Mise en place en environnement Windows d'une Authentification Radius

Prérequis

Les services **Active Directory Domain Service** (AD DS), **Dynamic Host Configuration Protocol** (DHCP), **Domain Name Service** (DNS) et **contrôleur de domaine** sont déjà configurés.

Fonction

Le protocole **RADIUS** (Remote Authentication Dial-In User Service) est un protocole d'authentification standard.Le fonctionnement de RADIUS est basé sur un système client/serveur chargé de définir les accès d'utilisateurs distants à un réseau. Il repose principalement sur un serveur (le **serveur RADIUS**), relié à une **base d'identification** (base de données, annuaire LDAP, etc.) et un **client RADIUS, appelé NAS** (Network Access Server), faisant office d'intermédiaire entre l'utilisateur final et le serveur. L'ensemble des transactions entre le client RADIUS et le serveur RADIUS est chiffrée et authentifiée grâce à un secret partagé.

EAP (Extensible Authentication Protocol) est un protocole conçu pour étendre les fonctions du protocole Radius à des types d'identification plus complexes; il est indépendant du matériel du client Radius et négocié directement avec le supplicant (poste client, terminal d'accès). C'est ce qui a permis de le mettre en place rapidement sur un maximum d'appareils réseau puisqu'il n'utilise que deux attributs Radius servant de protocole de transport, et a conduit à une explosion de types **EAP** : **EAP-MD5** défini dans le RFC comme exemple, mais aussi **EAP-TLS**, **EAP-TTLS**, **EAP-PEAP**, **EAP-MS-CHAP-V2**, **EAP-AKA**, **EAP-LEAP** et **EAP-FAST** (Cisco), **EAP-SIM**, etc

On va ici utiliser le protocole PEAP (Protected EAP) qui utilise une infrastructure à clés publiques seulement du coté serveur pour protéger l'authentification par un tunnel TLS.

Procédure de configuration de Radius

1. Installation des rôles NPS et AD CS
2. Ajout du groupe autorisé dans l'AD
3. Configuration de la CA :
    - Type d'Autorité de Certification
    - Création de la clé privée
    - Nommer la CA
    - Création du modèle
4. Configuration du serveur Radius :
    - Demande de certificat
    - Inscription du serveur dans l'AD
    - Ajout des clients Radius (Bornes Wi-Fi)
    - Création des stratégies de connexions (ajout du

certificat demandé)
5. Configuration de la borne Wi-Fi :
    - Configuration du type d'authentification (802.1X ou WPA-Enterprise)
    - Ajout de l'IP du serveur Radius
6. Connexion depuis un terminal sur la borne avec un compte dans le groupe Radius de l'AD

Mode opératoire de l'installation de Radius

Installation des rôles NPS (Network Policy Server) et AD CS (Active Directory Certificate Services)

Accéder à l'assistant Ajout de rôles et de fonctionnalités : ***gestionnaire de serveur*** –> ***« Gérer »*** –> ***« Ajouter des rôles et des fonctionnalités »***. Les services bureaux à distance étant destinés seulement à installés une infrastructure virtuelle de bureaux à distance; choisir : ***« Installation basée sur un rôle ou une fonctionnalité »*** :

Choisir le ***serveur local*** pour installer ces rôles :

Sélectionner les rôles intéressants : ***« Services de certificats Active Directory »*** & ***« Services de stratégie et d'accès réseau »***

Aucune fonctionnalités supplémentaires nécessaires –> ***Suivant***

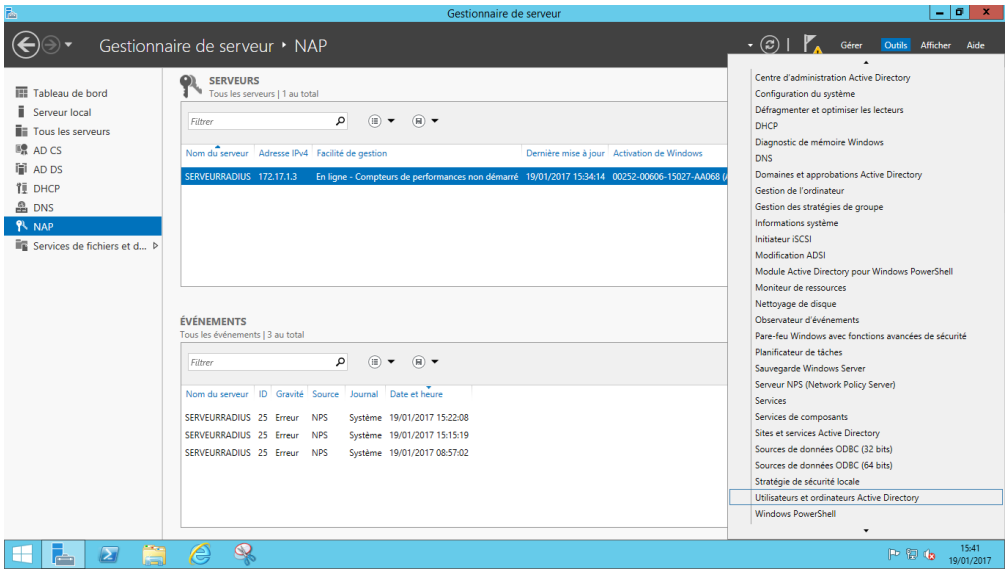
Autorité HRA (Health Registration Authority) servant dans le cadre d'un réseau Intranet fonctionnant avec des VPN. HCAP (Host Credential Authorization Protocol) permettant de faire fonctionner Radius dans un environnement Cisco. Sélectionner ***« Serveur NPS (Network Policy Server) »*** :

Idem rôle AD CS ne choisir que ***« Autorité de certification »*** :

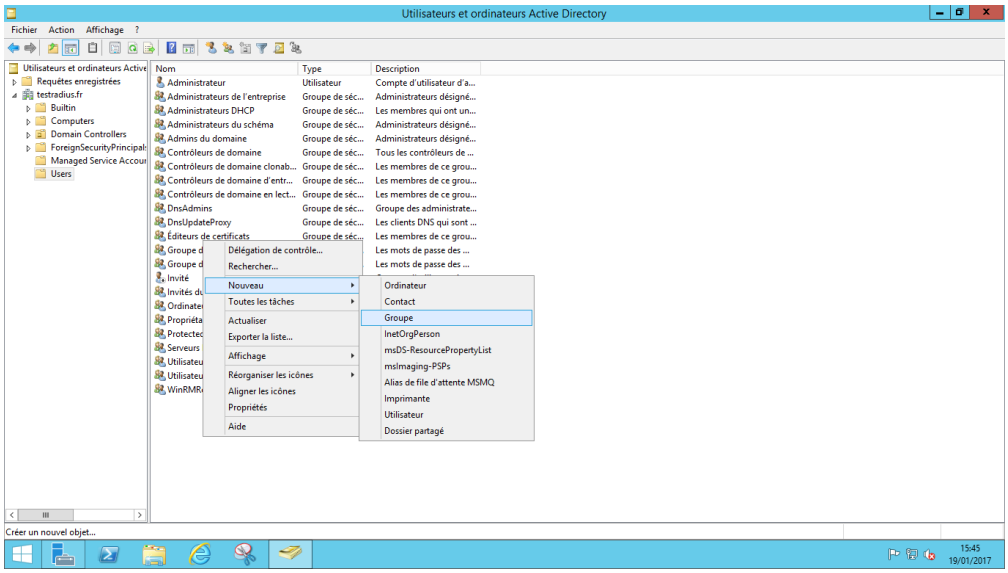
Vérifier données du récapitulatif puis ***installer***.

Configuration de l'AD

On va maintenant préparer l'AD en ajoutant les comptes autorisés à se connecter à notre Wifi RADIUS dans un groupe dédié. ***Gestionnaire de serveur*** –> « ***outils*** » –> « ***utilisateur et ordinateur active directory*** »



Créer un groupe à l'endroit souhaité : ***clic droit –> « nouveau » –> « groupe »***



Ajouter un nom au groupe

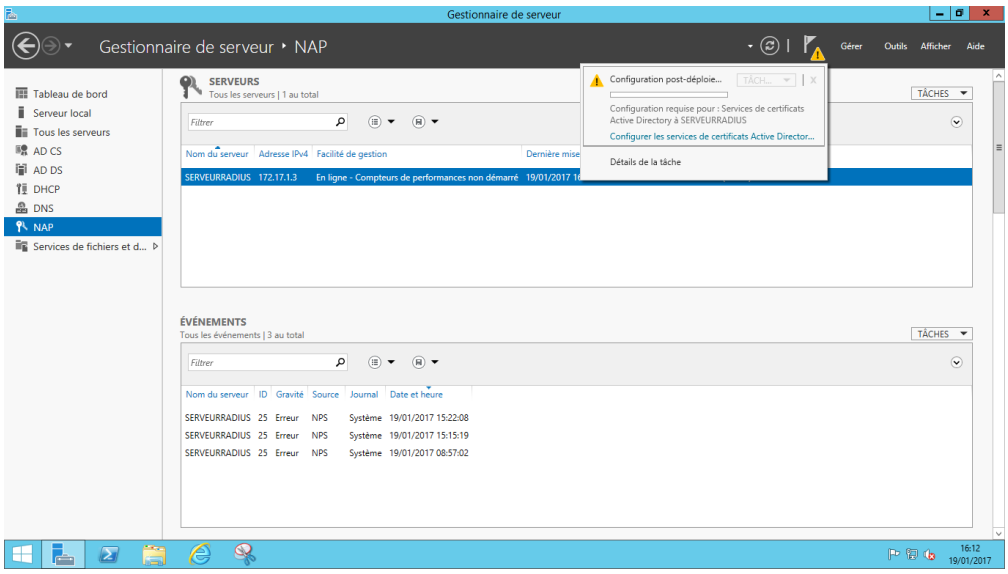
Ajouter utilisateurs au groupe : ***double clic –> "Membres" –> "Ajouter"***

Entrer les noms des utilisateurs concernés –> ***"vérifier les noms"*** –> ***« Ok »*** –> ***« Appliquer »***

Configuration de l'autorité de certification

Configuration des services de certificats Active Directory

Après l'installation du service d'autorité de certification on s'aperçoit dans le gestionnaire de serveur que des configurations supplémentaires sont nécessaires pour finaliser l'installation de ce service. Cliquer sur ***« Configurer les services de certificats Active Directory sur le serveur de destination »***.



Renseigner le compte d'un utilisateur étant membre des groupes Administrateurs local et Administrateurs d'entreprise pour installer les services de rôle nécessaires. Cliquer ***"suivant"***.

Sélectionner autorité de certification.

Choisir ***« Autorité de certification d'entreprise »*** étant celui qui utilise les services de domaine Active Directory et qui facilite donc la gestion des certificats.

Choisir ***« Autorité de certification racine »*** (première autorité de certification). L'autorité de certification secondaire est utile lorsqu'il existe déjà une autorité de certification racine.

Créer une clé privée, qui va permettre au serveur de générer et d'émettre des certificats aux clients.

Cette page permet de sélectionner un fournisseur de chiffrement qui proposera des algorithmes de hachage qui eux servent à signer les certificats afin de garantir qu'ils n'ont pas été falsifiés. Garder les paramètres de bases.

Choisir le nom de l'autorité de certification –> ***« Nom commun de cette AC »***

Configurer la période de validité du certificat authentifiant l'Autorité de Certification.

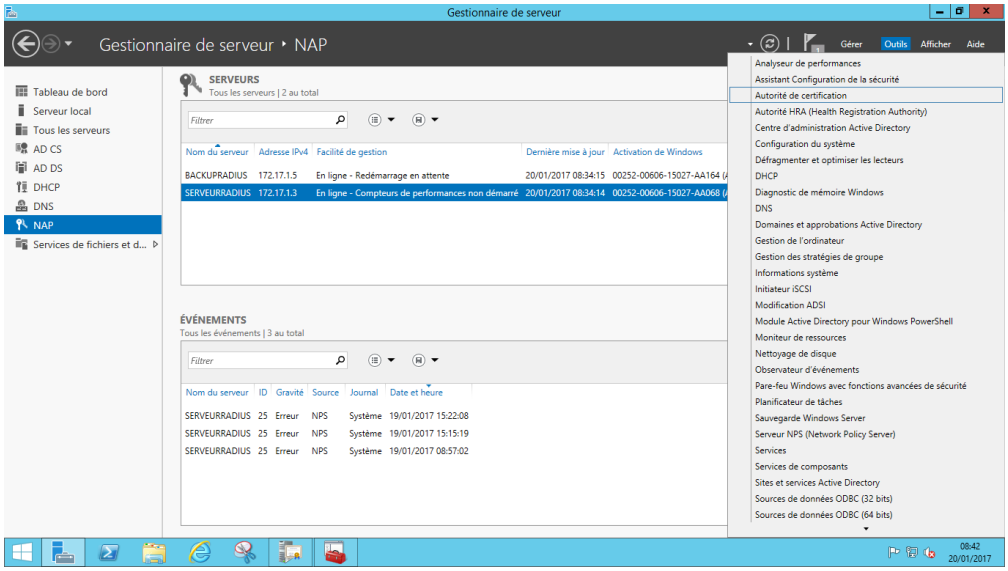
Vérifier le récapitulatif –> cliquer sur « ***Configurer*** ».

Configuration du modèle de certificat authentifiant le serveur Radius

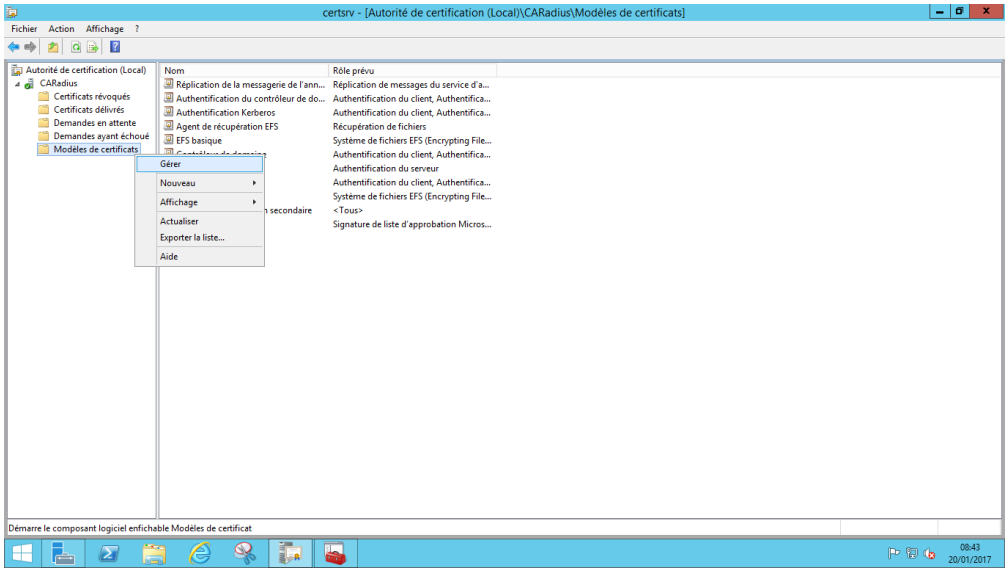
L'autorité de certification (CA) doit délivrer un ***certificat garanti*** au serveur Radius. Lorsque la borne Wifi interrogera le serveur Radius, elle recevra le ***certificat garanti*** du Radius et en vérifiera l'authenticité auprès de l'AC. Le serveur Radius sera ainsi bien authentifié.

Il faut commencer par créer un ***modèle de certificat*** qui permettra ensuite de générer le ***certificat garanti***.

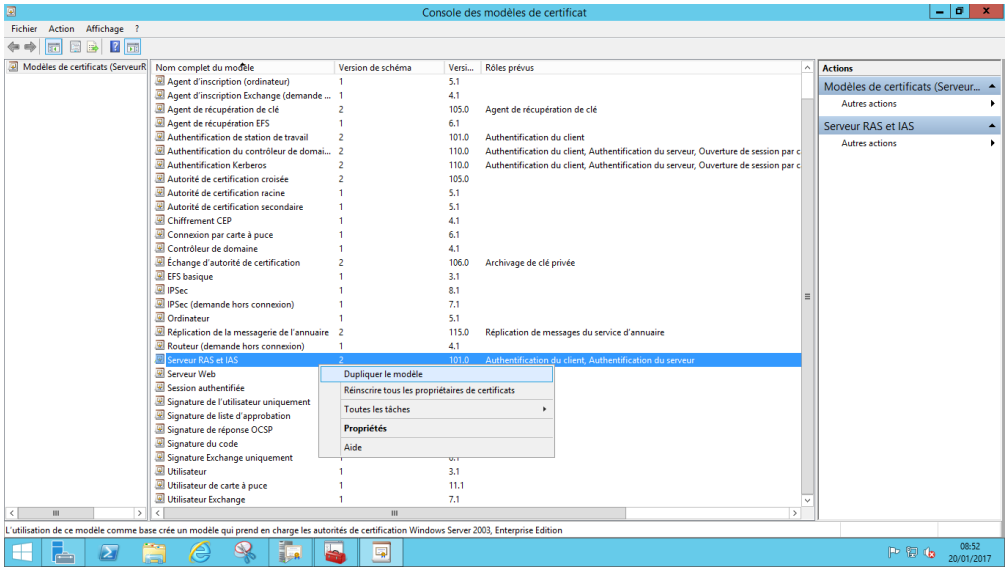
Gestionnaire de serveur –> « outils » –> « Autorité de certification ».



Développer l'autorité de certification –> clic droit sur « Modèles de certificats » –> « Gérer ».



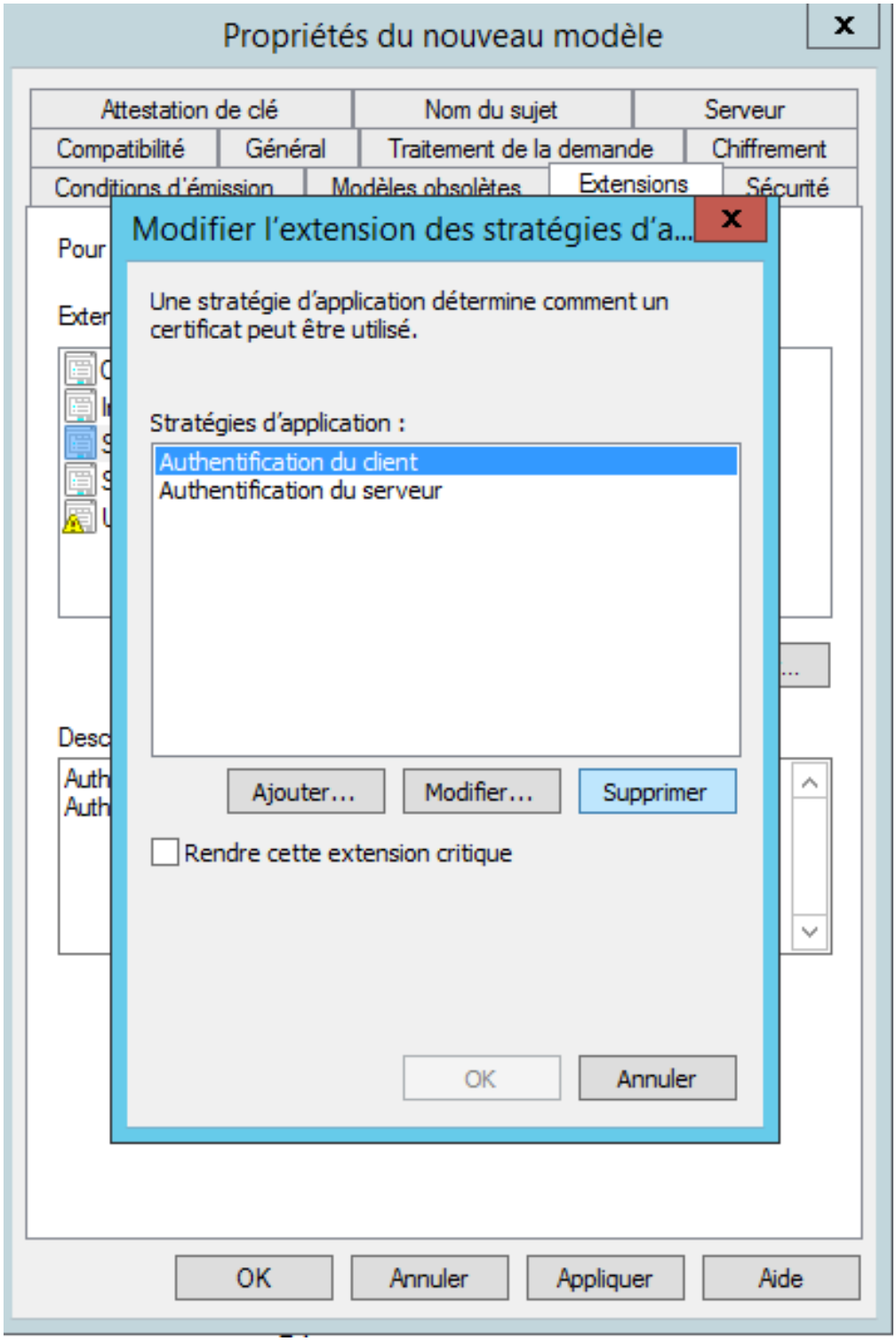
Choisir le modèle de certificat **Serveur RAS et IAS** car c'est celui qui se rapproche le plus du modèle que l'on veut créer (Authentification du serveur); ***clic droit*** –> ***dupliquer le modèle***.



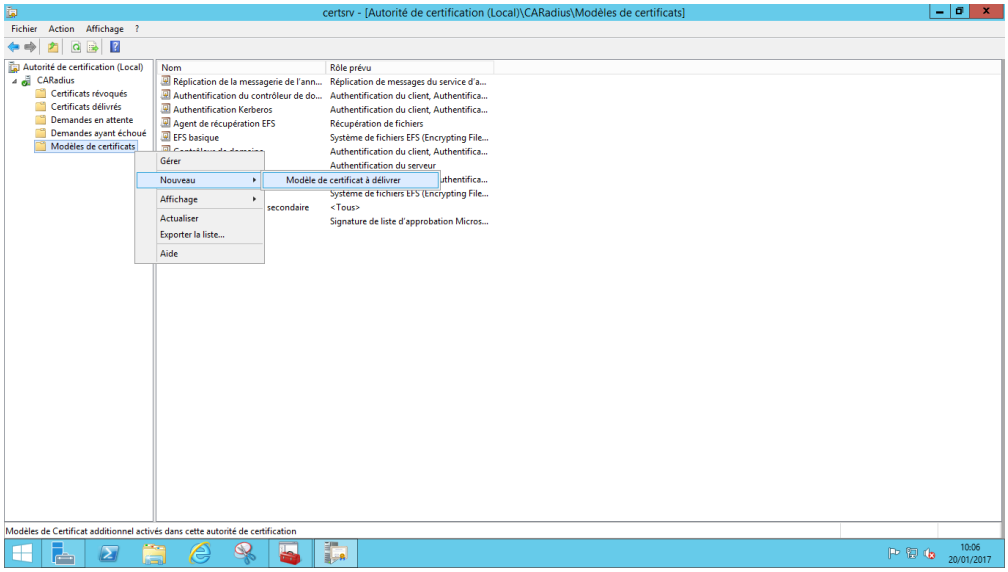
Choisir le nom du nouveau modèle –> choisir la période de validité du modèle

« Extensions » –> « Stratégies d'application » –> « Modifier ».

Cliquer sur ***"Authentification du client" –> "Supprimer"***. Le rôle n'est pas intéressant il faut juste que ce modèle authentifie le serveur.



On va maintenant inscrire ce modèle de certificat dans notre autorité de certification pour pouvoir délivrer des certificats sur ce modèle. Pour ce faire on va rouvrir la gestion de notre autorité de certification si elle ne l'est pas restée en allant sur le ***gestionnaire de serveur –> Outils –> Autorité de certification***. ***Clic droit sur modèle de certificats –> Nouveau –> Modèle de certificat à délivrer***.



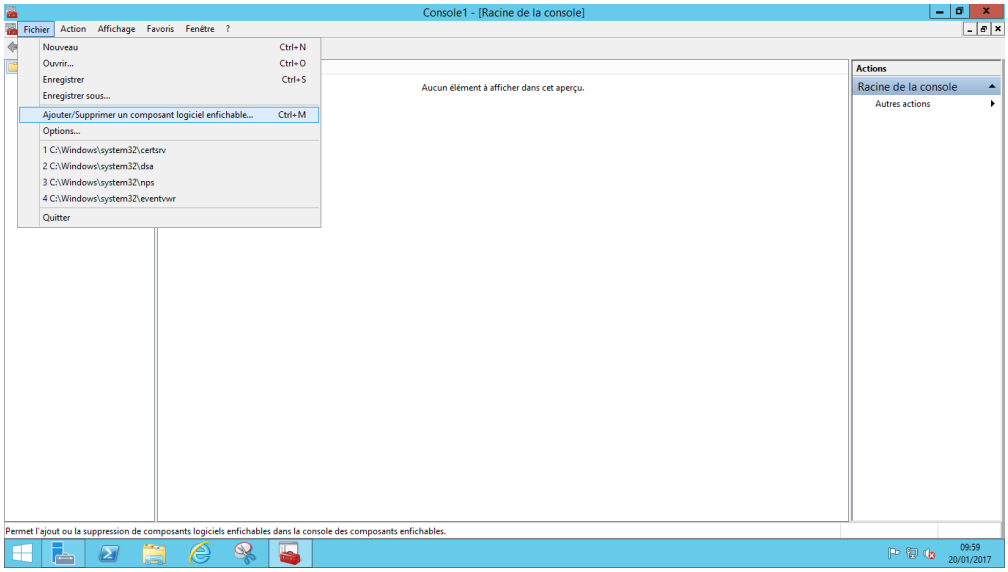
Choisir dans la liste le ***modèle de certificat*** –> ***« OK »***

Le modèle se retrouve dans les modèles de certificats de l'Autorité de certification prêt à délivrer des certificats.

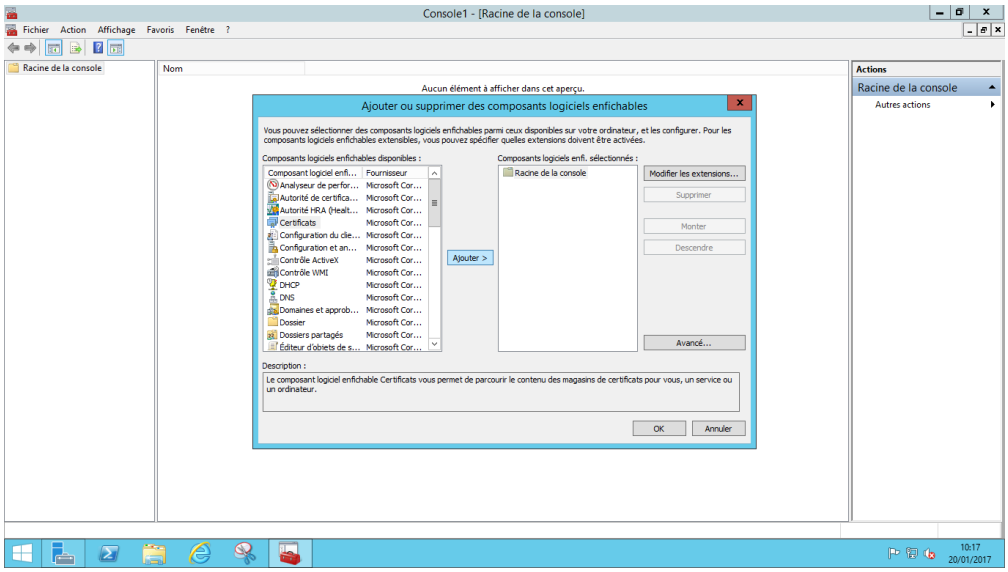
Génération du certificat

On va maintenant créer une demande de certificat s'appuyant sur notre modèle de certificat sur le serveur Radius car il s'agit de ce serveur que l'on veut approuver. Ce certificat va nous servir plus tard, dans la configuration du serveur Radius, pour authentifier le serveur auprès des clients Wi-Fi. Ouvrir une console MMC (Microsoft Management Console) : ***appuyer simultanément sur les touches « + R » du clavier –> écrire « mmc »***.

Cette console est un tableau de bord ou l'on peut regrouper plusieurs outils de configurations de la machine locale (DHCP, DNS, Editeur de stratégie de groupe, etc...). On va donc ajouter l'outil certificats. ***"Fichier" –> "Ajouter/Supprimer des composants logiciels enfichables"***



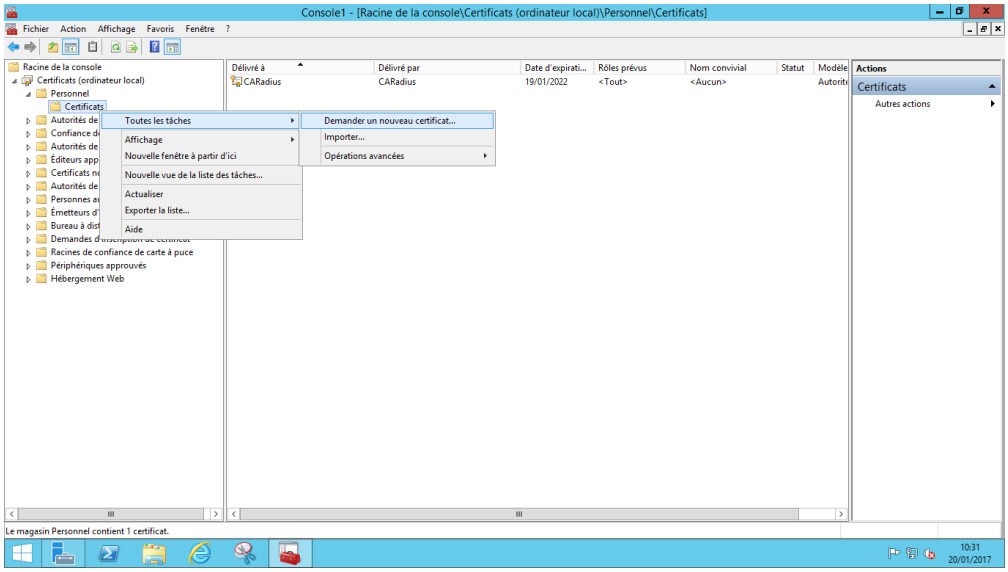
Choisir ***« Certificats »***



Choisir ***« Un compte d'ordinateur »*** (le certificat authentifiant la machine)

Choisir l'ordinateur local -> Terminer.

Sur le serveur Radius -> ouvrir une console MMC -> Certificats (ordinateur local) -> personnel -> clic droit sur « Certificats » -> « Toutes les tâches » -> « Demander un nouveau certificat… »



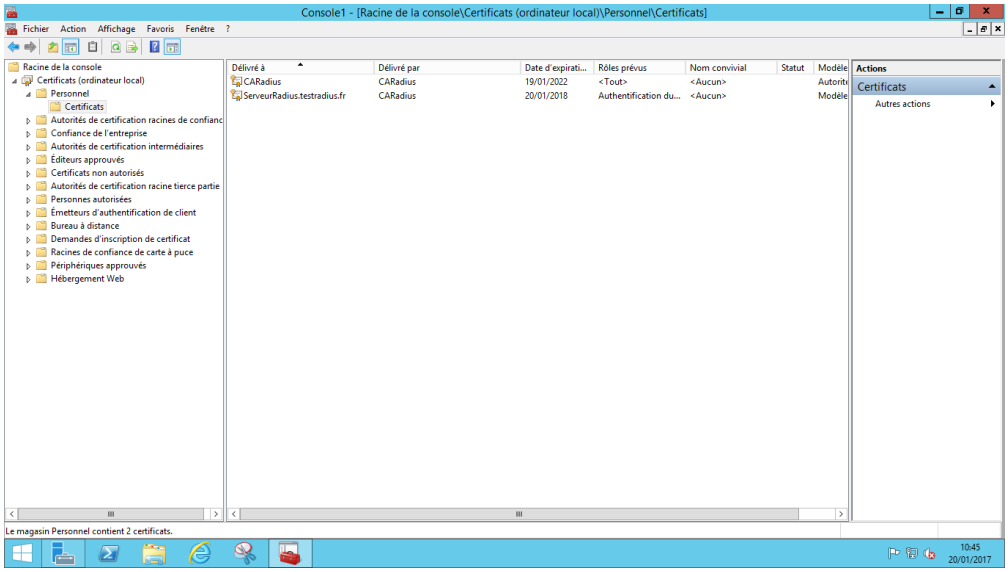
Cliquer sur ***“suivant”***.

Cliquer sur ***“suivant”***.

Choisir le modèle de certificat créé précédemment –> ***“Inscription”***.

L’installation du certificat nous indique qu’elle s’est terminée avec succès.

Le certificat s’est correctement installé dans le magasin personnel. C’est lui qui va authentifier le serveur auprès des clients.

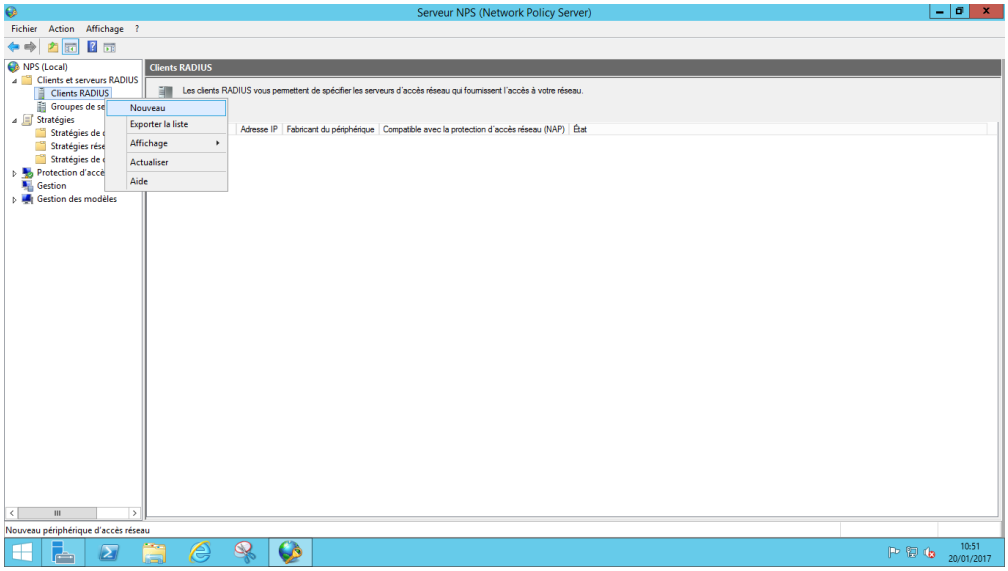


Configuration du service NPS

On va maintenant s'attaquer à la partie configuration du serveur Radius. ***Gestionnaire de serveur –> « outils » –> « Serveur NPS (Network Policy Server) »***.

Ajout des clients RADIUS

Cliquer sur ***« Clients et serveurs RADIUS » puis clic droit sur Client RADIUS –> Nouveau***.

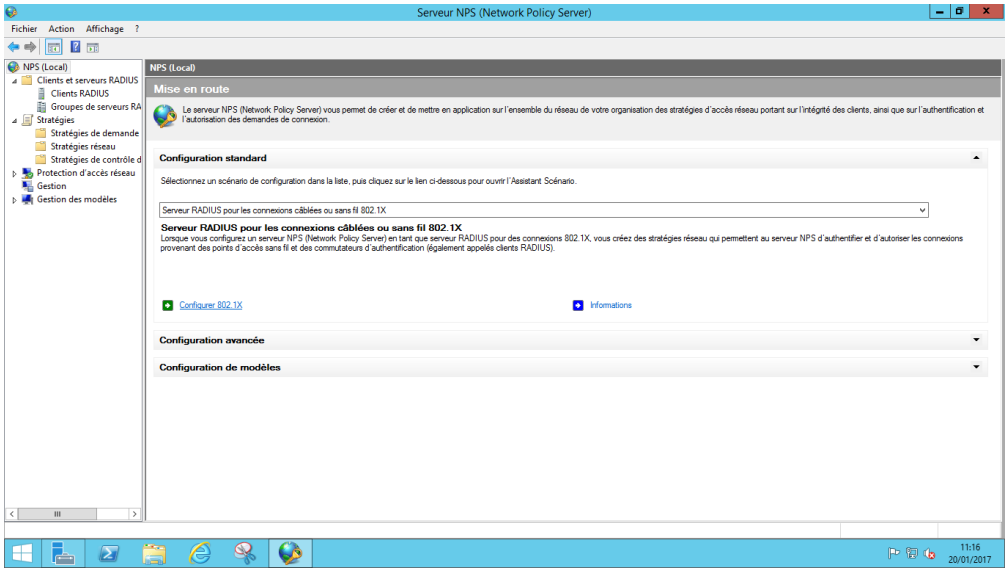


"Activer ce client RADIUS" –> ***Ajouter un nom à cette borne*** –> ***ajouter son @IP*** –> ***« Vérifier »*** –> ***créer ou générer un secret partagé***

Onglet avancé –> ***choisir le nom du fournisseur de la borne*** (différencier les différentes bornes) –> ***appliquer***

Création des stratégies de connexions

On va maintenant créer une stratégie que vont devoir respecter les clients pour accéder au réseau. ***Cliquer sur NPS (Local)*** –> ***« Serveur RADIUS pour les connexions câblées ou sans fil 802.1X »*** –> ***configurer 802.1X***

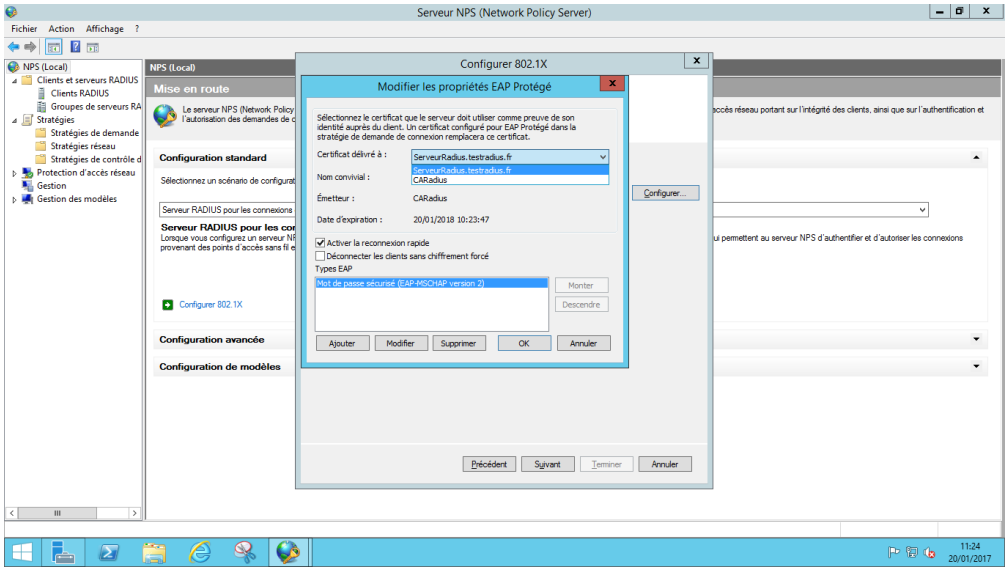


Sélectionner "Connexions sans fil sécurisées"** –> **configurer un nom pour la stratégie

Sélectionner le ou les client(s) RADIUS

Choisir Microsoft : PEAP (Protected EAP)** –> **« Configurer… »

Ajouter le certificat demandé précédemment : **« *Certificat délivré à :* » *choisir le certificat délivré au serveur Radius et non à la CA***



Cliquer sur ajouter pour ajouter le groupe autorisé défini précédemment dans l'AD.

***choisir le groupe ou l'utilisateur souhaité** –> **"Vérifier les noms"** –> **OK**.*

Cette page sert à configurer une infrastructure à VLAN (Virtual Local Area Network). Cliquer sur ***“suivant”***.

Cliquer sur ***“Terminer”***

Configuration de la borne Wi-Fi (client Radius)

Créer un SSID –> ***authentification : 802.1x ou WPA-Enterprise*** –> ***renseigner l'adresse IP du serveur Radius sur le port 1812***.

Connexion à la borne Wi-Fi (client Radius)

Se connecter sur un terminal Wi-Fi avec un compte de l'AD qui soit dans le groupe Radius