ESIEE [it]
L'école de l'expertise numérique

Présentation de solution Radius et son installation

Auteurs : *Carvalho Tom, Bagassien Stephen, Dez Sofiane*

Référence : *Assurmer*

Date : *24/10/2023*

DIFFUSION

Diffusion				
Société / Entité	Destinataires	Fonction	Diffusion	Pour info
Assumer	Service IT	Procédure	Réseau	

SUIVI DES VERSIONS

Version	Date	Auteur	Raison	Nombre de page
V1.0	24/10/2023	Carvalho Tom Bagassien Stephen Dez Sofiane	Présentation de solution Radius et son installation	12

COORDONNEES

Nom	E-mail	Téléphone
Carvalho Tom	tom.carvalho@assurmer.fr	01.47.10.00.00
Bagassien Stephen	stephen.bagassien@assurmer.fr	01.47.10.00.00
Dez Sofiane	sofiane.dez@assurmer.fr	01.45.10.00.00

SOMMAIRE

Table des matières

Présentation du fonctionnement d'une solution Radius

Radius, qui signifie Remote Authentication Dial-In User Service, est un protocole d'authentification et d'autorisation largement utilisé dans les réseaux informatiques, en particulier dans les réseaux sans fil et les réseaux d'accès à distance.

Pour comprendre le fonctionnement de RADIUS, nous pouvons diviser le processus en trois parties principales : l'authentification, l'autorisation et l'accounting.

Authentification

Lorsqu'un utilisateur tente de se connecter à un réseau protégé par Radius, la première étape consiste en une demande d'authentification. Cette demande est généralement initiée par le serveur d'accès réseau, tel qu'un point d'accès WIFI, lorsque l'utilisateur essaie de se connecter. Le serveur d'accès réseau envoie alors une demande d'authentification au serveur Radius.

Le serveur Radius reçoit la demande et vérifie les informations d'identification fournies par l'utilisateur. Ces informations peuvent inclure un nom d'utilisateur et un mot de passe, ou d'autres types d'informations d'identification telles que des certificats numériques. Le serveur Radius utilise alors sa base de données interne ou se connecte à d'autres sources d'authentification, telles que des bases de données LDAP ou Active Directory, pour valider les informations d'identification de l'utilisateur.

Une fois que l'utilisateur a été authentifié avec succès, le serveur RADIUS envoie une réponse au NAS, indiquant si l'authentification a réussi ou échoué.

Autorisation

Après avoir authentifié l'utilisateur, le serveur Radius peut également être utilisé pour déterminer les autorisations que cet utilisateur a sur le réseau. Cela peut inclure des informations telles que les services auxquels l'utilisateur est autorisé à accéder, les limitations de bande passante, les restrictions d'accès à certaines ressources, etc.

Le serveur Radius envoie ces informations d'autorisation au serveur d'accès réseau sous forme de réponse à la demande initiale. Le serveur d'accès réseau utilise ensuite ces informations pour configurer les paramètres de la session réseau de l'utilisateur conformément aux politiques définies.

Accounting

Enfin, le protocole Radius prend également en charge la fonction d'accounting, qui consiste à enregistrer les détails des sessions réseau des utilisateurs. Cela inclut des informations telles que les heures de début et de fin de session, la quantité de données transférées pendant la session, etc. Ces informations peuvent être utilisées à des fins de facturation, de surveillance de l'utilisation du réseau, ou à des fins de sécurité et de conformité.

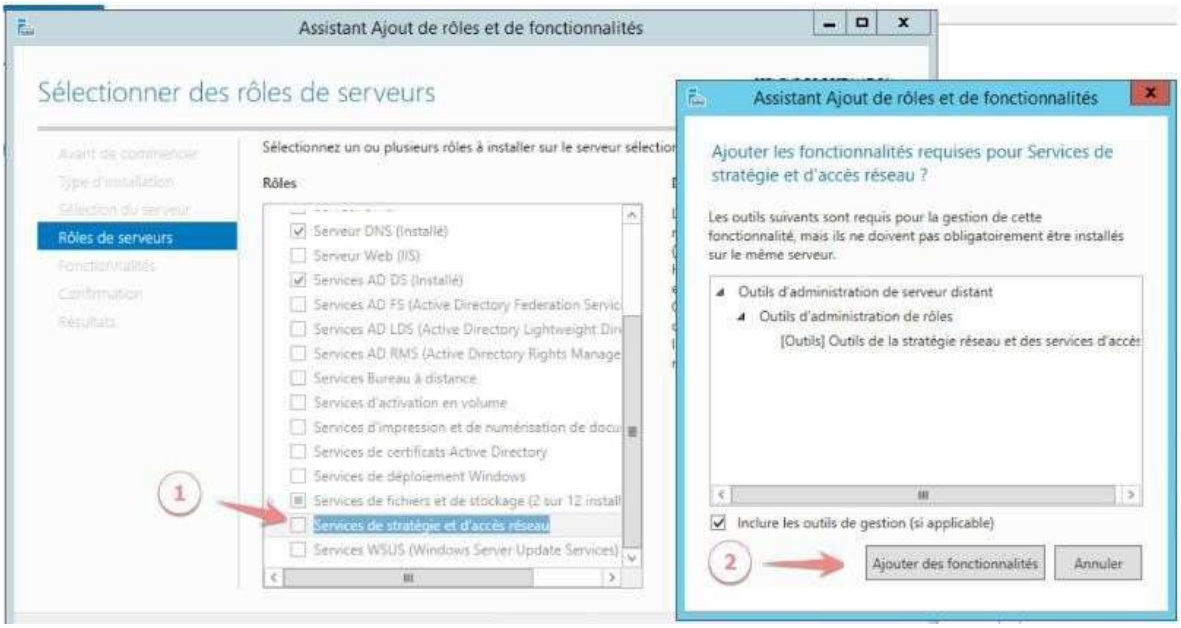
Radius est donc un protocole d'authentification et d'autorisation largement utilisé dans les réseaux informatiques pour contrôler l'accès des utilisateurs au réseau et pour enregistrer les détails de leurs sessions. Il offre une solution centralisée et sécurisée pour gérer l'accès aux réseaux, ce qui en fait un choix populaire dans de nombreux environnements réseau.

Procédure d'installation et de configuration de la solution Radius sous Windows server 2019

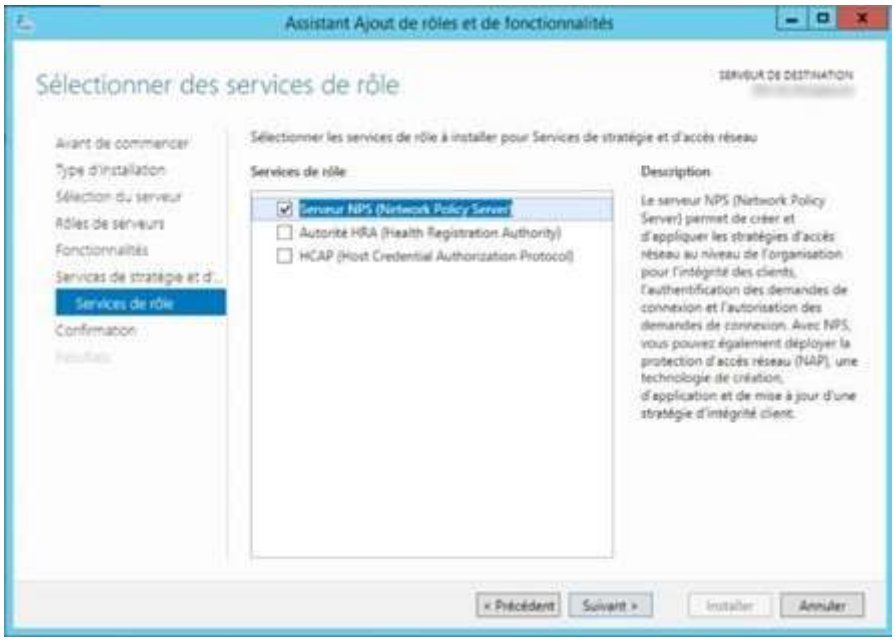
I. Installation du service Radius sur le serveur

a. Aller dans le gestionnaire de serveur, cliquer sur gérer puis Ajouter des rôles et fonctionnalités

b. Sélectionner le rôle Services de stratégie et d'accès réseau, puis Ajouter des fonctionnalités

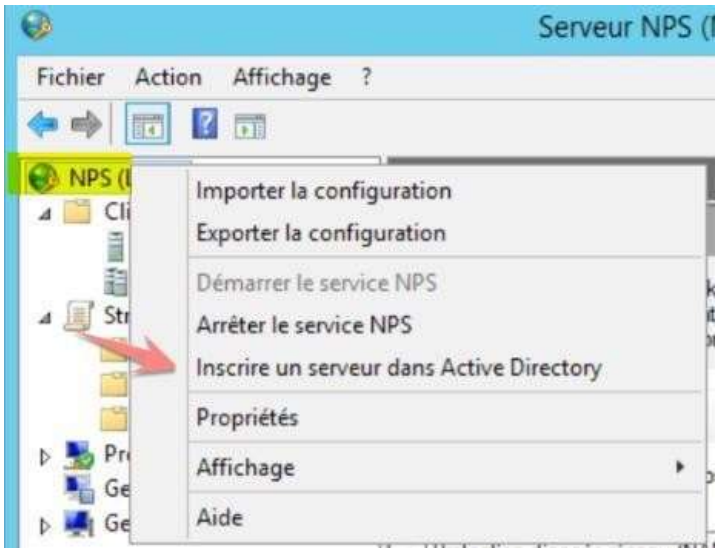


d. Ajouter le rôle Serveur NPS

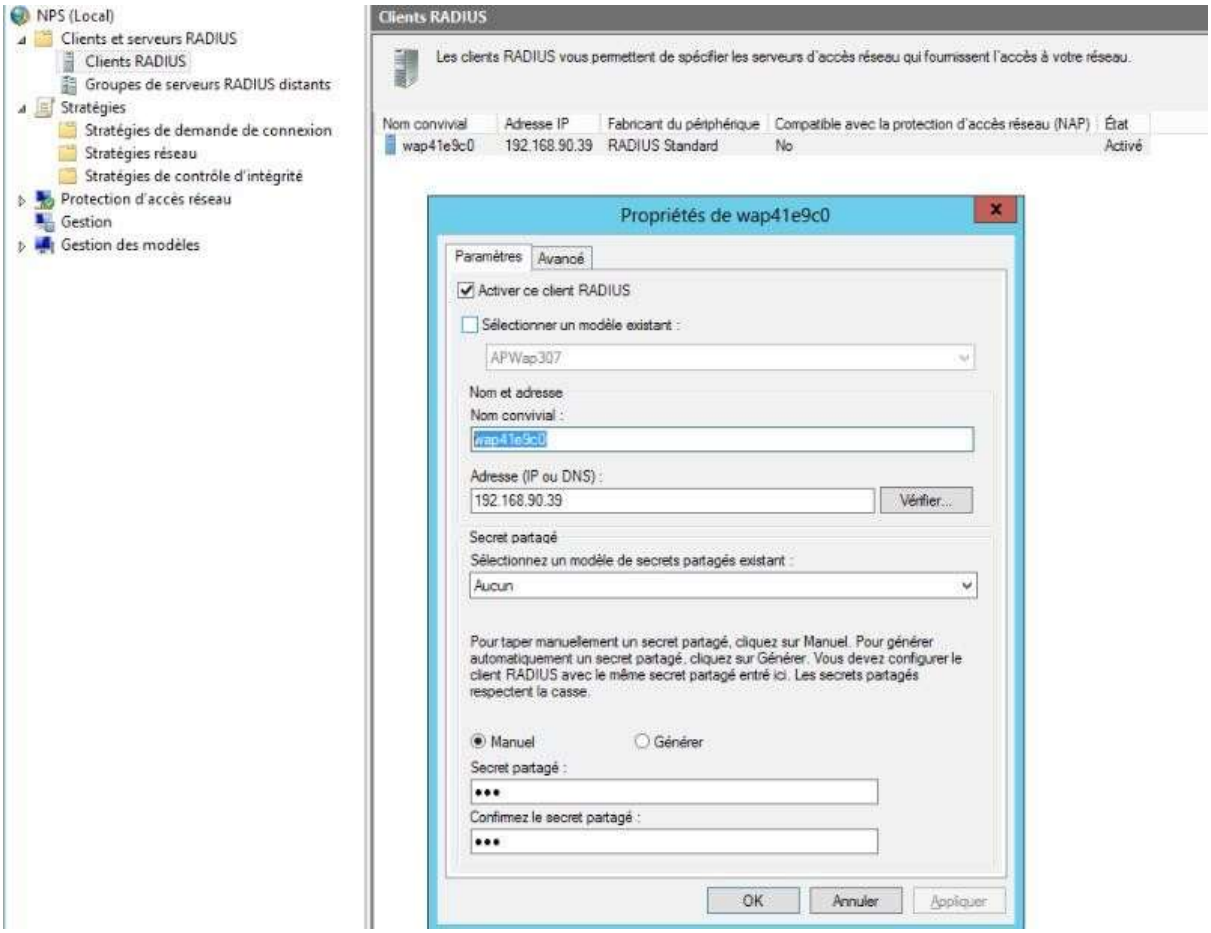


Configurer Radius pour une borne WIFI

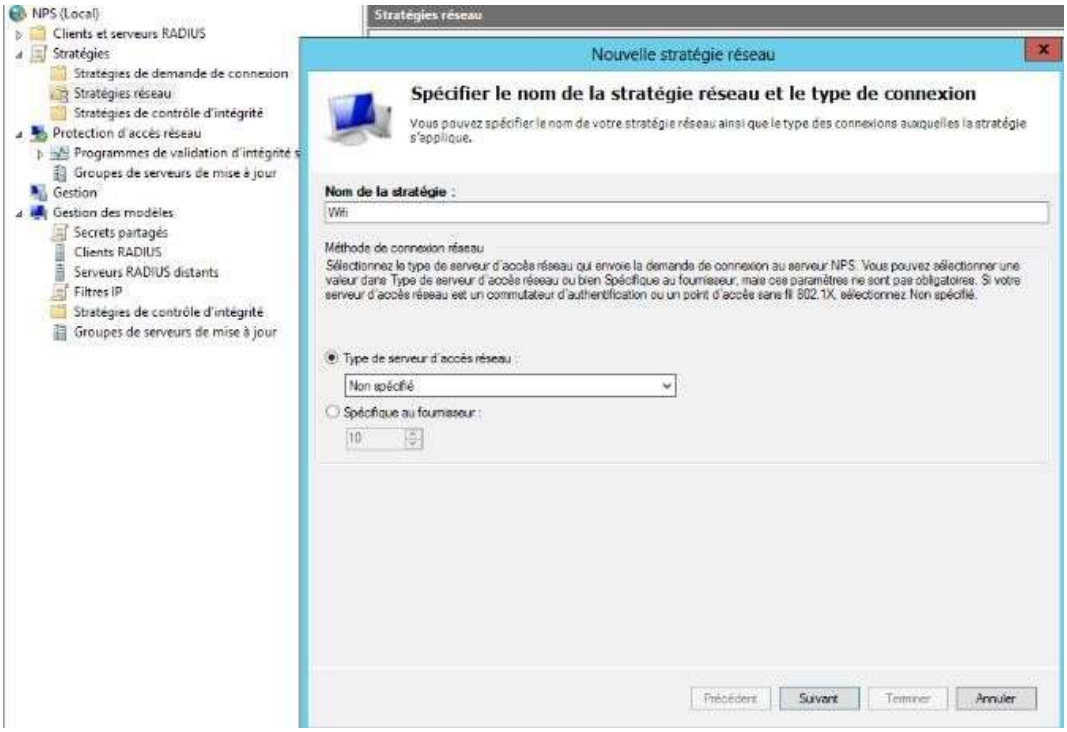
a. Lancer le service et faire un clic droit sur NPS
b. Cliquer sur Inscrire un serveur dans l'Active Directory



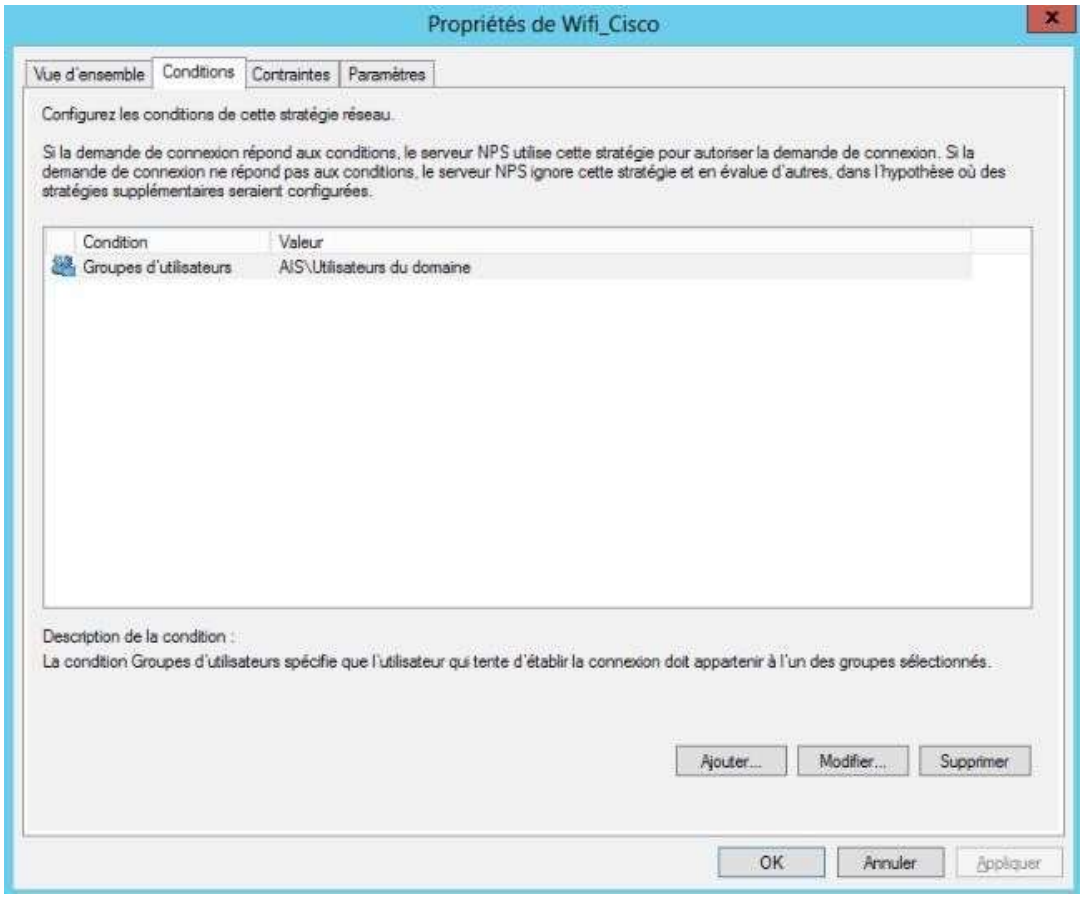
d. Faire un clic droit sur Client RADIUS pour créer un nouveau client Radius sur la console NPS
e. Rentrer la configuration souhaitée



f. Créer une nouvelle Stratégie de réseau et la nommer



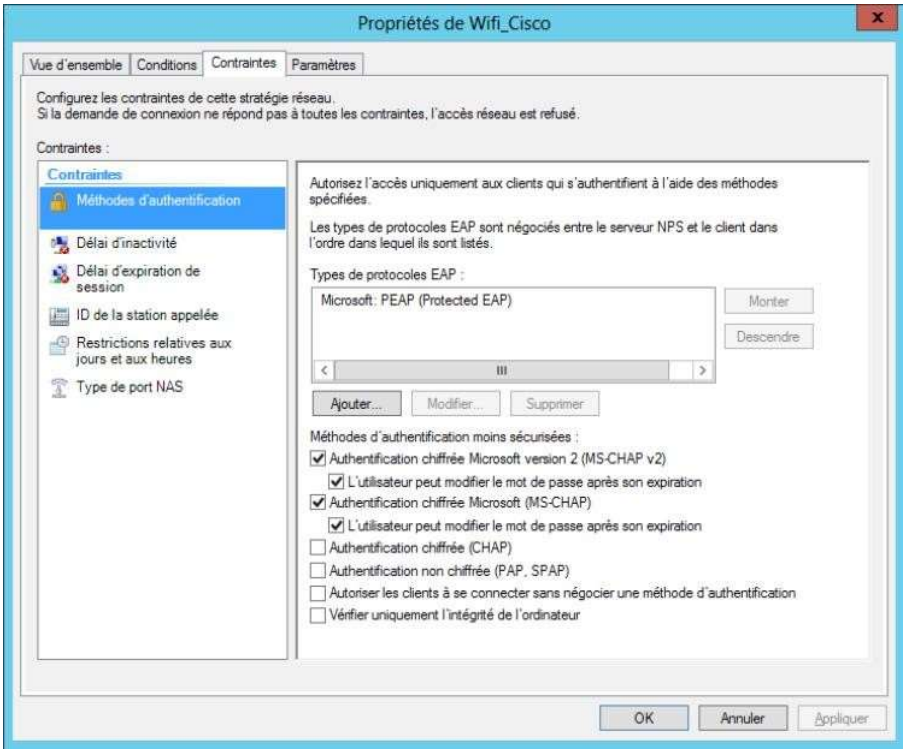
g. Ajouter le groupe utilisateurs du domaine



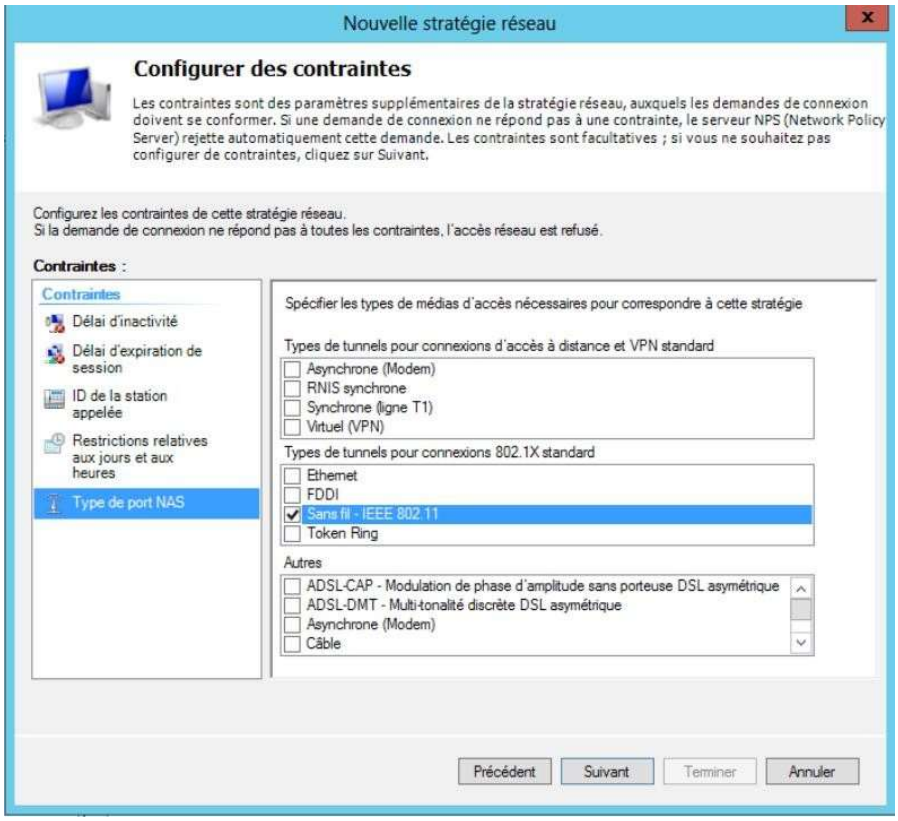
h. Sélectionner MS-CHAP v2 et MS-CHAP pour l'authentification par mot de passe

i. Monter le Extended Authentication Protocol qui sert pour le transport des données nécessaires à l'authentification

j.

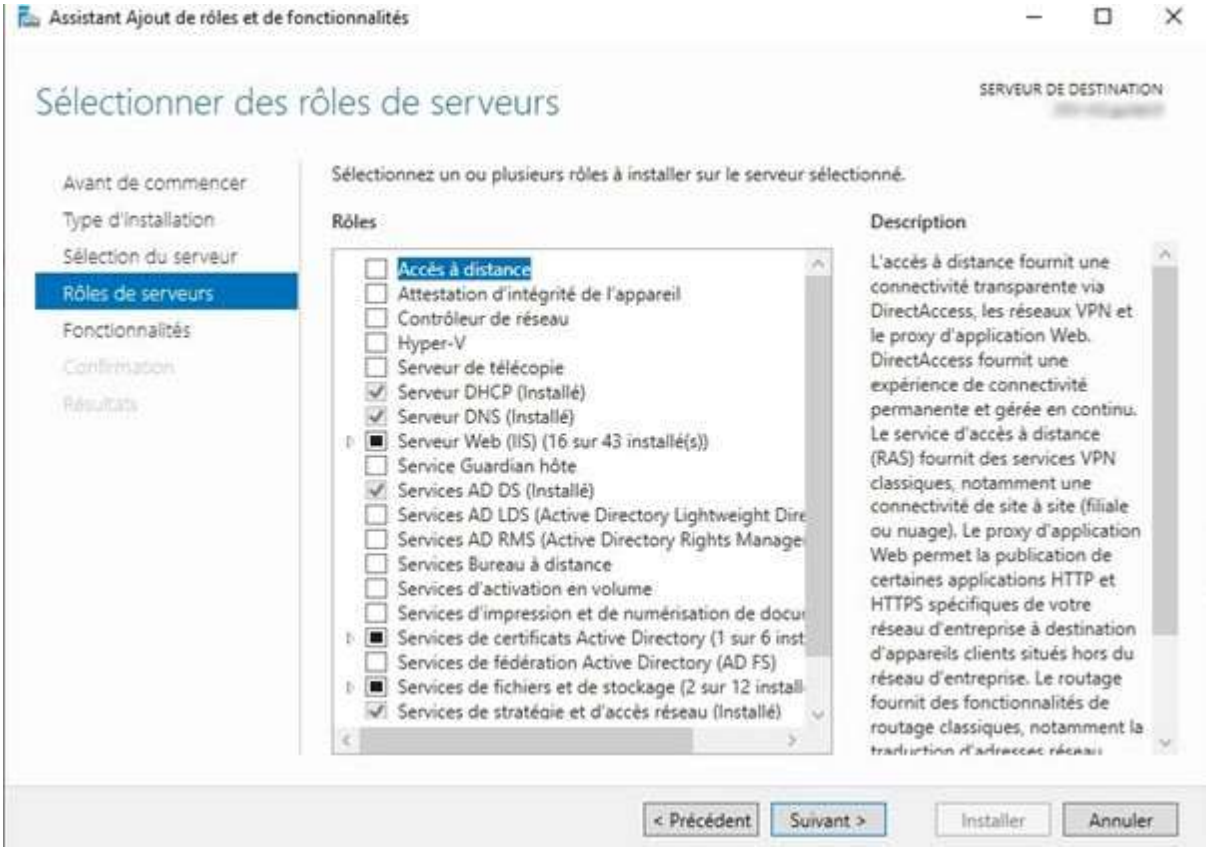


k. Dans type de port NAS sélectionner Sans fil – IEEE 802.11

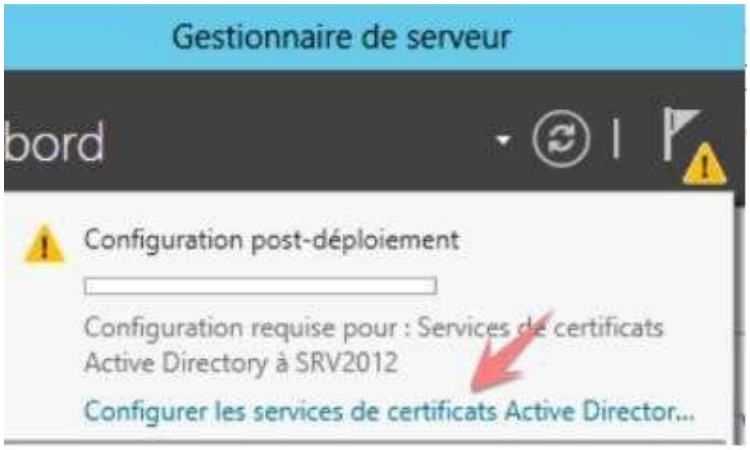


Installation et configuration d'une autorité de certification

a. Installation du rôle adcs et outil de gestion

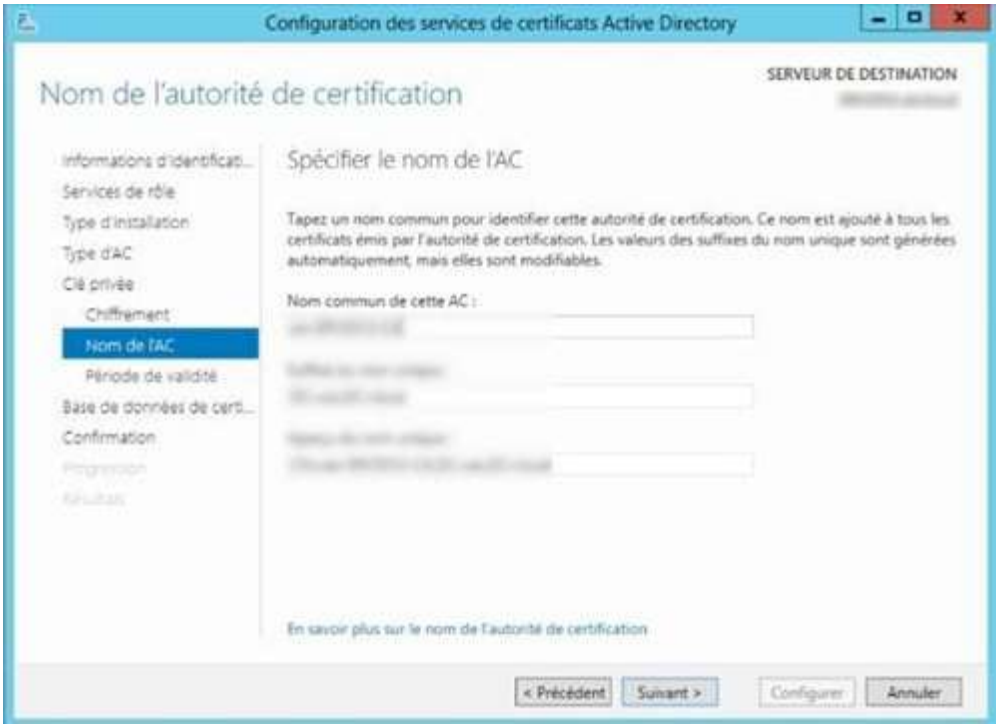


b. Démarrer le gestionnaire de serveur et cliquer sur l'icône drapeau en haut à droite, pour démarrer la configuration



d. Sur la page Services de rôle, sélectionner Autorité de certification et cliquer sur Suivant
e. Sur le type d'installation, sélectionner Autorité de certification d'entreprise et cliquer sur Suivant
f. Sur la page type d'autorité de certification, sélectionner Autorité de certification racine
g. Sur la page Clé privée, sélectionner Créer une nouvelle clé privée et cliquer sur Suivant
h. Sur la page Chiffrement, entrer les informations comme suit (Recommandation NIST et globalsign : longueur de clé minimal 2048 et algorithme SHA256)

i. Sur la page Nom de l'autorité de certification, accepter les valeurs par défaut et cliquer sur Suivant
j. Donner un nom au certificat



k. Sur la page Période de validité, par défaut la valeur est de 5 année, cliquer sur Suivant
l. Sur la page Base de données de certificats, cliquer sur Suivant
m. Sur la page Confirmation, passer en revue les informations fournies et cliquer sur Configurer

Sélection du certificat autosigné sur la console NPS

a. Aller dans Console NPS, stratégie d'accès réseau, propriétés de la stratégie wifi, dans l'onglet contraintes
b. Sélectionner Microsoft PEAP
c. Cliquer sur Modifier
d. Sélectionner le certificat serveur autosigné
e. Cliquer sur OK pour valider