Documentation

Serveur Radius

Hourlay Nolann - Le Henaff Noah

Sommaire

Contexte

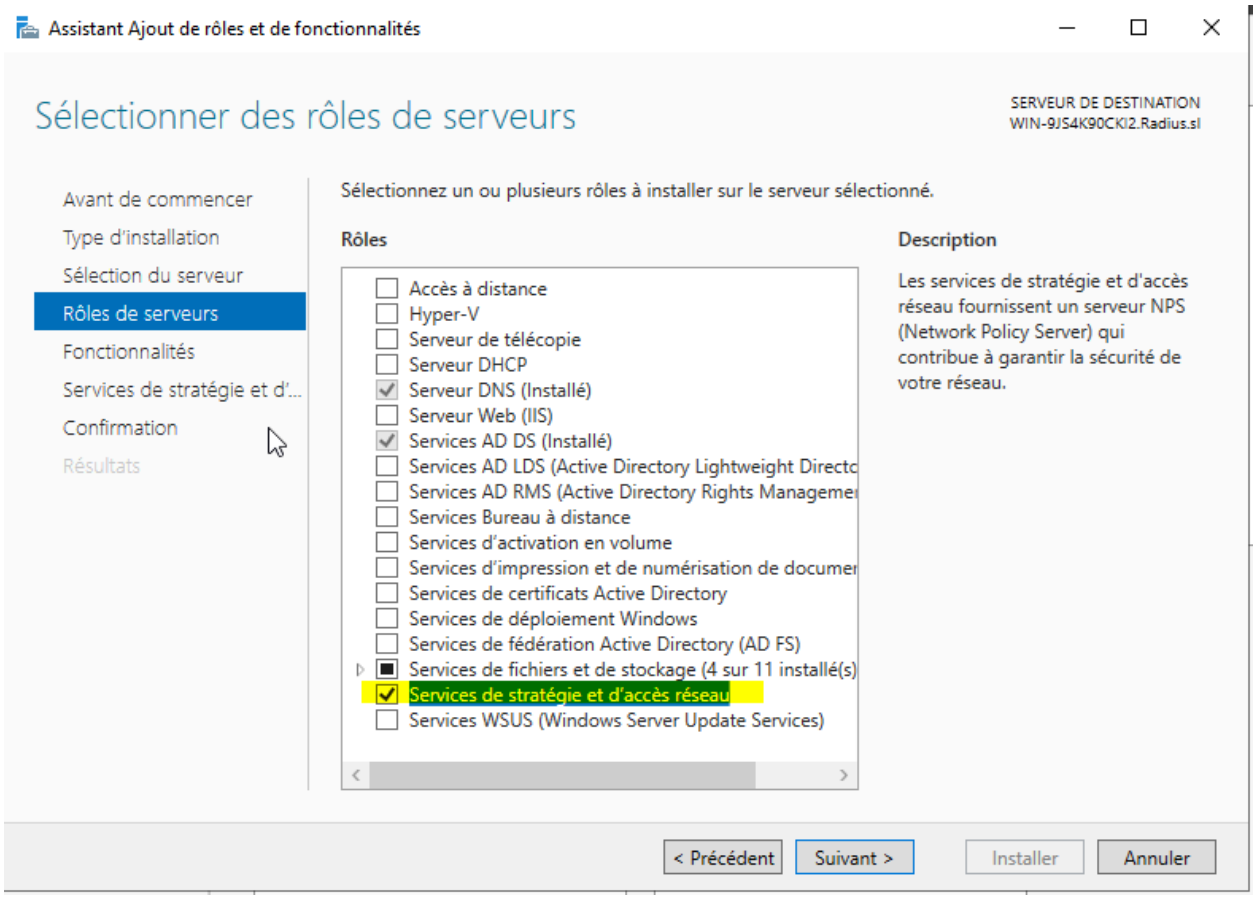
On possède actuellement une infrastructure fonctionnelle similaire à une entreprise, mais sur notre routeur wifi, on souhaiterait avoir une sécurité plus forte au niveau des connexions. Pour pallier ce problème, on va installer un serveur Radius.

Un serveur RADIUS (Remote Authentication Dial-In User Service) est un serveur qui vérifie l'identité des utilisateurs qui essaient d'accéder à un réseau ou à un service informatique.

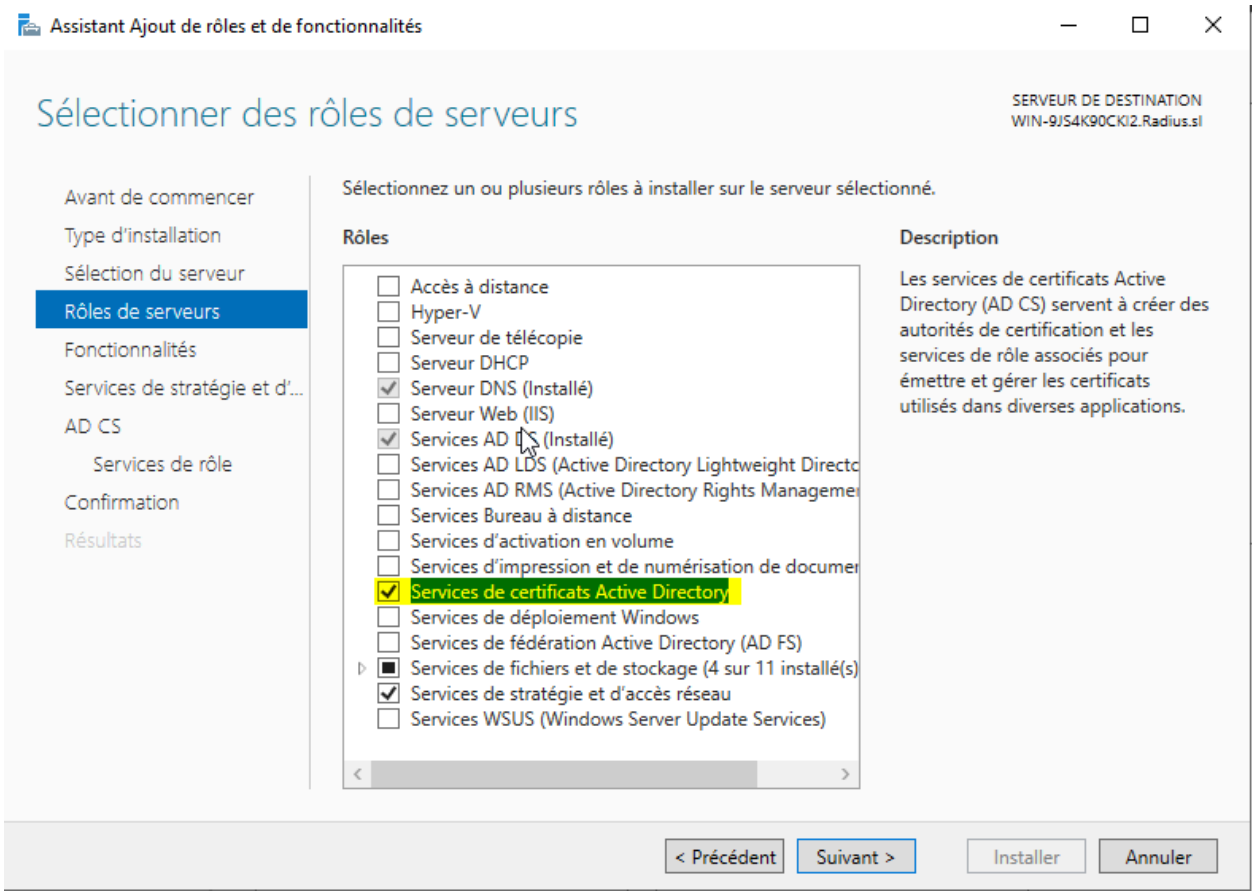
Dans notre infrastructure, on va le rattacher à notre Active Directory, les authentifications pour accéder au réseau sans fil se feront avec les comptes utilisateurs Active Directory (LDAP).

Installation des rôles

Après avoir configuré le serveur de domaine, nous ajoutons le rôle “Services de stratégie et d’accès réseau”.

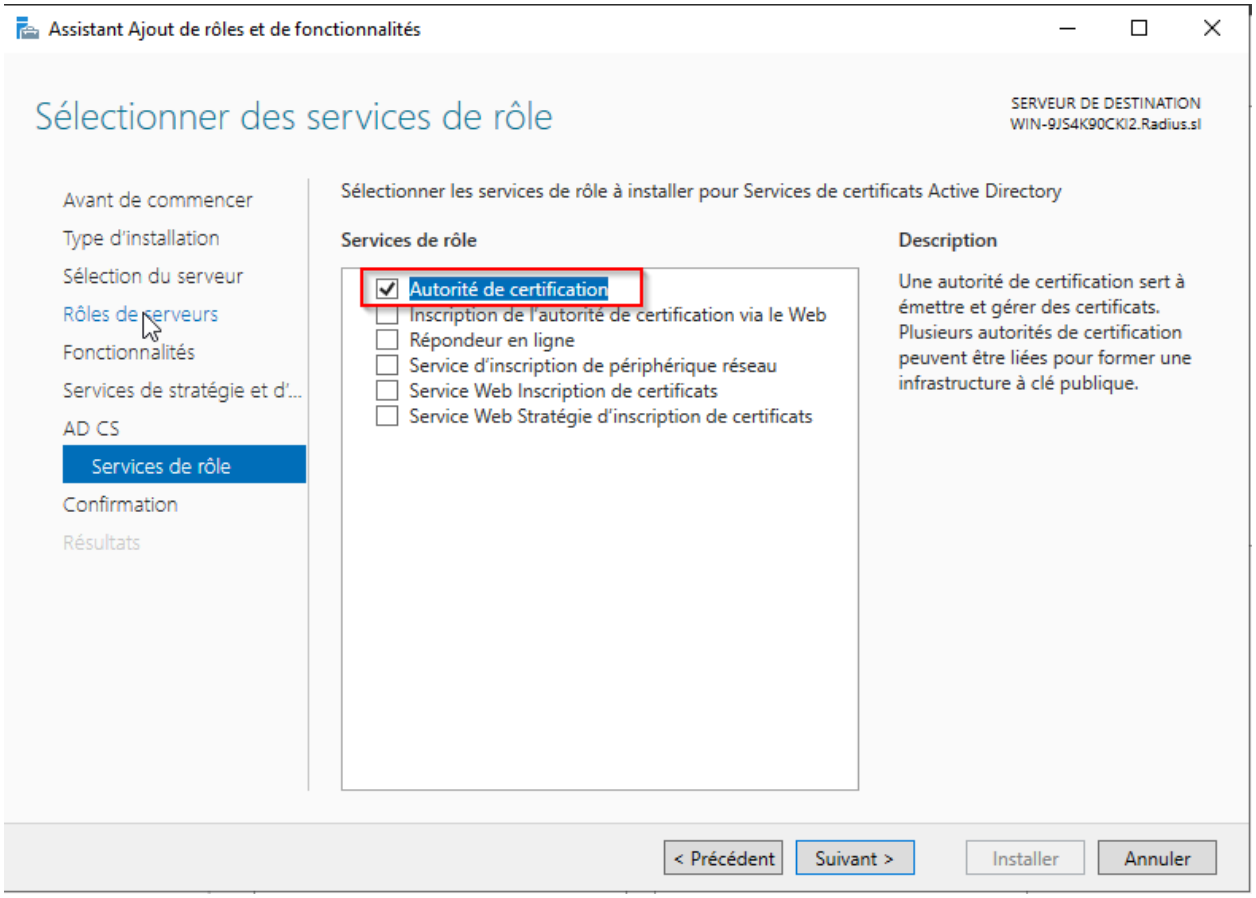


Ensuite, il faut installer le service de certificats Active Directory.



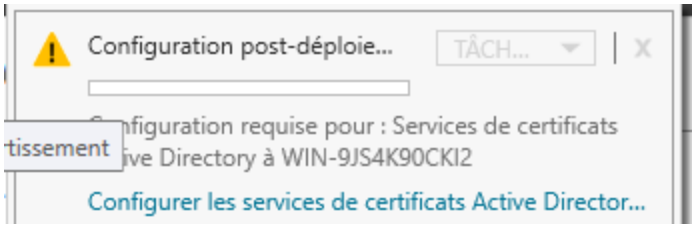
Vous pouvez cliquer sur “suivant”, jusqu'à la catégorie “Services de rôle”

Dans la catégorie “Service de rôle”, vérifiez bien que la case “Autorité de certification” est cochée.

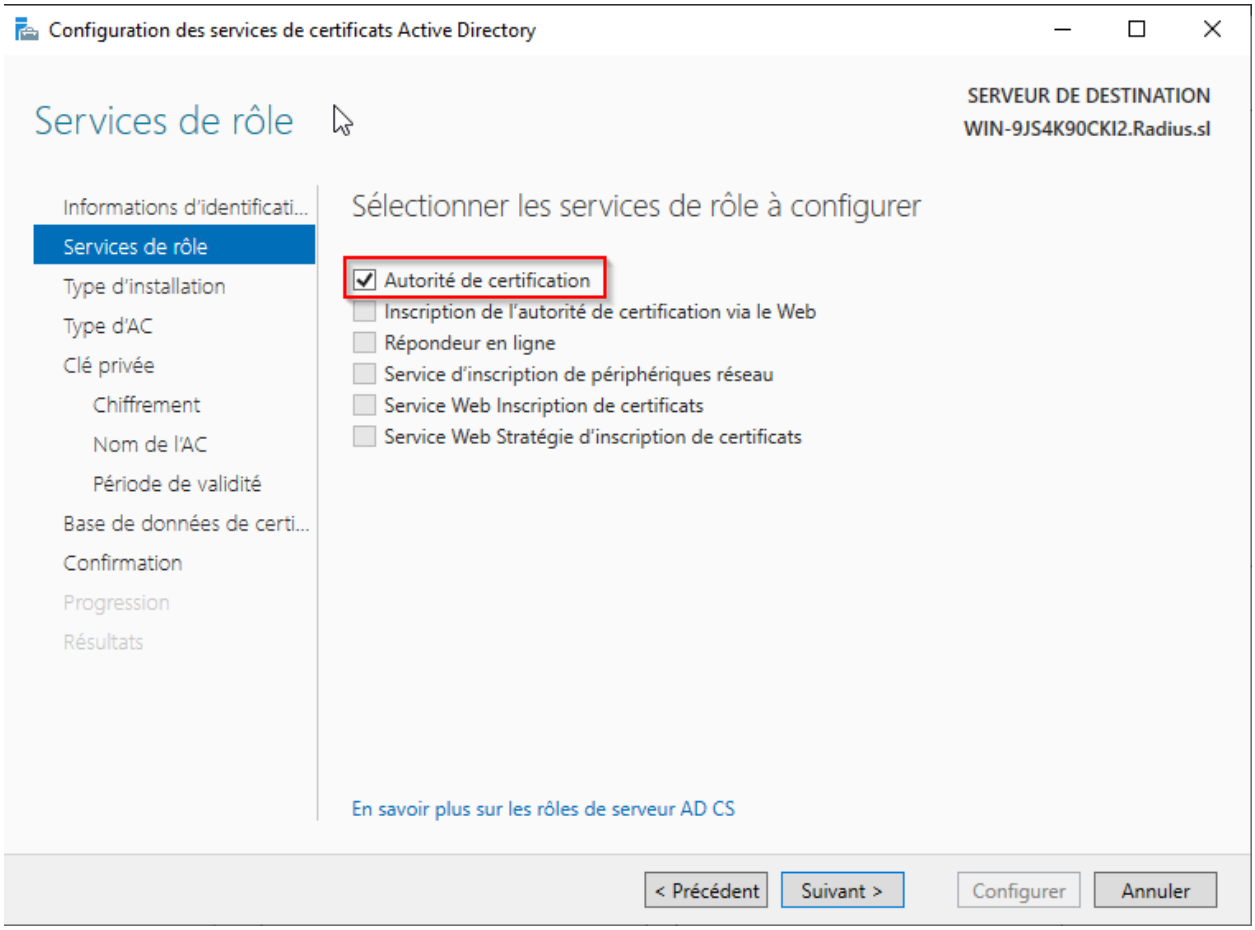


Création d’un certificat d’authentification

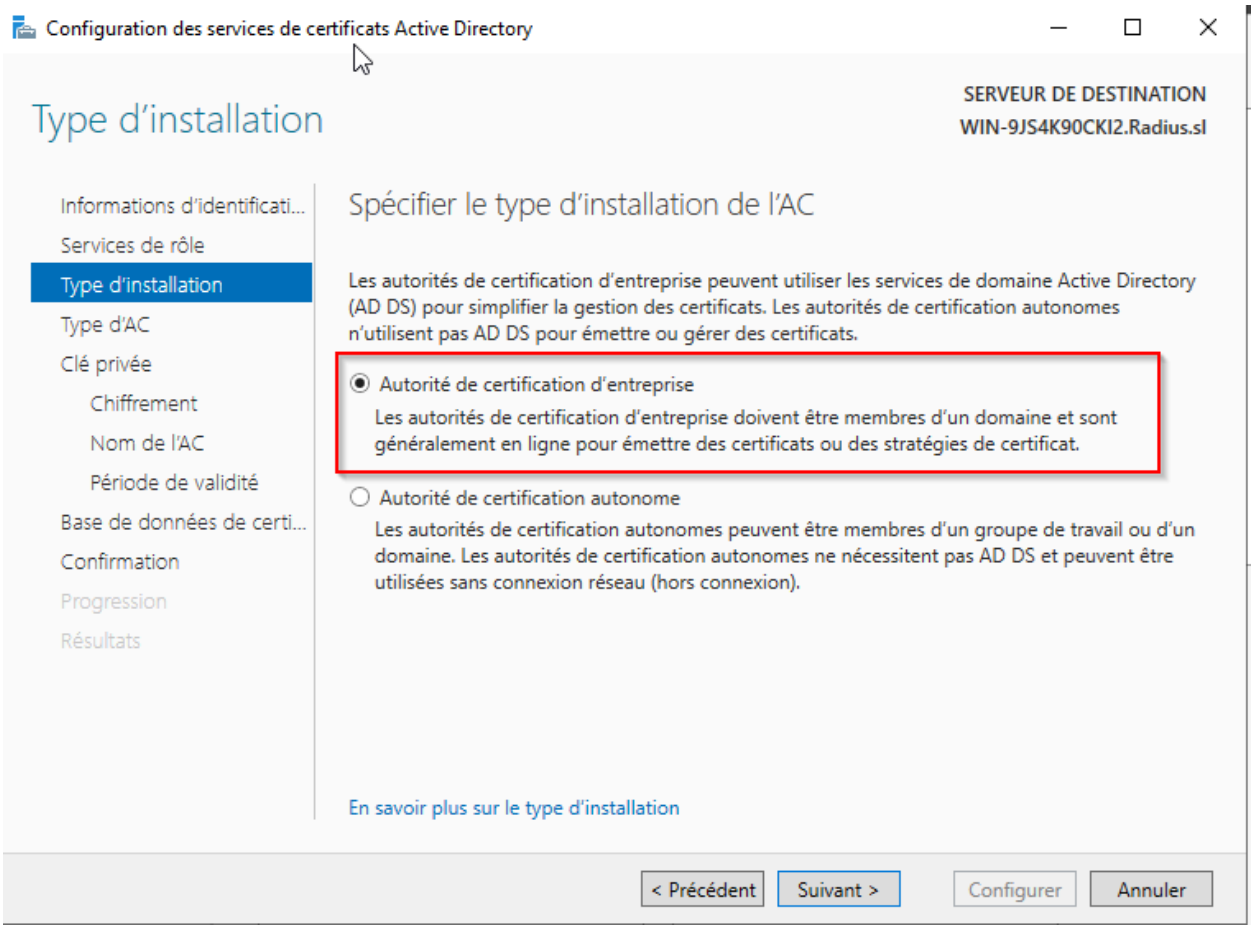
Pour pouvoir créer le certificat, il faut la configuration post-déploiement :



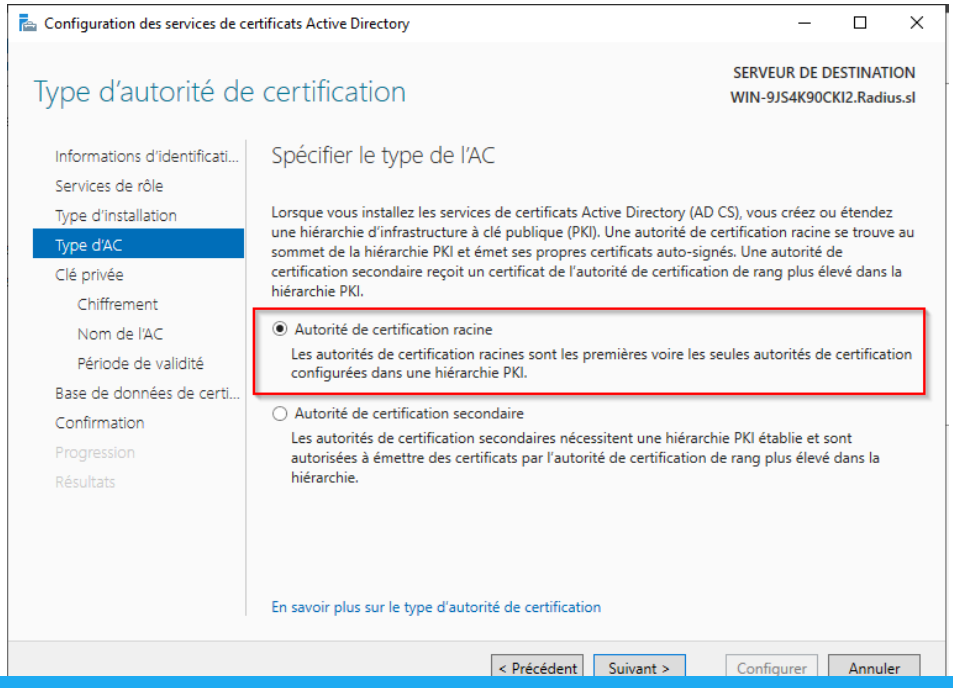
Cliquez sur “suivant” et cochez la case “Autorité de certification”.



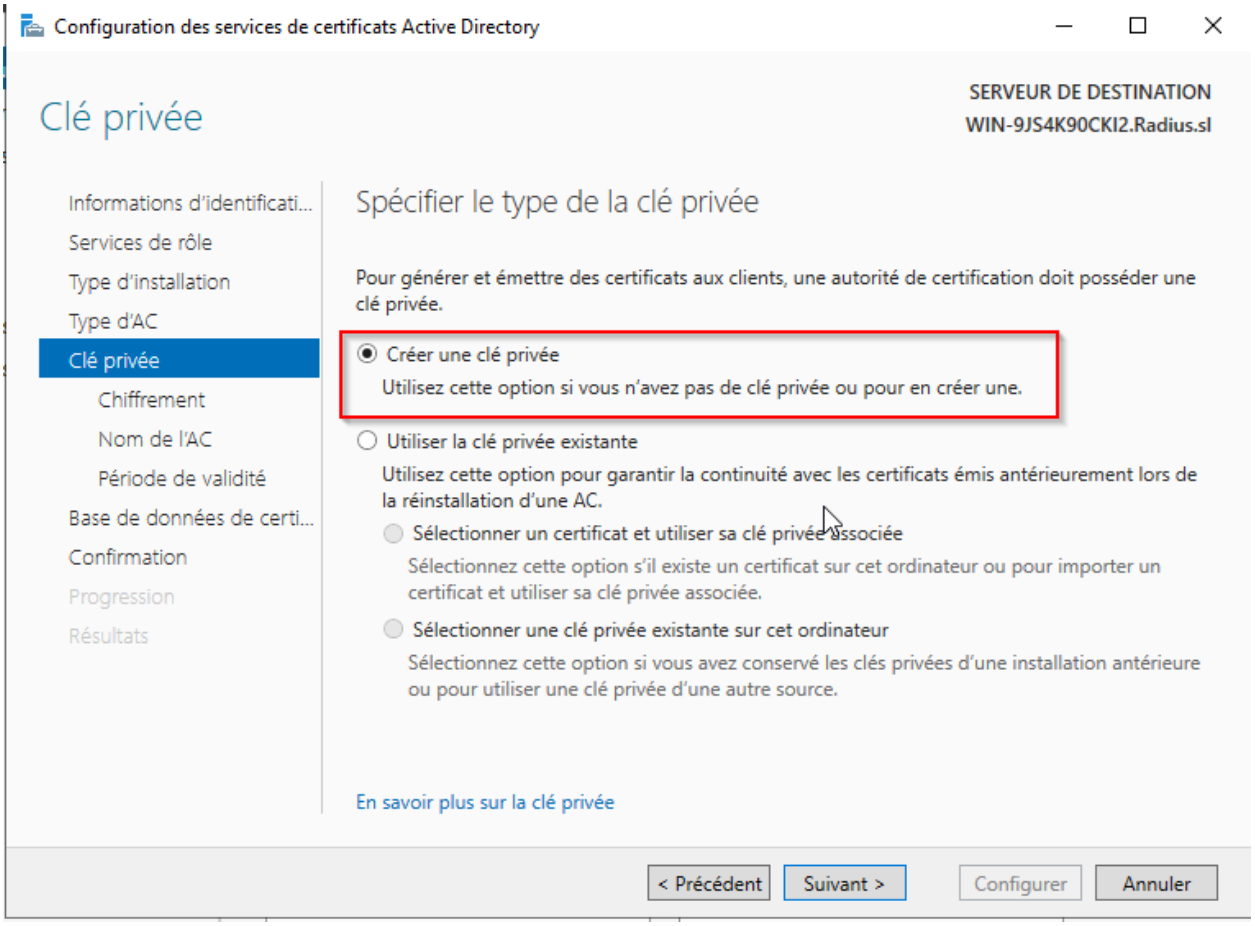
Il faut choisir “Autorité de certification d’entreprise”.



Ensuite, on choisit “Autorité de certification racine”.

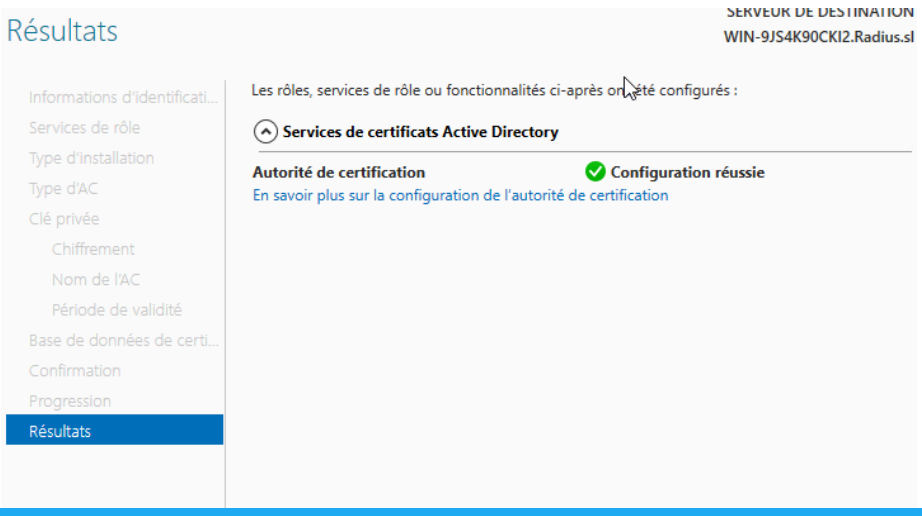


Nous créons une clé privée.



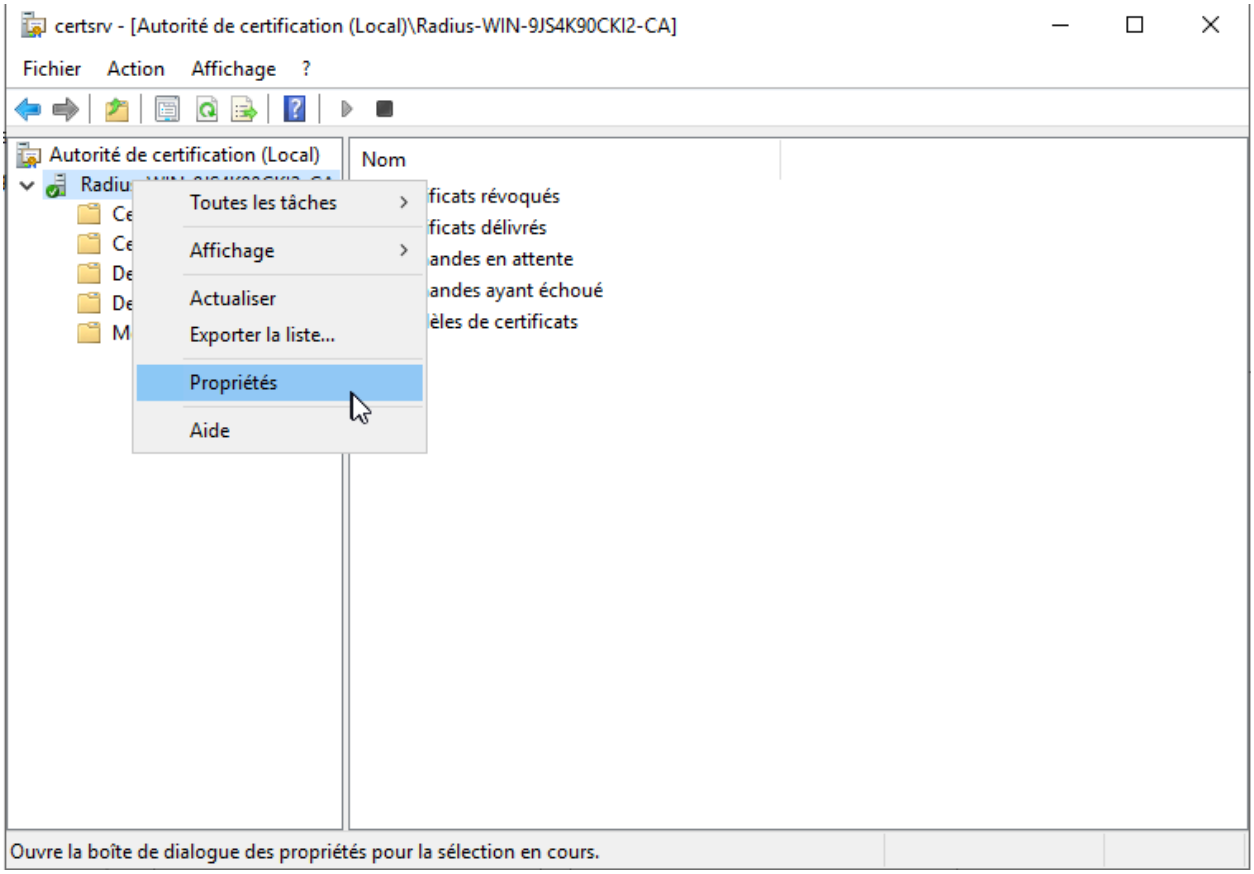
Par la suite, nous pouvons appuyer sur “suivant” jusqu'à la création car nous laissons tout par défaut.

Nous pouvons voir que la configuration du certificat est réussie.

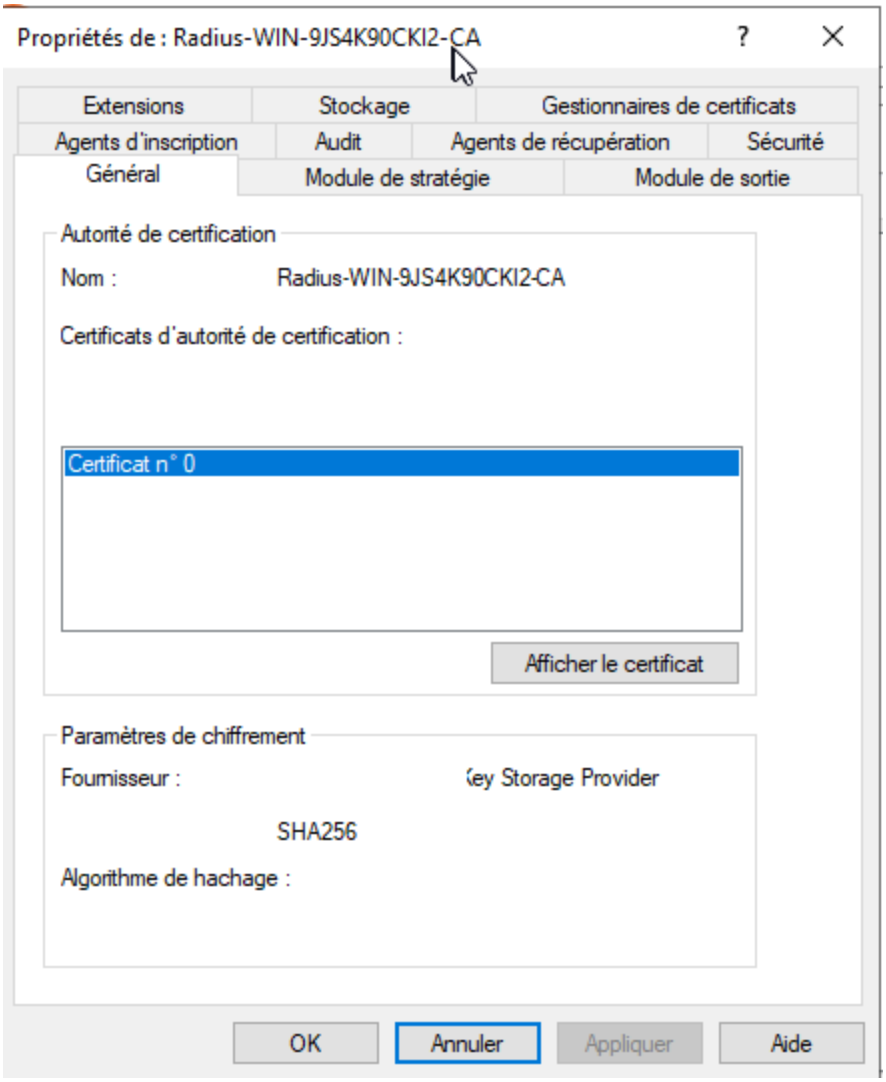


Maintenant, on va exporter le certificat. Pour cela, ouvrez “l'autorité de certification”.

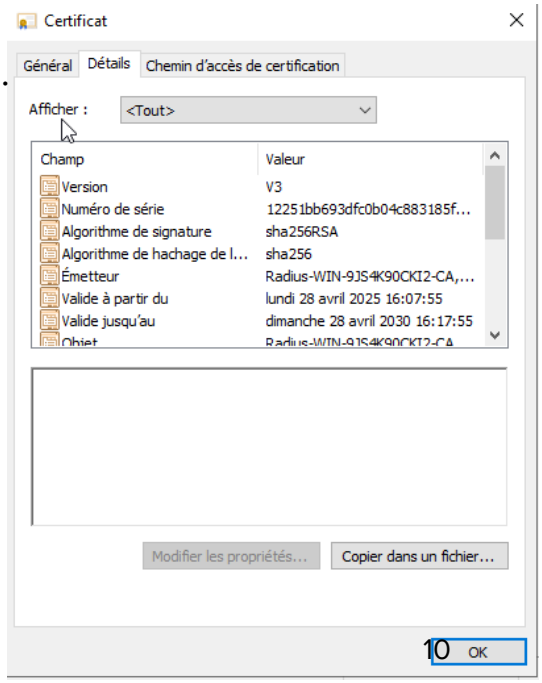
Faites clic droit, propriété sur le nom de votre serveur.



Vous arriverez ici :



Cliquer sur Afficher le certificat, ensuite sur détail.



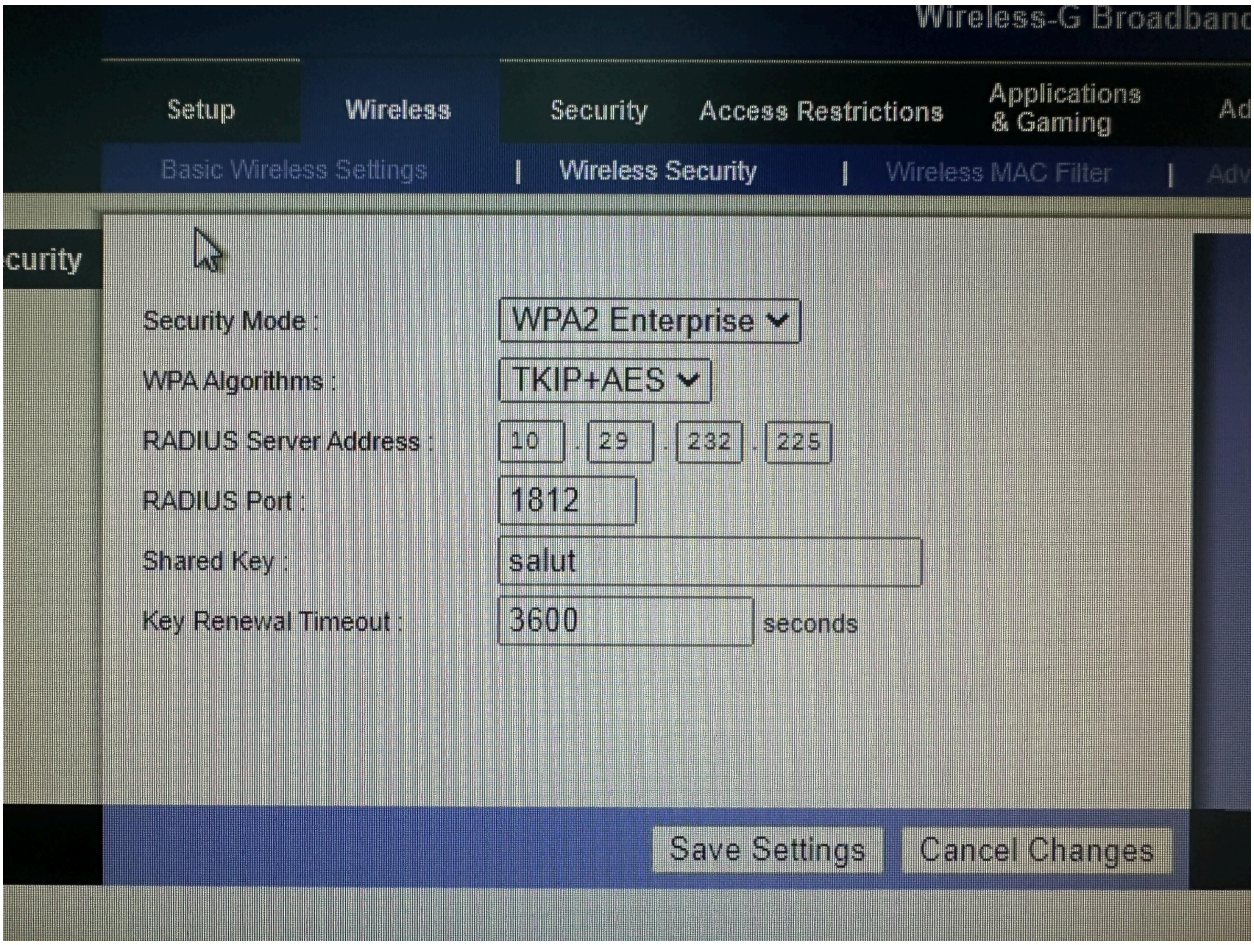
Cliquez sur “Copier dans un fichier”.

Créer un dossier, et placer la certification dedans. Laisser les valeurs par défaut.

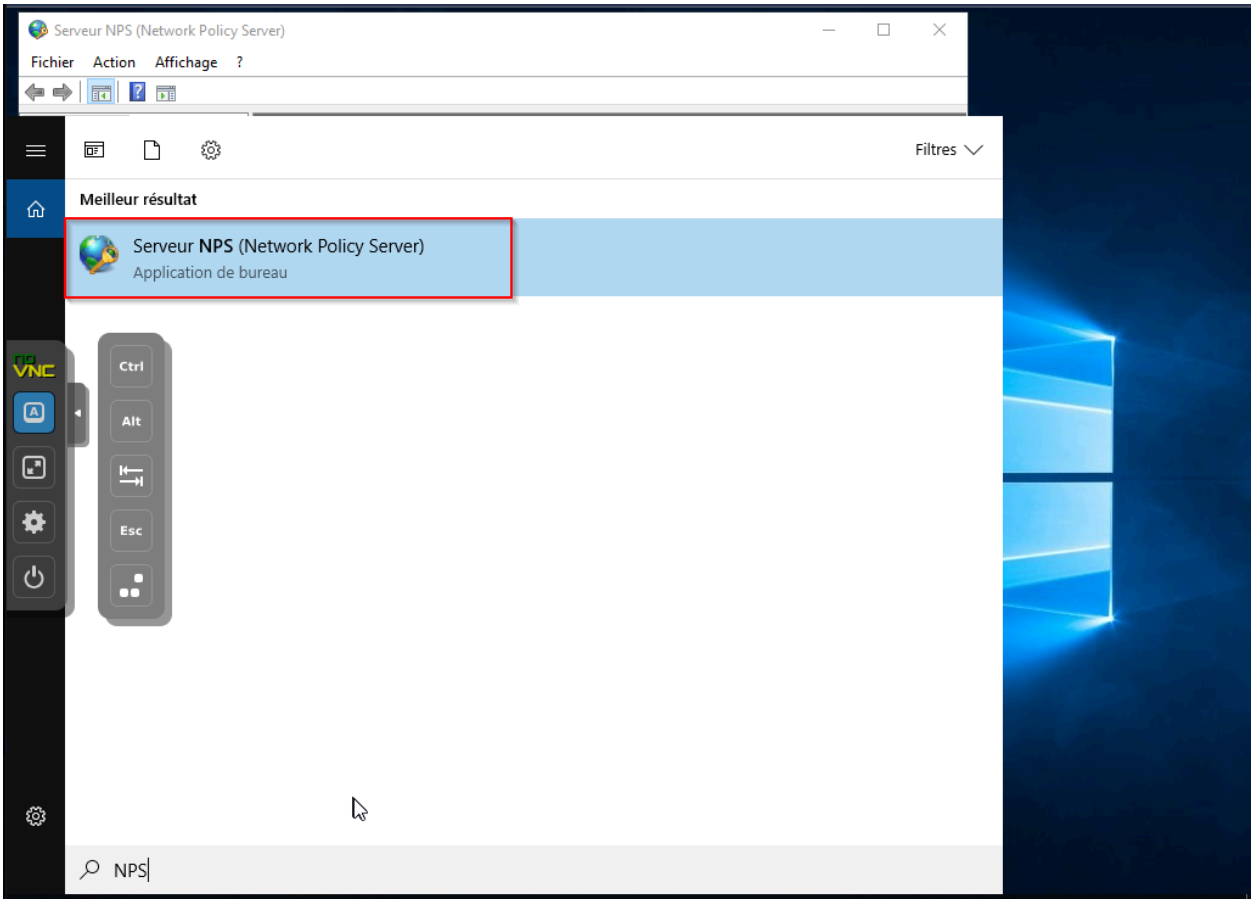
Configuration des éléments d'authentification

Sur le routeur wifi, dans Wireless puis Wireless Security. Renseigner certains éléments :

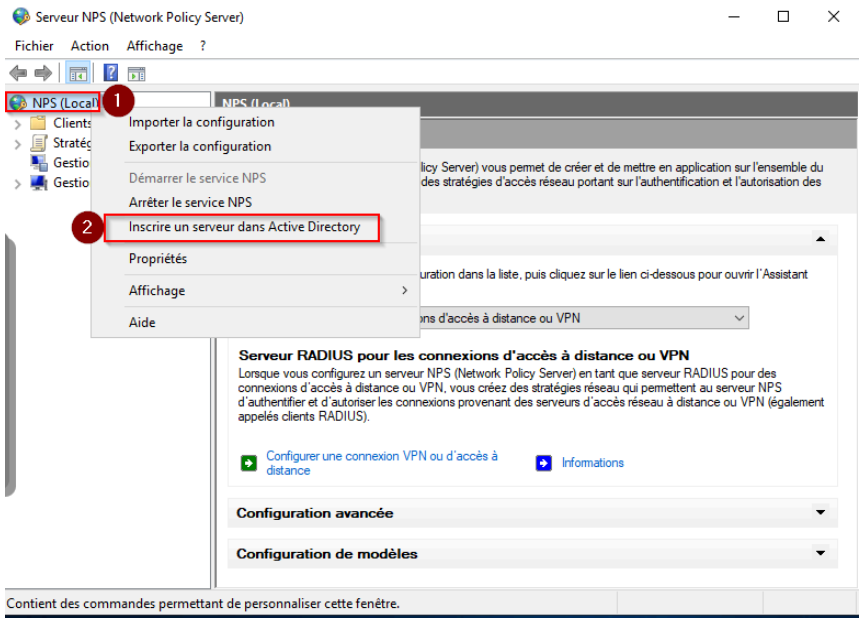
- mode de sécurité : WPA2 Entreprise
- adresse IP du serveur RADIUS
- Clé partagée



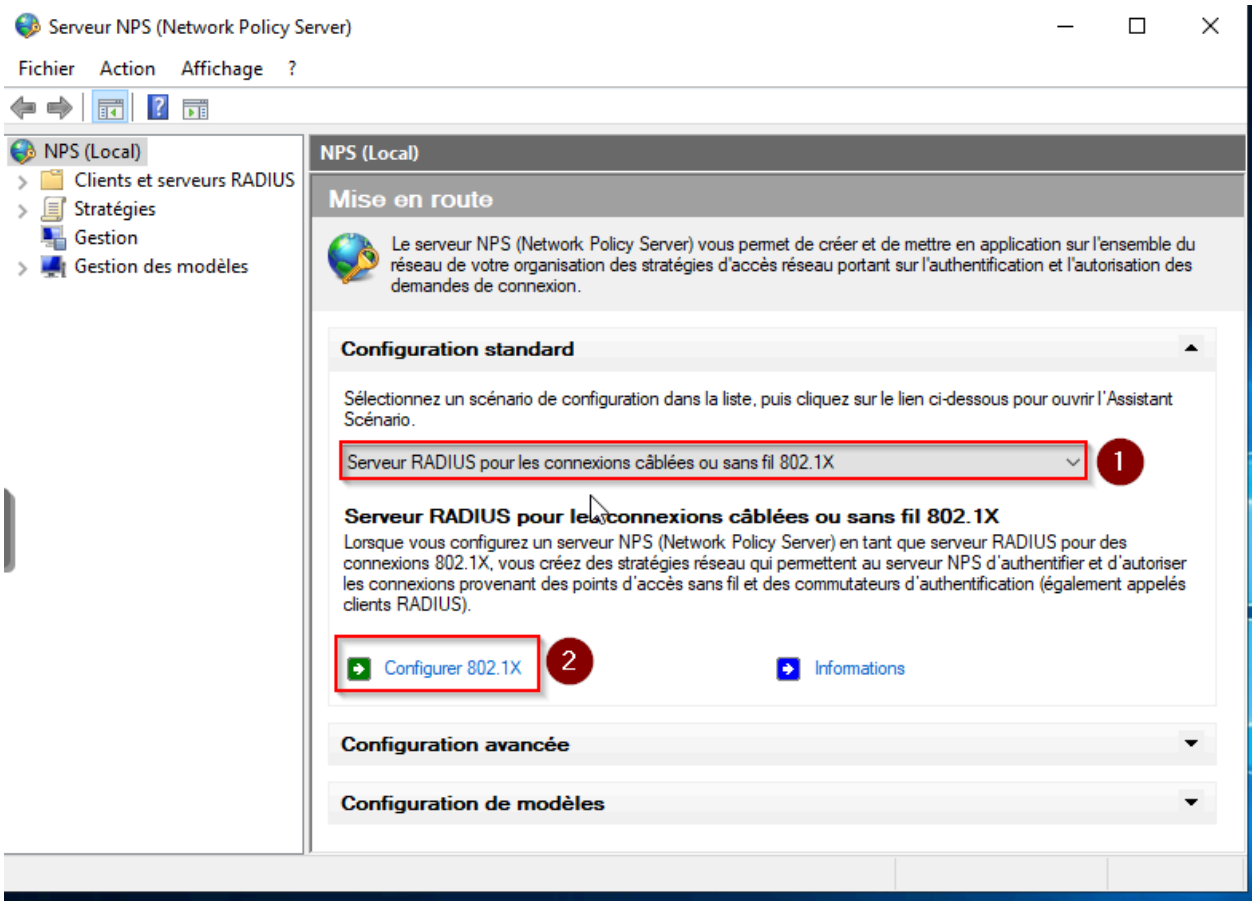
Ensuite, on se retrouve sur l'AD. Il faut ouvrir la console NPS.



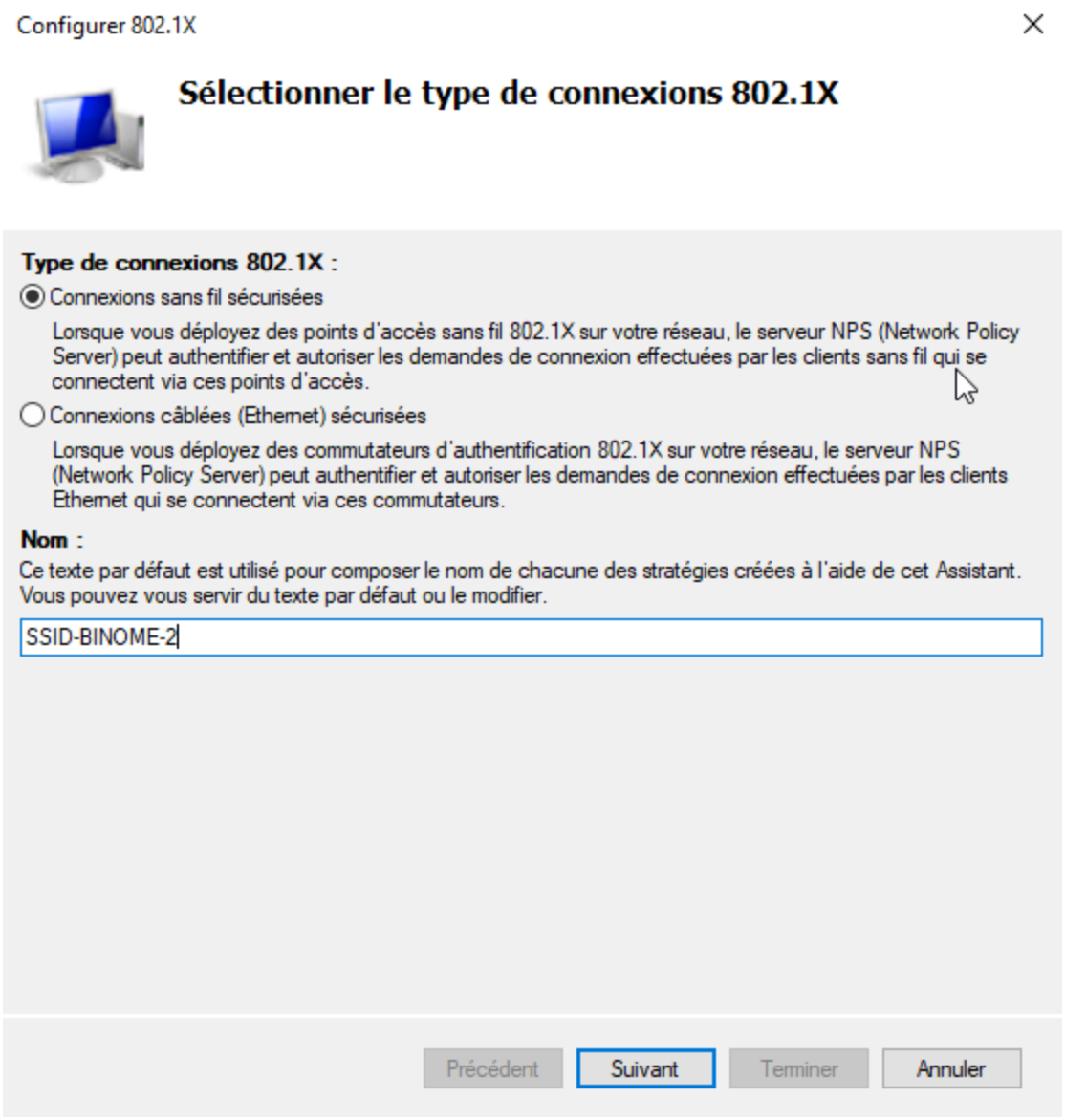
Faites clic droit sur NPS local et cliquez sur "Inscrire un serveur dans un Active Directory".



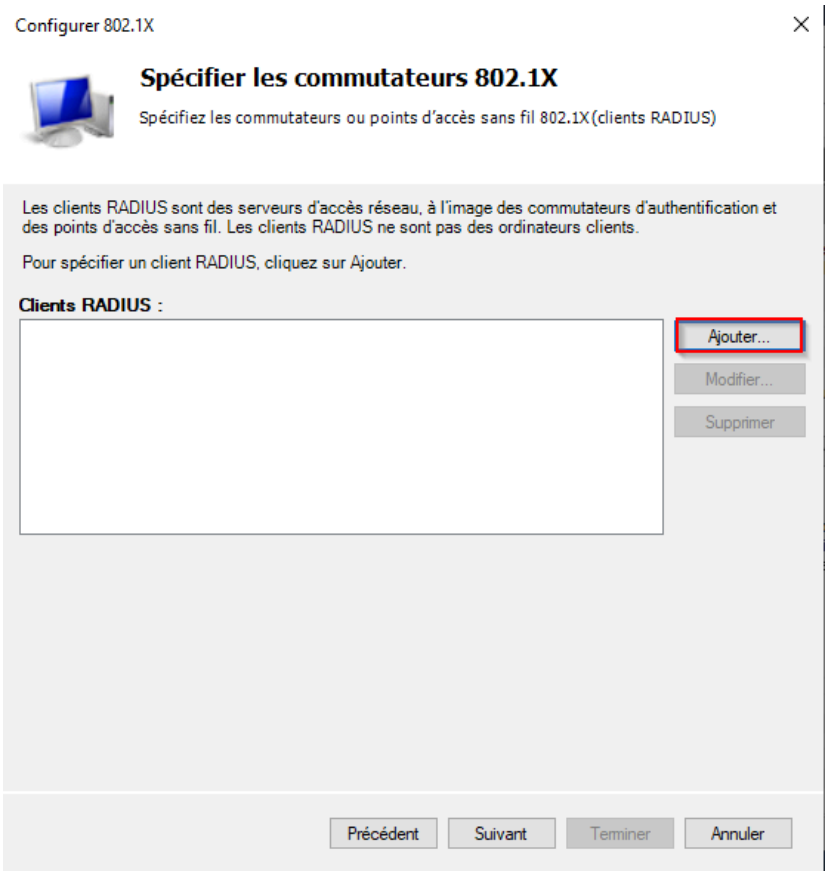
Après, nous allons sélectionner plusieurs informations.



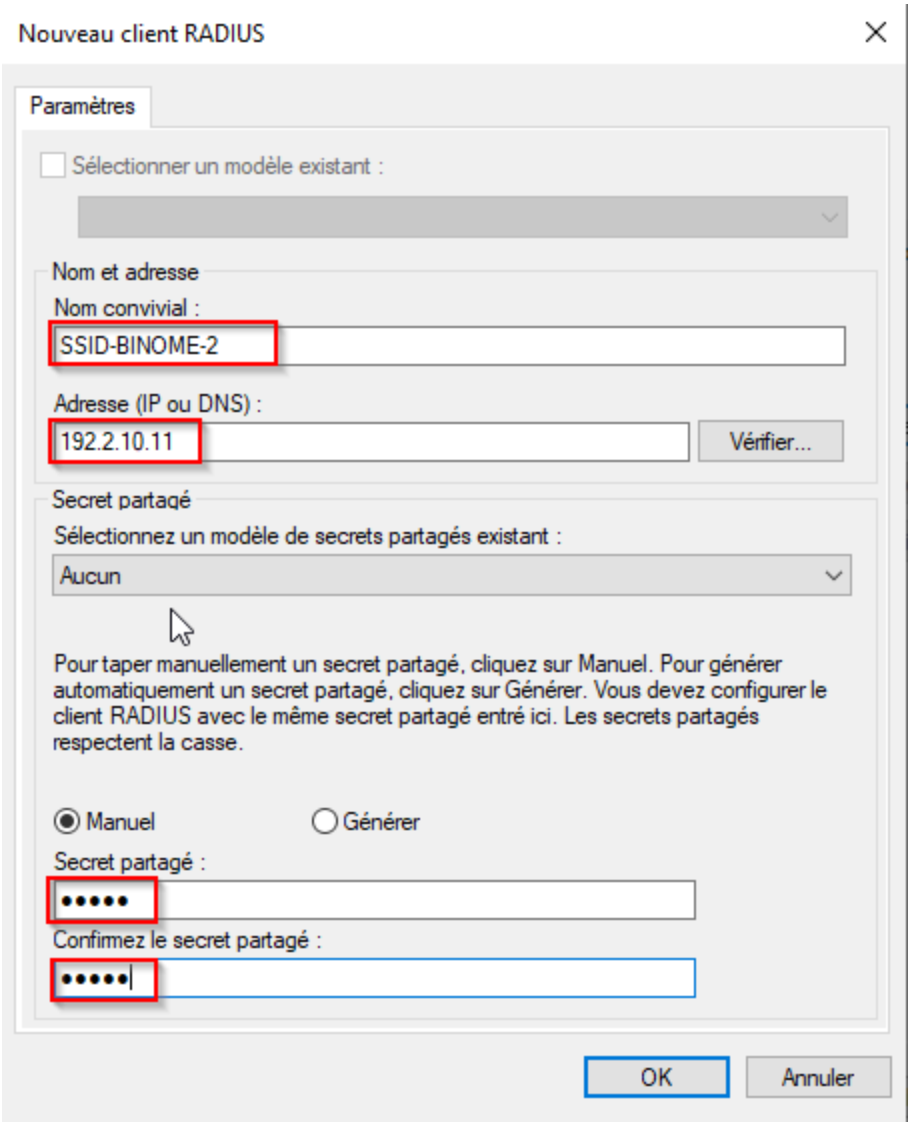
Ensuite, cochez la case “Connexions sans fil sécurisé” et renseignez un nom :



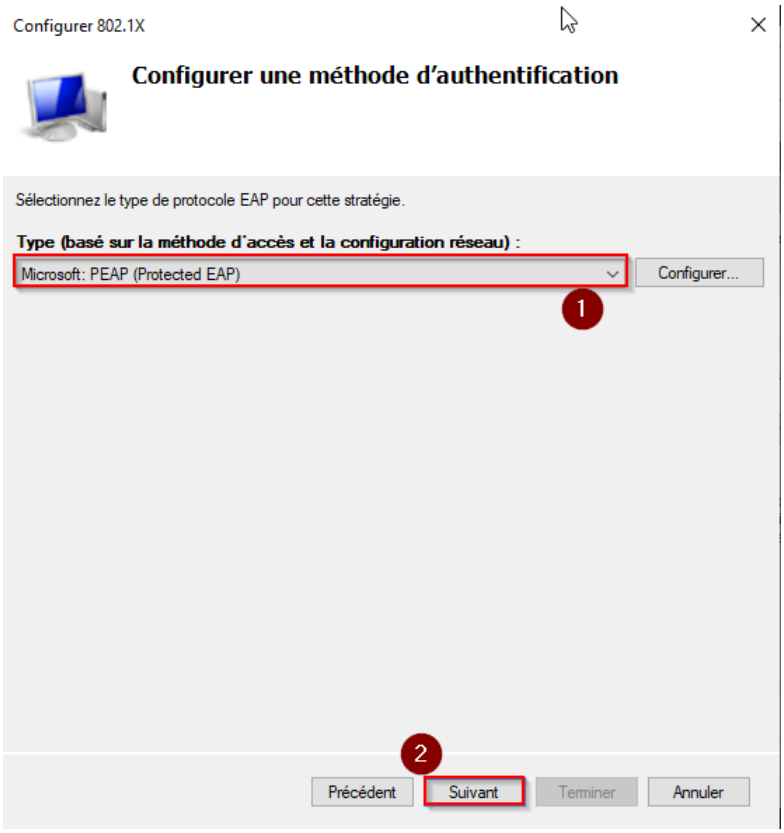
Maintenant, on clique sur “Ajouter” :



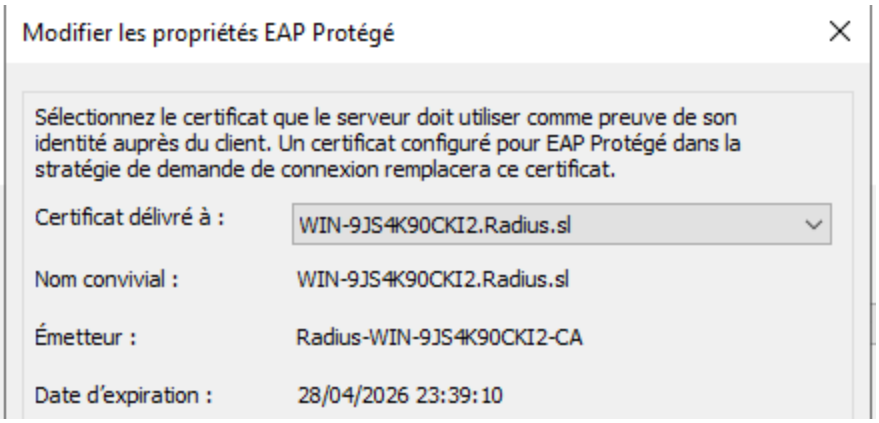
Par la suite, il faut renseigner des informations sur le Routeur Wifi comme son nom, son adresse IP et ne pas oublier de renseigner le secret partagé.



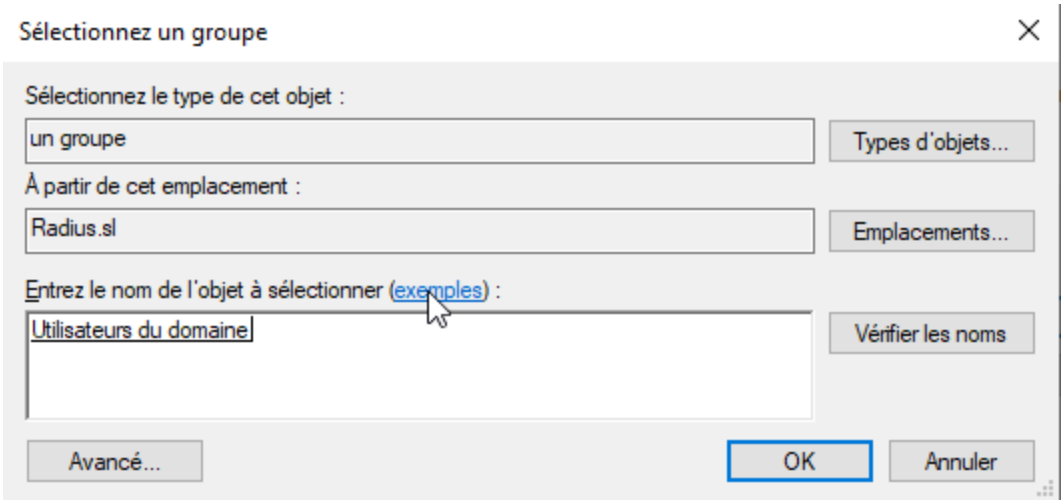
Ensuite, il faut choisir le type “Microsoft : PEAP (Protected EAP).



Il faut cliquer sur “configurer” et choisir le certificat créé précédemment.



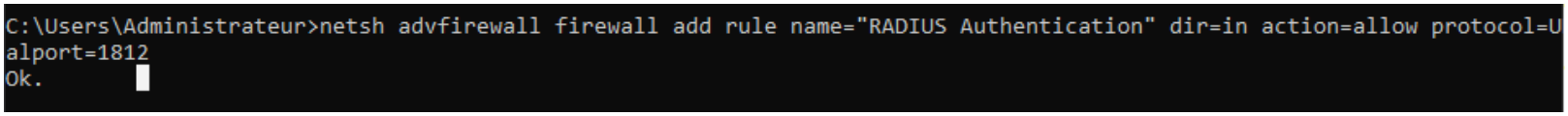
Maintenant, on va choisir le groupe d'utilisateurs concerné. Dans notre cas, c'est "utilisateurs du domaine".



Quand cela est fait, cliquer sur suivant, puis terminer.

Il ne faut surtout pas oublier de mettre une règle de filetage sur le pare-feu car d’origine, il bloque les requêtes d'authentification.

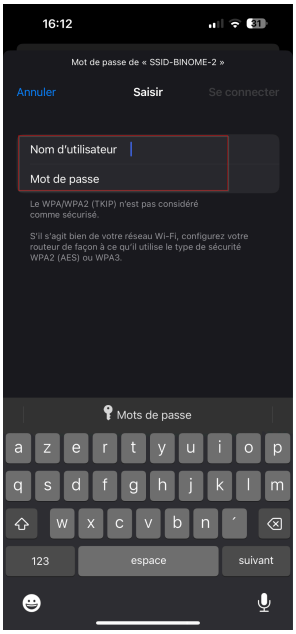
```
netsh advfirewall firewall add rule name="RADIUS Authentication" dir=in
action=allow protocol=UDP localport=1812
```



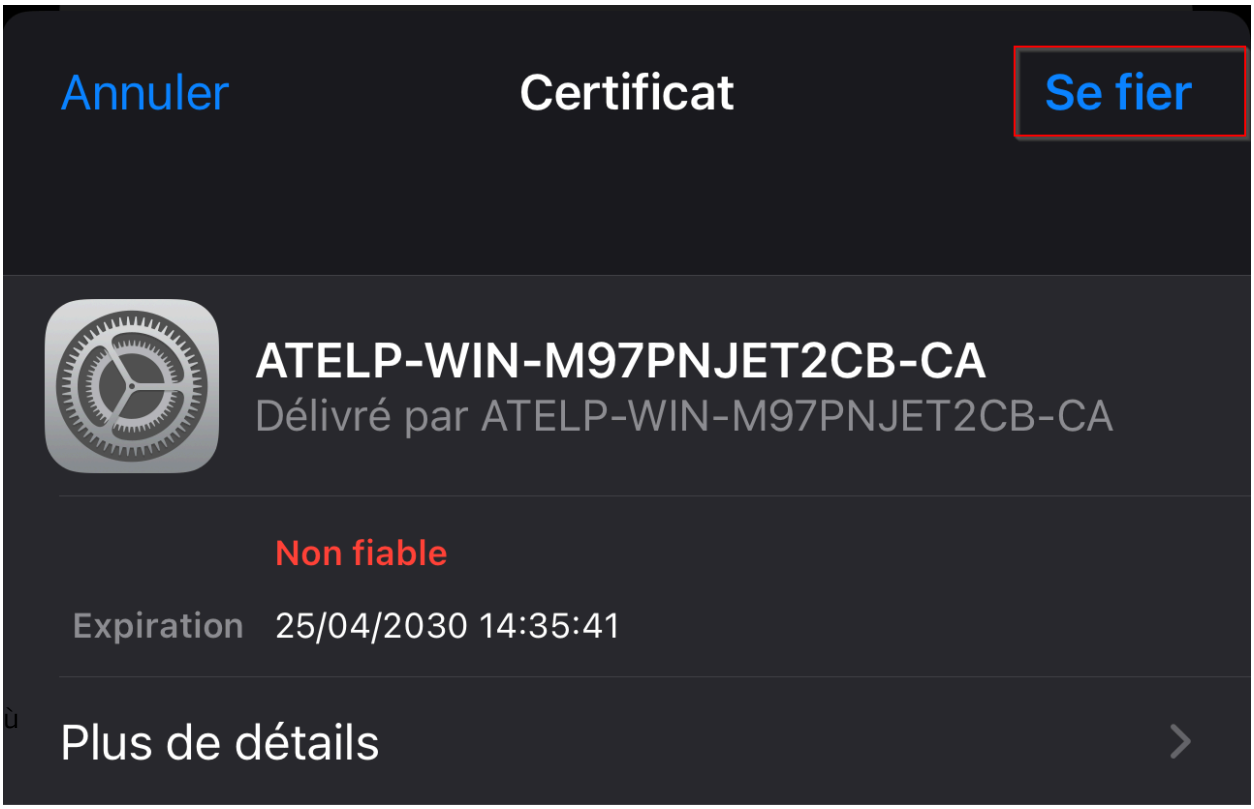
Test

Pour tester la connexion au réseau wifi, sur l'appareil, on va rechercher notre réseau wifi.

Pour se connecter, il vous nous demande un login et mot de passe d'un compte Active Directory.



Une fois que vous avez entré les éléments nécessaires, ils vont vous demander si vous faites confiance au certificat. Mettez “Se fier” car c’est le certificat que vous avez créé précédemment.



Une fois accepté, vous serez connecté au réseau wifi.