

Procédure d'installation du service RADIUS





SOMMAIRE PROCEDURE

20

Installation du rôle Radius sur le serveur

23

Configuration du rôle

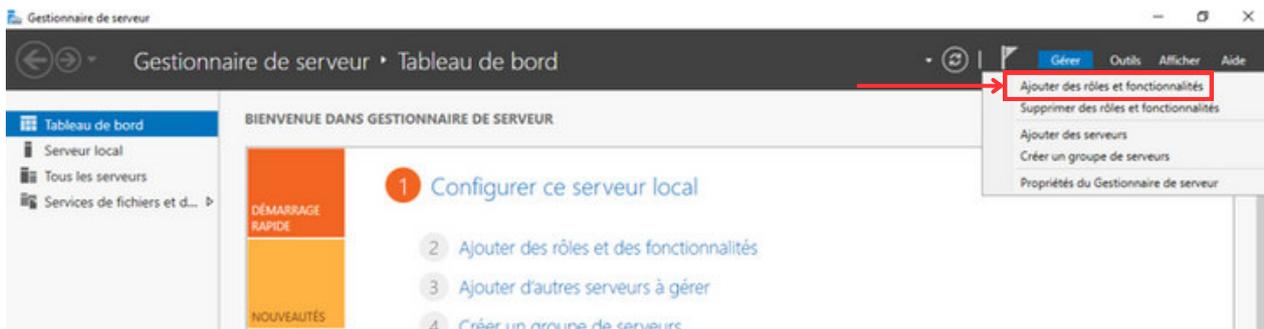
31

Ajout de la borne Wi-Fi

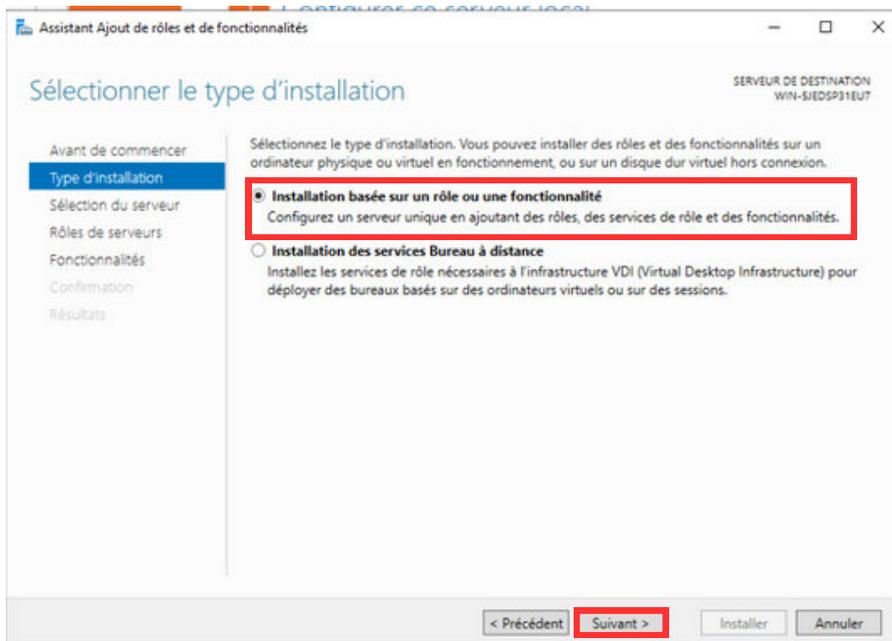


1. Installation du rôle Radius sur le serveur

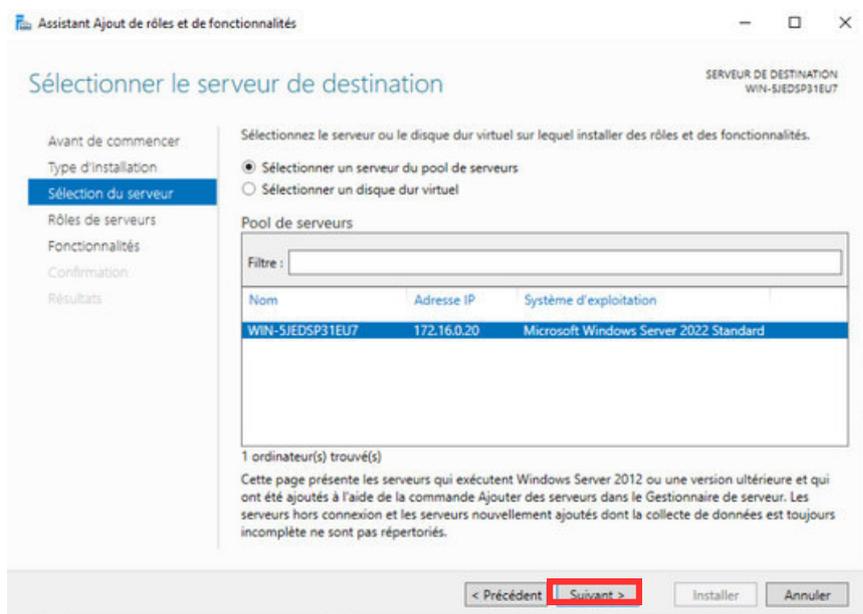
- Tout d'abord, il faut attribuer le rôle au serveur.
- Aller dans le gestionnaire de serveur et cliquer sur "Gérer" puis sur "Ajouter des rôles et fonctionnalités".



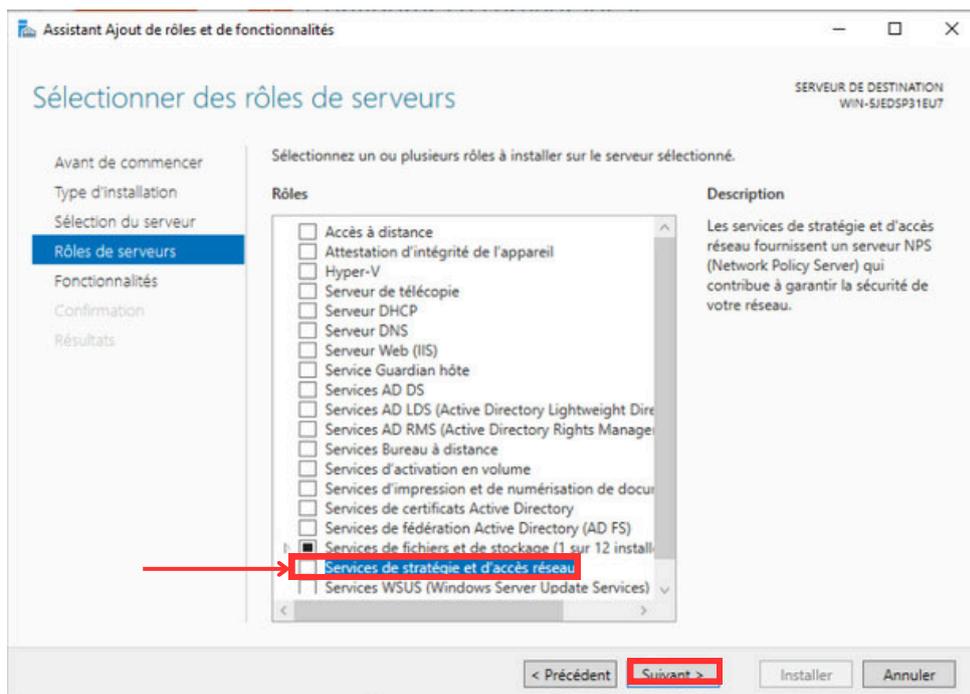
- Cliquer ensuite sur "Installation basée sur un rôle ou une fonctionnalité" puis sur "suivant".



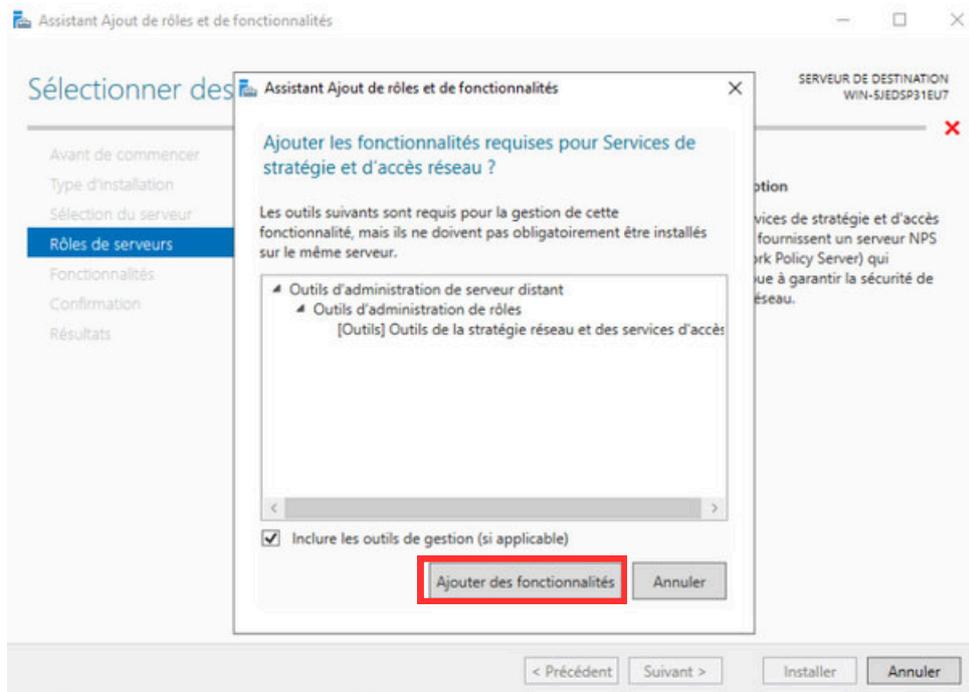
- Sélectionner le serveur et cliquer sur "suivant".



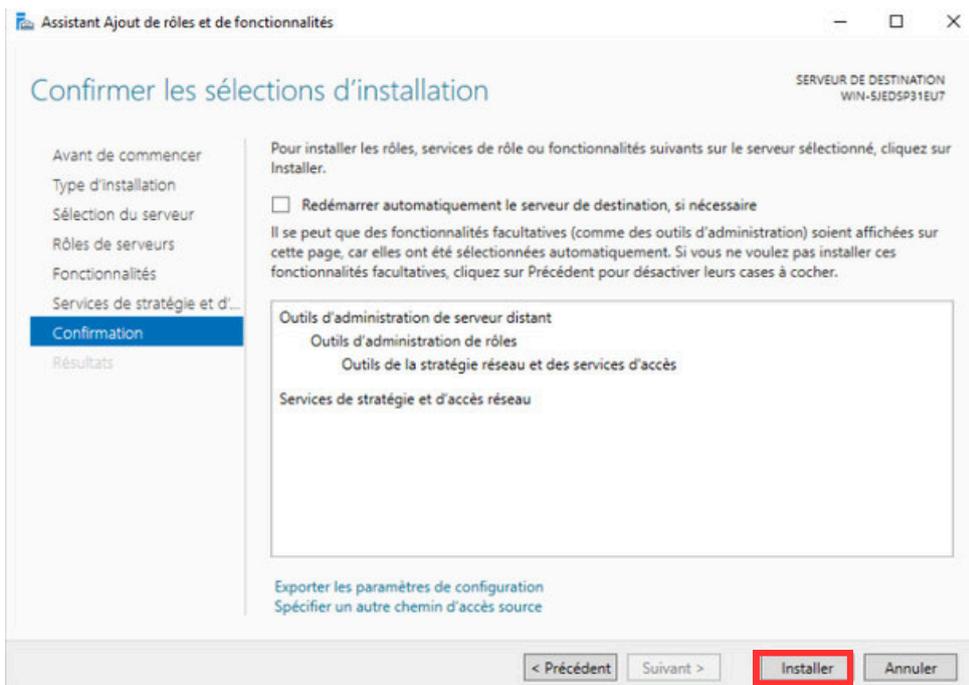
- Choisir "Services de stratégies et d'accès réseau" et cliquer sur "suivant".



- Cliquer sur “Ajouter des fonctionnalités”.

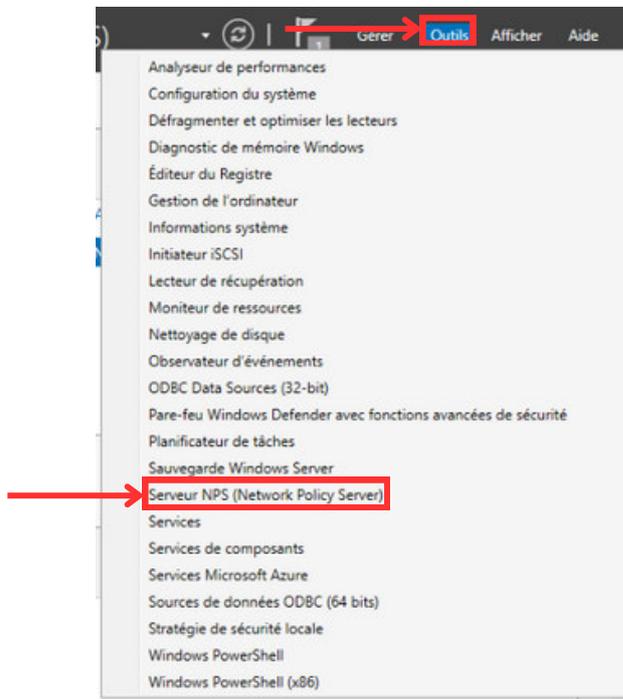


- Enfin, cliquer sur “Installer”, l’installation va ensuite commencer et durer quelques minutes.

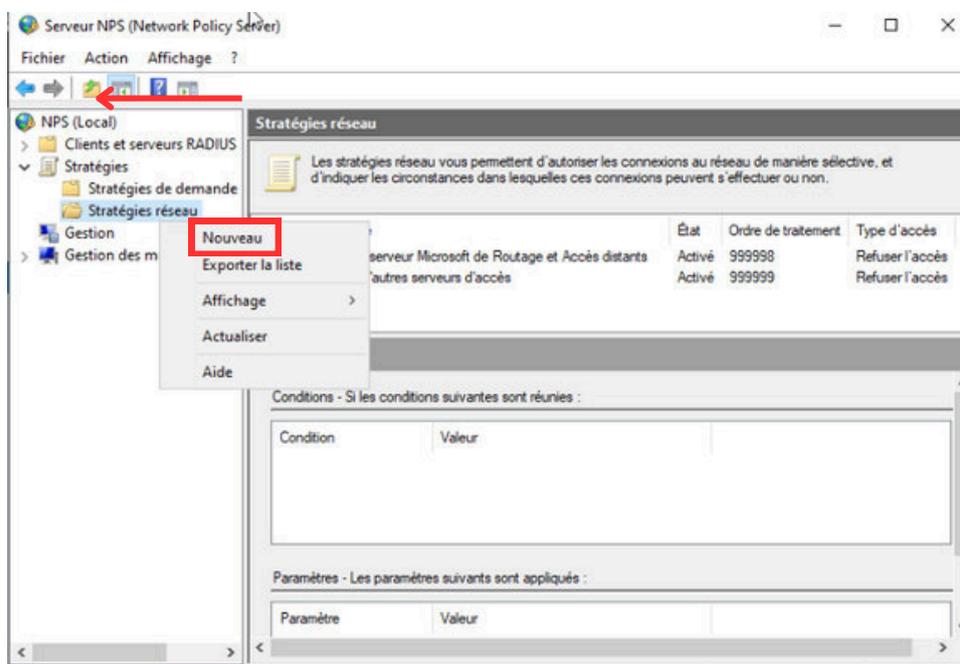


2. Configuration du rôle

- Cliquer cette fois sur "Outils" et ensuite sur "Serveur NPS (Network Policy Server)"



- La fenêtre d'administration de RADIUS s'ouvre, qui va servir à paramétrer la stratégie de connexion à notre réseau Wifi.
- Déplier le menu "Stratégie", faire un clic droit sur "Stratégies réseau" et sélectionnez "Nouveau".



3. Paramétrage de la stratégie de connexion

- Entrer le nom de la stratégie et cliquez sur "Suivant".

Nouvelle stratégie réseau

Spécifier le nom de la stratégie réseau et le type de connexion

Vous pouvez spécifier le nom de votre stratégie réseau ainsi que le type des connexions auxquelles la stratégie s'applique.

Nom de la stratégie :
connexion_wifi

Méthode de connexion réseau
Sélectionnez le type de serveur d'accès réseau qui envoie la demande de connexion au serveur NPS. Vous pouvez sélectionner une valeur dans Type de serveur d'accès réseau ou bien Spécifique au fournisseur, mais ces paramètres ne sont pas obligatoires. Si votre serveur d'accès réseau est un commutateur d'authentification ou un point d'accès sans fil 802.1X, sélectionnez Non spécifié.

Type de serveur d'accès réseau :
Non spécifié

Spécifique au fournisseur :
10

Précédent **Suivant** Terminer Annuler

5. Ajout des groupes d'utilisateurs pour l'authentification avec l'AD

- Cliquer sur "Ajouter", sélectionner "Groupes Windows" et encore une fois sur "Ajouter".

Nouvelle stratégie réseau

Spécifier les conditions

Spécifiez les conditions qui déterminent si cette stratégie réseau est évaluée pour une demande de connexion. Au minimum, une condition est nécessaire.

Sélectionner une condition

Sélectionnez une condition, puis cliquez sur Ajouter.

Groupes

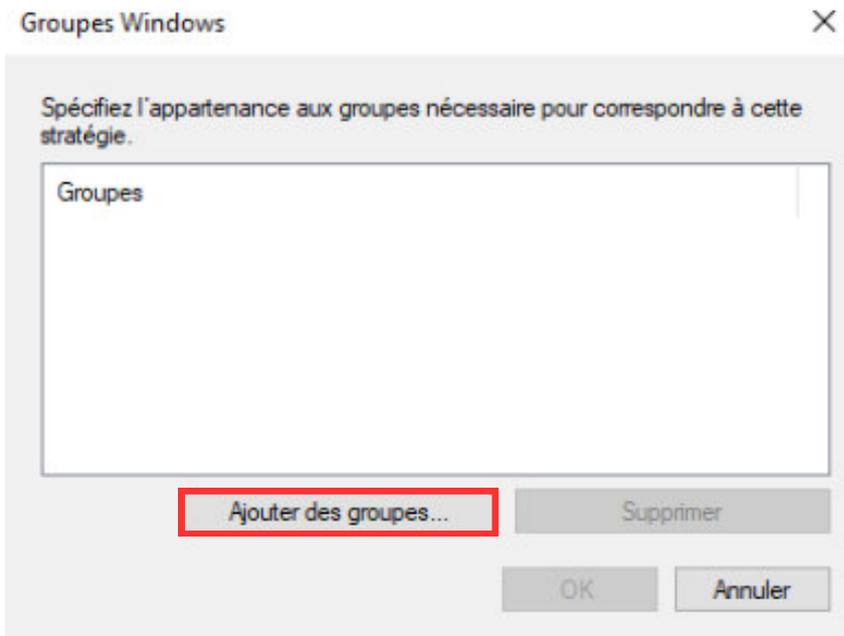
- Groupes Windows**
La condition Groupes Windows spécifie que l'utilisateur ou l'ordinateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.
- Groupes d'ordinateurs**
La condition Groupes d'ordinateurs spécifie que l'ordinateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.
- Groupes d'utilisateurs**
La condition Groupes d'utilisateurs spécifie que l'utilisateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.

Restrictions relatives aux jours et aux heures

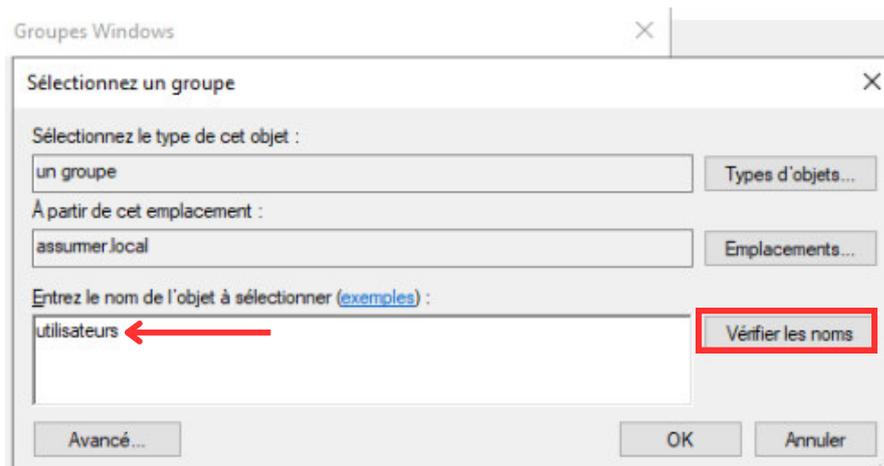
Restrictions relatives aux jours et aux heures
Les restrictions relatives aux jours et aux heures indiquent les jours et les heures auxquels les tentatives de connexion sont autorisées ou non. Ces restrictions sont basées sur le fuseau horaire du serveur NPS (Network Policy Server).

Ajouter... Annuler

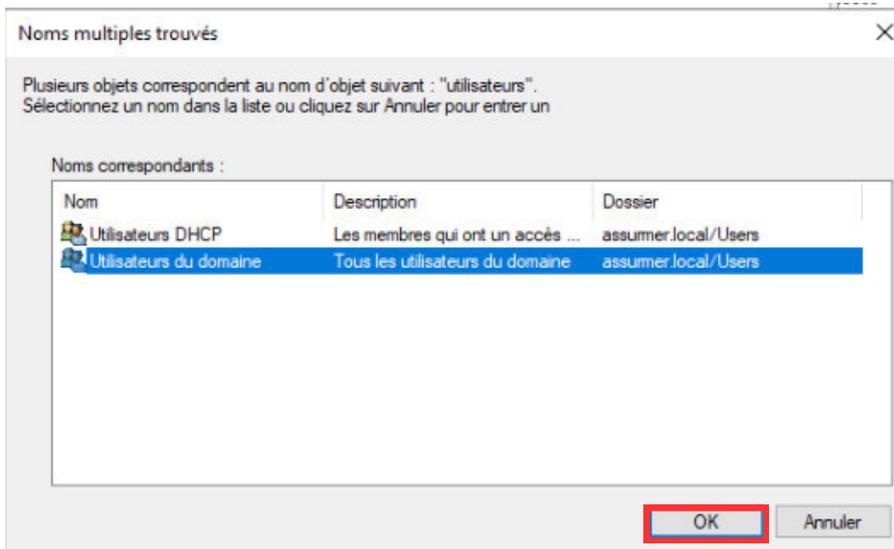
- Cliquer sur "Ajouter des groupes".



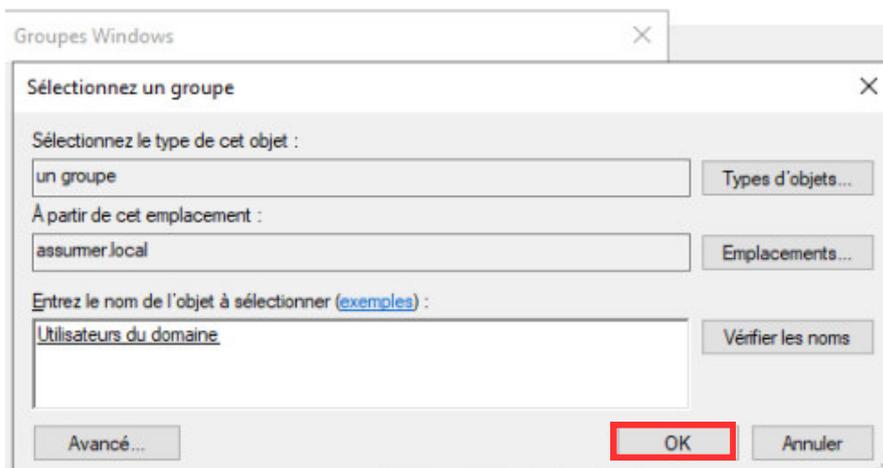
- Taper "utilisateurs" dans le champ de texte puis cliquer sur "Vérifier les noms".



- Sélectionner "Utilisateurs du domaine" et cliquer sur "OK".
- Ce choix va permettre d'ajouter les utilisateurs présent sur l'ensemble du domaine.

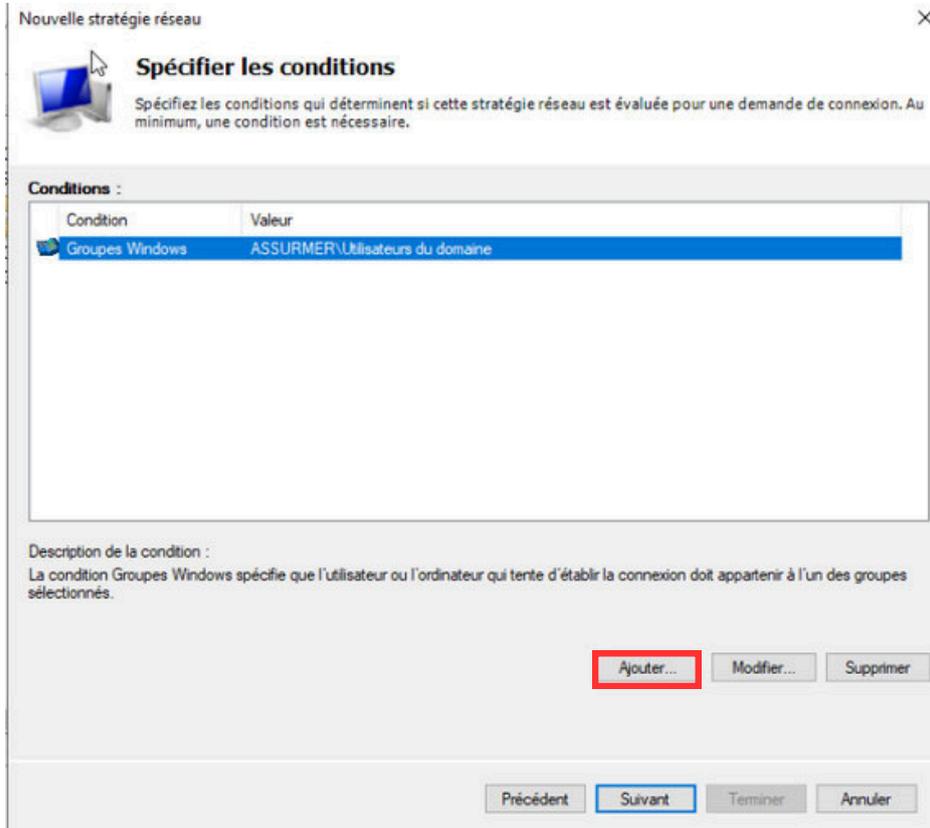


- Cliquer sur "OK".

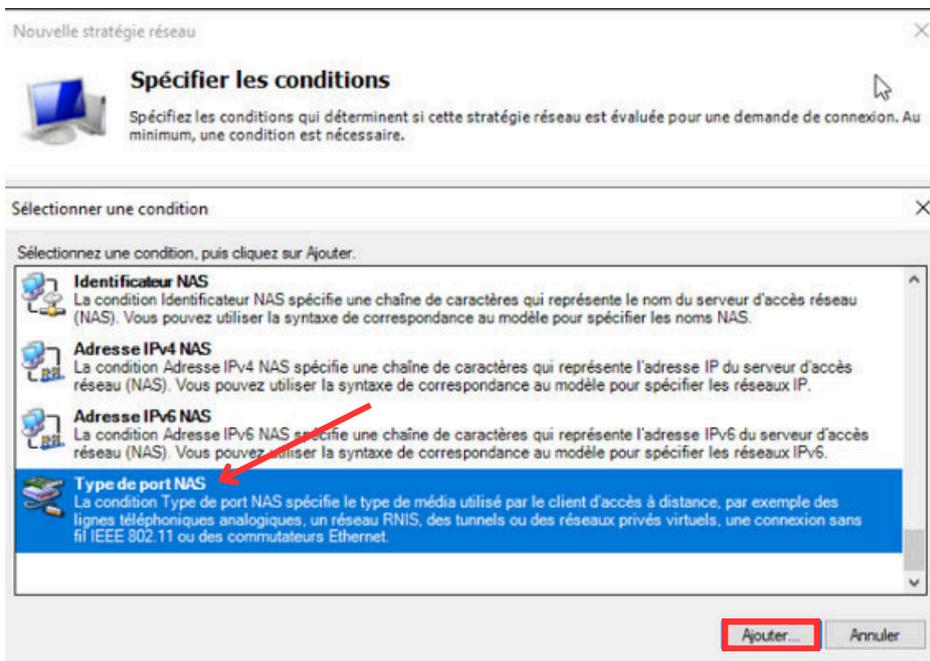


5. Paramétrage des conditions de la stratégie

- Il faut spécifier les conditions pour la connexion des utilisateurs. Pour cela, sélectionner le groupe et cliquer sur "Ajouter".



- Descendre en bas de la liste déroulante et sélectionner "Type de port NAS" et cliquer sur "Ajouter". Ce choix de sélection spécifie le borne Wifi.



- Ensuite, sélectionner "Sans fil - IEEE 802.11" dans les Types de tunnel pour connexions d'accès à distance et VPN standard et "Sans fil - Autre" dans "Autres" et cliquer sur "OK".

Type de port NAS

Spécifiez les types de médias d'accès nécessaires pour correspondre à cette stratégie.

Types de tunnels pour connexions d'accès à distance et VPN standard

- Asynchrone (Modem)
- RNIS synchrone
- Synchrone (ligne T1)
- Virtuel (VPN)

Types de tunnels pour connexions 802.1X standard

- Ethernet
- FDDI
- Sans fil - IEEE 802.11
- Token Ring

Autres

- RNIS asynchrone V.120
- RNIS synchrone
- Sans fil - Autre
- SDSL - DSL symétrique

OK Annuler

- Cliquer ensuite sur "Ajouter".

Nouvelle stratégie réseau

Spécifier les conditions

Spécifiez les conditions qui déterminent si cette stratégie réseau est évaluée pour une demande de connexion. Au minimum, une condition est nécessaire.

Conditions :

Condition	Valeur
Groupes Windows	ASSURMER\Utilisateurs du domaine
Type de port NAS	Sans fil - IEEE 802.11 OU Sans fil - Autre

Description de la condition :
La condition Type de port NAS spécifie le type de média utilisé par le client d'accès à distance, par exemple des lignes téléphoniques analogiques, un réseau RNIS, des tunnels ou des réseaux privés virtuels, une connexion sans fil IEEE 802.11 ou des commutateurs Ethernet.

Ajouter... Modifier... Supprimer

Précédent **Suivant** Terminer Annuler

6. Spécification de l'autorisation d'accès

- Laisser coché "Accès accordé" et cliquer sur "Suivant".

Nouvelle stratégie réseau

Spécifier l'autorisation d'accès

Effectuez la configuration nécessaire pour accorder ou refuser l'accès réseau si la demande de connexion correspond à cette stratégie.

Accès accordé ←
Accordez l'accès si les tentatives de connexion des clients répondent aux conditions de cette stratégie.

Accès refusé
Refusez l'accès si les tentatives de connexion des clients répondent aux conditions de cette stratégie.

L'accès est déterminé par les propriétés de numérotation des utilisateurs (qui remplacent la stratégie NPS)
Choisissez selon les propriétés de numérotation utilisateur si les tentatives de connexion des clients répondent aux conditions de la stratégie.

Précédent **Suivant** Terminer Annuler

- Ensuite, nous allons configurer les méthodes d'authentification désirées, cliquer sur "Ajouter".

Nouvelle stratégie réseau

Configurer les méthodes d'authentification

Configurez une ou plusieurs des méthodes d'authentification nécessaires pour que la demande de connexion corresponde à cette stratégie. Pour l'authentification EAP, vous devez configurer un type EAP.

Les types de protocoles EAP sont négociés entre le serveur NPS et le client dans l'ordre dans lequel ils sont listés.

Types de protocoles EAP :

Monter
Descendre

Ajouter... Modifier... Supprimer

Méthodes d'authentification moins sécurisées :

Authentification chiffrée Microsoft version 2 (MS-CHAP v2)
 L'utilisateur peut modifier le mot de passe après son expiration

Authentification chiffrée Microsoft (MS-CHAP)
 L'utilisateur peut modifier le mot de passe après son expiration

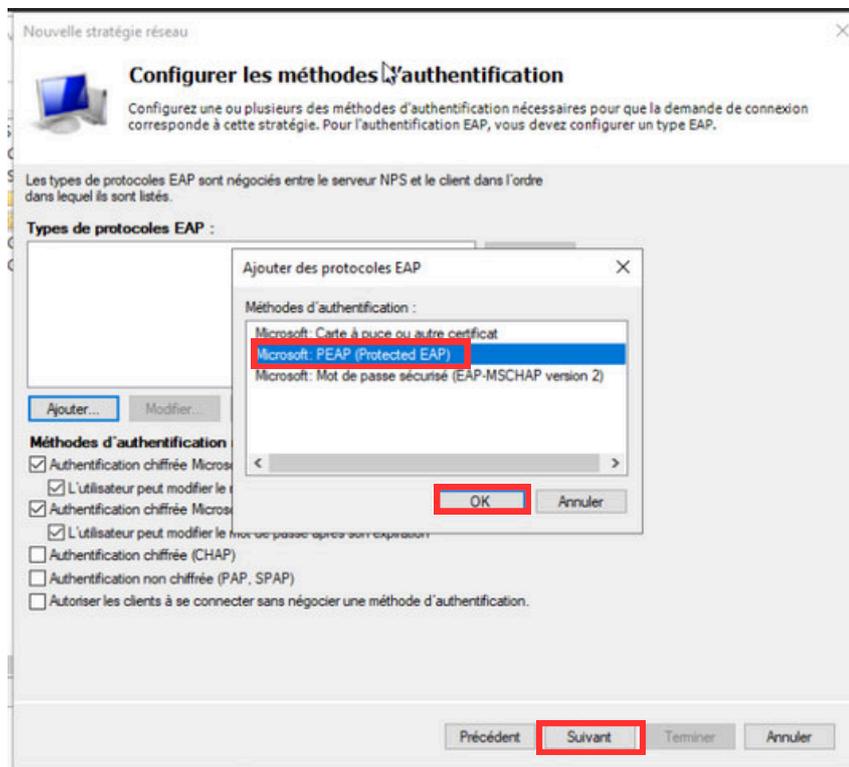
Authentification chiffrée (CHAP)

Authentification non chiffrée (PAP, SPAP)

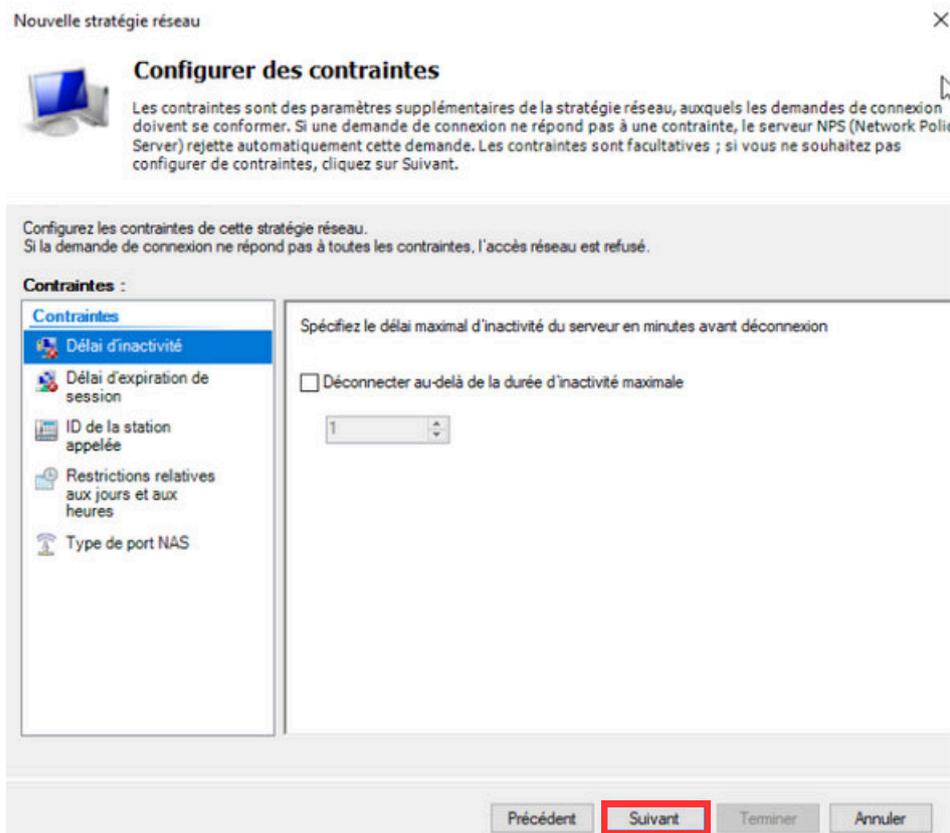
Autoriser les clients à se connecter sans négocier une méthode d'authentification.

7. Choix du protocole de sécurité EAP

- Sélectionner Microsoft PEAP et cliquer sur "OK", puis sur "Suivant".

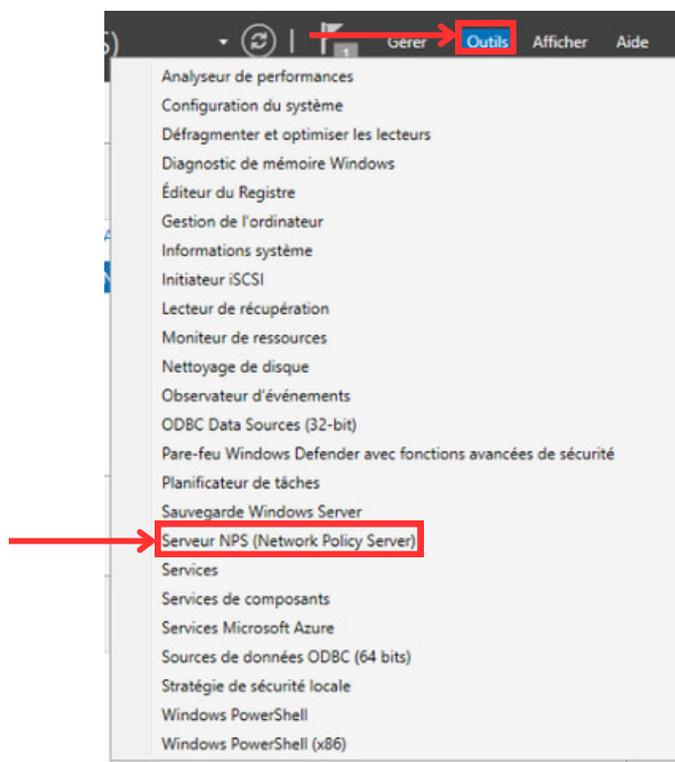


- Laisser par défaut et cliquer sur "Suivant" et faire de même sur la fenêtre suivante, et enfin, cliquer sur "Terminer".

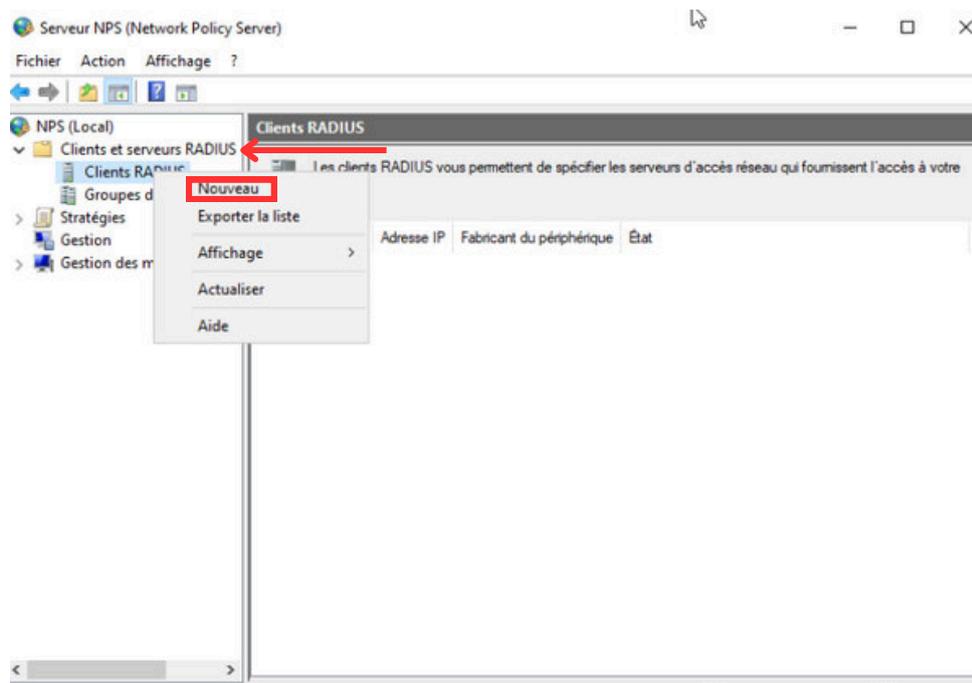


8. Ajout de la borne Wi-Fi

- La borne doit être paramétrée sur le serveur RADIUS pour que l'authentification fonctionne. Pour cela, elle prendra le rôle d'un NAS et sera l'intermédiaire entre le serveur RADIUS et l'utilisateur.
- Retourner dans le gestionnaire de serveur puis cliquer sur "Outils" et sur "Serveur NPS" encore une fois



- Dérouler “Clients et serveurs RADIUS” puis faire un clic droit sur “Client RADIUS” et cliquer sur “Nouveau”.



9. Configuration des informations de la borne Wi-Fi et du client RADIUS

- Enfin, renseigner les informations de la borne Wi-Fi.
- Laisser coché "Activer ce client RADIUS".
- Le "nom convivial" est un identifiant descriptif dans le serveur RADIUS pour faciliter la gestion et l'administration.
- L'adresse IP est celle préalablement paramétrée sur la borne Wi-Fi.
- Le secret partagé est un mot de passe ou une clé utilisée pour sécuriser les communications entre le serveur RADIUS (NPS) et un client RADIUS.

Nouveau client RADIUS

Paramètres Avancé

Activer ce client RADIUS

Sélectionner un modèle existant :

Nom et adresse

Nom convivial : ←
assumer_AB

Adresse (IP ou DNS) : ←
172.16.0.10 Vérifier...

Secret partagé

Sélectionnez un modèle de secrets partagés existant :
Aucun

Pour taper manuellement un secret partagé, cliquez sur Manuel. Pour générer automatiquement un secret partagé, cliquez sur Générer. Vous devez configurer le client RADIUS avec le même secret partagé entré ici. Les secrets partagés respectent la casse.

Manuel Générer

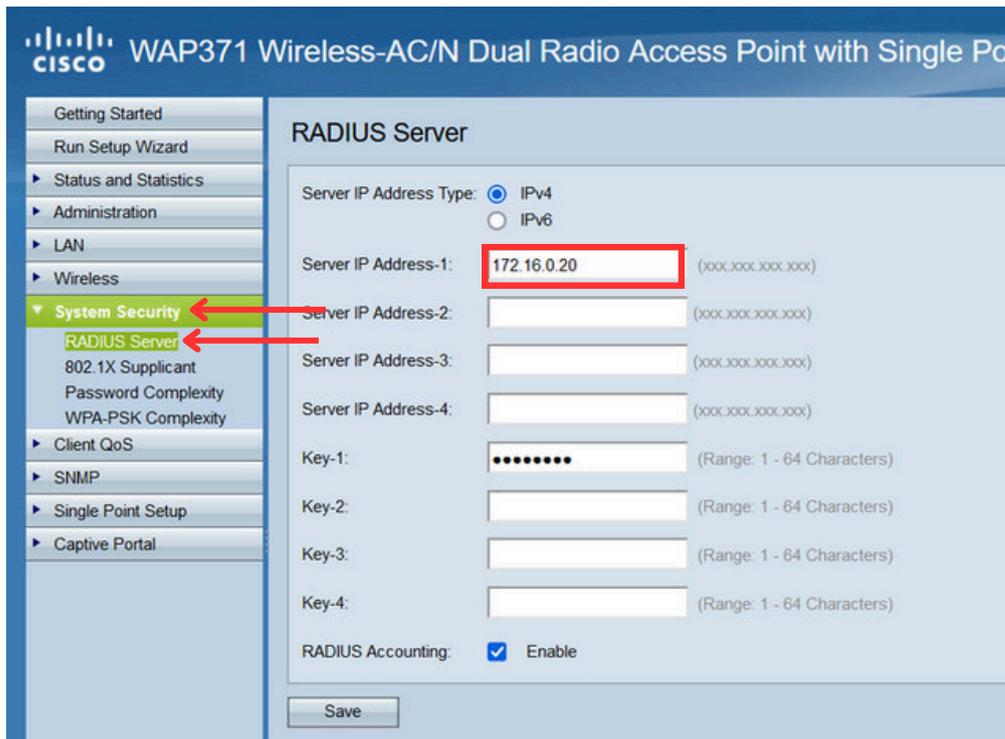
Secret partagé : ←
.....

Confirmez le secret partagé :
.....

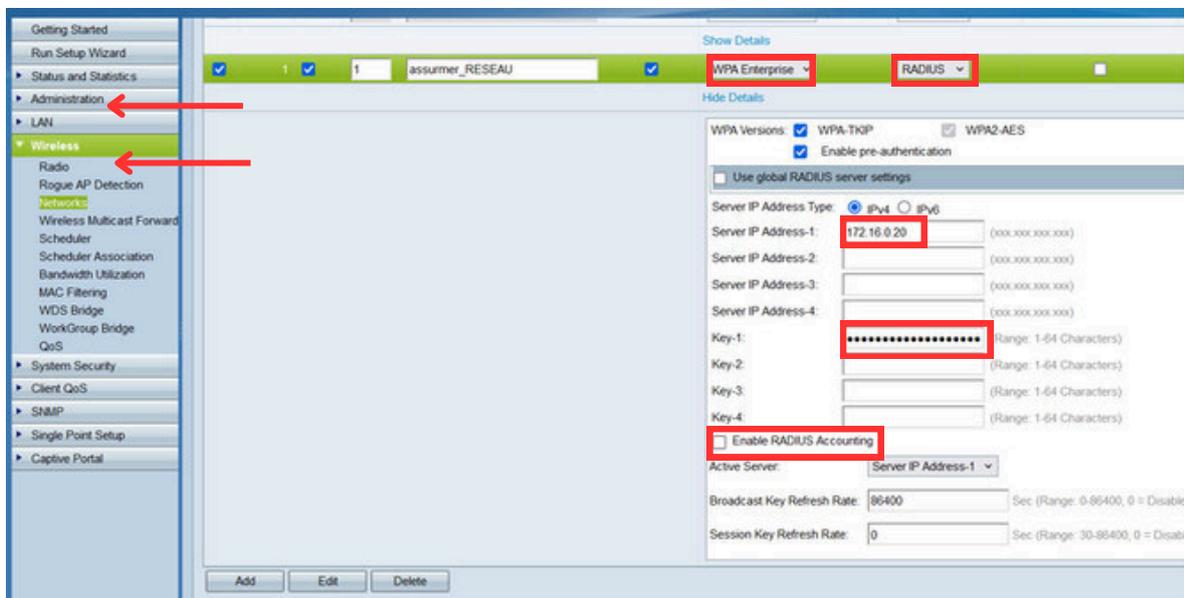
OK Annuler

10. Paramétrage du Radius sur la borne Wi-Fi

- Se rendre sur l'interface web de la borne Wi-Fi et aller dans System Security puis RADIUS Server. Dans le champ des adresses IP, renseigner l'IP du serveur Radius.

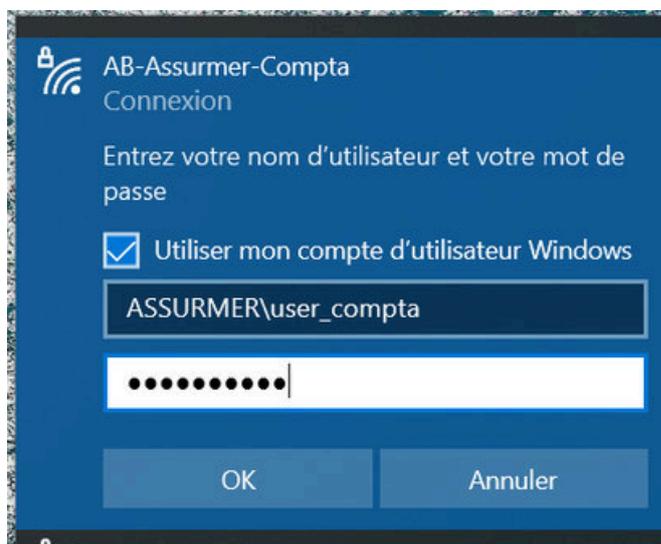


- Cliquer sur "Wireless" puis sur "Networks" pour paramétrer le SSID lié au RADIUS. Sélectionner sur le SSID "WPA Entreprise" et "RADIUS", ensuite cliquer sur "Show Details" pour ensuite rentrer l'IP du serveur Radius et sa clé paramétrée précédemment, décocher "Enable RADIUS Accounting".



11. Test d'une connexion sur le Wi-Fi

- Pour se connecter au Wi-fi précédemment paramétré en lien avec le serveur RADIUS, il suffit de cliquer sur l'icône d'Accès internet sur la barre des tâches de Windows et choisir le SSID correspondant au Radius.
- Ensuite nous pouvons rentrer les identifiants d'utilisateur pour se connecter.



- La mise en place du serveur RADIUS et la configuration du Wi-Fi sont désormais terminées, offrant ainsi une connexion sécurisée et une gestion efficace des utilisateurs.