Nadir DJEDIDEN
Nassim BENBOUHAMOU
ISMAEL BAHRI

12/02/2024

Installation et Configuration d’une borne WIFI

ESIEE-IT

Table des matières

Contexte

La Direction des Systèmes d'Information (DSI) envisage d'utiliser la solution Amazon RDS (Relational Database Service) pour héberger ses bases de données relationnelles. Cette solution cloud gérée permettra à l'entreprise de déployer, de gérer et de mettre à l'échelle facilement des bases de données relationnelles dans le cloud AWS.

Pour cela, la DSI prévoit de migrer progressivement ses bases de données actuelles vers Amazon RDS afin de bénéficier de la fiabilité, de la sécurité et de la facilité de gestion offertes par ce service. Cette migration nécessitera une analyse approfondie des besoins en termes de performances, de capacité et de sécurité, ainsi que la mise en place de stratégies de sauvegarde et de reprise après sinistre pour garantir la disponibilité continue des données.

De plus, des sessions de formation seront organisées pour familiariser les équipes techniques avec l'utilisation de la solution Amazon RDS et assurer une transition en douceur vers ce nouvel environnement de base de données dans le cloud.

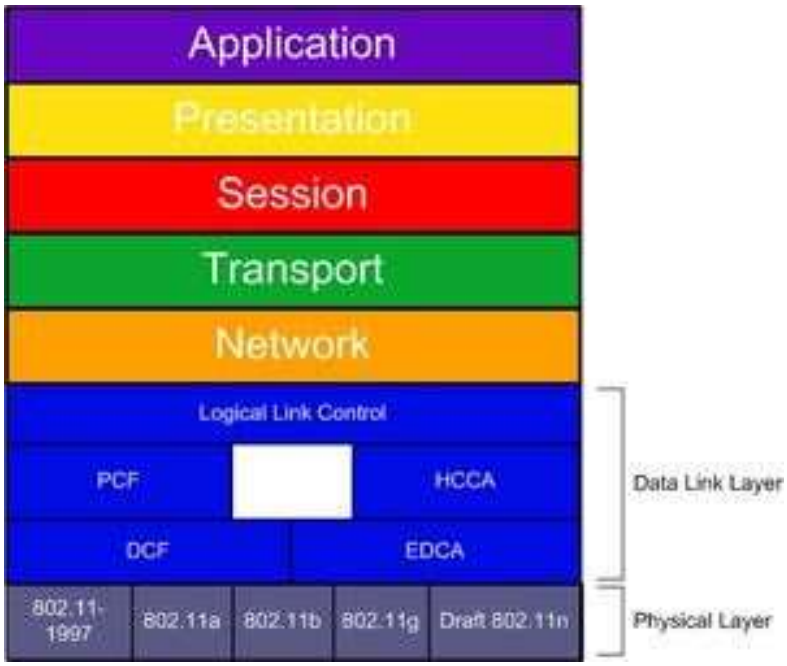
Etude des protocoles

Le WI-FI

Le Wi-Fi est un ensemble de protocoles de communications sans-fil, avec la IEEE802.11ax (Wi-Fi 6 et 6E) pour la plus répandue et le plus récent février 2021. Il se base sur une des fréquences variables elle débute à 1GHz et peut monter jusqu'à 7Ghz, cette norme utilise

Du fait qu'il permet l'échange de données sur un réseau, il est devenu très vite nécessaire de le sécuriser. Ainsi est apparu le premier protocole de sécurisation par mot de passe d'un réseau Wi-FI en 1999 : le WEP. La plupart des protocoles se reposent sur un cryptage de la connexion au réseau par un mot de passe.

La norme 802.11 dans le modèle OSI



Le WEP

Le WEP est la première solution de cryptage de réseau Wi-Fi apparu en 1999. Il a été vite remplacé car il souffrait de nombreuses failles de sécurités. Son fonctionnement reposait sur l'utilisation d'une clé de 64, ou 128 bits. Ainsi, à l'heure actuelle il faut moins de 2 minutes pour cracker une clé WEP grâce à des outils spécialisés comme aircrack-ng.

Le WPA

Le WPA, apparu en 2003, est le successeur direct du WEP. Il est beaucoup plus efficace en termes de cryptage et évolutif dans son fonctionnement. Comme son prédécesseur il se base sur une clé 128 bits. Il fonctionnait avec un système dit de TKIP, qui est une méthode de cryptage qui mélange des paquets pour après les remettre dans l'ordre. Le TKIP a été instauré afin de ne pas rendre obsolète le matériel WEP. Cette méthode présentait de nombreuses failles dont une majeure découverte en 2008 permettant de pirater un réseau en moins de 15 minutes.

Le mode de fonctionnement du WPA le plus répandu est le WPA-Personnel (WPA-PSK), qui est le WPA destiné à un usage personnel ou de petite entreprise. Ici le mot de passe wifi est le même pour tous les utilisateurs et est stocké sur la machine cliente.

On le distingue du WPA-Enterprise (ou MGT) qui est relié à un serveur RADIUS permettant l'utilisation du plusieurs identifiants pour s'identifier.

Le WPA2

Évolution directe du WPA parue en 2004, le WPA2 remplace le TKIP par l'AES qui est un algorithme de chiffrement dis symétrique considéré comme plus performant et sécurisé que son prédécesseur. Cependant, le WPA2 peut aussi fonctionner en TKIP pour assurer une rétrocompatibilité et repose toujours sur une clé en 128 bits.

Le mode de fonctionnement du WPA2 le plus répandu est le WPA2-Personnel (WPA2-PSK), comme son prédécesseur l'authentification se déroulera alors grâce à une clé unique à tous les clients.

On le distingue lui aussi de son homologue catégorisé entreprise : le WPA2Enterprise, qui consiste lui aussi à utiliser un serveur d'authentification RADIUS qui permet d'autoriser ou non la connexion.

Le dispositif WPA2 possède lui aussi des failles dont la majeure nommée Krack découverte en 2016.

Le WPS

Le WPS n'est pas un standard à proprement parler, il a été instauré en 2007 et est un standard permettant de se connecter plus facilement aux réseaux WiFi sans entrer le mot de passe PSK. Le WPS se déclinait en 4 modes : le code PIN, le PBC (un bouton à appuyer sur le routeur et le client), le NFC, ou un branchement USB.

Cependant, 4 ans après de grave vulnérabilité ont été trouvée liées au WPS, permettant des piratages rapides. Il est conseillé de désactiver ce protocole.

Le WPA3

Afin de corriger la faille présente dans le WPA2, le WPA3 a été créé par la Wi-Fi Alliance en 2018. Il suppose un changement radical dans la sécurisation de l''authentification tout en gardant le principe d'unicité du mot de passe. Un des principaux problèmes liés au Wi-Fi auparavant étant la facilité d'effectuer des attaques par dictionnaire, le WPA3 instaure le remplacement du PSK par le SAE car il oblige aux attaquant de ne pouvoir faire qu'un seul essai de mot de passe hors ligne. Ainsi, si un attaquant veut faire du brute-force il devra être à proximité du réseau Wi-Fi et pourra se faire bloquer par le routeur. Une autre innovation implémentée est l'IDP, mettant en place une clé unique par clients, permettant aux clients de voir leur donnée protégée même si un attaquant récupère la clé. Enfin, le WPA3 met fin aux réseaux ouvert en mettant en place un chiffrement systématique grâce au système d'OWE. Enfin, le WPA3 instaure un successeur au WPS, le DPP, ce successeur corrige toutes les vulnérabilités du WPS.

Comme ses prédécesseurs, le WPA3 se décline en deux utilisations, la personnelle se basant sur une clé de chiffrement en 128 bits qui peut optionnellement être passée en 192 bits et la version Entreprise qui impose l'utilisation d'une clé en 192 bits.

Bien que le WPA3 soit extrêmement récent et très peu répandu, des failles ont déjà été trouvées en 2019 comme la Dragonblood.

La comparaison

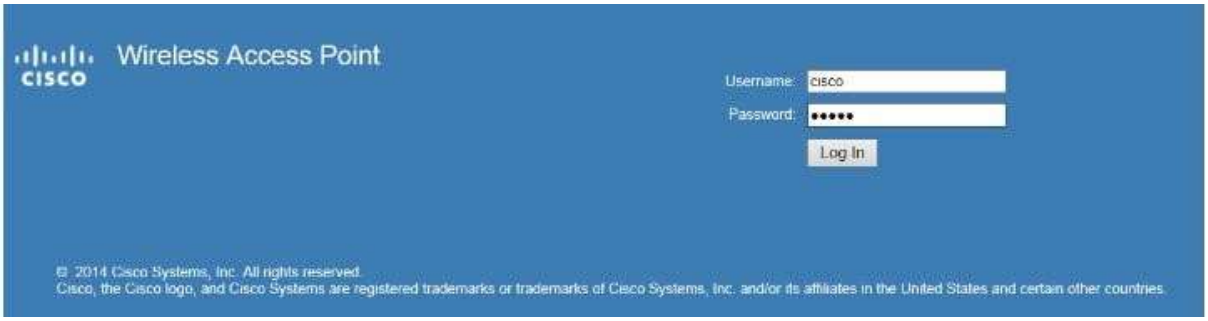
	Cryptologie	Authentification
WPA-Personnel	Basée sur le TKIP, avec une clé en 128 bits	Par une clé unique pour tous les clients en utilisant le protocole PSK
WPA2-Personnel	Basée sur le protocole AES, avec une clé en 128 bits	Par une clé unique pour tous les clients en utilisant le protocole PSK
WPA-Enterprise	Basée sur le TKIP, avec une clé en 128 bits	Par un serveur d'authentification, permettant à chaque client d'avoir son mot de passe
WPA2-Enterprise	Basée sur le protocole AES, avec une clé en 128 bits	Par un serveur d'authentification, permettant à chaque client d'avoir son mot de passe
WPA3	Basée sur le protocole AES, avec une clé en 128 bits voir 196 bits	Par une clé unique pour tous les clients en utilisant le protocole SAE

Accéder à l'interface d'administration de la borne wifi

Les recharges de Point d'accès et est placées aux configurations de configuration par défaut.

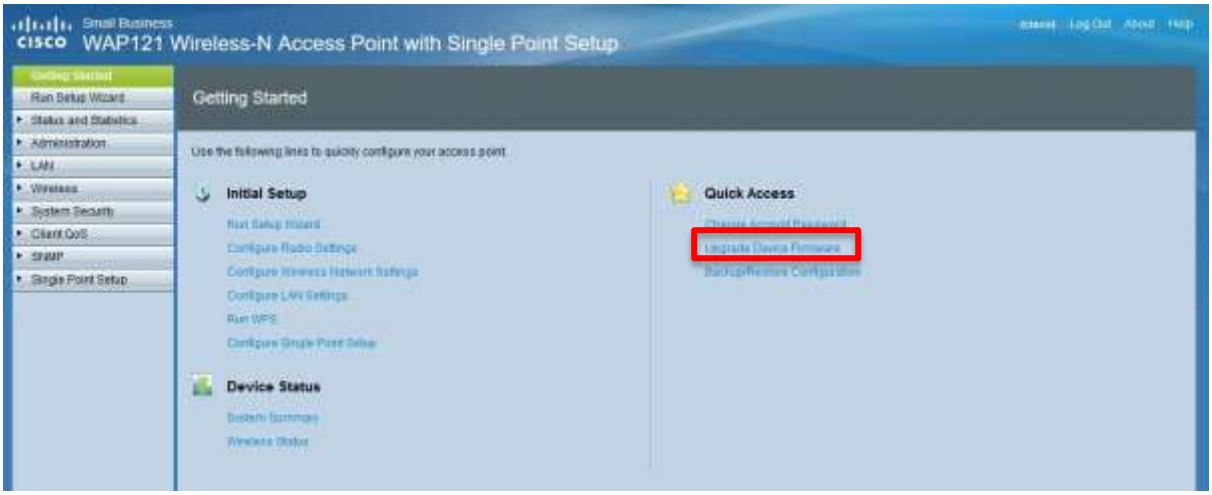
1. Lancez un navigateur Web, tel que l'Internet Explorer ou le Mozilla Firefox. Tapez l'adresse IP statique par défaut 192.168.1.245 dans la barre URL et l'appuyez sur entrent. Pour atteindre cette adresse IP, soyez sûr que votre ordinateur est sur le réseau 192.168.1.xxx.

2. Procédure de connexion avec les qualifications par défaut. Le nom d'utilisateur par défaut est Cisco, et le mot de passe par défaut est Cisco.



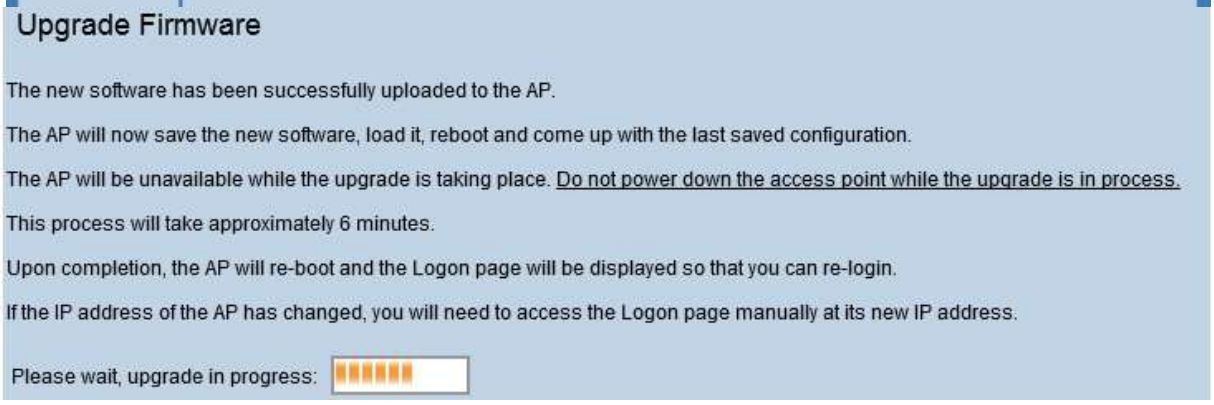
Mettre à jour la borne WI-FI

4. Cliquer sur Upgrade Device Firmware



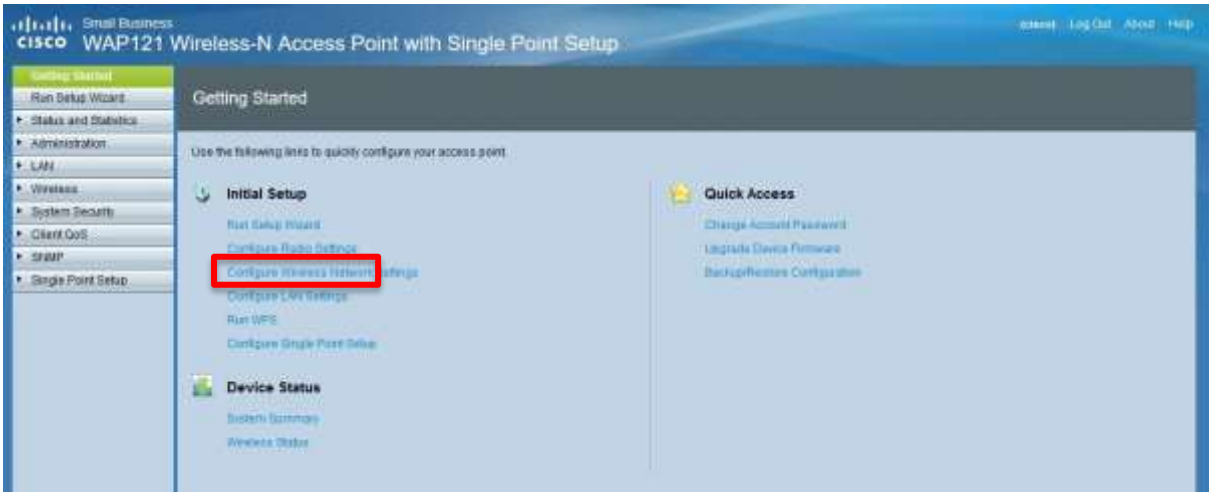
5. Rendez-vous sur le site du constructeur puis télécharger le firmware :
https://software.cisco.com/download/home/284152657/type/282463166/release/1.0.6.8?i=!p p

6.Utiliser la méthode HTTP/HTTPS, parcourir et ajouter le fichier tar téléchargé et cliquer sur upgrade

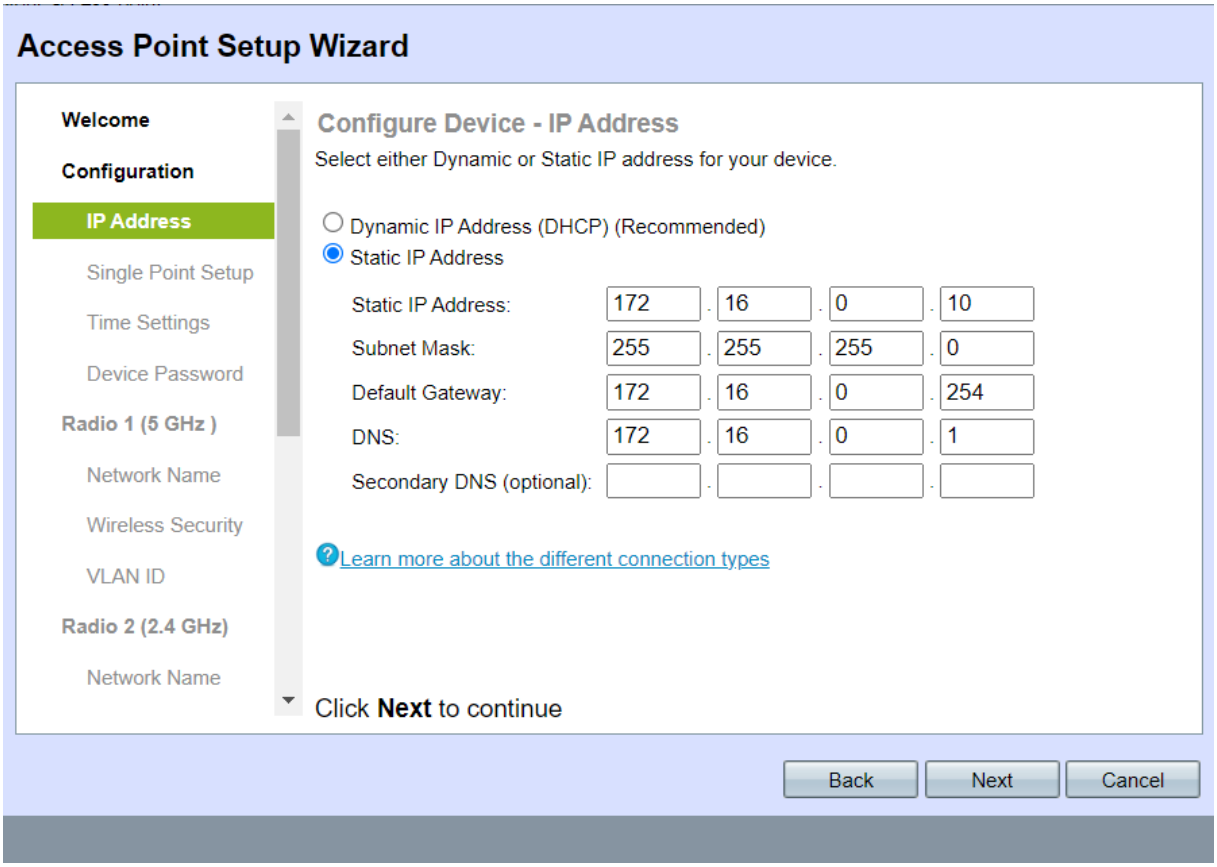


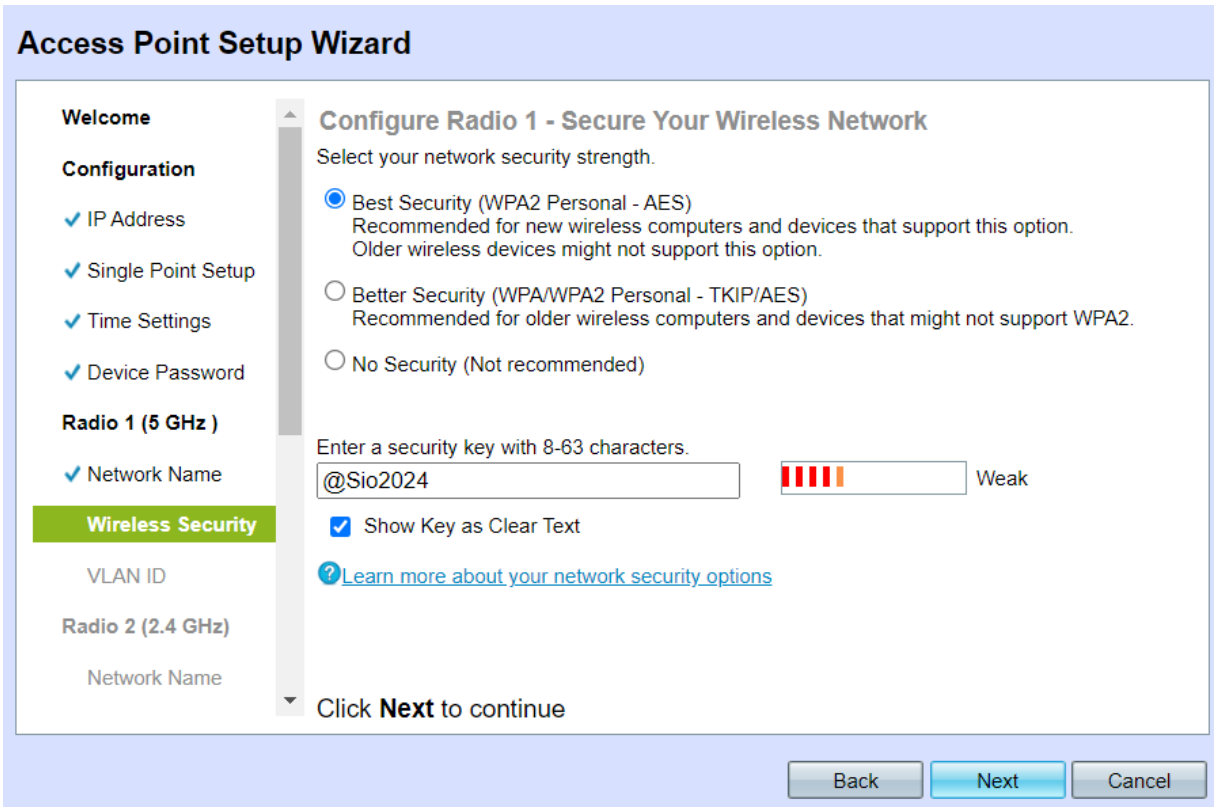
Configuration de la borne WI-FI

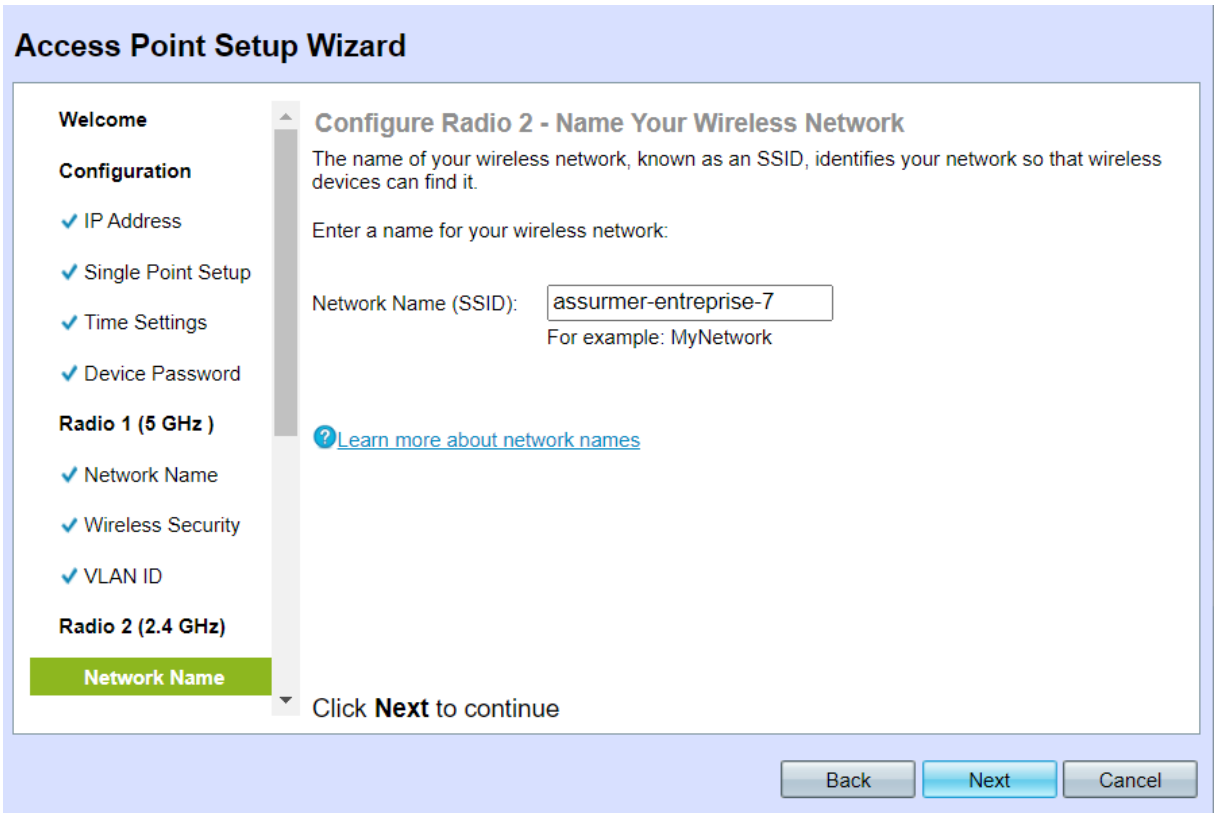
7. Une fois installer connectez-vous et cliquer Configure LAN Settings



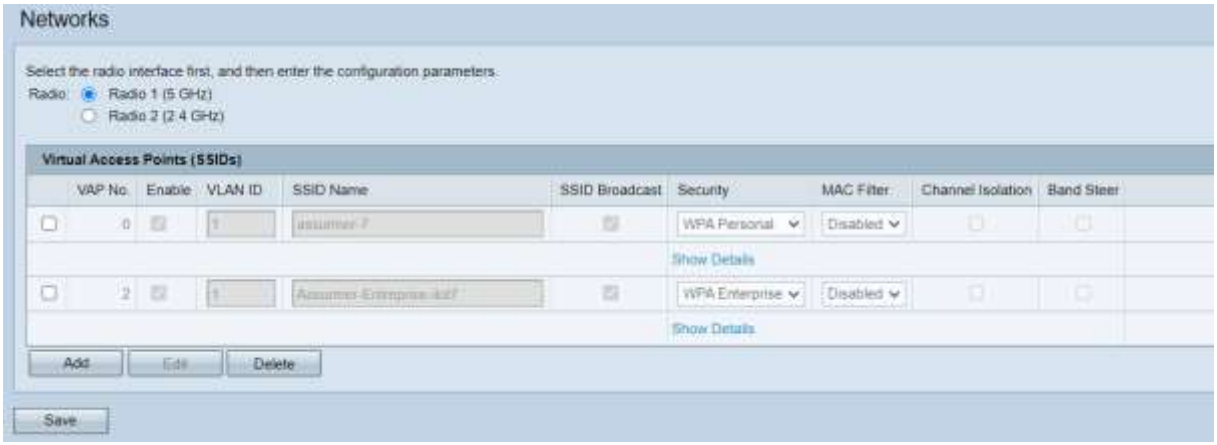
8. Configurer l'IPv4 statique de la borne, le masque, la passerelle, le DNS de votre réseau et éventuellement indiqué lui VLAN si votre switch et configurer avec des vlans




Access Point Setup Wizard
Welcome
Configuration
IP Address
Single Point Setup
Time Settings
Device Password
Radio 1 (5 GHz)
Network Name
Wireless Security
VLAN ID
Radio 2 (2.4 GHz)
Network Name
Configure Radio 1 - Secure Your Wireless Network
Select your network security strength.
Best Security (WPA2 Personal - AES)
Recommended for new wireless computers and devices that support this option.
Older wireless devices might not support this option.
Better Security (WPA/WPA2 Personal - TKIP/AES)
Recommended for older wireless computers and devices that might not support WPA2.
No Security (Not recommended)
Enter a security key with 8-63 characters.
@Sio2024
Weak
Show Key as Clear Text
Learn more about your network security options
Click Next to continue
Back
Next
Cancel

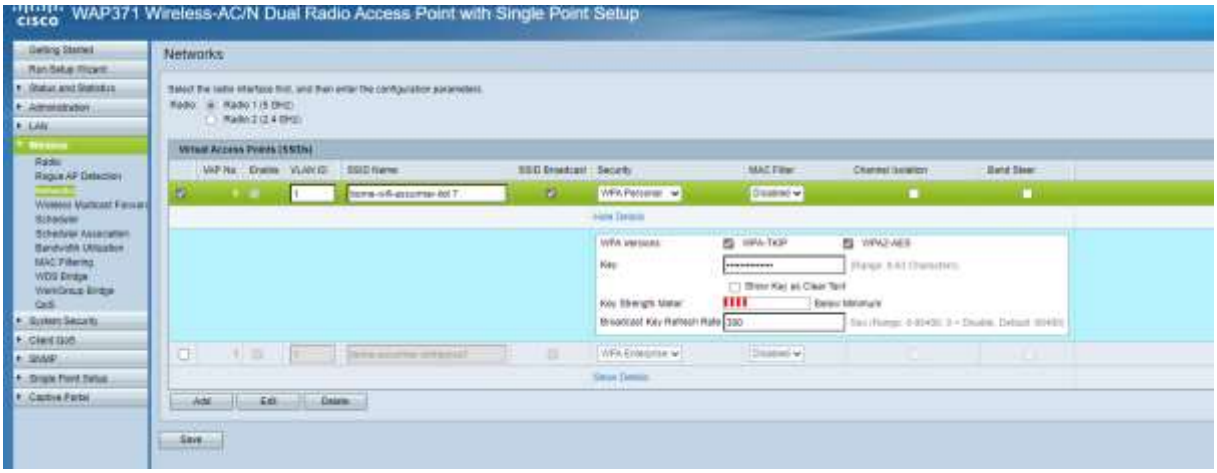

Access Point Setup Wizard
Welcome
Configuration
IP Address
Single Point Setup
Time Settings
Device Password
Radio 1 (5 GHz)
Network Name
Wireless Security
VLAN ID
Radio 2 (2.4 GHz)
Network Name
Configure Radio 2 - Name Your Wireless Network
The name of your wireless network, known as an SSID, identifies your network so that wireless devices can find it.
Enter a name for your wireless network:
Network Name (SSID):
assurmer-entreprise-7
For example: MyNetwork
Learn more about network names
Click Next to continue
Back
Next
Cancel

9. Retourner au menu et cliquer maintenant sur Configure Wireless Network Settings

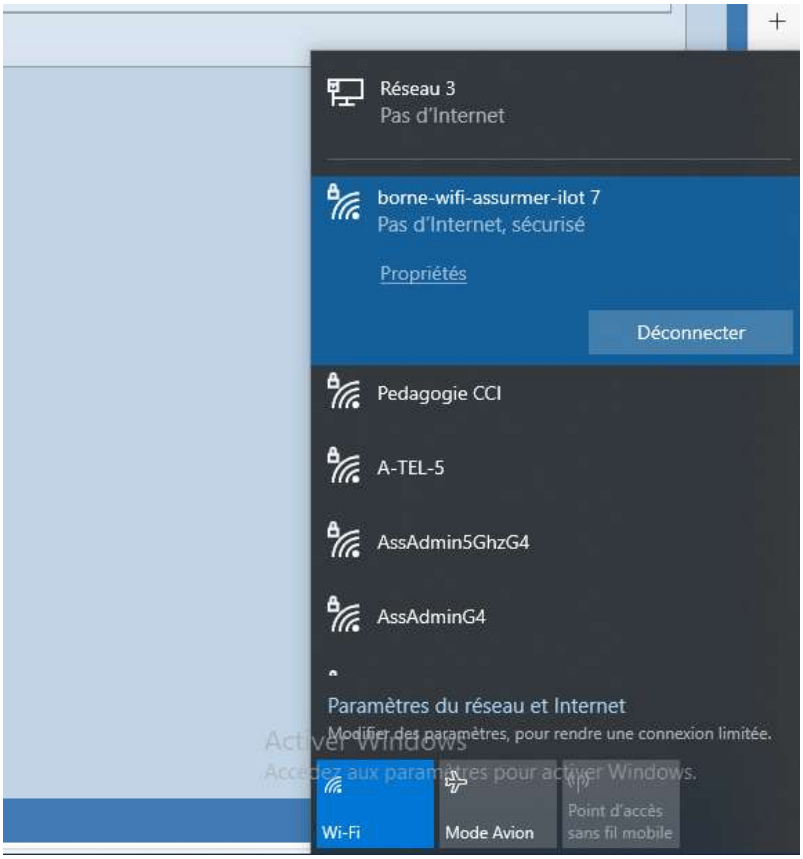


Création des différents points d'accès WI-FI

11. Cliquer sur le point d'accès par défaut et faite édit
12. Indiquer le vlan à utiliser si c'est le cas donner un SSID au point d'accès laisser cocher le SSID Broadcast enfin pour le premier point d'accès on utilise la sécurité WPA Personal. Ensuite nous définissons la clé puis on sauvegarde.



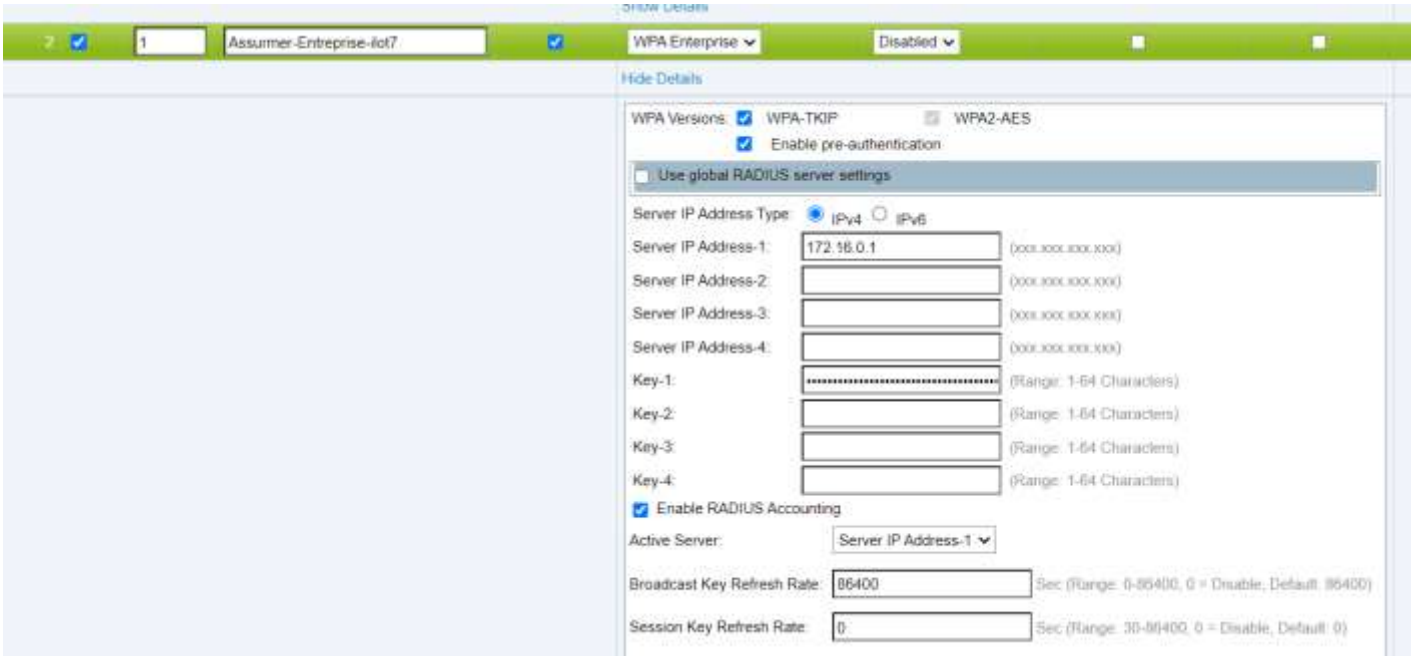
13.Votre premier point d'accès WI-FI et fonctionnel il vous suffit de vous connecter à l'aide de la clé créer pour celui-ci.



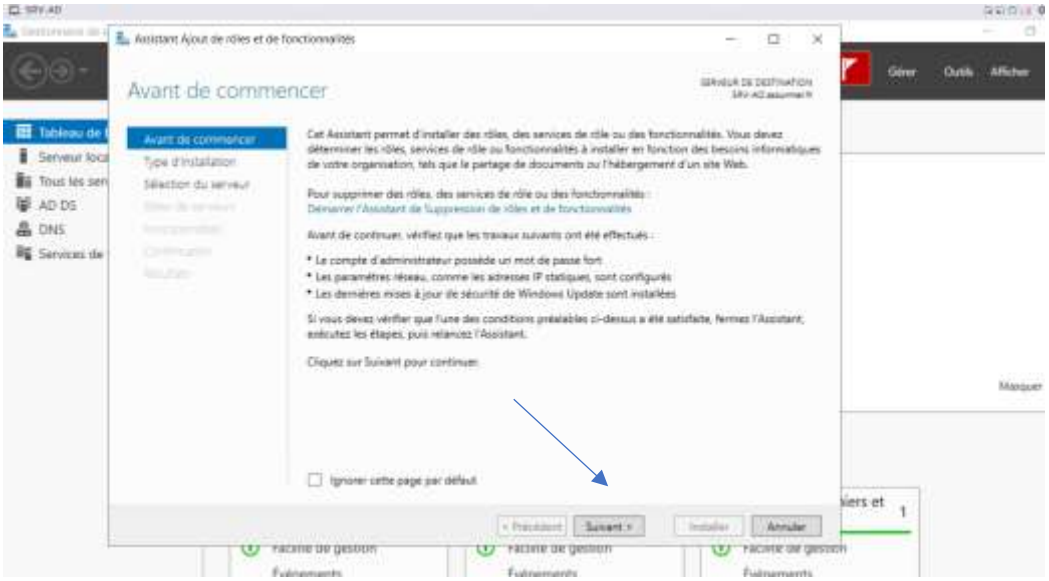
14. Nous allons créer un point d'accès WI-FI d'entreprise
15.On add puis on edit

16. Indiquer le vlan à utiliser si c'est le cas donner un SSID au point d'accès laisser cocher le SSID Broadcast enfin pour le premier point d'accès on utilise la sécurité WPA Entreprise. Ensuite nous définissons l'adresse IP ou point nos service AD, DHCP … éventuellement ca réplication et une clé puis on sauvegarde.

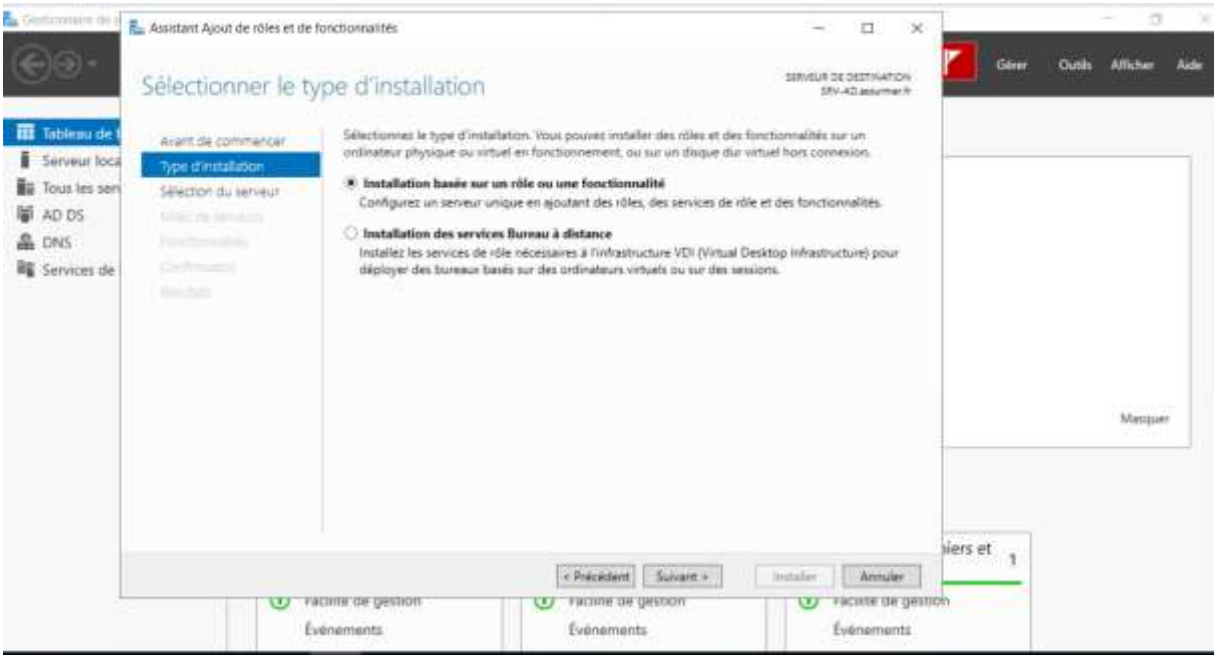
Le point d'accès sera alors visible, mais il ne sera pas possible de la rejoindre nous devons effectuer une manipulation sur le serveur AD. Il pourra ensuite se connecter avec ses identifiants d'entreprise sur la borne WI-Fi



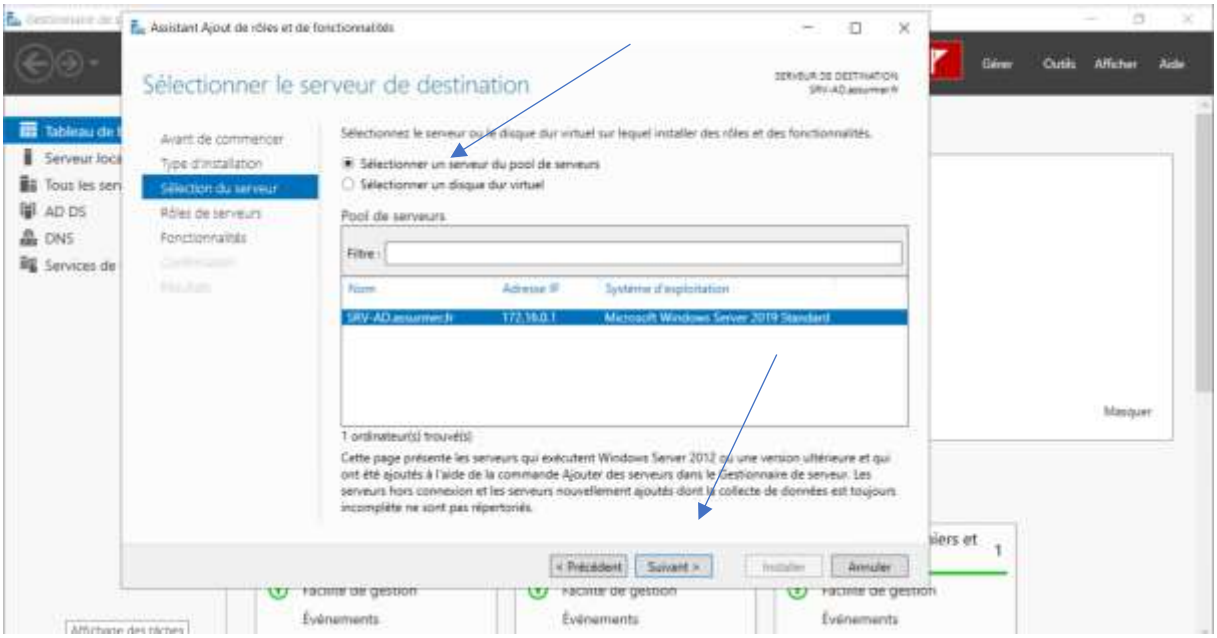
Installation du service radius sur le premier serveur AD



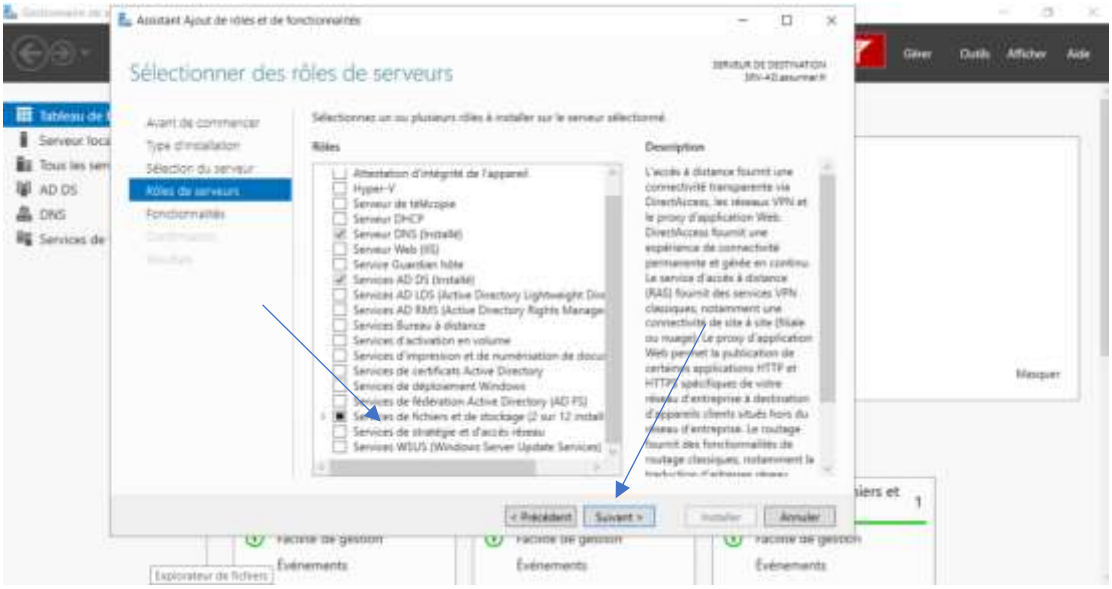
Cliquer sur « suivant » pour continuer



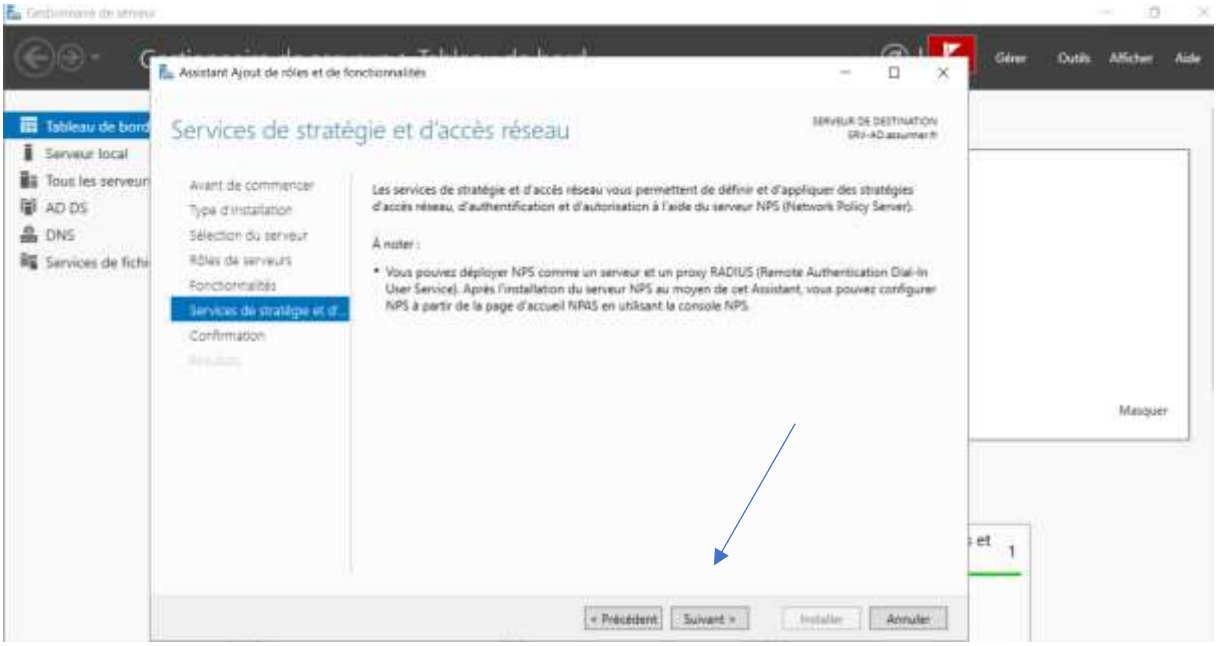
Cliquer sur « Installation basée sur un rôle ou une fonctionnalité puis cliquer sur « suivant »



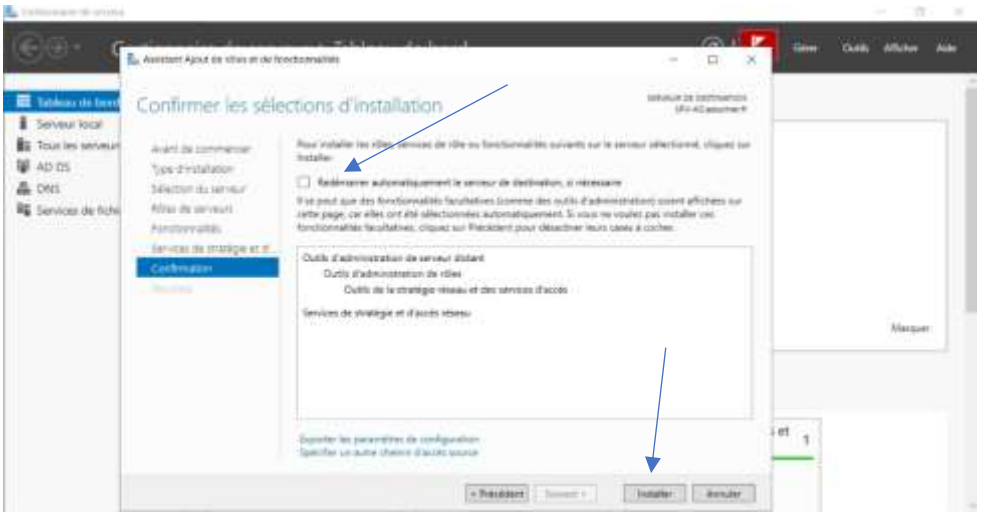
Cliquer sur « sélectionner un serveur de pool de serveurs », sélectionner le serveurs AD « SRV-AD assurmer.fr » puis cliquer sur suivant



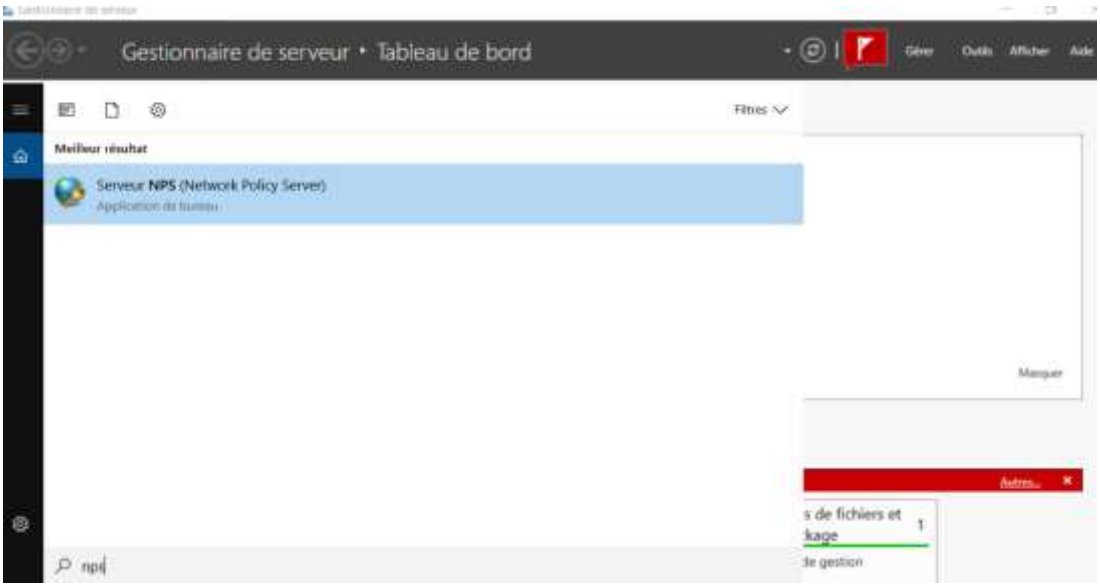
Sélectionner « Services de stratégie et d'accès réseau » puis cliquer sur suivant pour continuer



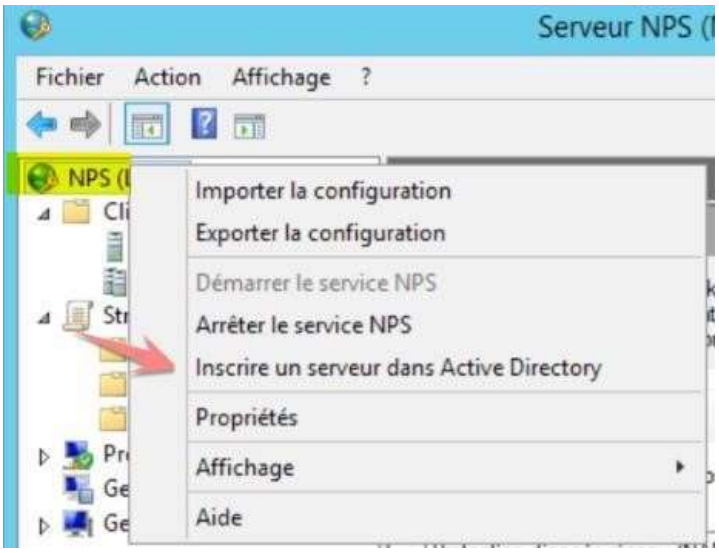
Cliquer sur suivant pour continuer



Cliquer sur « Redémarrer automatiquement le serveur de destination, si nécessaire » puis cliquer sur installer



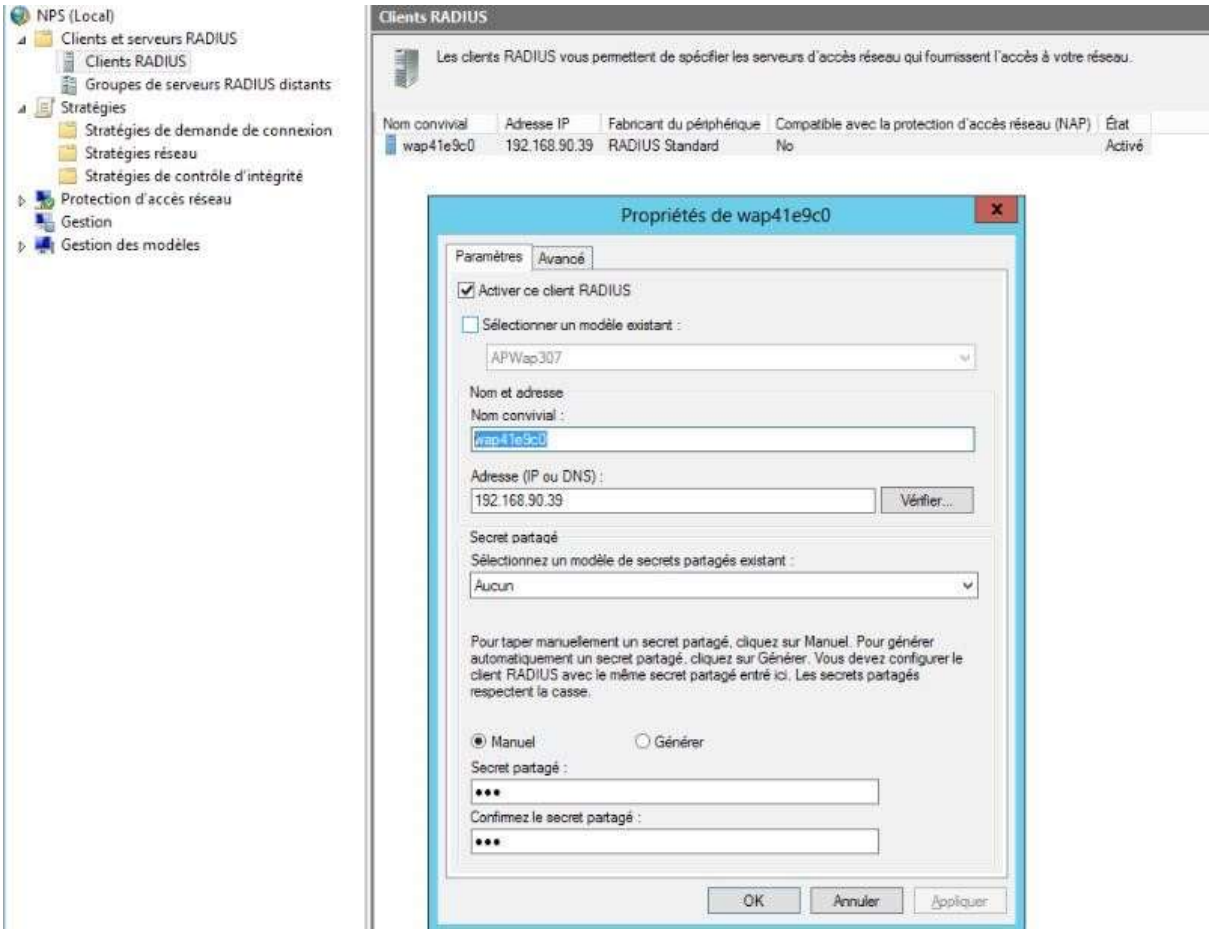
Aller dans la barre de recherche et rechercher NPS



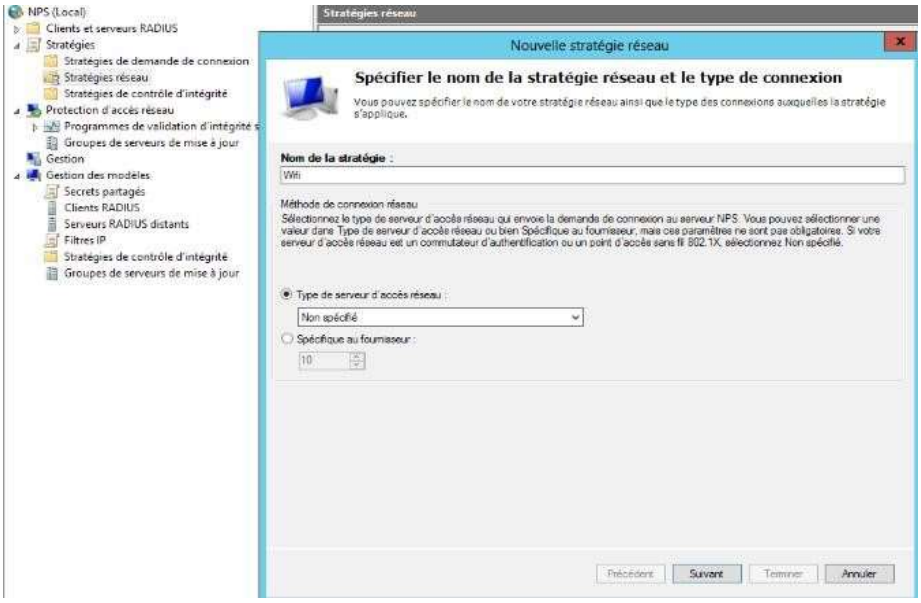
23.Lancer le service et faite clic droit sur NPS

24. Inscrire le serveur dans l'Active directory sinon il sera impossible de définir les conditions liées aux groupes/utilisateurs dans la stratégie d'accès distant !

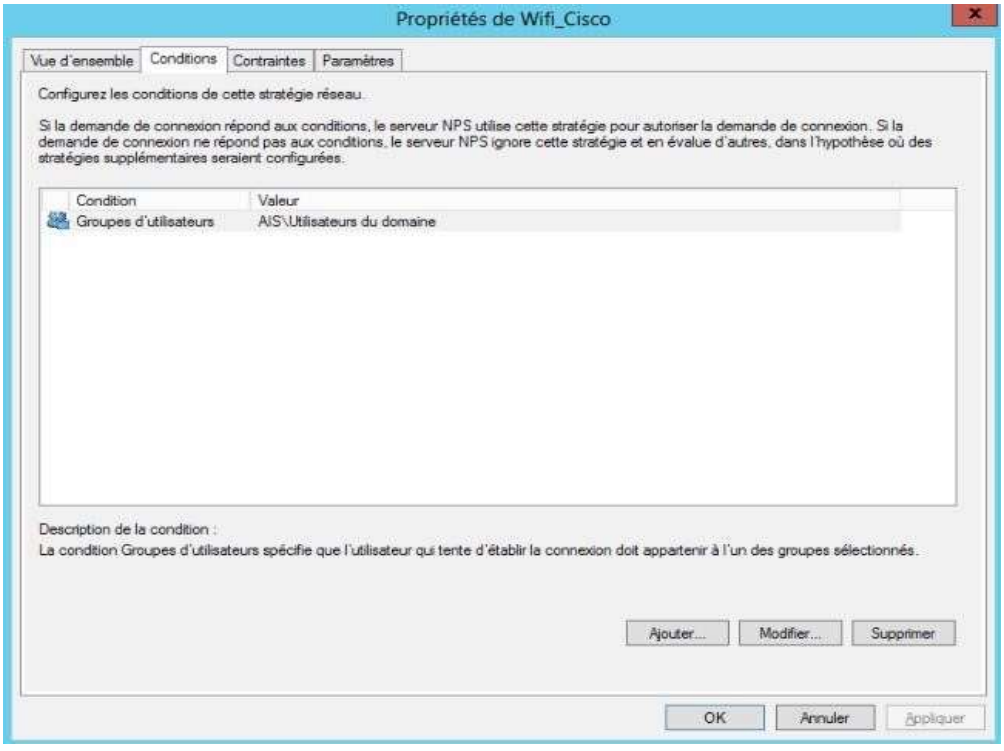
25.Création d'un nouveau client radius sur la console NPS,
Clic droit sur client radius et ajouter une nouvelle borne.
Renseigner le nom de la borne et son adresse ip ainsi que le mot de passe que vous avez définit en amont.



26.Configuration de la stratégie réseau nouvelle stratégie réseau – nom de la stratégie : Wifi

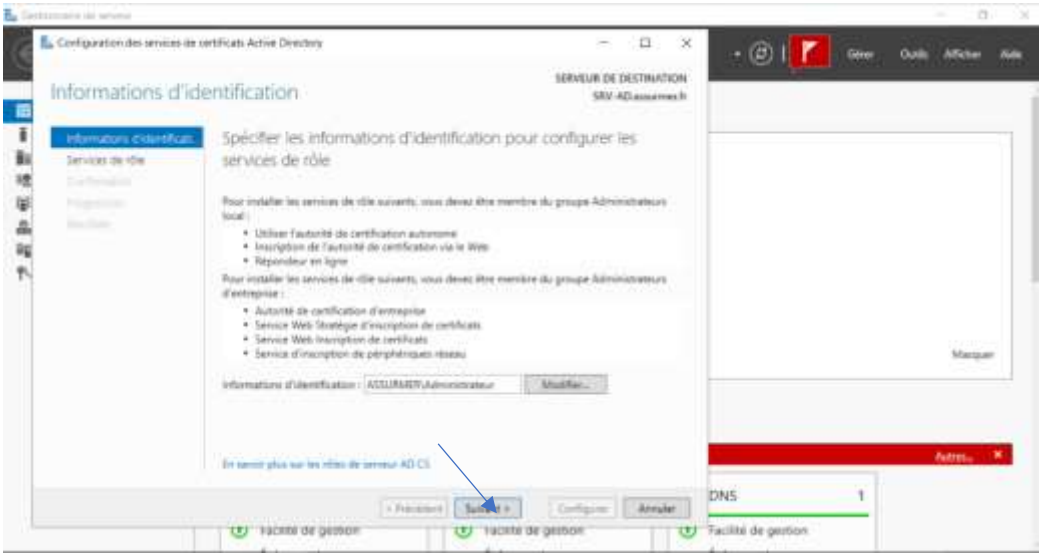


27.Nous ajouterons le Groupes utilisateurs du domaine

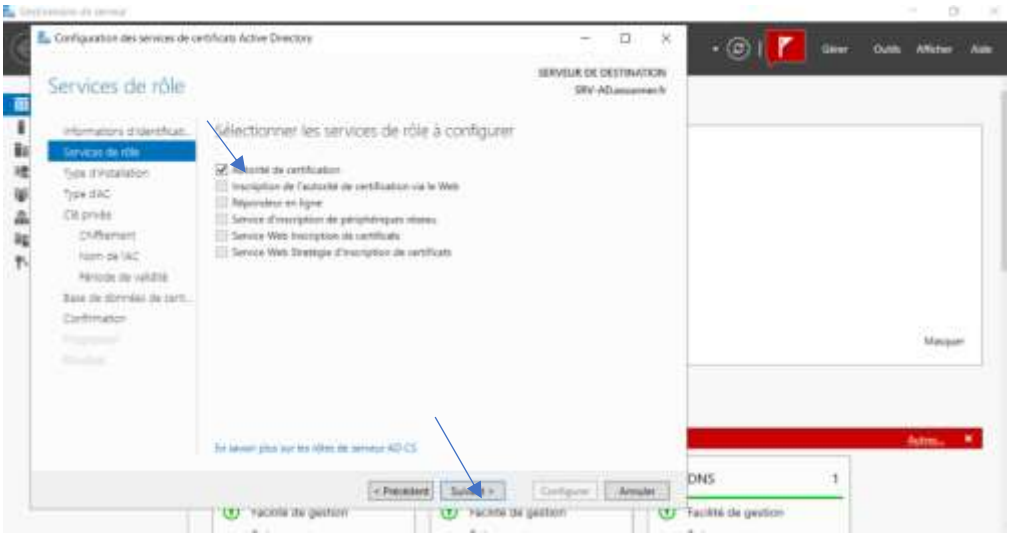


28.Selectionner MS-CHAP v2 et MS-CHAP pour authentification par mot de passe.

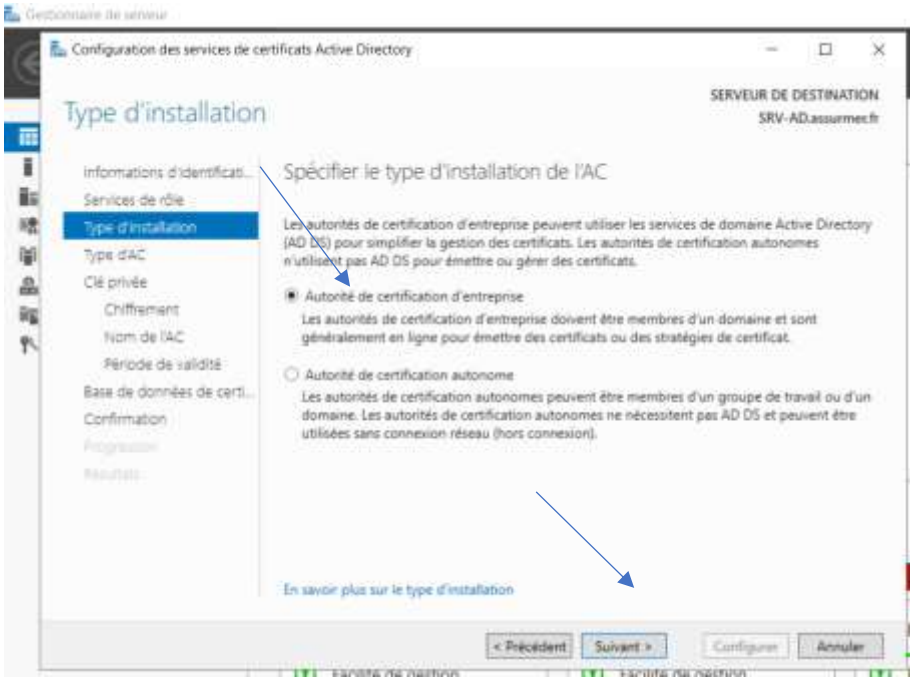
29.Monter Le protocole Extended Authentication Protocole qui servira pour le transport des données nécessaire à l'authentification.



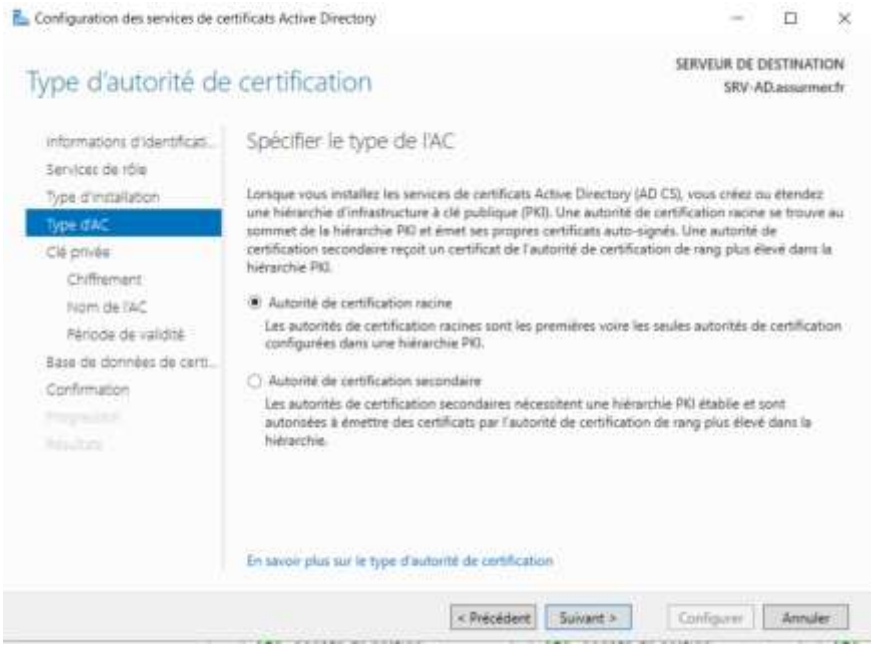
28. laisser par defaut le compte admin puis cliquez sur suivant



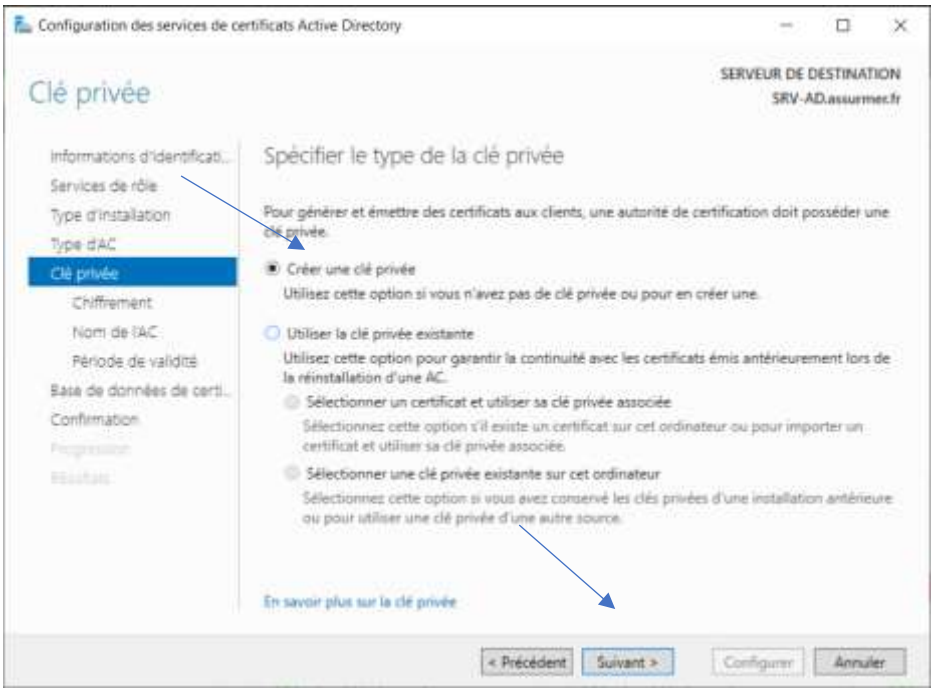
29. Selectionner « Autorité de certification » puis ensuite cliquer sur « suivant »



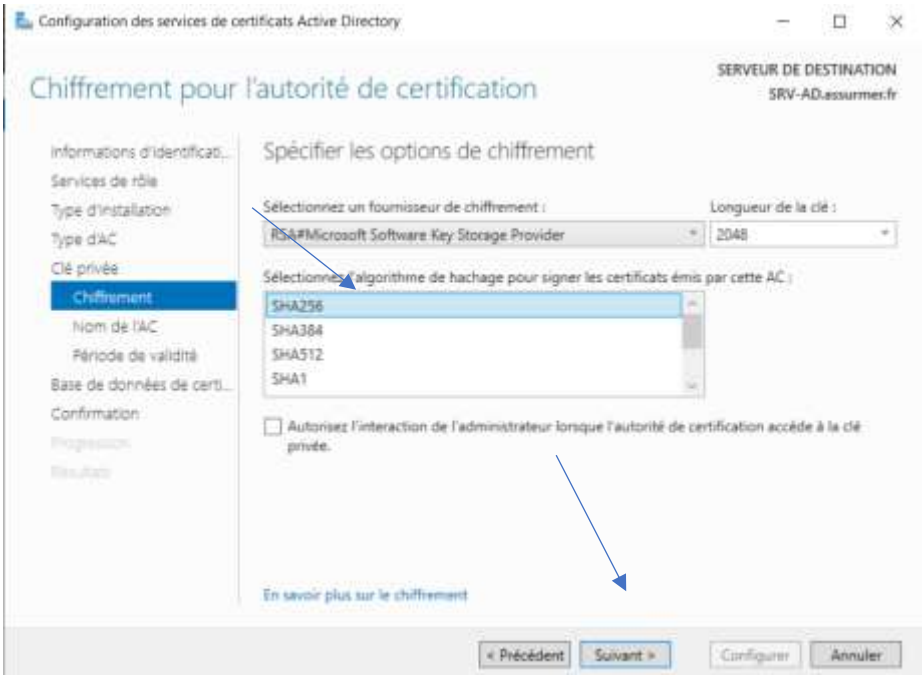
30. Sélectionner « Autorité de certification d'entreprise » puis cliquer sur suivant



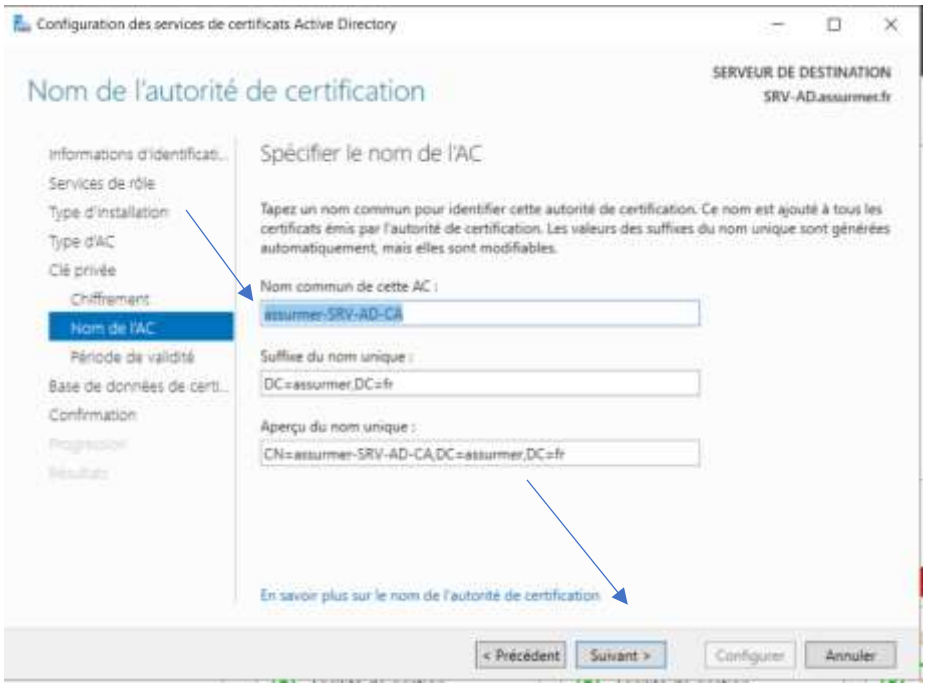
31. Sélectionner « Autorité de certification racine » puis cliquer sur suivant



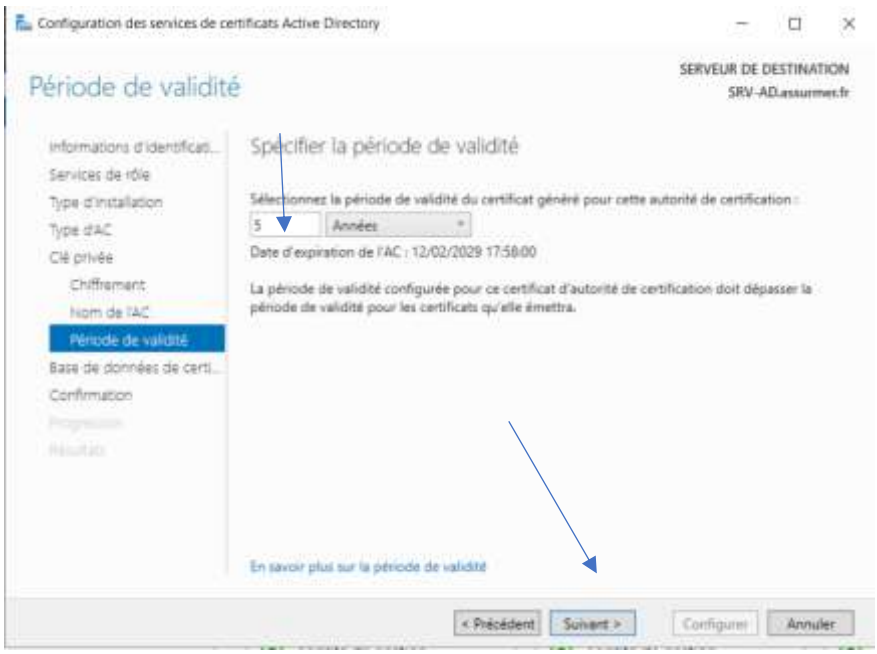
32. Cliquer sur « Créer une clé privée » puis cliquer sur suivant



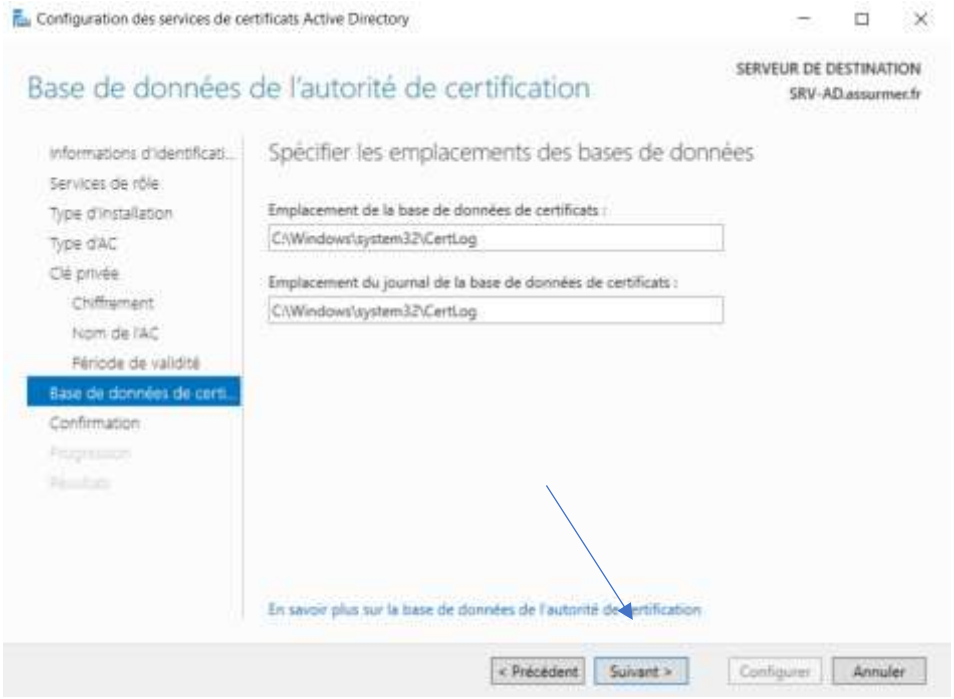
33. Sélectionner «SHA256 » pour l'algorithme de hachage pour signer les certificats émis par cette AC puis cliquer sur suivant



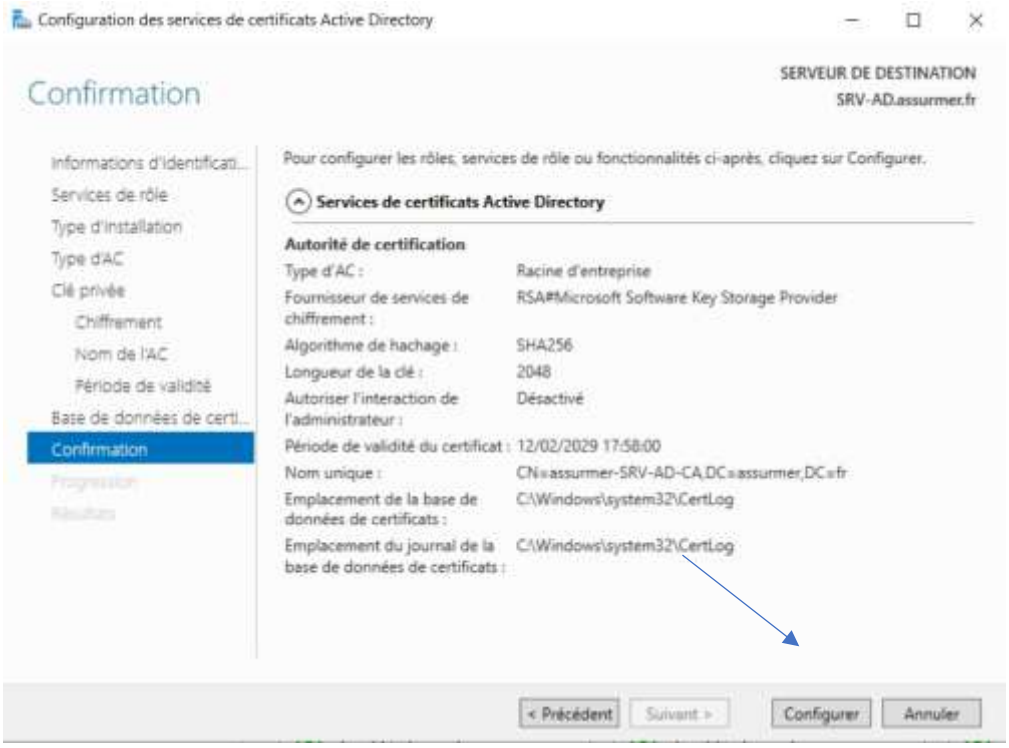
34. Ecrire le nom du serveur « Assurmer-SRV-AD-CA » puis cliquer sur suivant



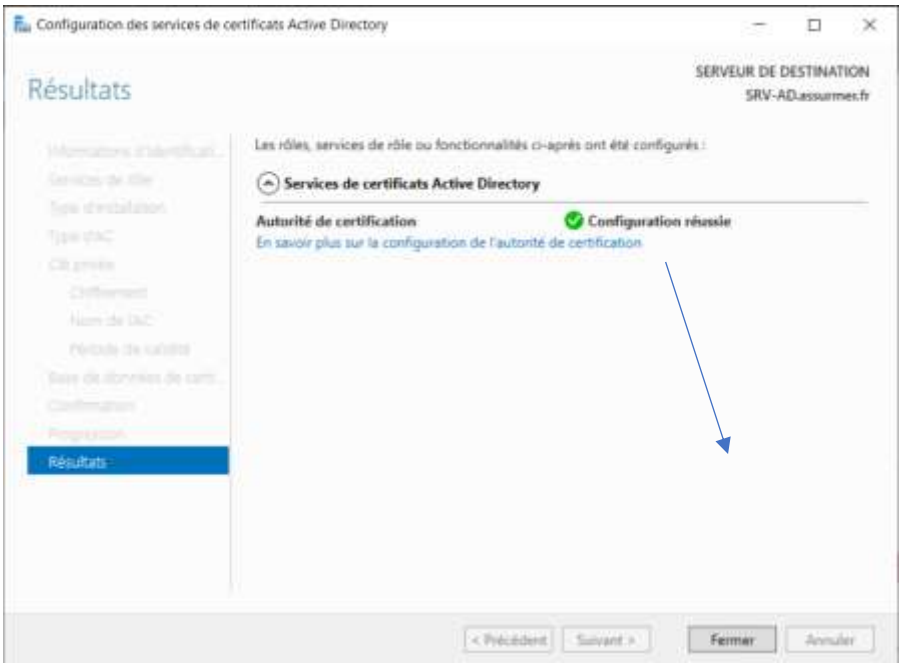
35. Validé les 5 années de période de validité du certificat géneré pour cette autorité de certification puis cliquer sur suivant



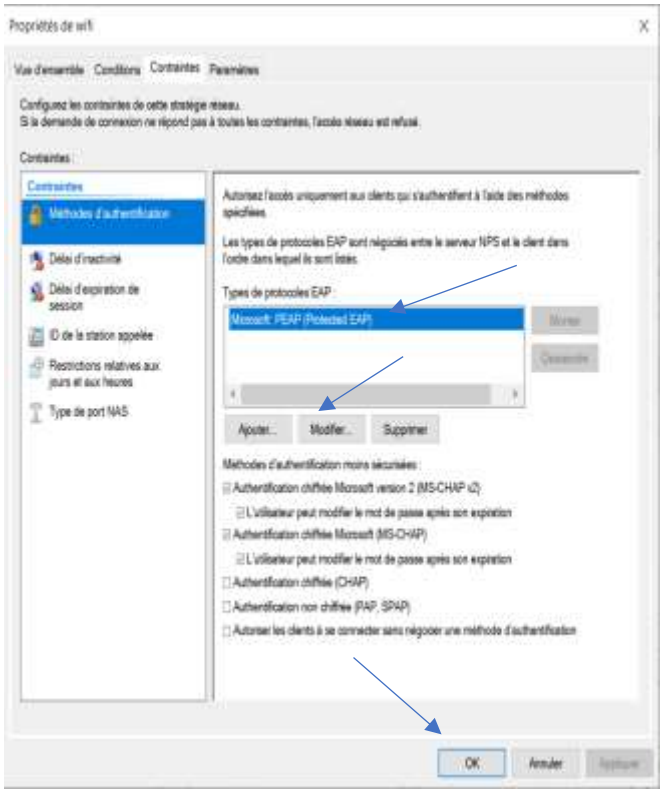
36. Vérifier l'emplacement de la base de données de certificats et vérifier aussi l'emplacement du journal de la base de données de certificats puis cliquer sur suivant

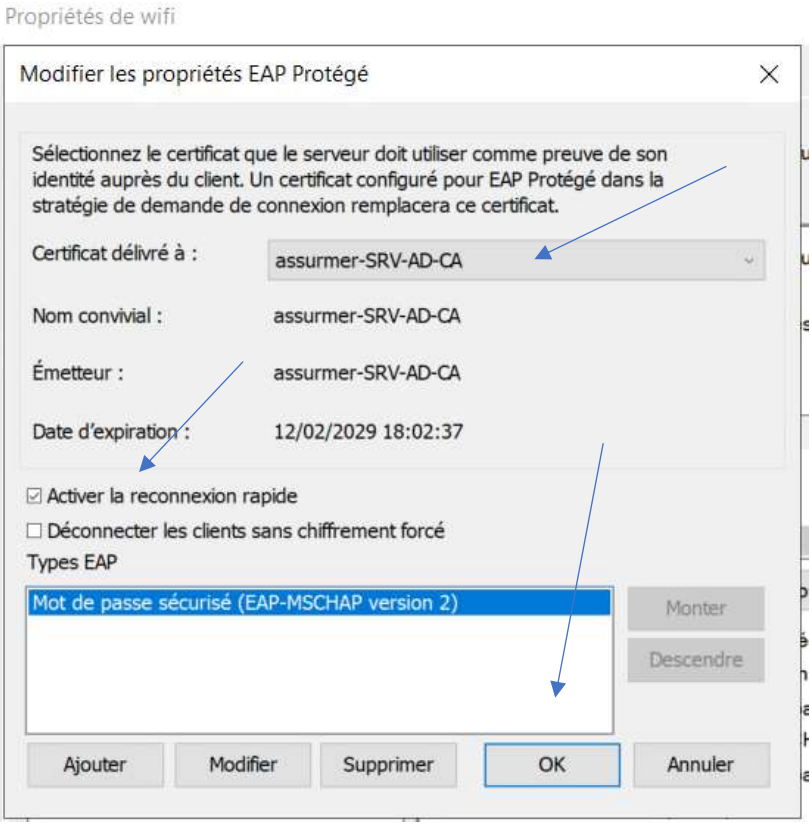


37. Cliquer sur « Configurer »



38. Attendre que la configuration soit réussie puis cliquer sur fermer





39. Sélectionner Microsoft PEAP , appuyer sur « modifier » puis sélectionner le certificat serveur et appuyer sur « ok » pour valider

Test de la connexion avec les identifiants AD