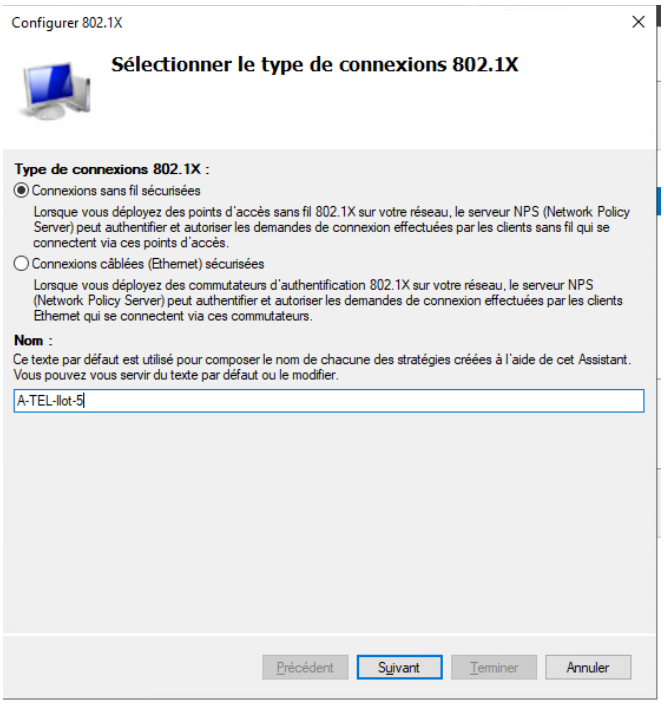


Ajouter les informations comme vu ci-dessous, puis appuyer « OK »

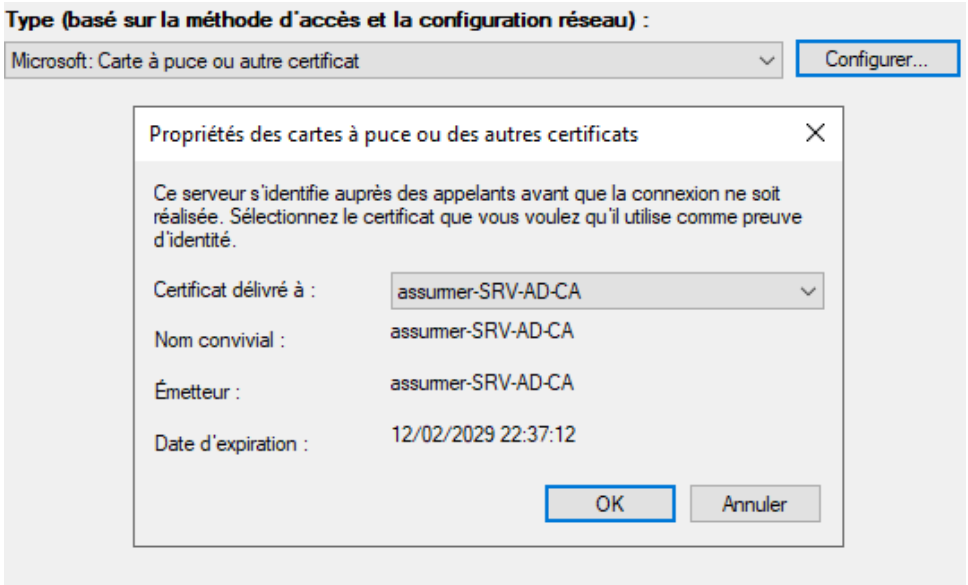


Aller sur « NPS (Local) », puis passer la configuration standard en « 802.1X ». Ensuite « Configurer 802.1X ».

Une nouvelle fenêtre s'ouvre. Cocher « Connexion sans fil sécurisées » puis donner un nom et faire "Suivant" deux fois

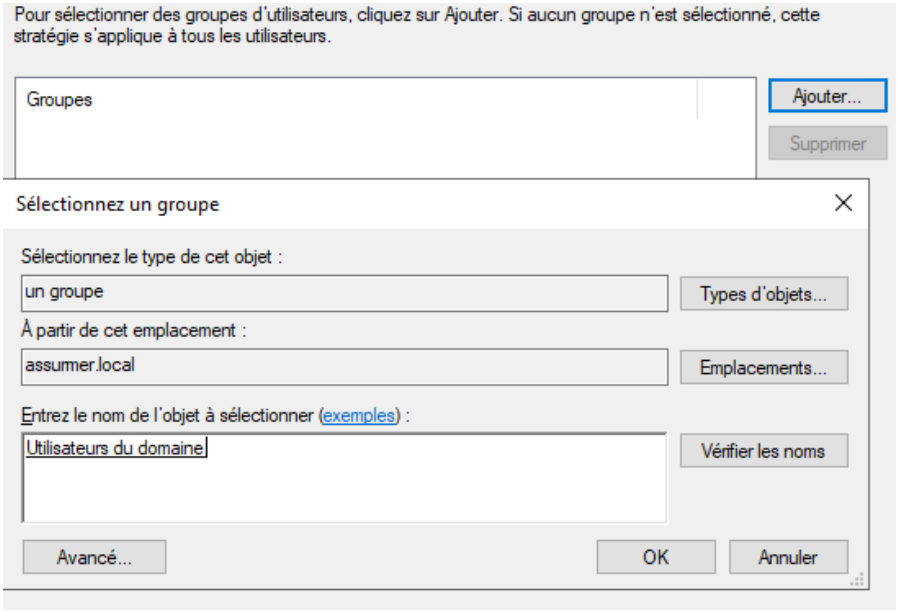


Cliquer sur « Configurer », puis choisir l'AD CS comme certificat et continuer

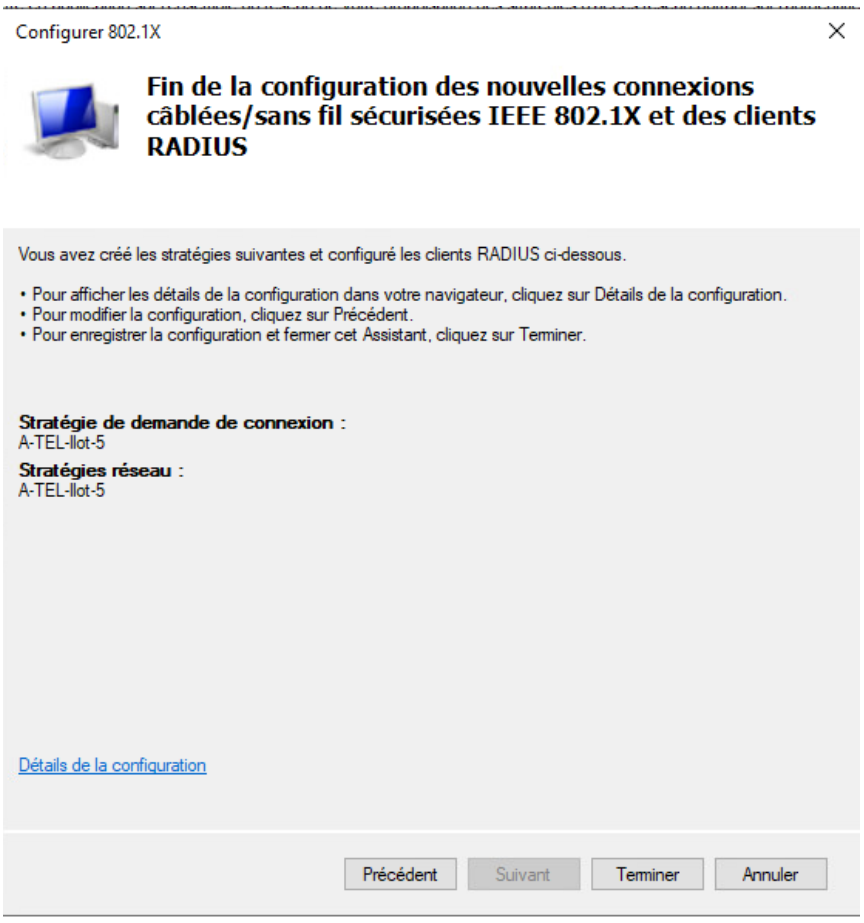


Faire « ajouter », et sélectionner le groupe “Utilisateurs du domaine”.

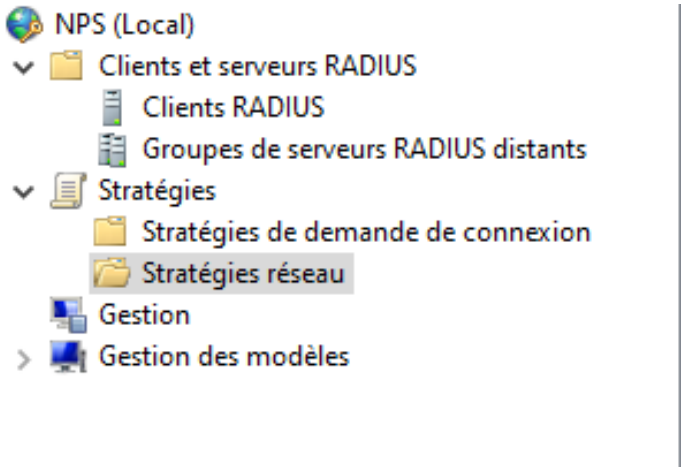
Appuyer “OK” puis “Suivant”



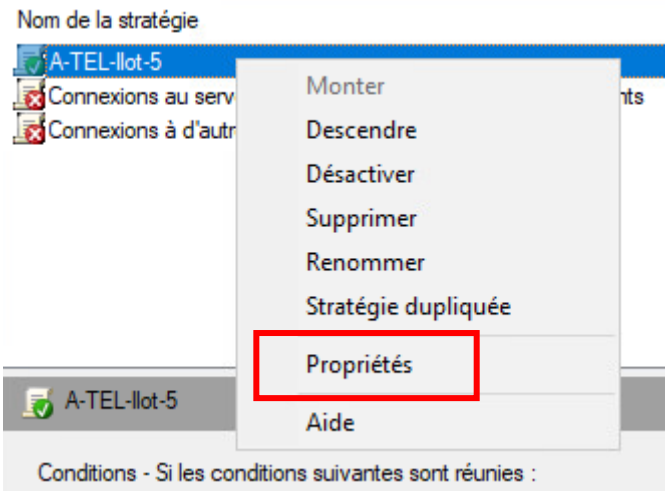
Refaites « Suivant » une fois, puis « Terminer »



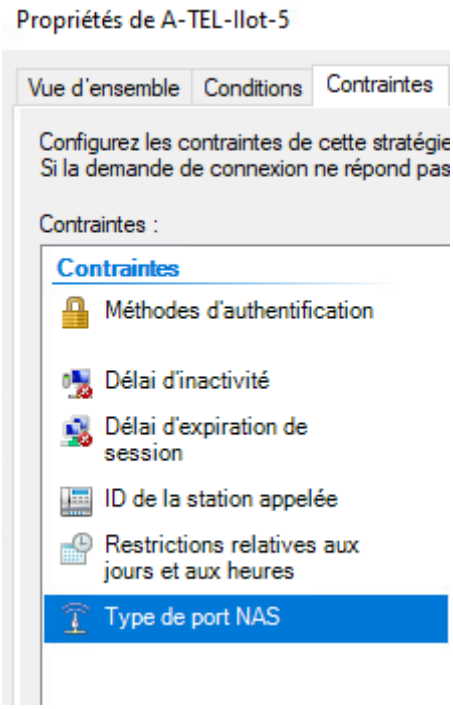
Aller dans “Stratégies”, et “Stratégies réseau”



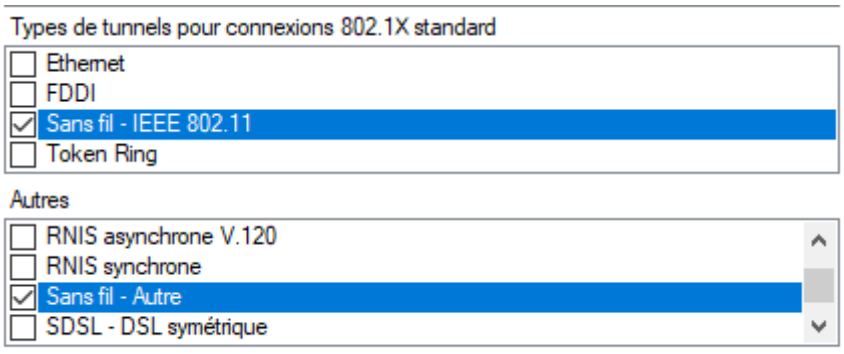
Faire un clic droit puis “Propriétés” sur “WI-FI_TEST”



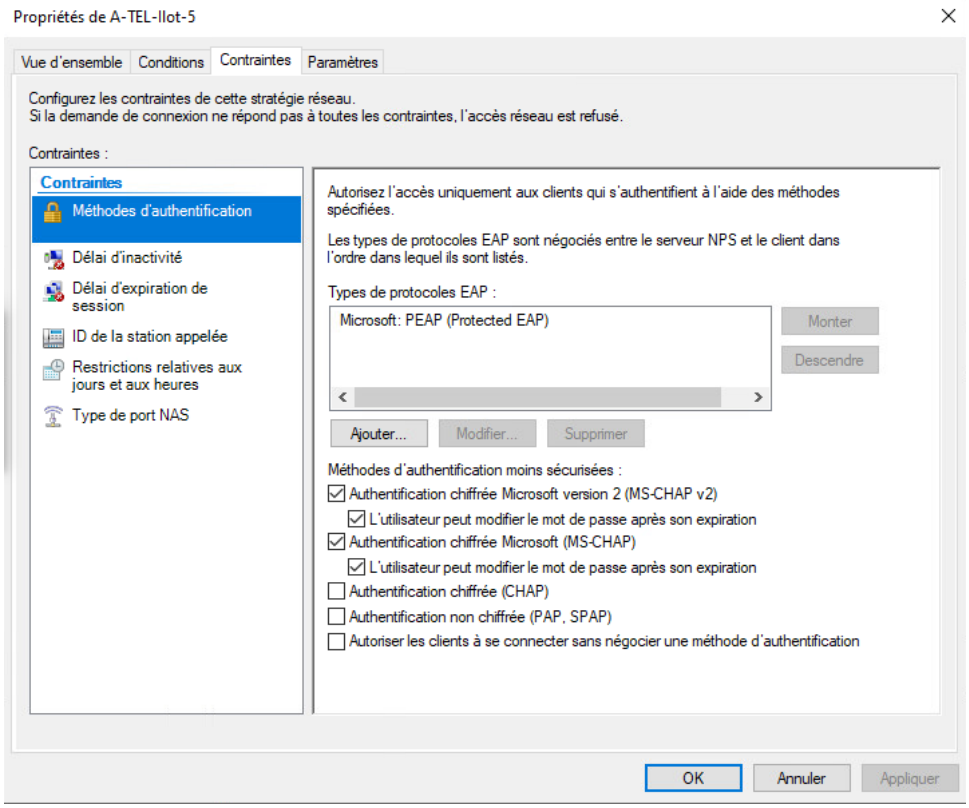
Dans « Contraintes » puis « Type de port NAS »,



Cocher “Sans fil – IEEE 802.11” dans “Types de tunnels 802.1X” et “Sans fil – Autre" dans “Autres”



Dans « Méthodes d'authentification », cliquer sur « Ajouter » puis sélectionner « Microsoft : PEAP (Protected EAP) »



"Appliquer" et terminer par appuyer sur "OK".

La configuration est désormais terminée.