ASSURMER

ASSURMER

PROCEDURE DE CONFIGURATION DE RADIUS

Bruno LEVESQUE & Ugo BERNARD

BTS SIO SISR 2B

PROCEDURE DE CONFIGURATION DE RADIUS

ETAT DU DOCUMENT

☐ Validé ☒ En cours de validation ☐ En projet ☐ Périmé

LISTE DES REVISIONS

Version	Date	Auteur	Description de la révision	Page
1	08/01/2024	Bruno Levesque	Création du document et détail de la configuration	14

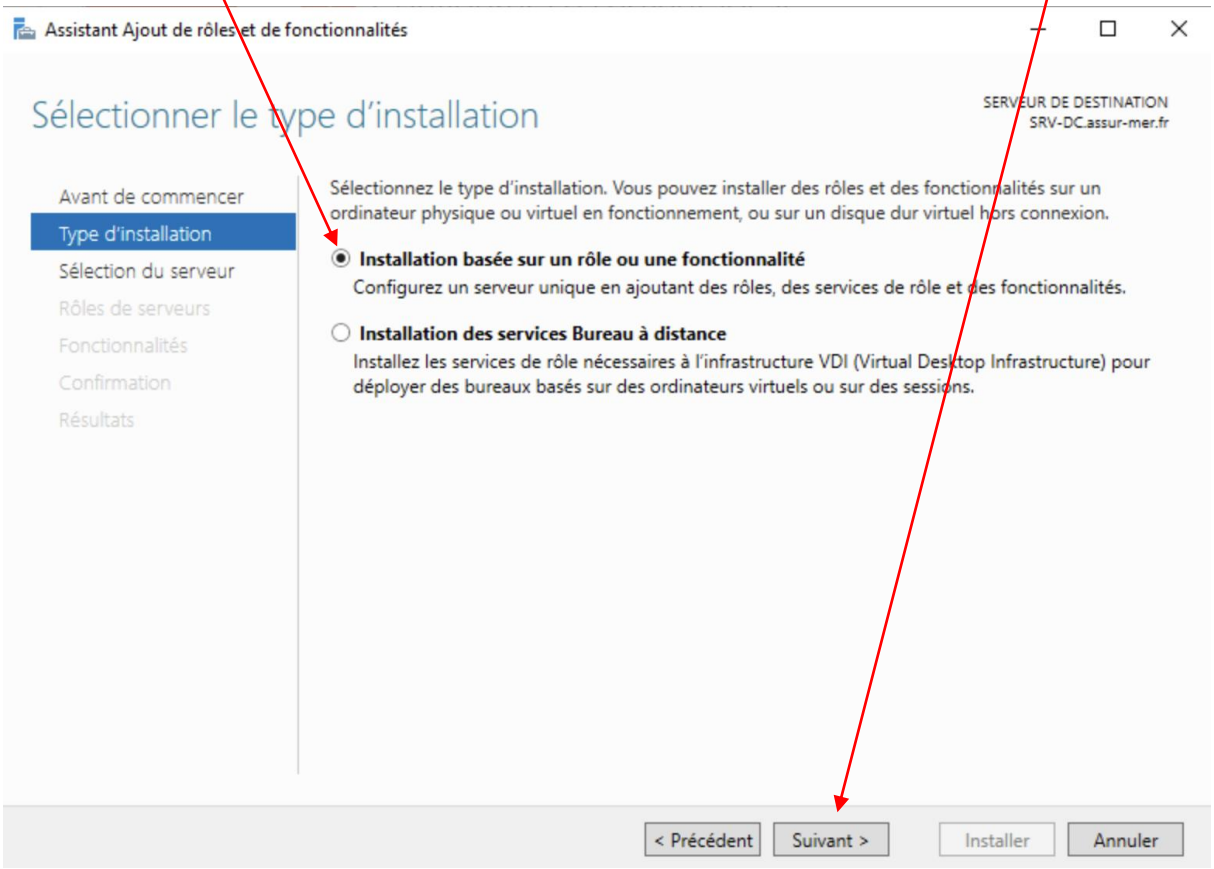
REDACTEURS ET APPROBATEURS

	Nom	Fonction	Visa
Rédacteurs	LEVESQUE Bruno Ugo BERNARD	Techniciens Systèmes et Réseaux	OK
Approbateurs & Signataires	Mme MONSIRE Claire Mr DEGEN Loïc	DSI	
Lecteur	LEVESQUE Bruno Ugo BERNARD	Techniciens Systèmes et Réseaux	OK

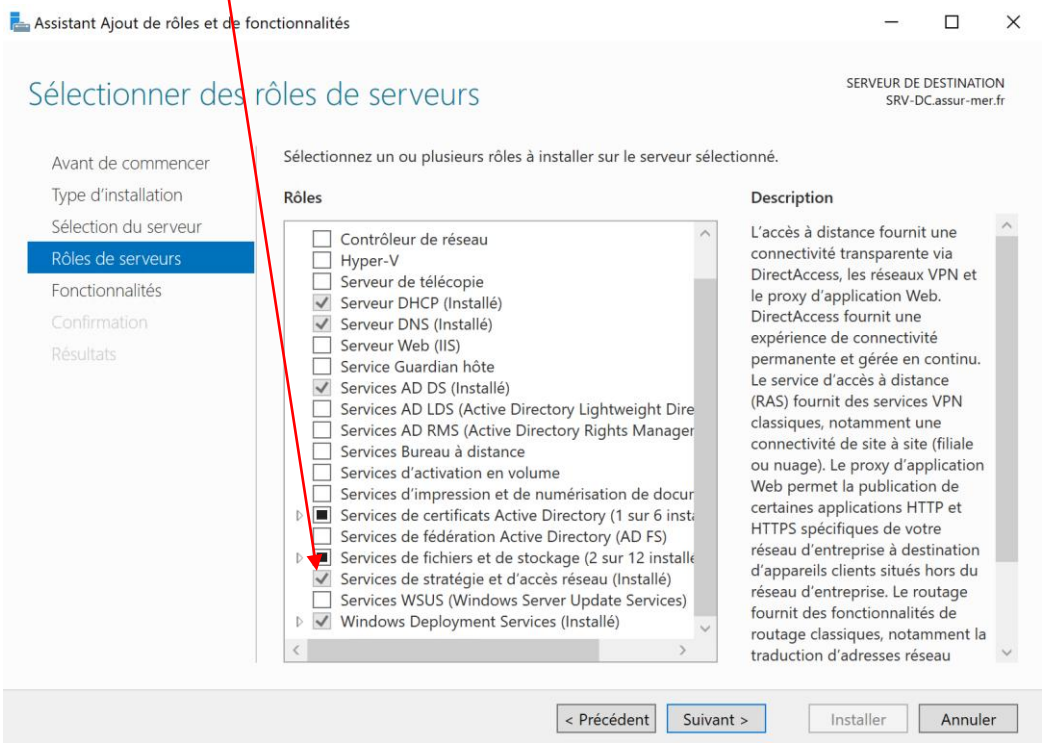
Table des matières

1. INSTALLATION DE RADIUS SUR WINDOWS SERVER 2022

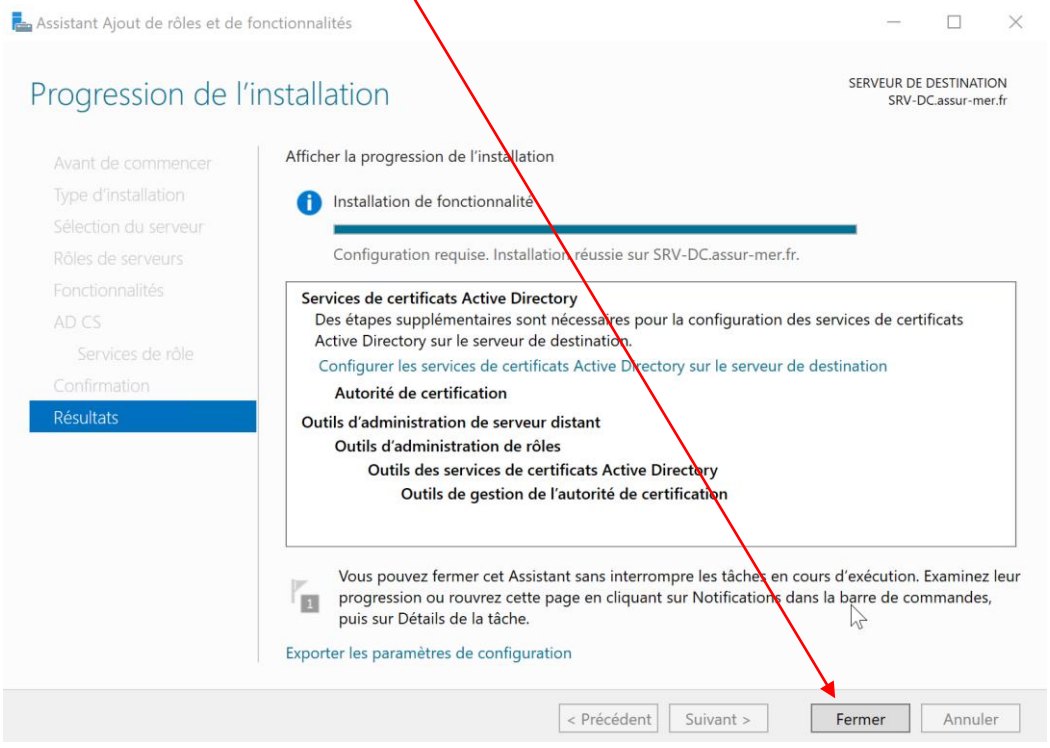
Sur le gestionnaire de serveur, rendez-vous sur « Ajouter des rôles et des fonctionnalités » et sélectionnez « Installation basée sur un rôle ou une fonctionnalité », enfin, cliquez sur « Suivant ».



Maintenant, cliquez sur « Services de Stratégie et d'accès réseau » puis sur « Suivant ».

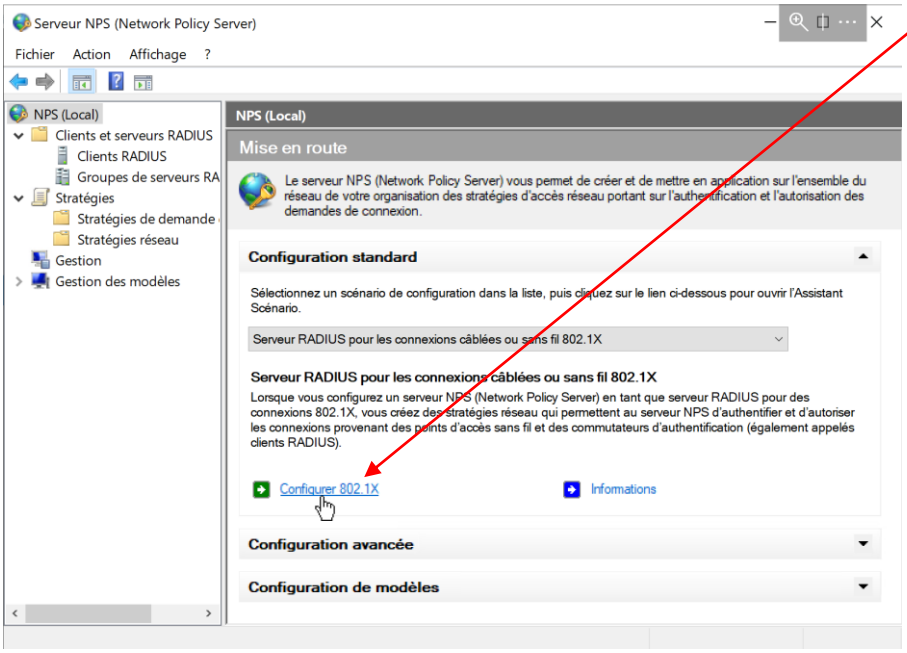


Dorénavant, le service peut être installé, cliquez sur « Installer ». Une fois l'installation terminée, vous pouvez fermer cette fenêtre.

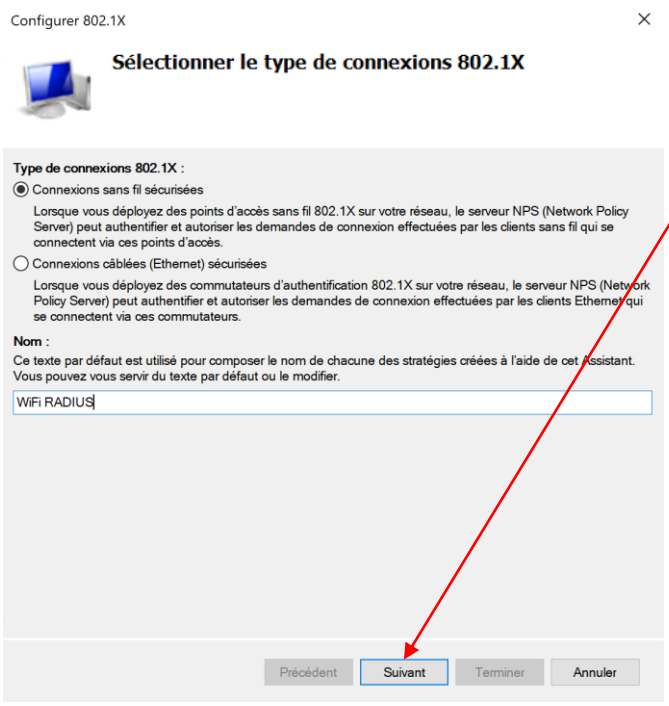


2. CONFIGURATION DE LA SOLUTION RADIUS (NPS)

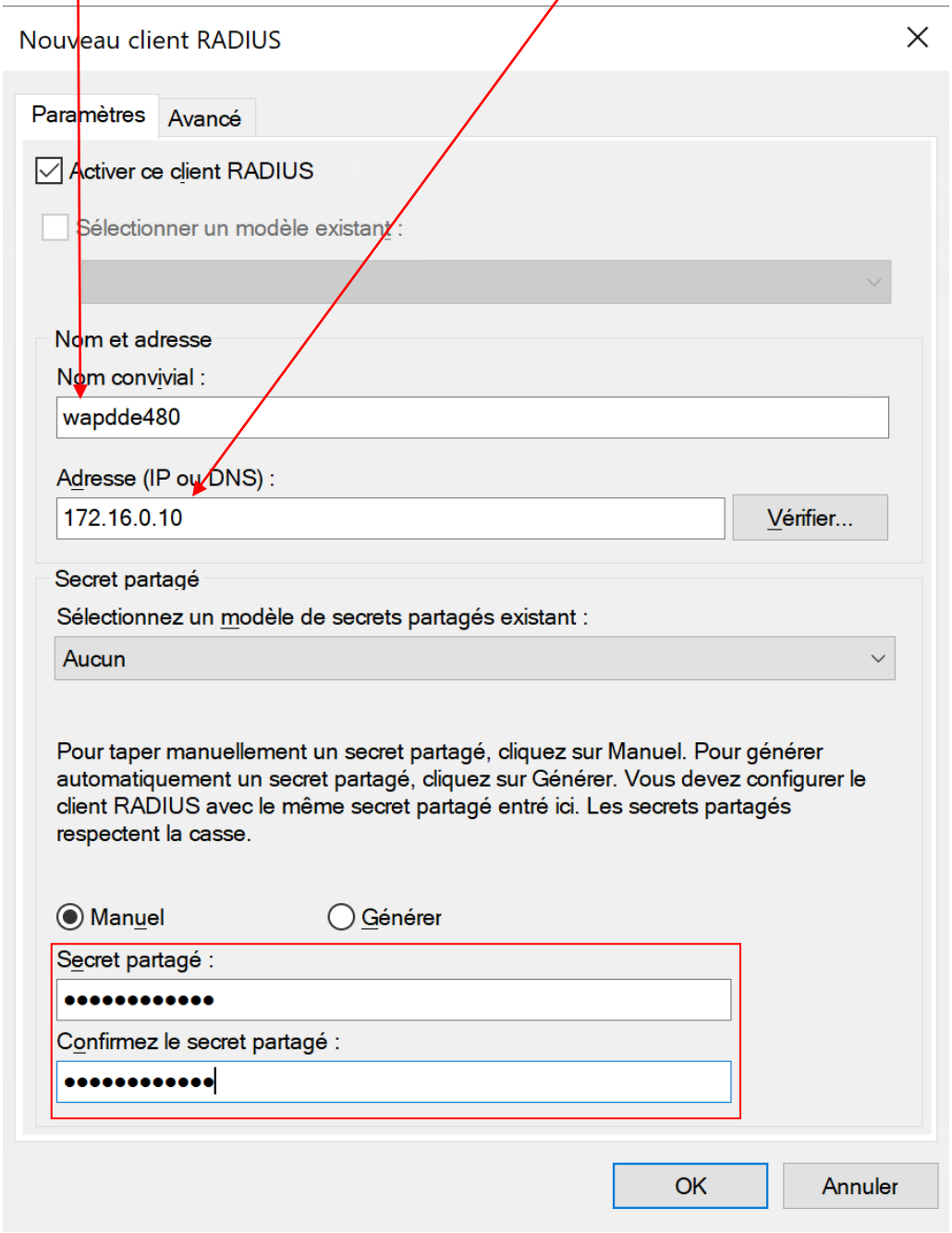
Dans le gestionnaire de serveur, cliquez sur « Outils » puis ouvrez « Serveur NPS (Network Policy Server) ». Après avoir inscrit un serveur dans Active Directory, cliquez sur « Configurer 802.1X ».



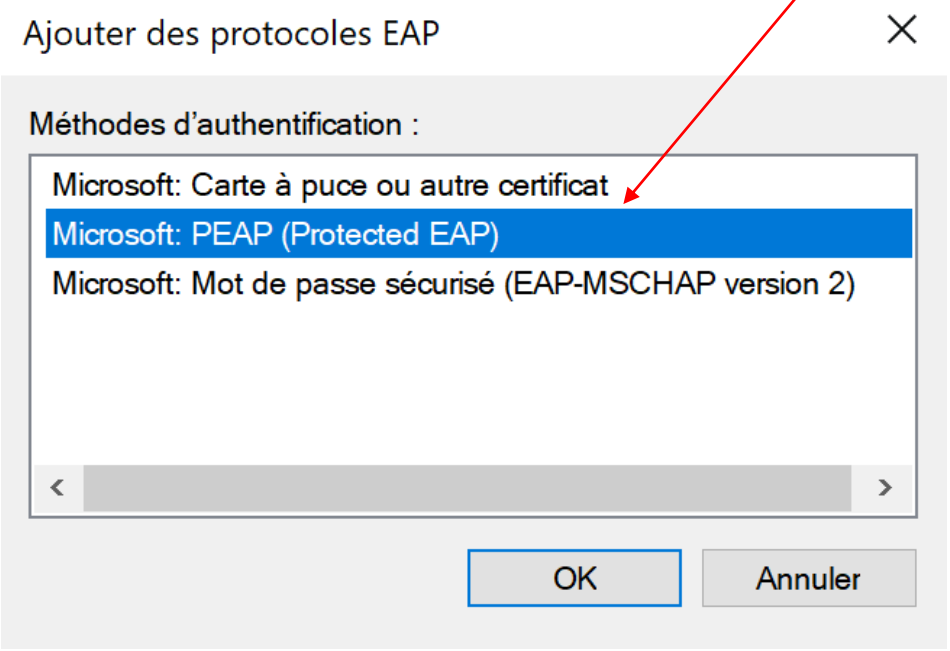
Dans le champ « Nom », inscrivez le nom que vous souhaitez et cliquez sur « Suivant ».



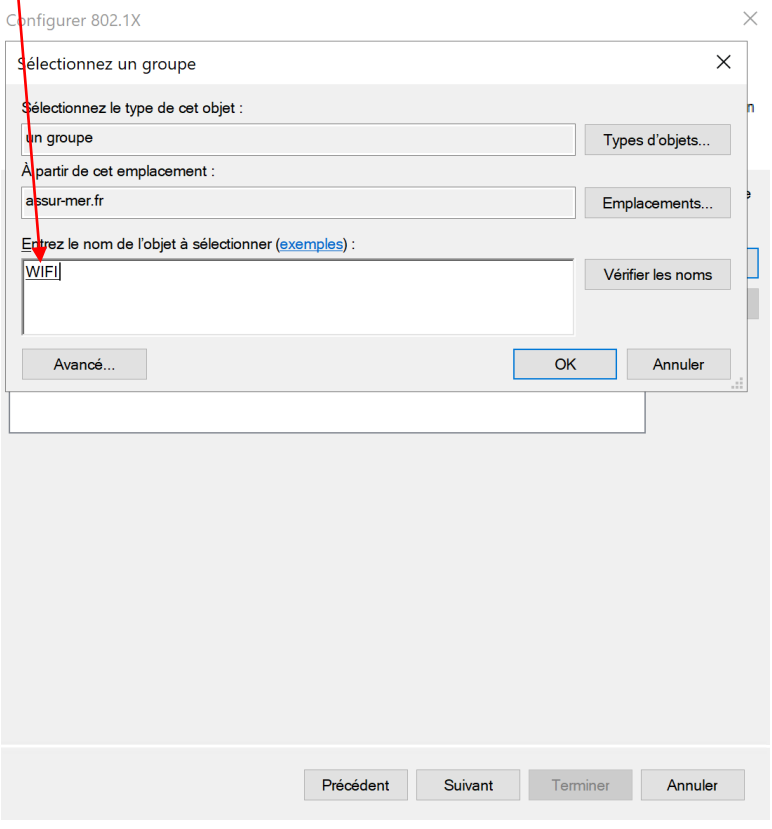
Vous avez maintenant la possibilité d'ajouter un nom convivial pour votre serveur RADIUS. Renseignez le nom exact de votre borne WiFi. Renseignez également l'adresse IP de votre borne Wi-Fi. Enfin, complétez les champs « Secret partagé » avec un mot de passe robuste.



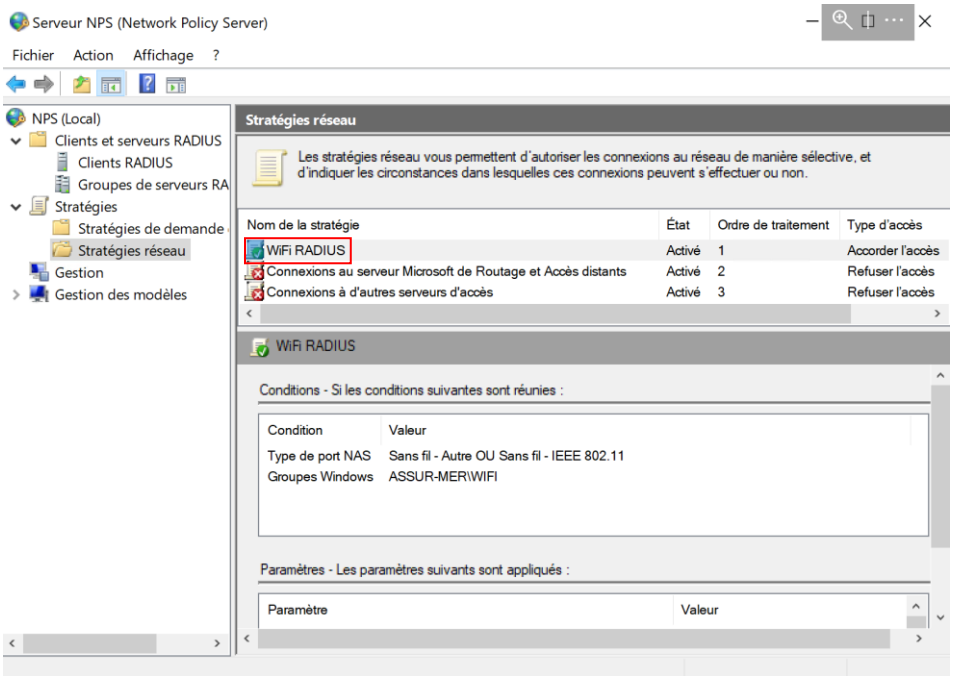
Vous devez maintenant choisir une méthode d'authentification. Sélectionnez « Microsoft PEAP ».

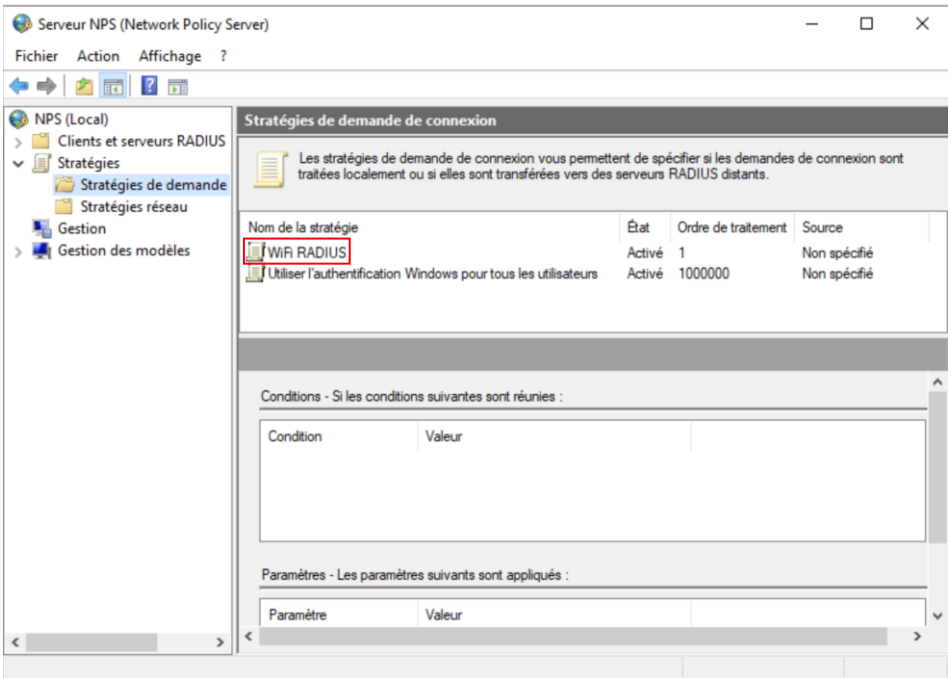


Ajoutez maintenant l'Unité d'Organisation créée à cet effet pour le WiFi.

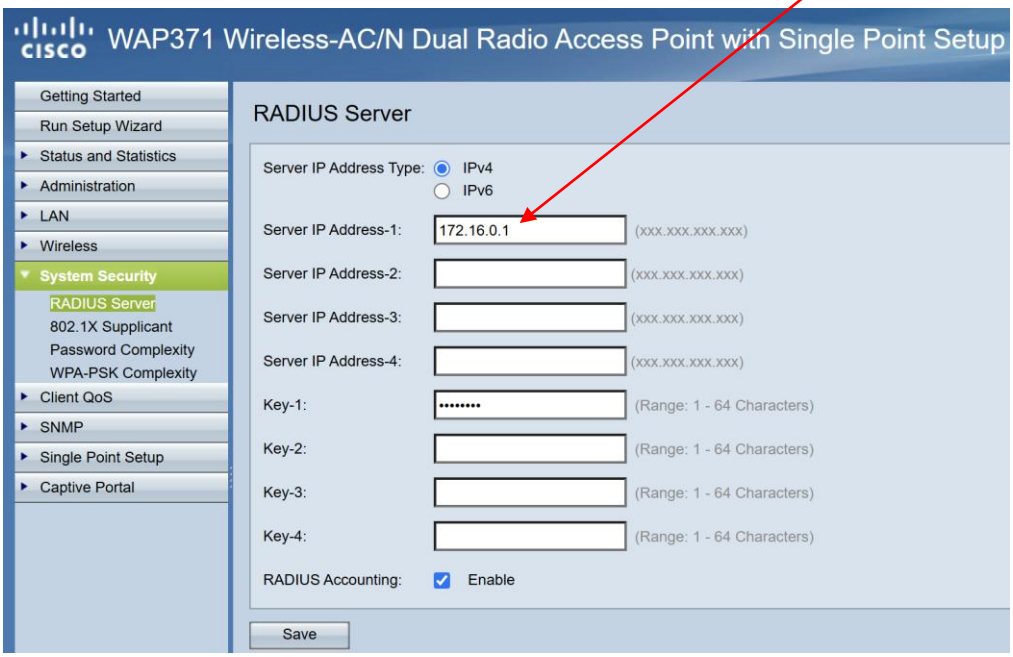


Les stratégies de demande et de réseau sont maintenant créées.



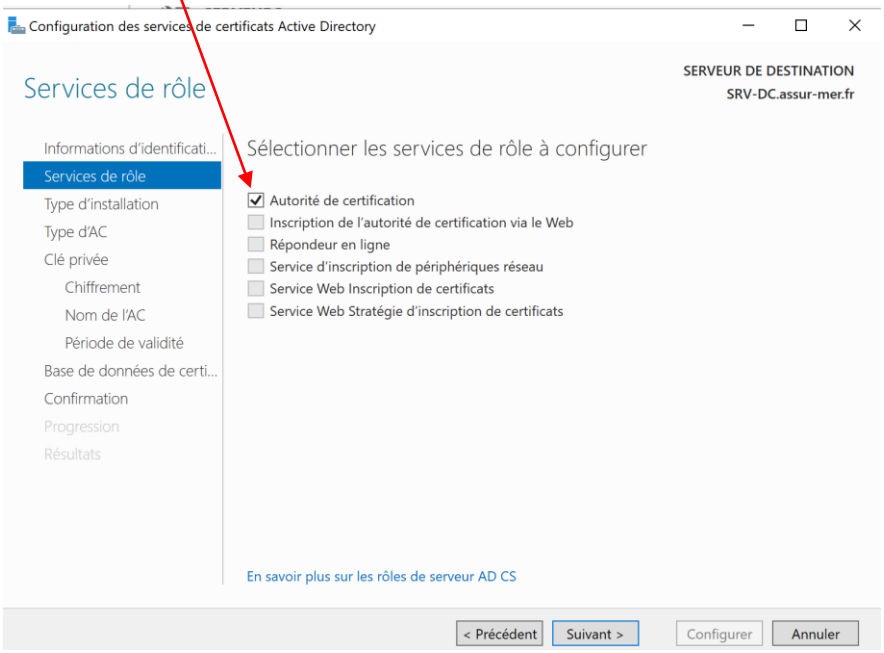


Dorénavant, sur la console d'administration de la borne WiFi, renseignez l'IP de votre serveur AD dans l'onglet « RADIUS Server » et le secret partagé.

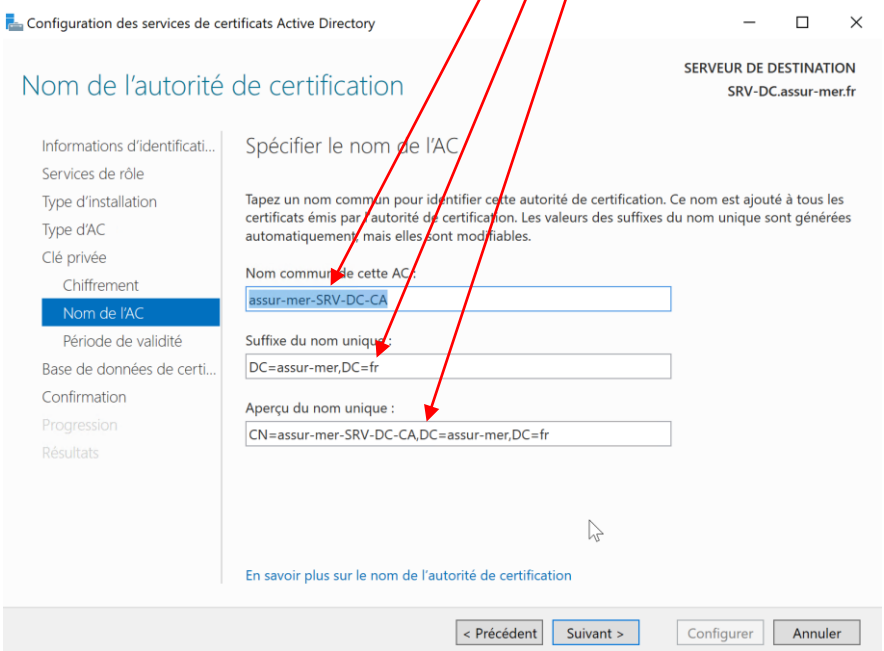


3. MISE EN PLACE DU CERTIFICAT D'AUTHENTIFICATION

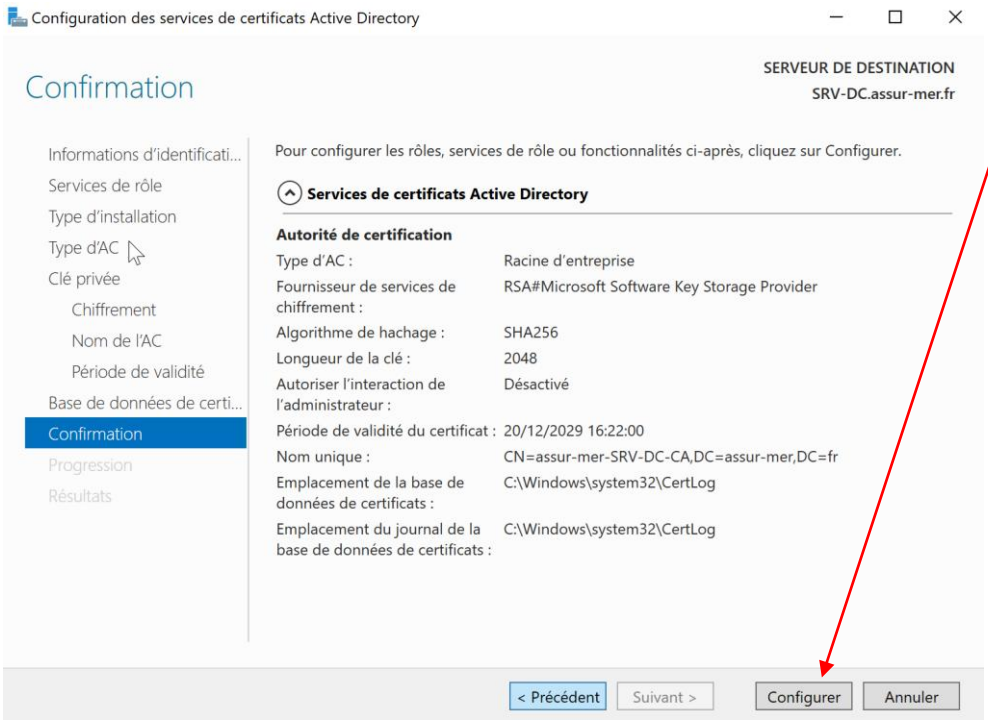
Ajoutez maintenant des services de certificats Active Directory. Dans l'onglet « Services de rôle », cochez « Autorité de certification ».



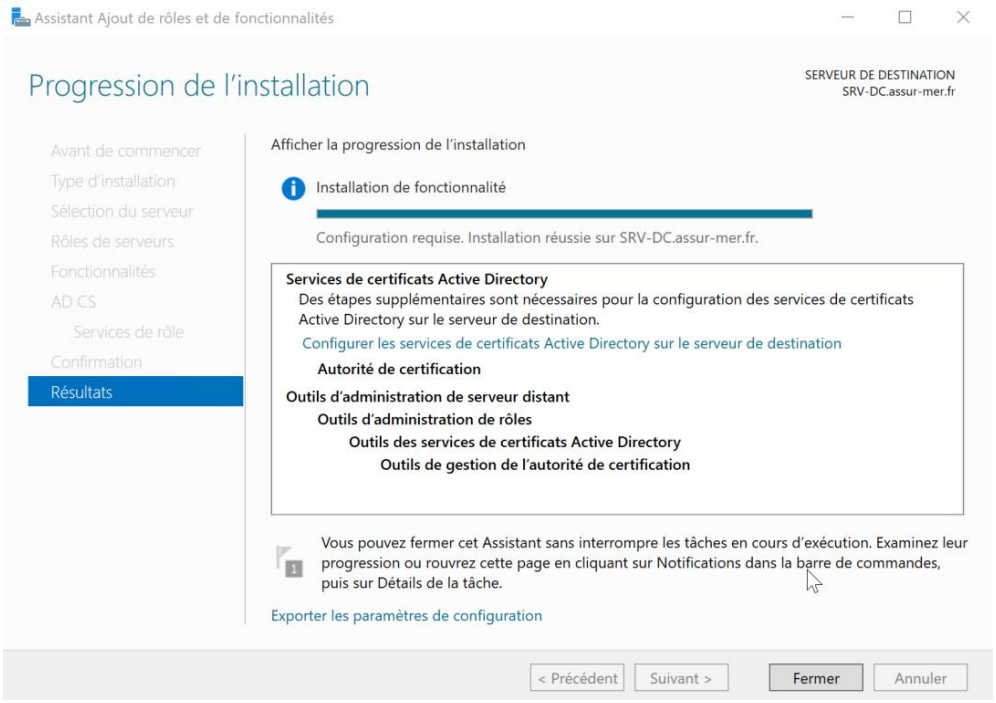
Dans l'onglet « Nom de l'AC », renseignez les informations afin de joindre votre Active Directory puis cliquez sur « Suivant ».



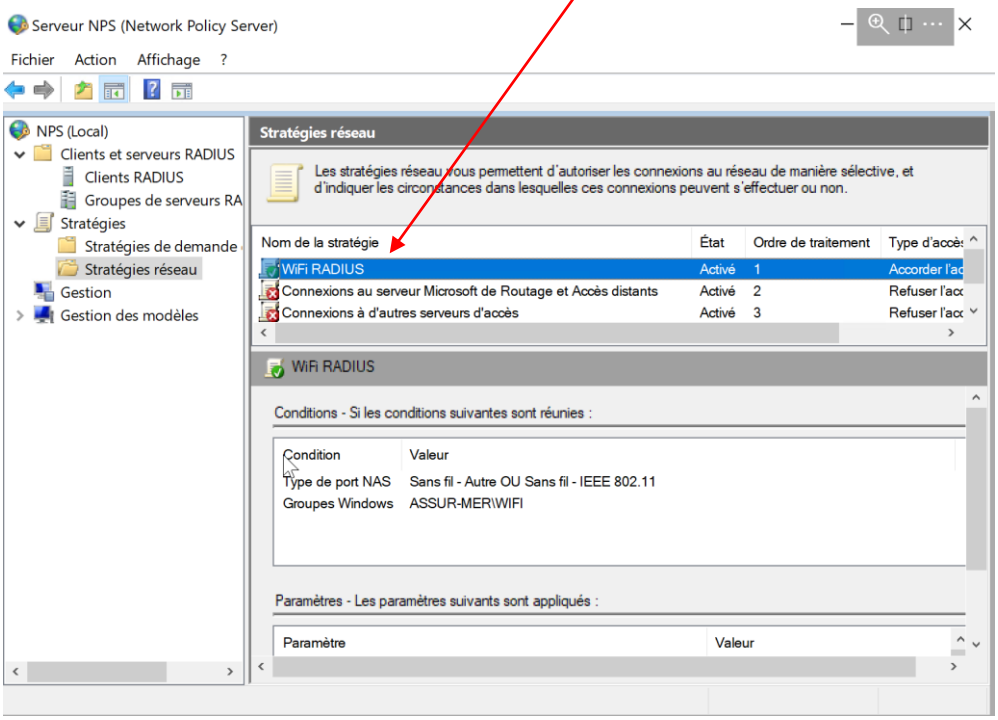
Vérifiez maintenant les informations précédemment renseignées puis cliquez sur « Configurer ».



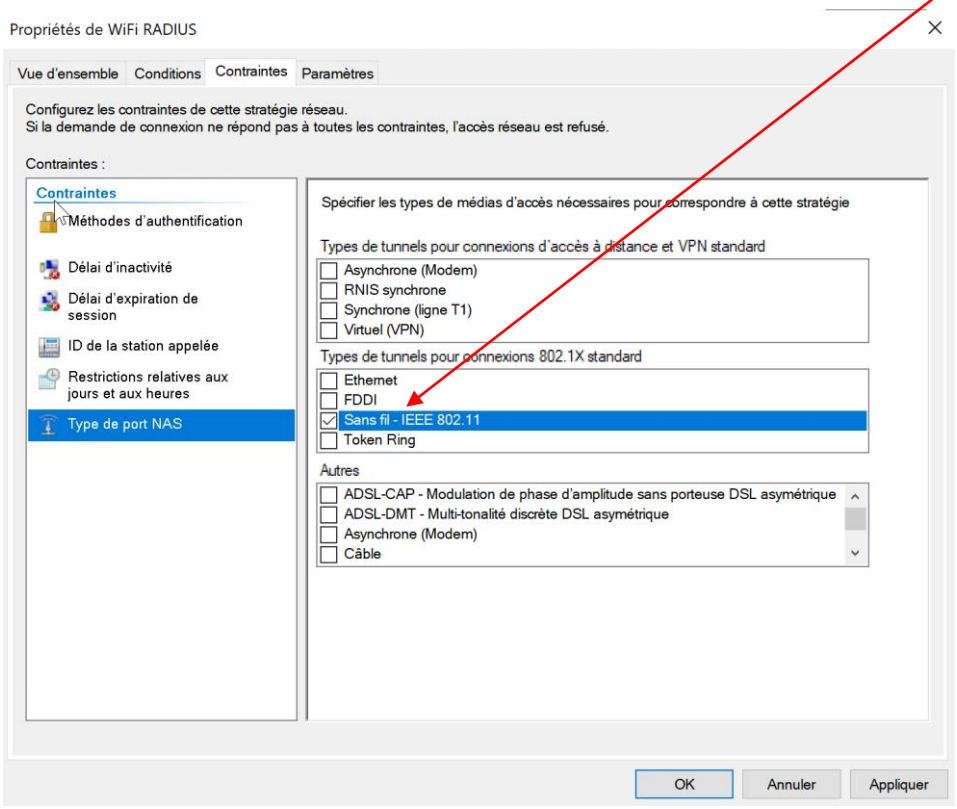
Une fois l'installation de la fonctionnalité terminée, vous pouvez fermer cette fenêtre.



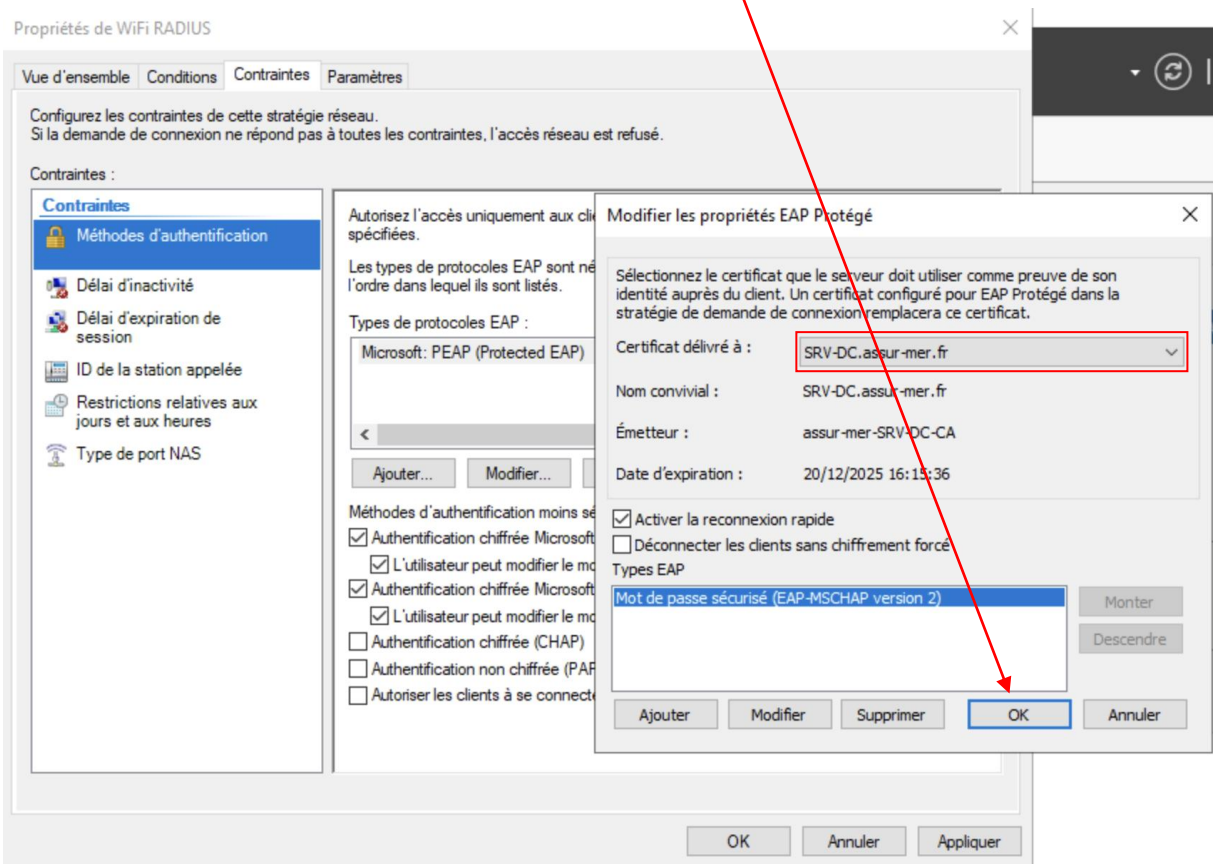
Retournez maintenant dans l'outil NPS, double-cliquez sur le nom de votre stratégie.



Rendez-vous maintenant dans l'onglet « Contraintes » de cette fenêtre et sélectionnez « Sans fil – IEEE 802.11 ».



Toujours dans l'onglet « Contraintes », dans « Méthodes d'authentification », ajoutez le type de protocole EAP, sélectionnez votre SRV-DC et cliquez sur « OK ».



Enfin, nous pouvons voir que le certificat est valide pour une durée certaine.