ASSURMER

Dylan CHAU
Axel BAUGÉ

2A-SISR

Présentation RADIUS et procédure d'installation et configuration

Date de création : 26/09/2023
Version : 1.0
Pour validation : DSI
A destination : DSI
Mode de diffusion : Intranet
Nombre de pages : 33
Auteur : CHAU Dylan

Métadonnées

Diffusion			
Périmètre de diffusion	Contrôlé	Interne	Libre

Historique des évolutions		
Auteur	Version	Objet de la version et liste des modifications
Dylan Chau et Axel Baugé	1.0	Initialisation du document

Validation			
Rédacteur		Validateur	
Nom	Date	Nom	Date
Dylan Chau et Axel Baugé	22/11/2023	DSI	20/12/2023
Date d'application : 13/01/2024			

Table des matières

Prérequis

- Avoir réalisé la procédure « Procédure d'installation et de configuration du Cisco WAP371 ».

Présentation

1) Qu'est-ce que RADIUS ?

Développé 1991 pour devenir la norme de l'IETF, le protocole RADIUS (Remote Authentication Dial-In User Service) est un protocole réseau qui autorise et authentifie les utilisateurs qui accèdent à un réseau distant.

Le protocole fournit une gestion centralisée de l'authentification, de l'autorisation et de la comptabilité (protocole AAA) pour les utilisateurs se connectant à un réseau, empêchant les utilisateurs non autorisés d'accéder au réseau.

Il fonctionne sur un modèle client-serveur, où le serveur RADIUS gère les informations d'authentification, les autorisations et la comptabilisation, tandis que les clients RADIUS ou serveurs d'accès réseau (NAS) fournissent l'accès au réseau et envoient une demande au serveur RADIUS. Son fonctionnement se rapproche du protocole LDAP (Lightweight Directory Access Protocol). Le protocole fonctionne sur les ports 1812 et 1813.

2) Fonctionnement

- Le processus commence lorsque l'utilisateur tente de se connecter au réseau via un client RADIUS/NAS. (La borne Wi-Fi ici)
- Ensuite, le client RADIUS/NAS envoie une requête d'accès au serveur RADIUS, incluant les identifiants de l'utilisateur qu'il vient de récupérer.
- Le serveur vérifie les identifiants à partir de sa base de données.
- En fonction de la vérification, le serveur envoie un message d'acceptation, de rejet, ou de contestation au client RADIUS/NAS.
- Le client RADIUS/NAS applique les attributs d'autorisation fournis par le serveur à la session de l'utilisateur. Des informations de comptabilité sont envoyées au serveur RADIUS pendant la session de l'utilisateur.

Bien que RADIUS soit largement utilisé, il présente des préoccupations de sécurité.

Il est possible d'atténuer ces préoccupations en implémentant des mesures de sécurité supplémentaires et en envisageant des protocoles AAA alternatifs (TACACS+) pour les environnements nécessitant une sécurité plus avancée. TACACS+ est l'abréviation de Terminal Access Controller Access-Control System Plus. L'avantage de ce protocole est que toutes les informations d'authentification, d'autorisation et de comptabilité sont chiffrées.

3) Recommandation de l'ANSSI

L'ANSSI indique qu'il est important de s'assurer que toute information sensible ou secrète échangée durant l'authentification (mot de passe, clé de session...) ne puisse pas être récupérée par un attaquant, au moyen d'une écoute passive ou d'une attaque active (attaque de l'homme du milieu par exemple).

Les méthodes d'authentification EAP-TLS, EAP-TTLS et EAP-PEAP dans ses dernières versions peuvent respecter les recommandations. En revanche, les méthodes d'authentification non encapsulées telles que EAP-MSCHAPv2 et EAP-MD5 ne respectent pas cette recommandation

Recommandations :

- Utilisation d'une couche cryptographique standard ;
- Authentification mutuelle entre le supplicant et le serveur;
- Masquage de l'identité du supplicant durant la phase d'authentification, si le contexte le justifie.
- Utiliser une version de TLS récente et une suite cryptographique robuste.

Plusieurs modifications sont nécessaires pour garantir la disponibilité, l'intégrité et la confidentialité du SI. (Affectation de VLAN, ACL, cloisonnement des flux, supervision, blocage des adresses MAC inconnues)
En cas de perte ou de vol, modifier le mot de passe de l'utilisateur compromis est une solution pour se protéger.

4) Protocole d'authentification

Avec le protocole RADIUS est associé avec le protocole Extended Authentication Protocol qui sert pour le transport des données nécessaire à l'authentification. Le déploiement de l'IEEE 802.1X fournit une couche de sécurité pour l'utilisation des réseaux câblés et sans fil.

Ce protocole est extensible, car on peut définir de nouvelles méthodes d'authentifications, il est indépendant de la méthode utilisée :

- EAP-MD5 : Authentification avec un mot de passe
- EAP-TLS : Authentification avec un certificat électronique
- EAP-TTLS : Authentification avec n'importe quelle méthode d'authentification, au sein d'un tunnel TLS
- EAP-PEAP : Authentification avec n'importe quelle méthode d'authentification EAP, au sein d'un tunnel TLS
- EAP-TLS (Transport Layer Security) : Comme d'autres protocoles (SMTP-TLS, IMAP-TLS, HTTPS, etc.), EAP s'appuie sur TLS pour proposer une authentification sécurisée. Cette méthode s'appuie sur les certificats électroniques. Ainsi, chaque partie (serveur et client) doit posséder un certificat pour prouver son identité.
- MS-CHAP (Microsoft Challenge Handshake Authentication Protocol) : Authentification Microsoft avec Hash du mot de passe. MS-CHAP v2 ajoute une authentification mutuelle client/serveur permettant de vérifier leur identité respective.

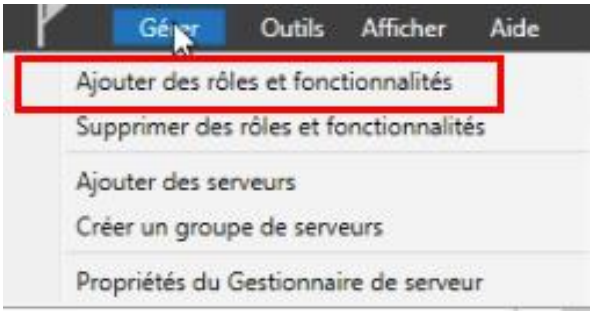
Nous avons donc décidé pour ASSURMER de mettre en place une connexion au Wi-Fi avec une authentification PEAP utilisant les identifiants AD avec un certificat émis par l'autorité de certification d'ASSURMER qui permettra de vérifier l'identité du serveur NPS.

Procédure

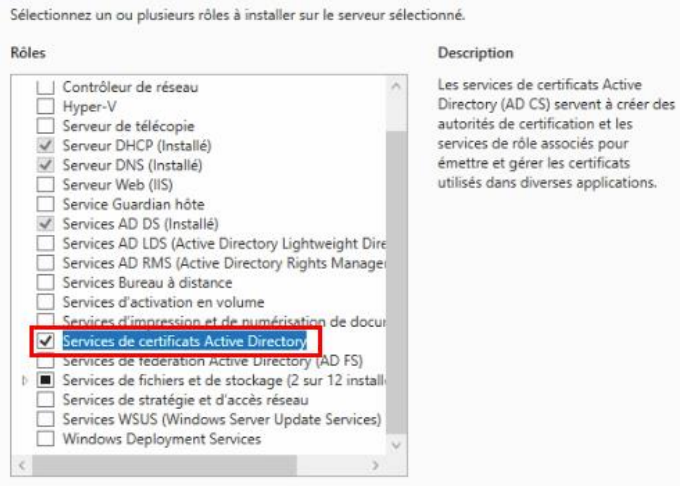
1) Installation de l'autorité de certification

ADCS va permettre de générer un certificat qui permettra aux clients de vérifier l'identité du serveur NPS. En cas de mise en place de l'EAP-TLS, il permettra de déployer un certificat sur les clients sans fil également.

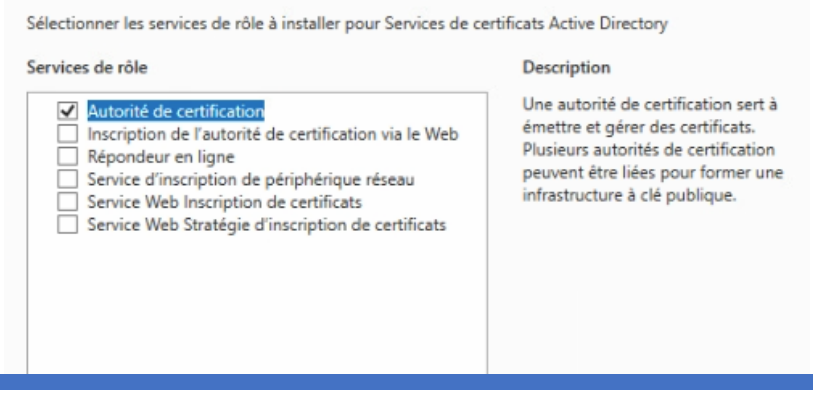
- Sur le DC01, cliquer sur « Gérer » puis « Ajouter des rôles et fonctionnalités ».



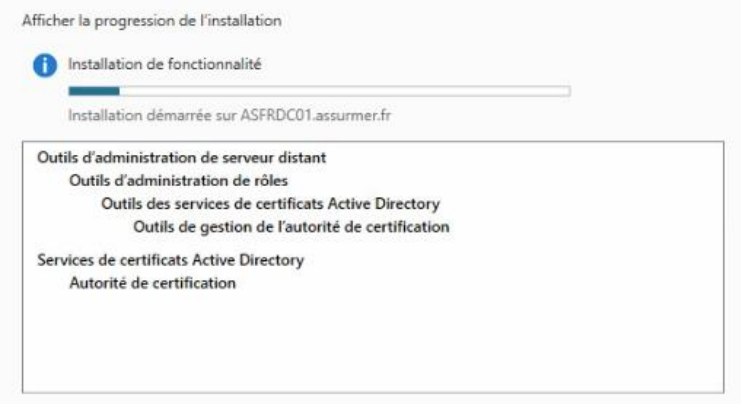
- Sélectionner « Services de certificats Active Directory ».



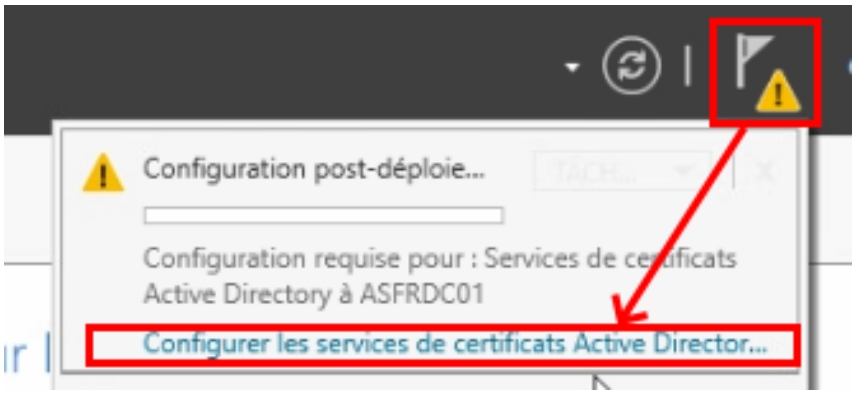
- Dans les « Services de rôles », cocher uniquement « Autorité de certification ».



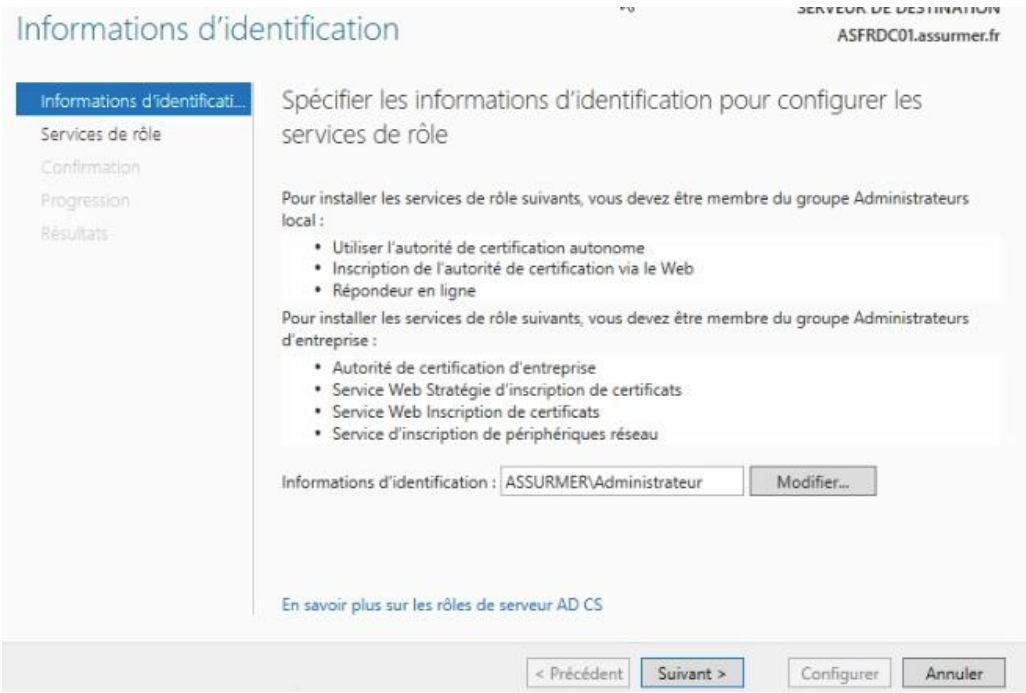
- Lancer l'installation.



- Lancer la configuration post-déploiement en cliquant sur le drapeau.



- Dans « Informations d'identification », laisser par défaut.



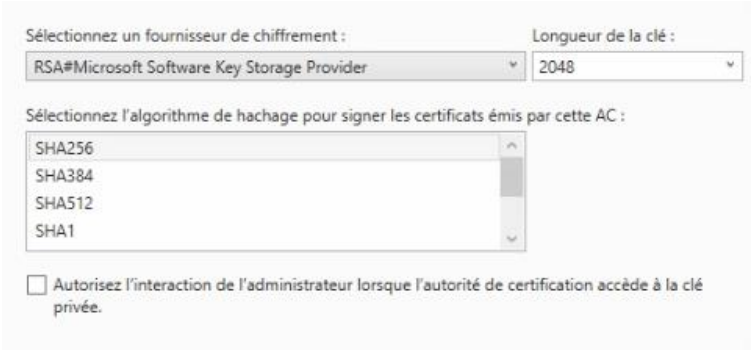
- Pour le « service de rôle », laisser par défaut.

- Sélectionner « Autorité de certification de l'entreprise » dans le type d'installation de l'AC.

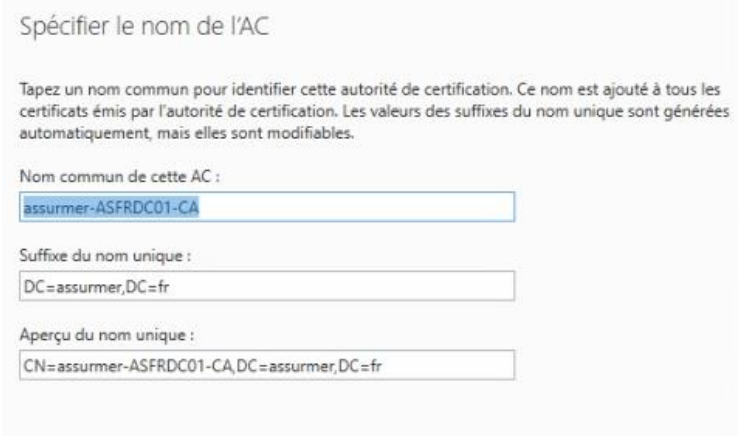
- Sélectionner « Autorité de certification racine » dans le type de l'AC.

- Choisir « Créer un clé privée ».

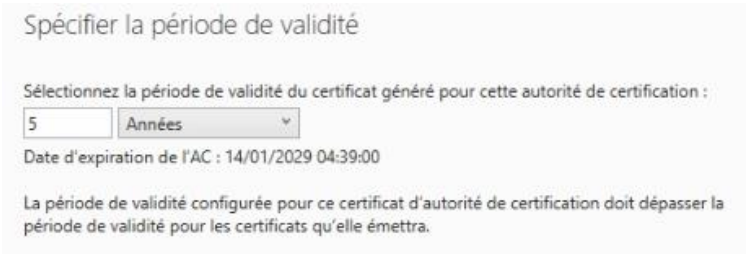
- Pour le chiffrement, laisser les paramètres par défaut.



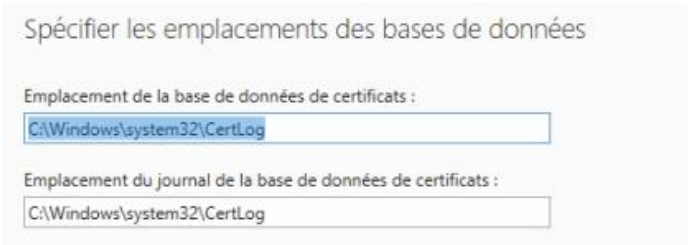
- Pour le nom de l'AC, laisser les paramètres par défaut.



- Pour la période de validité, laisser les paramètres par défaut.



- Pour l'emplacement de la base de données, laisser les paramètres par défaut.

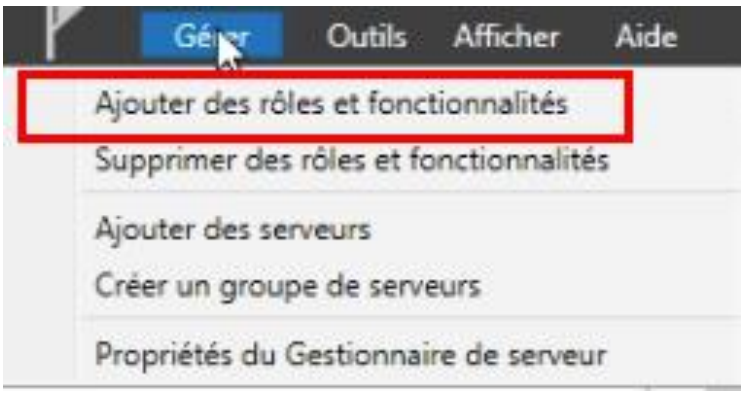


- Finaliser la configuration. L'ADCS est prêt.

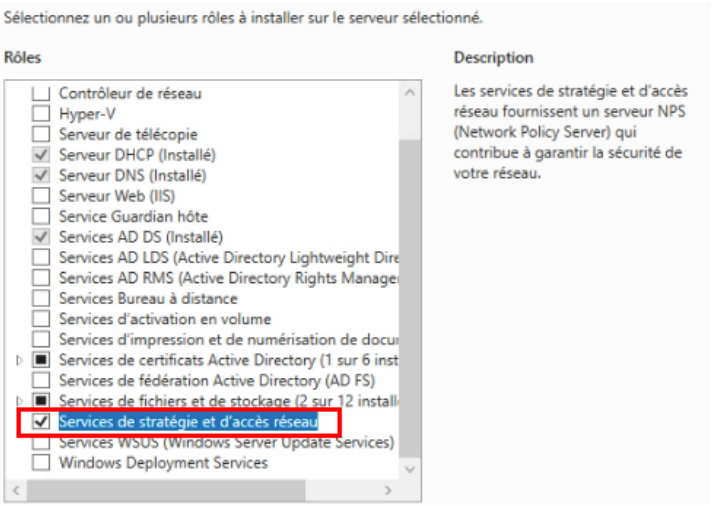
2) Installation du serveur NPS

Le serveur NPS (RADIUS Windows) servira de contrôleur LAN sans fil et permettra de mettre en place le protocole PEAP avec MS-CHAPv2 et EAP-TLS pour l'authentification.

- Sur le DC01, cliquer sur « Gérer » puis « Ajouter des rôles et fonctionnalités ».



- Sélectionner « Services de stratégie et d'accès réseau ».

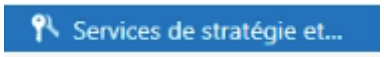


- Terminer l'installation du service.

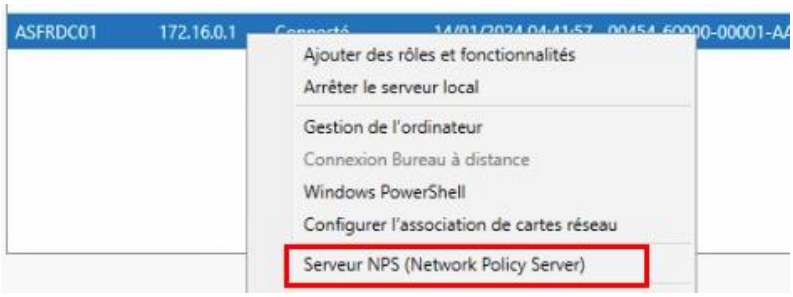
3) Configuration du serveur NPS

Nous allons maintenant configurer la console NPS pour ajouter le client RADIUS et la stratégie de connexion sans fil.

- Cliquer sur « Services de stratégie et d'accès réseau ».



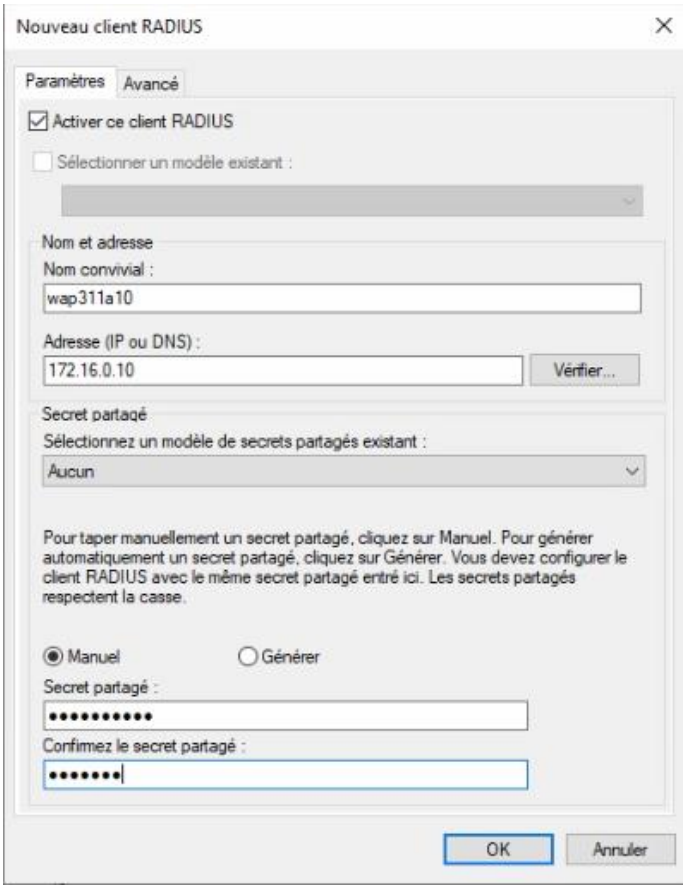
- Sur le serveur, faire clic droit puis cliquer sur « Serveur NPS (Network Policy Server) ».



- Faire clic droit sur « NPS (Local) puis cliquer sur « Inscrire un serveur dans Active Directory » afin de récupérer les informations de l'Active Directory.

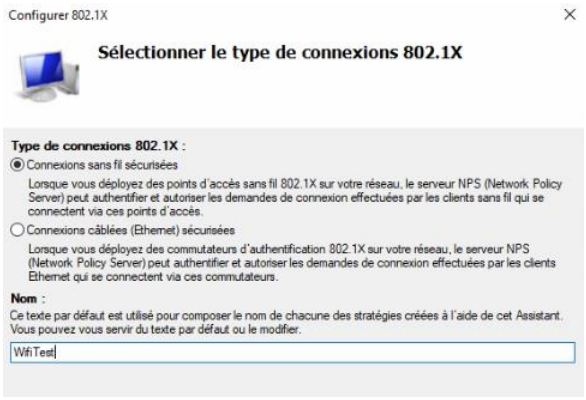
- Sur « Client RADIUS », faire clic droit puis « Nouveau ».

- Ajouter les informations de la borne Wifi et la clé précédemment définie dans « Secret partagé ».



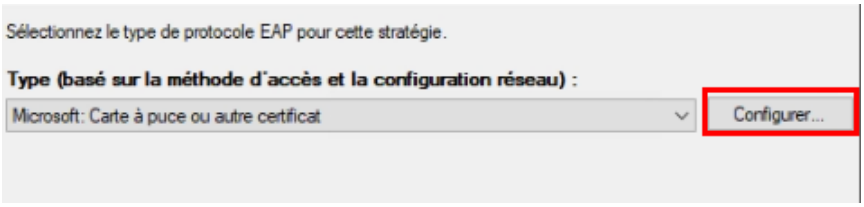
- Sur « NPS (Local) », dans l'onglet « Configuration standard », choisir le scénario « Serveur RADIUS pour les connexions... » puis cliquer sur « Configurer 802.1X ».

- Pour le « Type de connexions », cocher « Connexions sans fil sécurisées ». Donner un nom.

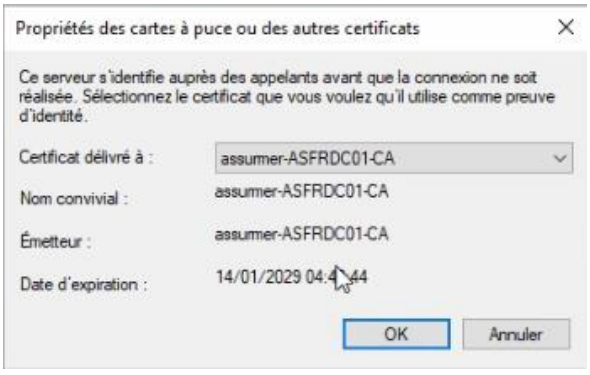


- Ajouter le client RADIUS.

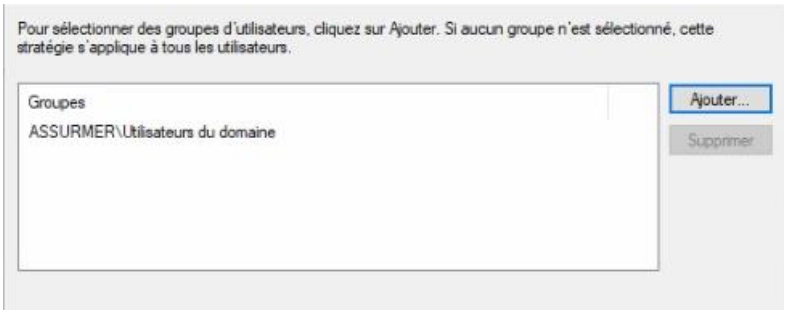
- Pour le protocole EAP, laisser « Carte à puce ou autre certificat ». Cliquer sur configurer.



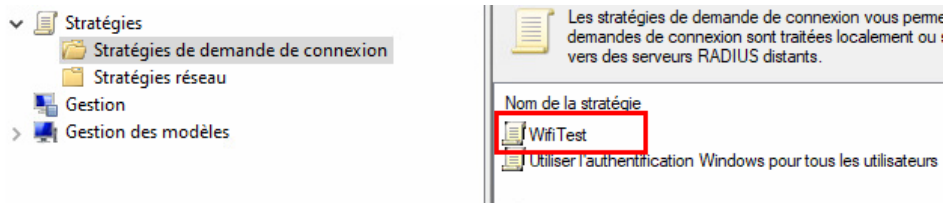
- Choisir l'ADCS pour le certificat.



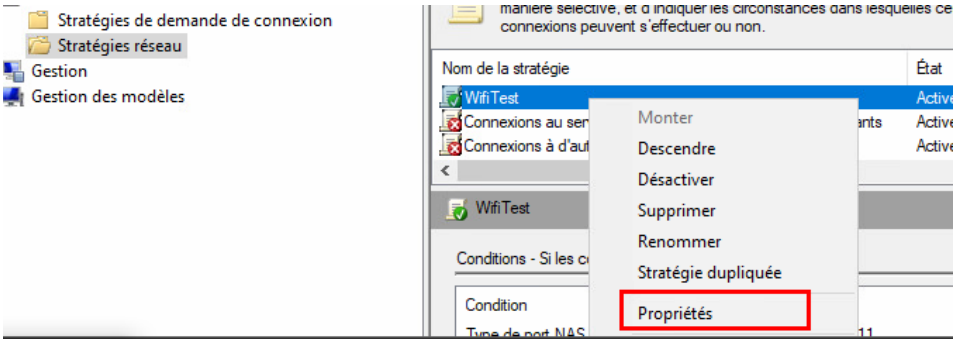
- Pour les groupes d'utilisateurs, ajouter les utilisateurs du domaine.



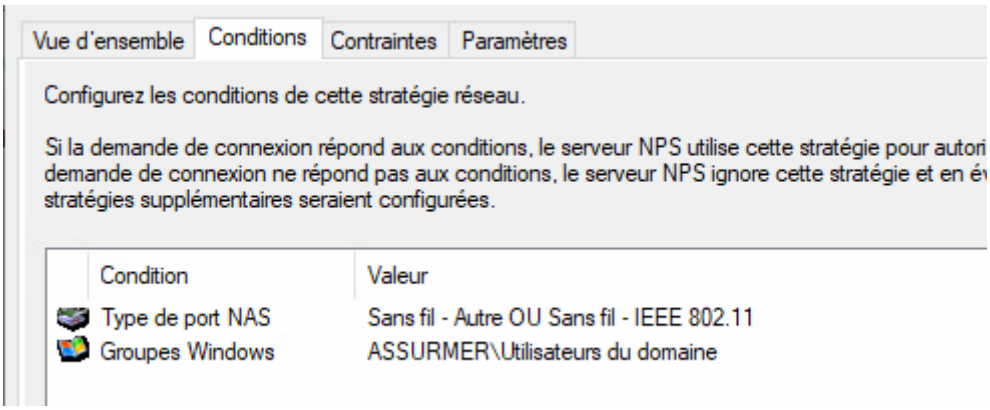
- Cliquer sur « Terminer ».
- La stratégie apparaît alors dans « Stratégies de demande de connexion » et « Stratégies réseau ».



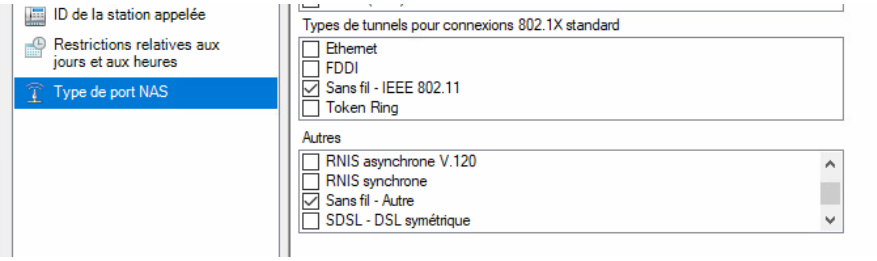
- Cliquer sur « Stratégies réseau ». Puis ouvrir les propriétés de « WifiTest ».



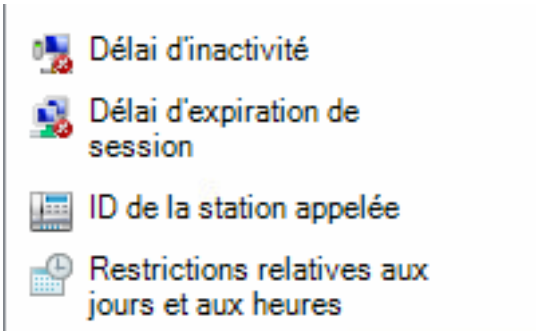
- Dans « Vue d'ensemble », laisser les paramètres par défaut.
- Dans « Conditions », on peut voir que seuls les utilisateurs du domaine et les appareils sans fil sont concernées.



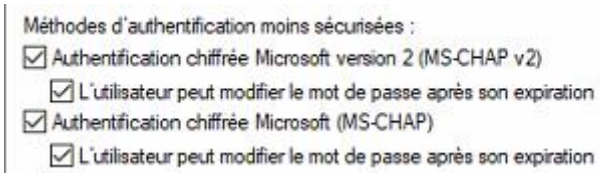
- Dans « Contraintes », sur « Type de port NAS », cocher « Sans fil – Autre » et « Sans fil – IEEE 802.11 »



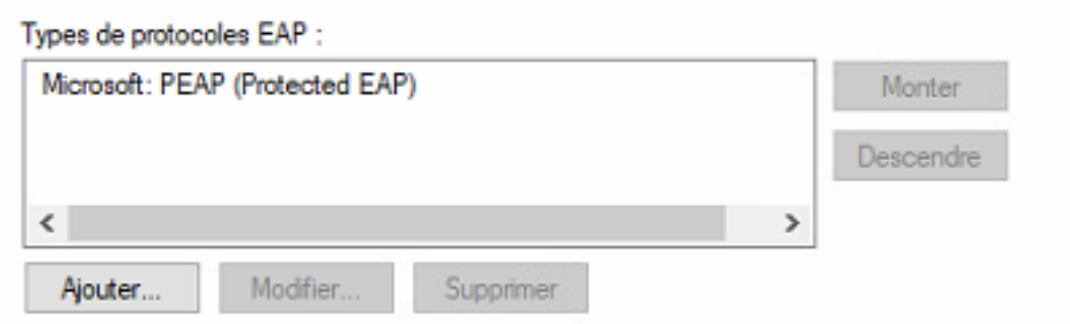
- Il est possible de mettre des restrictions relatives aux jours et aux heures, des délais d'inactivité et d'expiration.



- Dans « Méthodes d'authentification », activer le MS-CHAP v2 et le MS-CHAP. Ces options permettent la connexion avec le compte AD.



- Supprimer « Microsoft : Carte à puce ou autre certificat » et mettre « Microsoft PEAP » à la place. Puis « Modifier ».



- Choisir le certificat de l’ADCS.