Mise en place d’un serveur RADIUS - Windows Server 2019

[**Installation des services**](#_heading=h.upxmuttj35zj) **2**

[**Création d’un certificat d’authentification**](#_heading=h.11pdjy6ixzog) **4**

[**Configuration des éléments d’authentification**](#_heading=h.avweuz2r59i4) **8**

[**Exporter le certificat**](#_heading=h.3lqdmlyz1e2u) **13**

[**Tests**](#_heading=h.vhcgm9fdvttc) **13**

## 

## Installation des services

| Après avoir configuré le serveur de domaine, nous ajoutons le rôle “Services de stratégie et d’accès réseau”. |
| --- |
|  |
| Puis nous installons le service de certificats Active Directory. |
|  |

## Création d’un certificat d’authentification

| Sous le gestionnaire de serveur, nous procédons dans un premier temps à la configuration du service ADCS. Nous installons le rôle autorité de certification. |
| --- |
|  |
| Nous choisissons autorité de certification entreprise.  (La CA d'Entreprise nécessite un serveur intégré au domaine et elle stockera des données directement dans l’Active Directory (certificats, clés privées, etc. avec une notion d'archivage), et facilitera la distribution de certificats auprès des postes intégrés au domaine notamment car ils seront automatiquement approuvés car dit de confiance. Une CA autonome peut être installée sur un serveur hors domaine, par conséquent elle ne stocke aucune donnée dans l’AD, ce qui empêche notamment d'utiliser l'inscription automatique.) |
|  |
| Nous choisissons ensuite la certification racine. |
|  |
| Nous créons une clé privée. |
|  |
| Nous laissons tous les paramètres par défaut à partir d’ici. |
|  |
| La configuration du certificat est réussie. |
|  |
| Pour exporter le certificat, nous ouvrons l’autorité de certification et accédons aux certificats délivrés. |
|  |
| Nous accédons aux détails du certificat et choisissons la copie dans un fichier. |
|  |
|  |

## 

## Configuration des éléments d’authentification

| Sur le routeur wifi, nous choisissons le mode de sécurité WPA2 Entreprise. Nous renseignons l’adresse IP du serveur et la clé statique partagée. |
| --- |
|  |
| Dans l’Active Directory, nous créons un groupe et l’attribuons aux utilisateurs autorisés à se connecter en Wifi. |
|  |
| Ensuite, nous ouvrons les serveurs NPS. Dans un premier temps, nous inscrivons le serveur dans l’Active Directory. |
|  |
| Après, nous sélectionnons un scénario de configuration pour configurer le 802.1x avec un assistant. |
|  |
| Nous renseignons et nommons la connexion 802.1x. |
|  |
| Nous renseignons ici les informations de notre point d’accès wifi. |
|  |
| Nous choisissons la méthode de connexion Microsoft PEAP. En cliquant sur configurer, il faut choisir le certificat précédemment créé. |
|  |
| Nous sélectionnons le groupe GR\_UtilisateursWifi afin d’autoriser ses membres à se connecter. |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

## 

## Exporter le certificat

| Pour explorer |
| --- |
|  |
|  |

## Tests

|  |
| --- |
|  |