AD CS : Autorité de certificat sous Windows en vue de l'authentification EAP-TLS

- Installation de l'autorité de certification racine
- Configuration Radius NPS pour l'authentification 802.1x via EAP-TLS
- Déploiement du wifi 802.1x PEAP-TLS par GPO
- Audit et sécurisation (hardening) d'AD CS

Installation de l'autorité de certification racine

Je m'inspire de cette documentation, très complète : Offline Root CA Setup | docs.mjcb.io

Un livre papier/kindle existe, je le recommande très fortement.

> Cette documentation est en cours de rédaction.

J'utilise ici les bonnes pratiques de Microsoft qui consiste à mettre en place 2 serveurs :

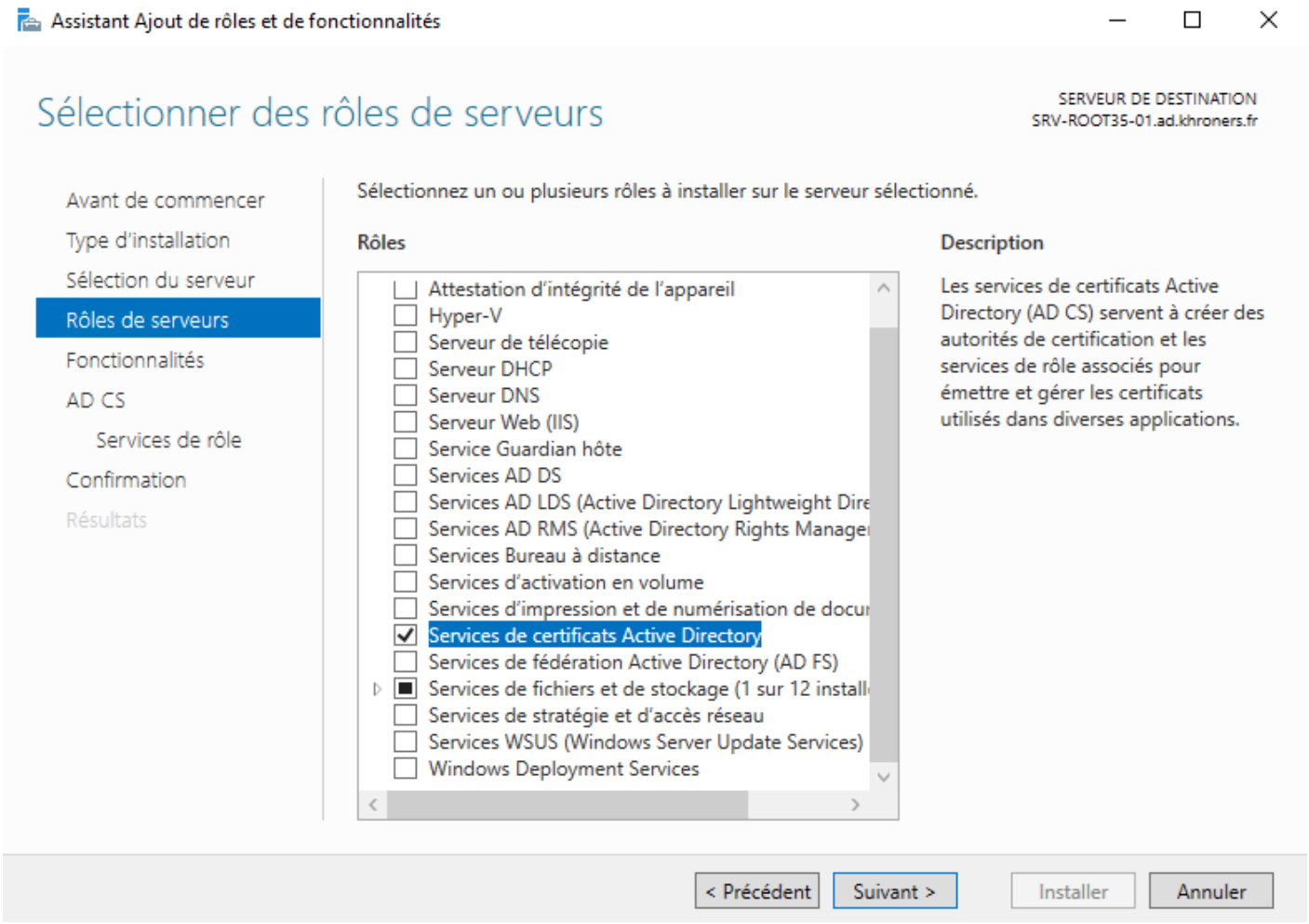
- Un serveur Windows Server 2022 qui aura le rôle d'autorité de certification racine, qui sera par la suite éteint,
- Un deuxième serveur Windows Server 2022 qui aura le rôle d'autorité de certification intermédiaire, en ligne en permanence, qui délivrera les certificats clients.

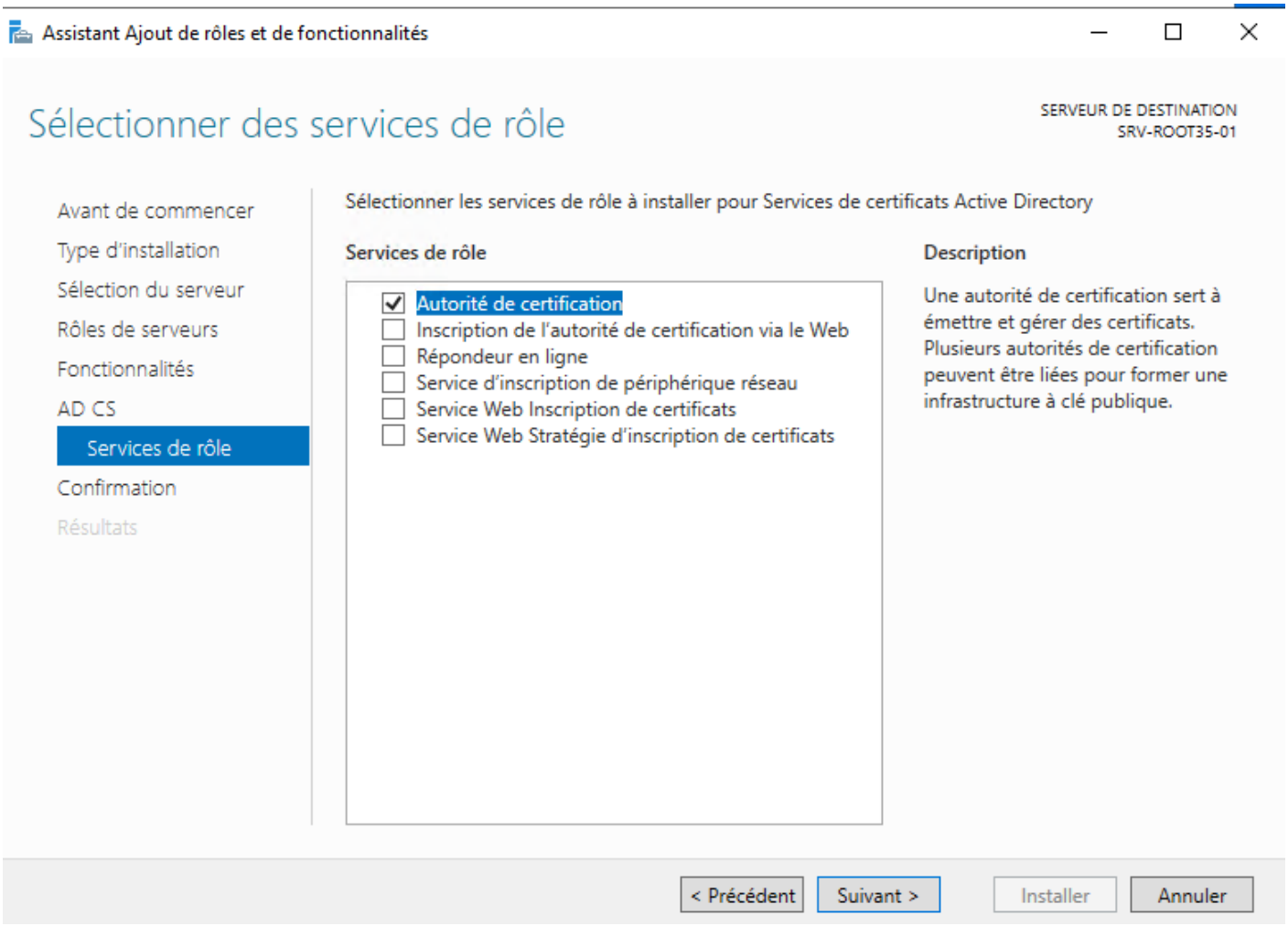
On commence par mettre en place l'autorité de certification racine, qui sera par la suite offline.

A la racine du C:, on ajoute un fichier CAPolicy.inf :

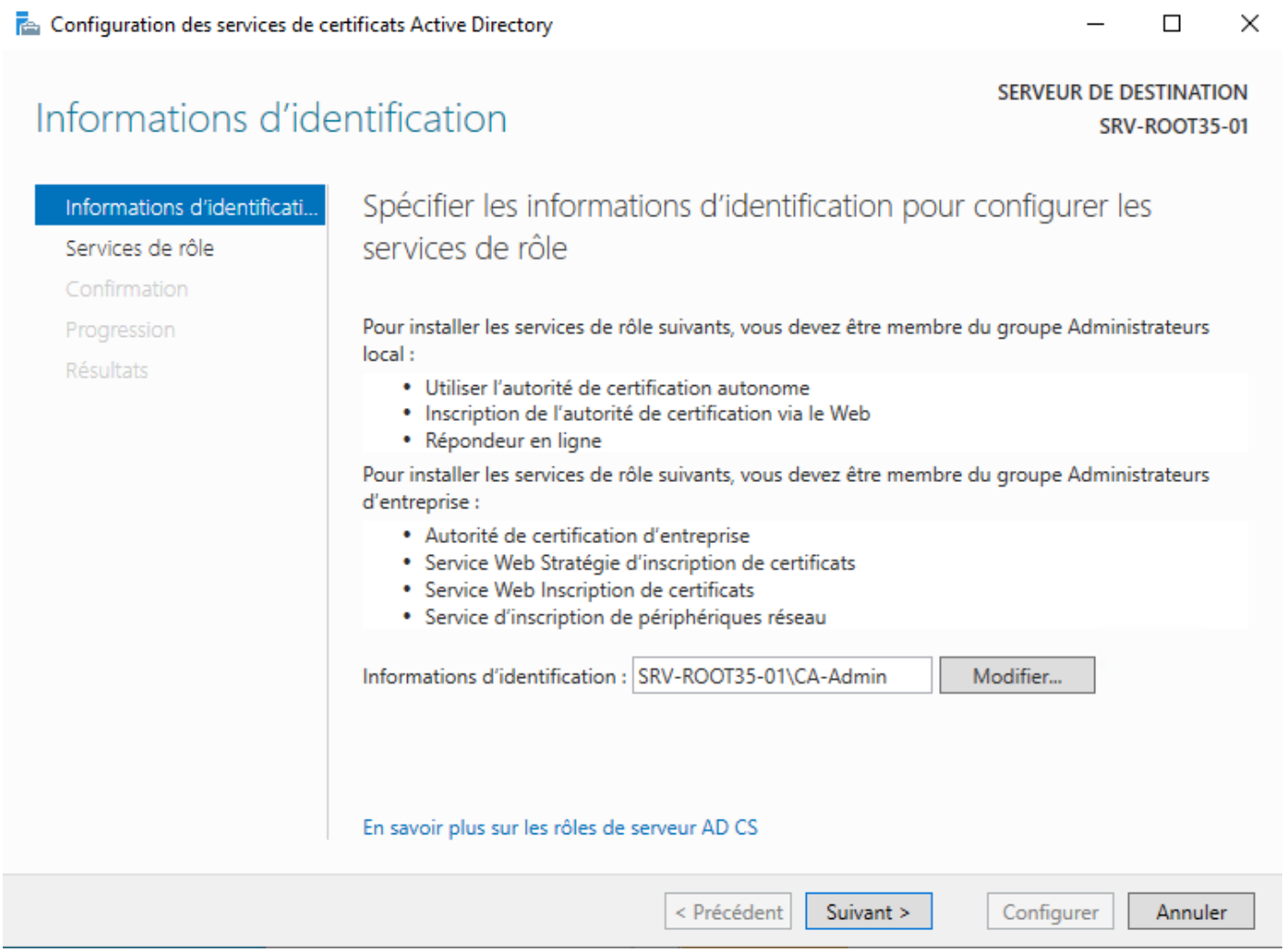
```
[Version]
Signature = "$Windows NT$"

[PolicyStatementExtension]
Policies = AllIssuancePolicy,InternalPolicy
Critical = FALSE

; AllIssuancePolicy is set to the OID of 2.5.29.32.0 to ensure all certificate templates are
available.
[AllIssuancePolicy]
OID = 2.5.29.32.0

[InternalPolicy]
OID = 1.2.3.4.1455.67.89.5
Notice = "The Khroners Labs Certification Authority is an internal resource. Certificates that
are issued by this Certificate Authority are for internal usage only."
```

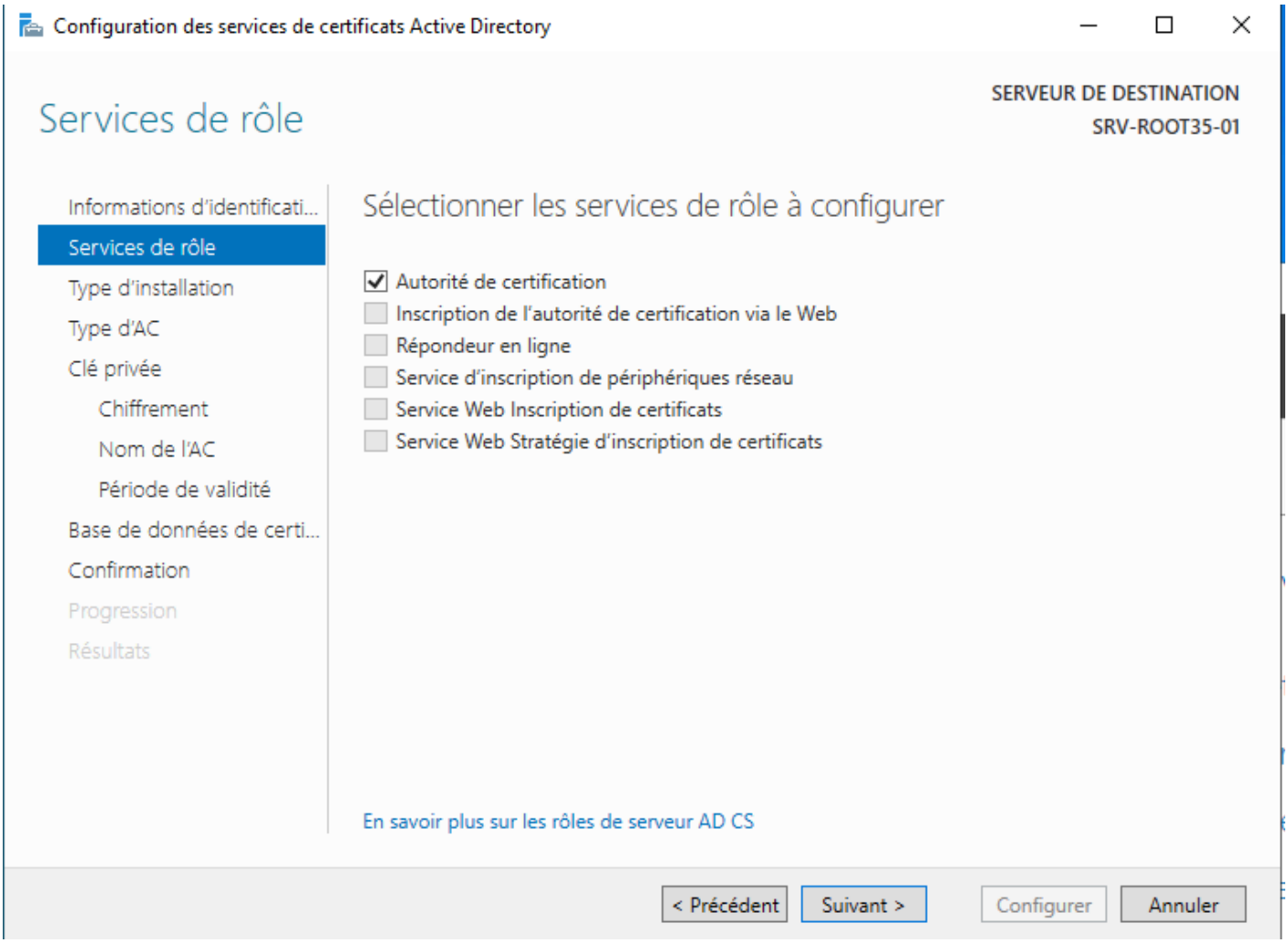
```
URL = http://pki.ad.khroners.fr/cps.html

[Certsrv_Server]
; Renewal information for the Root CA.
RenewalKeyLength = 4096
RenewalValidityPeriod = Years
RenewalValidityPeriodUnits = 10

; Disable support for issuing certificates with the RSASSA-PSS algorithm.
AlternateSignatureAlgorithm = 0

; The CRL publication period is the lifetime of the Root CA.
CRLPeriod = Years
CRLPeriodUnits = 10

; The option for Delta CRL is disabled since this is a Root CA.
CRLDeltaPeriod = Days
CRLDeltaPeriodUnits = 0
```


Assistant Ajout de rôles et de fonctionnalités
Sélectionner des rôles de serveurs
SERVEUR DE DESTINATION
SRV-ROOT35-01.ad.khroners.fr
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
AD CS
Services de rôle
Confirmation
Résultats
Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.
Rôles
Attestation d'intégrité de l'appareil
Hyper-V
Serveur de télécopie
Serveur DHCP
Serveur DNS
Serveur Web (IIS)
Service Guardian hôte
Services AD DS
Services AD LDS (Active Directory Lightweight Dire
Services AD RMS (Active Directory Rights Manage
Services Bureau à distance
Services d'activation en volume
Services d'impression et de numérisation de docu
Services de certificats Active Directory
Services de fédération Active Directory (AD FS)
Services de fichiers et de stockage (1 sur 12 install
Services de stratégie et d'accès réseau
Services WSUS (Windows Server Update Services)
Windows Deployment Services
Description
Les services de certificats Active Directory (AD CS) servent à créer des autorités de certification et les services de rôle associés pour émettre et gérer les certificats utilisés dans diverses applications.
< Précédent
Suivant >
Installer
Annuler



On configure le rôle :


Configuration des services de certificats Active Directory
Informations d'identification
SERVEUR DE DESTINATION
SRV-ROOT35-01
Informations d'identificati...
Services de rôle
Confirmation
Progression
Résultats
Spécifier les informations d'identification pour configurer les services de rôle
Pour installer les services de rôle suivants, vous devez être membre du groupe Administrateurs local :
Utiliser l'autorité de certification autonome
Inscription de l'autorité de certification via le Web
Répondeur en ligne
Pour installer les services de rôle suivants, vous devez être membre du groupe Administrateurs d'entreprise :
Autorité de certification d'entreprise
Service Web Stratégie d'inscription de certificats
Service Web Inscription de certificats
Service d'inscription de périphériques réseau
Informations d'identification : SRV-ROOT35-01\CA-Admin
Modifier...
En savoir plus sur les rôles de serveur AD CS
< Précédent
Suivant >
Configurer
Annuler


Configuration des services de certificats Active Directory
Services de rôle
SERVEUR DE DESTINATION
SRV-ROOT35-01
Informations d'identificati...
Services de rôle
Type d'installation
Type d'AC
Clé privée
Chiffrement
Nom de l'AC
Période de validité
Base de données de certi...
Confirmation
Progression
Résultats
Sélectionner les services de rôle à configurer
Autorité de certification
Inscription de l'autorité de certification via le Web
Répondeur en ligne
Service d'inscription de périphériques réseau
Service Web Inscription de certificats
Service Web Stratégie d'inscription de certificats
En savoir plus sur les rôles de serveur AD CS
< Précédent
Suivant >
Configurer
Annuler

Configuration des services de certificats Active Directory

Type d'installation

SERVEUR DE DESTINATION
SRV-ROOT35-01

- Informations d'identificati...
- Services de rôle
- Type d'installation
- Type d'AC
- Clé privée
  - Chiffrement
  - Nom de l'AC
  - Période de validité
- Base de données de certi...
- Confirmation
- Progression
- Résultats

Spécifier le type d'installation de l'AC

Les autorités de certification d'entreprise peuvent utiliser les services de domaine Active Directory (AD DS) pour simplifier la gestion des certificats. Les autorités de certification autonomes n'utilisent pas AD DS pour émettre ou gérer des certificats.

○ Autorité de certification d'entreprise

Les autorités de certification d'entreprise doivent être membres d'un domaine et sont généralement en ligne pour émettre des certificats ou des stratégies de certificat.

◉ Autorité de certification autonome

Les autorités de certification autonomes peuvent être membres d'un groupe de travail ou d'un domaine. Les autorités de certification autonomes ne nécessitent pas AD DS et peuvent être utilisées sans connexion réseau (hors connexion).

En savoir plus sur le type d'installation

< Précédent | Suivant > | Configurer | Annuler

Configuration des services de certificats Active Directory

Type d'autorité de certification

SERVEUR DE DESTINATION
SRV-ROOT35-01.ad.khroners.fr

- Informations d'identificati...
- Services de rôle
- Type d'installation
- Type d'AC
- Clé privée
  - Chiffrement
  - Nom de l'AC
  - Période de validité
- Base de données de certi...
- Confirmation
- Progression
- Résultats

Spécifier le type de l'AC

Lorsque vous installez les services de certificats Active Directory (AD CS), vous créez ou étendez une hiérarchie d'infrastructure à clé publique (PKI). Une autorité de certification racine se trouve au sommet de la hiérarchie PKI et émet ses propres certificats auto-signés. Une autorité de certification secondaire reçoit un certificat de l'autorité de certification de rang plus élevé dans la hiérarchie PKI.

(•) Autorité de certification racine

Les autorités de certification racines sont les premières voire les seules autorités de certification configurées dans une hiérarchie PKI.

( ) Autorité de certification secondaire

Les autorités de certification secondaires nécessitent une hiérarchie PKI établie et sont autorisées à émettre des certificats par l'autorité de certification de rang plus élevé dans la hiérarchie.

En savoir plus sur le type d'autorité de certification

< Précédent | Suivant > | Configurer | Annuler

Configuration des services de certificats Active Directory

Clé privée

SERVEUR DE DESTINATION
SRV-ROOT35-01.ad.khroners.fr

- Informations d'identificati...
- Services de rôle
- Type d'installation
- Type d'AC
- Clé privée
  - Chiffrement
  - Nom de l'AC
  - Période de validité
- Base de données de certi...
- Confirmation
- Progression
- Résultats

Spécifier le type de la clé privée

Pour générer et émettre des certificats aux clients, une autorité de certification doit posséder une clé privée.

(•) Créer une clé privée
Utilisez cette option si vous n'avez pas de clé privée ou pour en créer une.

( ) Utiliser la clé privée existante
Utilisez cette option pour garantir la continuité avec les certificats émis antérieurement lors de la réinstallation d'une AC.

( ) Sélectionner un certificat et utiliser sa clé privée associée
Sélectionnez cette option s'il existe un certificat sur cet ordinateur ou pour importer un certificat et utiliser sa clé privée associée.

( ) Sélectionner une clé privée existante sur cet ordinateur
Sélectionnez cette option si vous avez conservé les clés privées d'une installation antérieure ou pour utiliser une clé privée d'une autre source.

En savoir plus sur la clé privée

< Précédent | Suivant > | Configurer | Annuler

Configuration des services de certificats Active Directory

Chiffrement pour l'autorité de certification

SERVEUR DE DESTINATION
SRV-ROOT35-01

- Informations d'identificati...
- Services de rôle
- Type d'installation
- Type d'AC
- Clé privée
- **Chiffrement**
- Nom de l'AC
- Période de validité
- Base de données de certi...
- Confirmation
- Progression
- Résultats

Spécifier les options de chiffrement

Sélectionnez un fournisseur de chiffrement : RSA#Microsoft Software Key Storage Provider

Longueur de la clé : 4096

Sélectionnez l'algorithme de hachage pour signer les certificats émis par cette AC :

- SHA256
- SHA384
- SHA512
- SHA1

☐ Autorisez l'interaction de l'administrateur lorsque l'autorité de certification accède à la clé privée.

En savoir plus sur le chiffrement

< Précédent | Suivant > | Configurer | Annuler

Configuration des services de certificats Active Directory

Nom de l'autorité de certification

SERVEUR DE DESTINATION
SRV-ROOT35-01

- Informations d'identificati...
- Services de rôle
- Type d'installation
- Type d'AC
- Clé privée
  - Chiffrement
  - Nom de l'AC
  - Période de validité
- Base de données de certi...
- Confirmation
- Progression
- Résultats

Spécifier le nom de l'AC

Tapez un nom commun pour identifier cette autorité de certification. Ce nom est ajouté à tous les certificats émis par l'autorité de certification. Les valeurs des suffixes du nom unique sont générées automatiquement, mais elles sont modifiables.

Nom commun de cette AC :

Khroners Labs Certificate Authority

Suffixe du nom unique :

Aperçu du nom unique :

CN=Khroners Labs Certificate Authority

En savoir plus sur le nom de l'autorité de certification

< Précédent | Suivant > | Configurer | Annuler

Configuration des services de certificats Active Directory

Période de validité

SERVEUR DE DESTINATION
SRV-ROOT35-01

- Informations d'identificati...
- Services de rôle
- Type d'installation
- Type d'AC
- Clé privée
  - Chiffrement
  - Nom de l'AC
  - Période de validité
- Base de données de certi...
- Confirmation
- Progression
- Résultats

Spécifier la période de validité

Sélectionnez la période de validité du certificat généré pour cette autorité de certification :

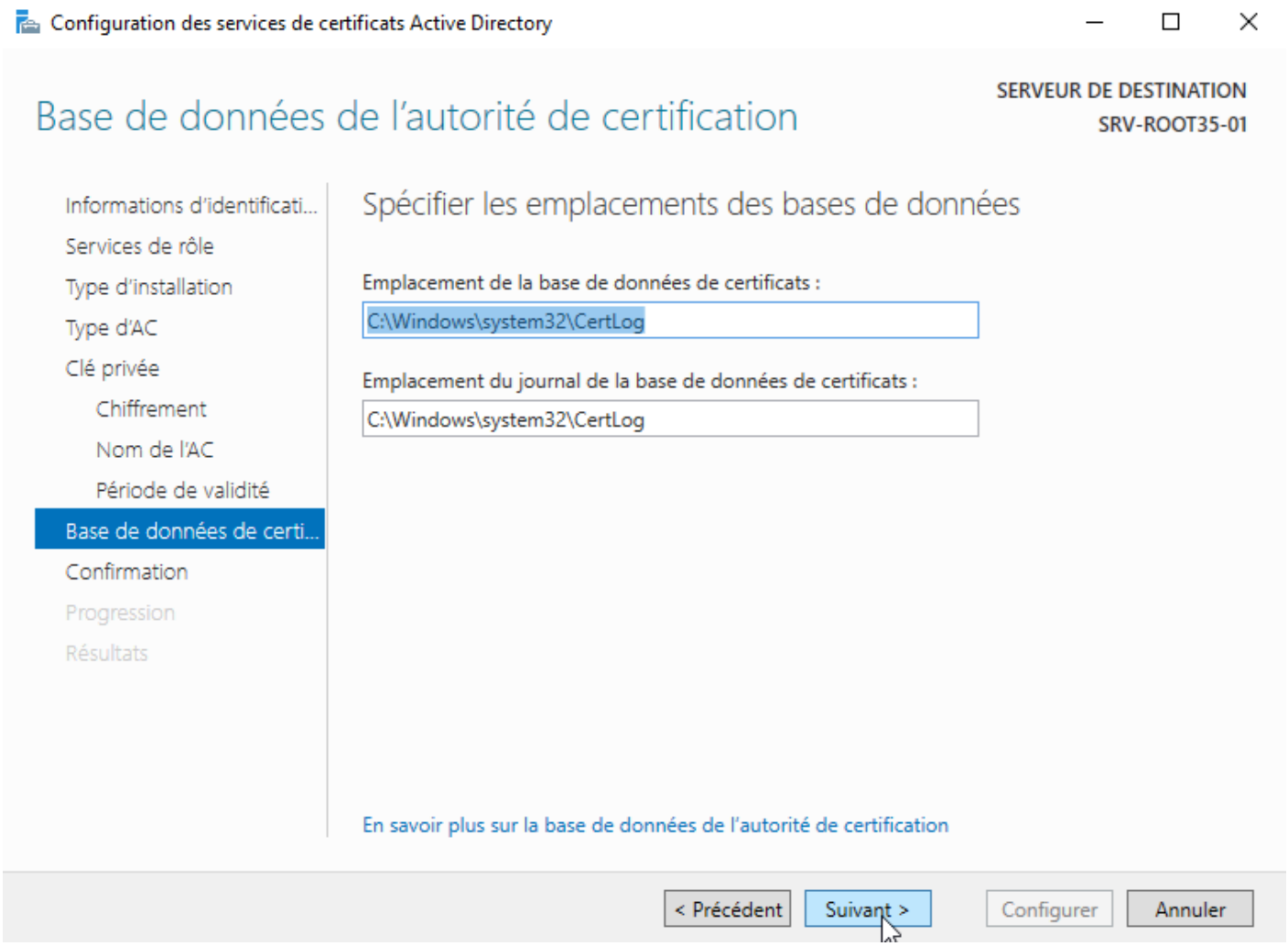
10 Années

Date d'expiration de l'AC : 30/09/2033 18:57:00

La période de validité configurée pour ce certificat d'autorité de certification doit dépasser la période de validité pour les certificats qu'elle émettra.

En savoir plus sur la période de validité

< Précédent | Suivant > | Configurer | Annuler




```
certutil.exe -setreg CA\DSConfigDN "CN=Configuration,DC=ad,DC=khroners,DC=fr"
certutil.exe -setreg CA\ValidityPeriodUnits 5
certutil.exe -setreg CA\ValidityPeriod "Years"
certutil.exe -setreg CA\CRLPeriodUnits 52
certutil.exe -setreg CA\CRLPeriod "Weeks"
certutil.exe -setreg CA\CRLOverlapPeriodUnits 12
certutil.exe -setreg CA\CRLOverlapPeriod "Hours"
net stop CertSvc
net start CertSvc
```

Offline Root CA Setup | docs.mjcb.io

Configuration Radius NPS pour l'authentification 802.1x via EAP-TLS

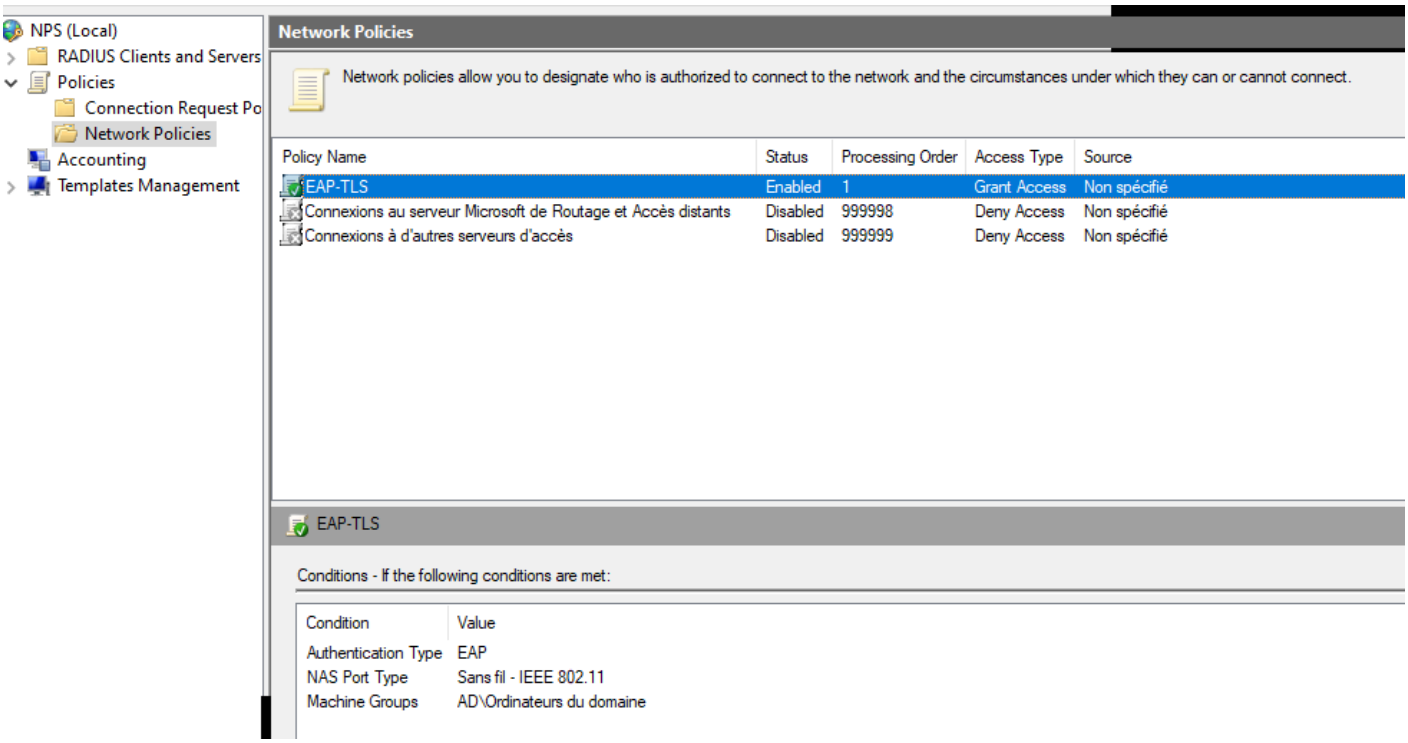
Cette documentation détaille la configuration du rôle NPS (Network Policy Server) sous Windows Server 2022 afin d'authentifier les utilisateurs ou ordinateurs au réseau Wifi. On peut également l'adapter pour la connexion filaire (non détaillée ici).

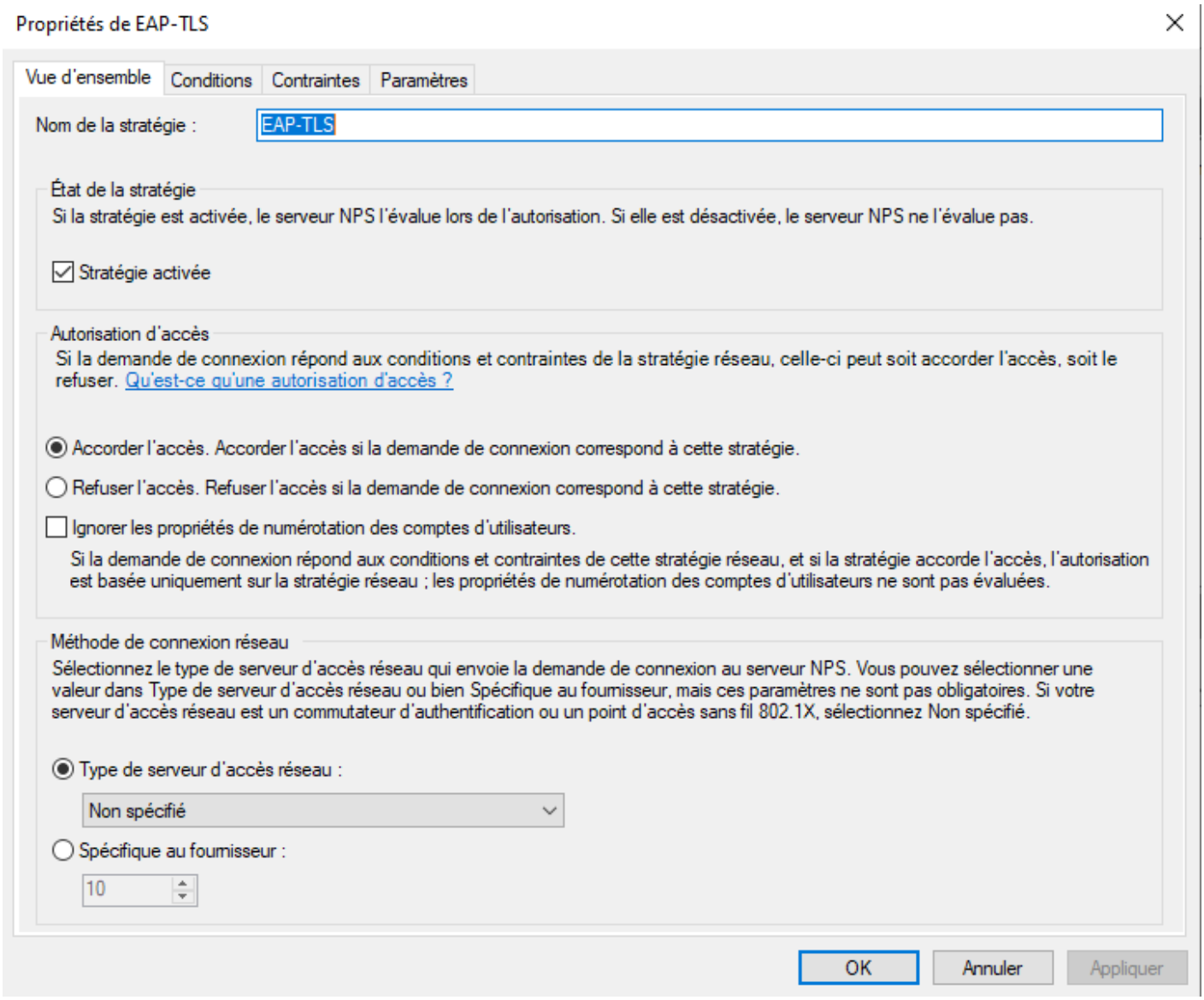
Parmi les méthodes d'authentification, le PEAP-TLS est la méthode la plus sécurisée, mais rarement supportée. De plus, elle chiffre la communication de la clé publique, qui n'a pas trop de sens.

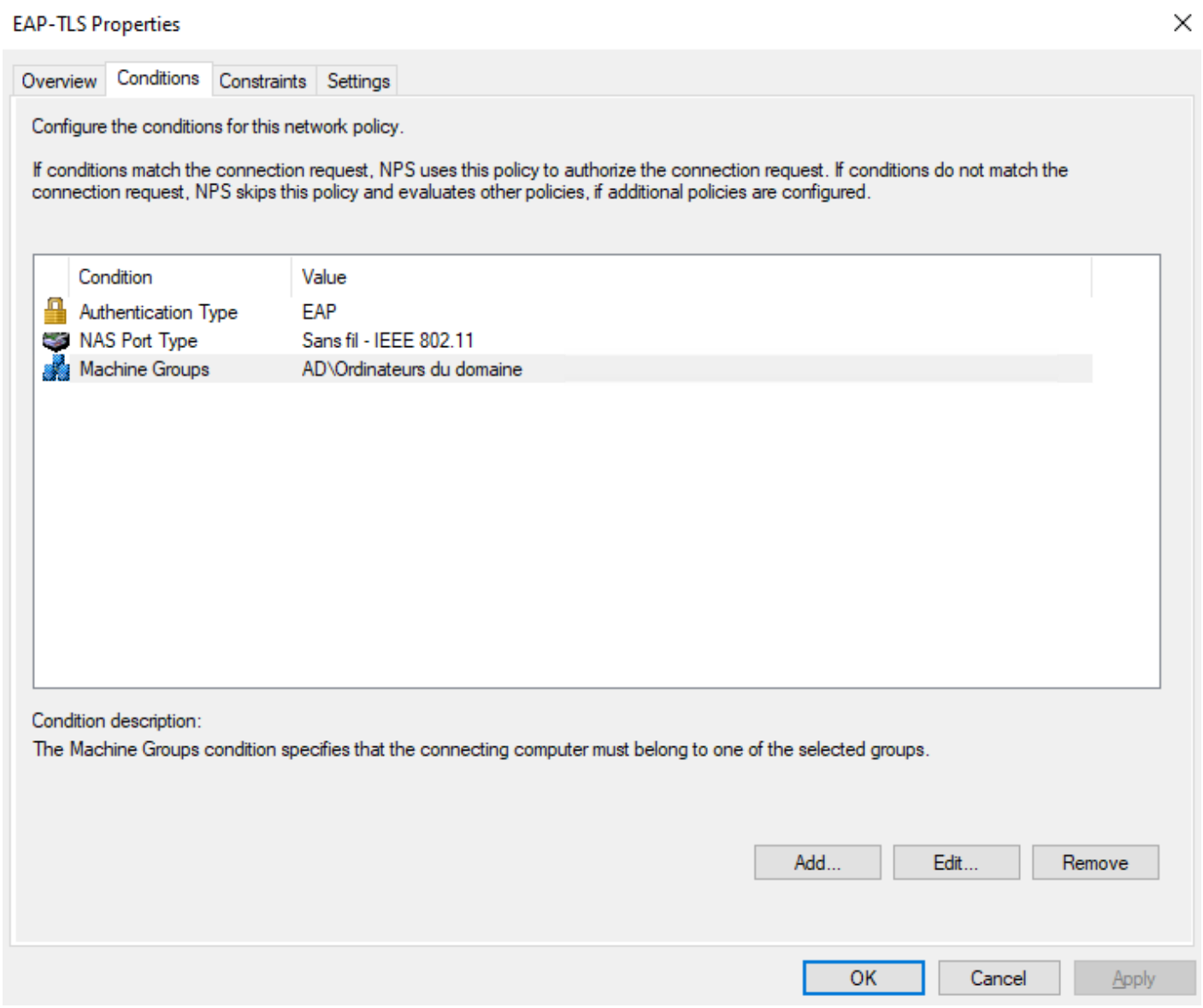
Authentication Methods	RADIUS NPS Server	Requirements for Client	Security Level
PAP	N/A	Username and Password	Least Safe
CHAP	N/A	Username and Password	Unsafe
MS-CHAP-v2	N/A	Username and Password	Unsafe
EAP-MS-CHAP-v2	N/A	Username and Password	Unsafe
PEAP-MSCHAP-v2	Computer Certificate	Username and Password	Safe
EAP-TLS	Computer Certificate	User Certificate	Safer
PEAP-TLS	Computer Certificate	User Certificate	The safest

Vous trouverez plus d'informations ici : Protocole EAP (Extensible Authentication Protocol) pour l’accès réseau dans Windows | Microsoft Learn

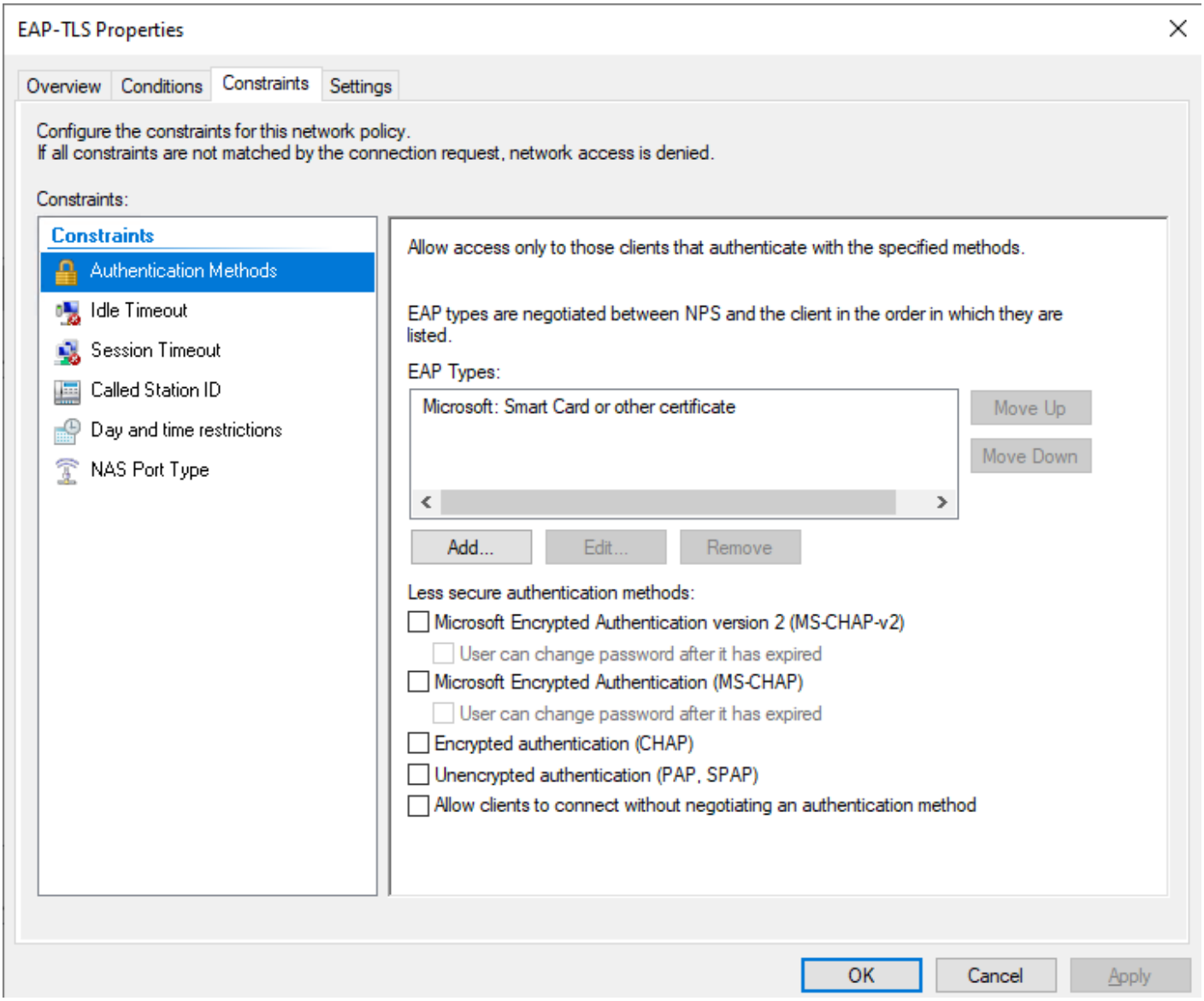
Après l'installation du rôle NPS, on définit la stratégie réseau comme ceci :


NPS (Local)
RADIUS Clients and Servers
Policies
Connection Request Po
Network Policies
Accounting
Templates Management
Network Policies
Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.
Policy Name
Status
Processing Order
Access Type
Source
EAP-TLS
Enabled
1
Grant Access
Non spécifié
Connexions au serveur Microsoft de Routage et Accès distants
Disabled
999998
Deny Access
Non spécifié
Connexions à d'autres serveurs d'accès
Disabled
999999
Deny Access
Non spécifié
EAP-TLS
Conditions - If the following conditions are met:
Condition
Value
Authentication Type
EAP
NAS Port Type
Sans fil - IEEE 802.11
Machine Groups
AD\Ordinateurs du domaine

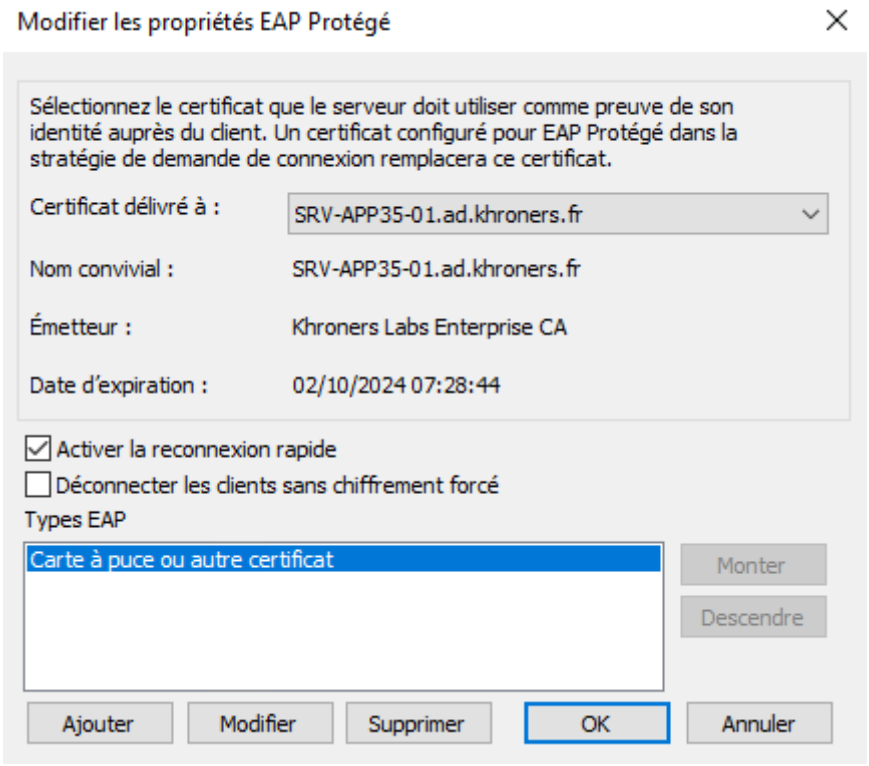

Propriétés de EAP-TLS
Vue d'ensemble
Conditions
Contraintes
Paramètres
Nom de la stratégie :
EAP-TLS
État de la stratégie
Si la stratégie est activée, le serveur NPS l'évalue lors de l'autorisation. Si elle est désactivée, le serveur NPS ne l'évalue pas.
Stratégie activée
Autorisation d'accès
Si la demande de connexion répond aux conditions et contraintes de la stratégie réseau, celle-ci peut soit accorder l'accès, soit le refuser. Qu'est-ce qu'une autorisation d'accès ?
Accorder l'accès. Accorder l'accès si la demande de connexion correspond à cette stratégie.
Refuser l'accès. Refuser l'accès si la demande de connexion correspond à cette stratégie.
Ignorer les propriétés de numérotation des comptes d'utilisateurs.
Si la demande de connexion répond aux conditions et contraintes de cette stratégie réseau, et si la stratégie accorde l'accès, l'autorisation est basée uniquement sur la stratégie réseau ; les propriétés de numérotation des comptes d'utilisateurs ne sont pas évaluées.
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
OK
Annuler
Appliquer



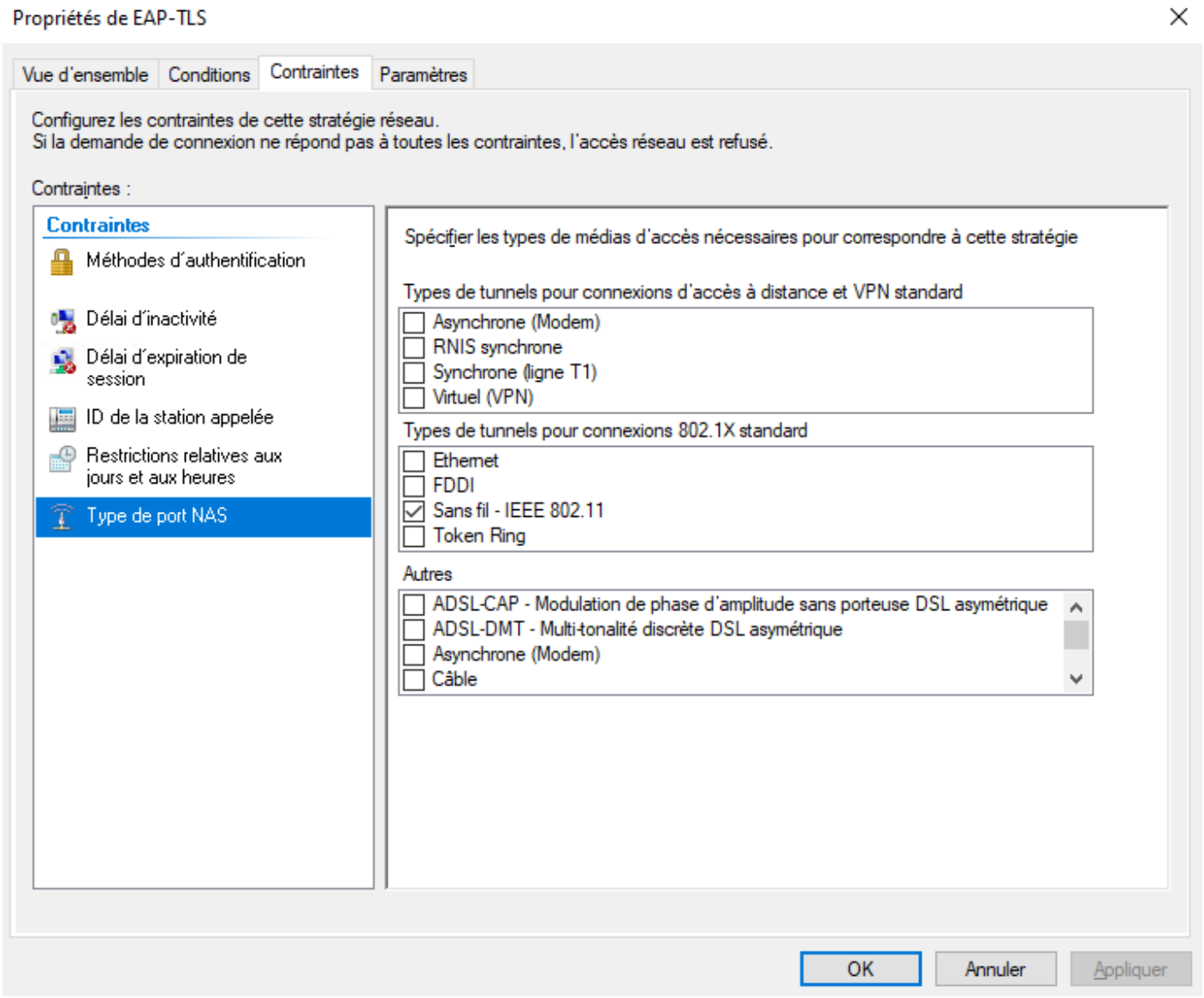
Le "TLS" de "EAP-TLS" correspond à "Microsoft: Smart Card or other certificate".



On clique sur "Microsoft: Smart Card or other certificate" et "Modifier..." :



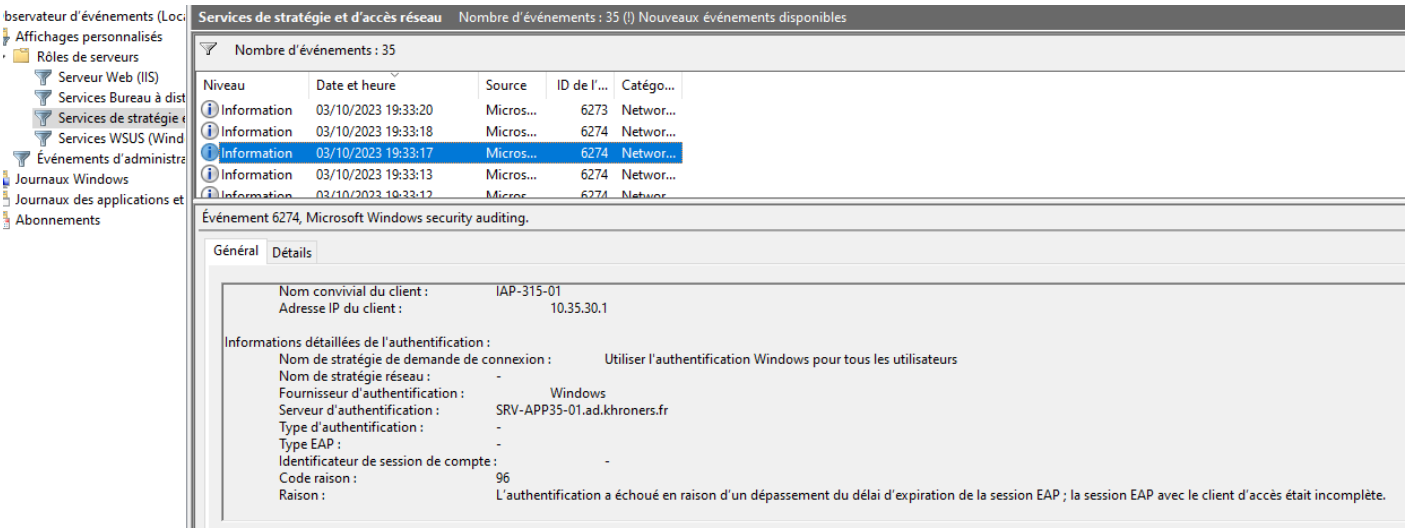
Cela correspond au PEAP-TLS (ou également dit PEAP-EAP-TLS).

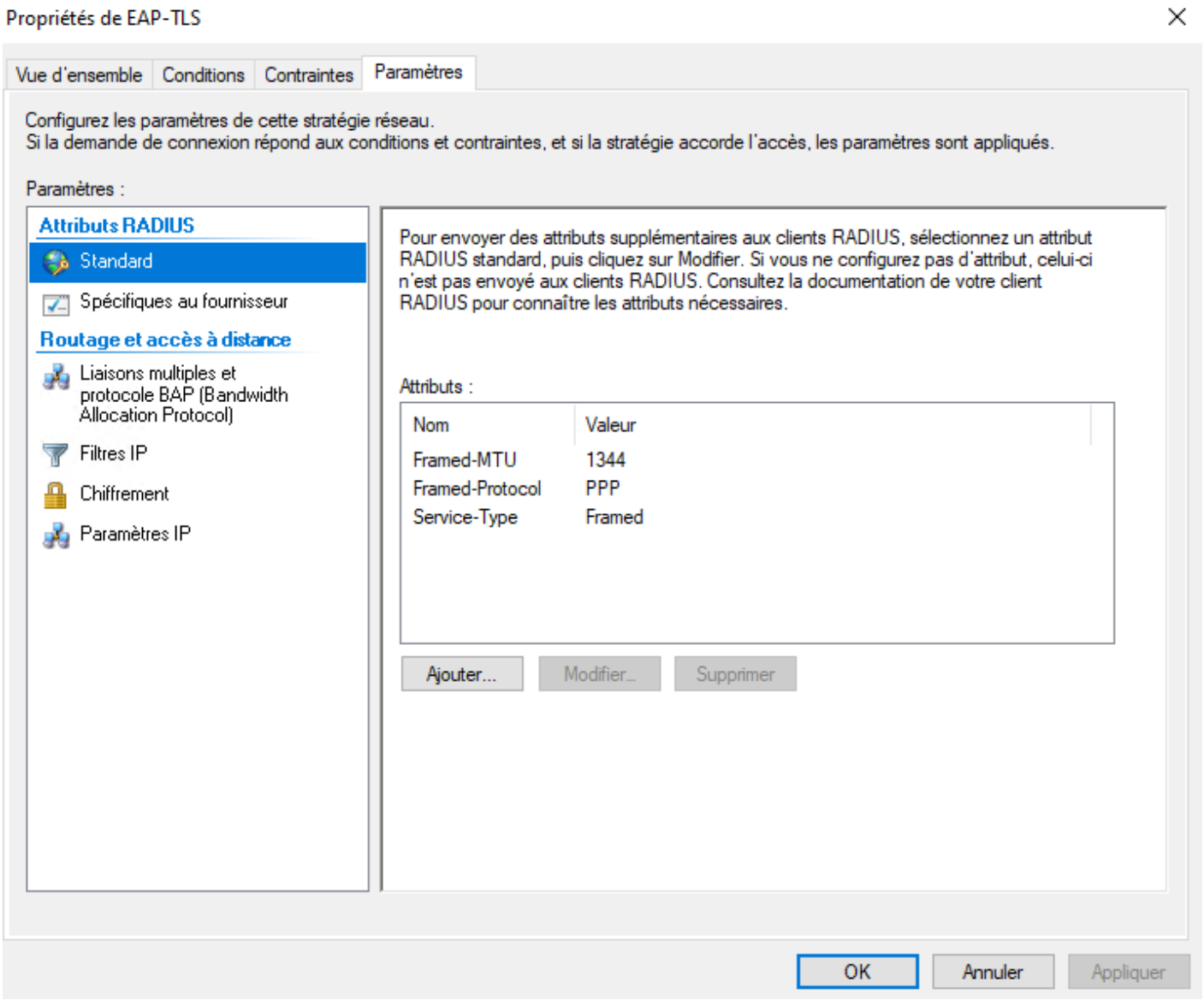


Dans mon cas, j'ai du ajouter l'attribut "Framed-MTU" avec une valeur de 1344, car j'ai l'erreur suivante :

> Authentication failed due to an EAP session timeout; the EAP session with the access client was incomplete.

Vous pouvez observer les logs dans l'observateur d'évènements, sous "Affichages Personnalisés" > "Rôles de serveurs" > Services de stratégie et d'accès réseau".





On ajoute également le(s) client(s) RADIUS en définissant un secret partagé.

Dans les bornes wifi, on choisit WPA2 Entreprise (ou WPA3 Entreprise si supporté), en renseignant l'adresse IP du serveur NPS et le secret partagé.

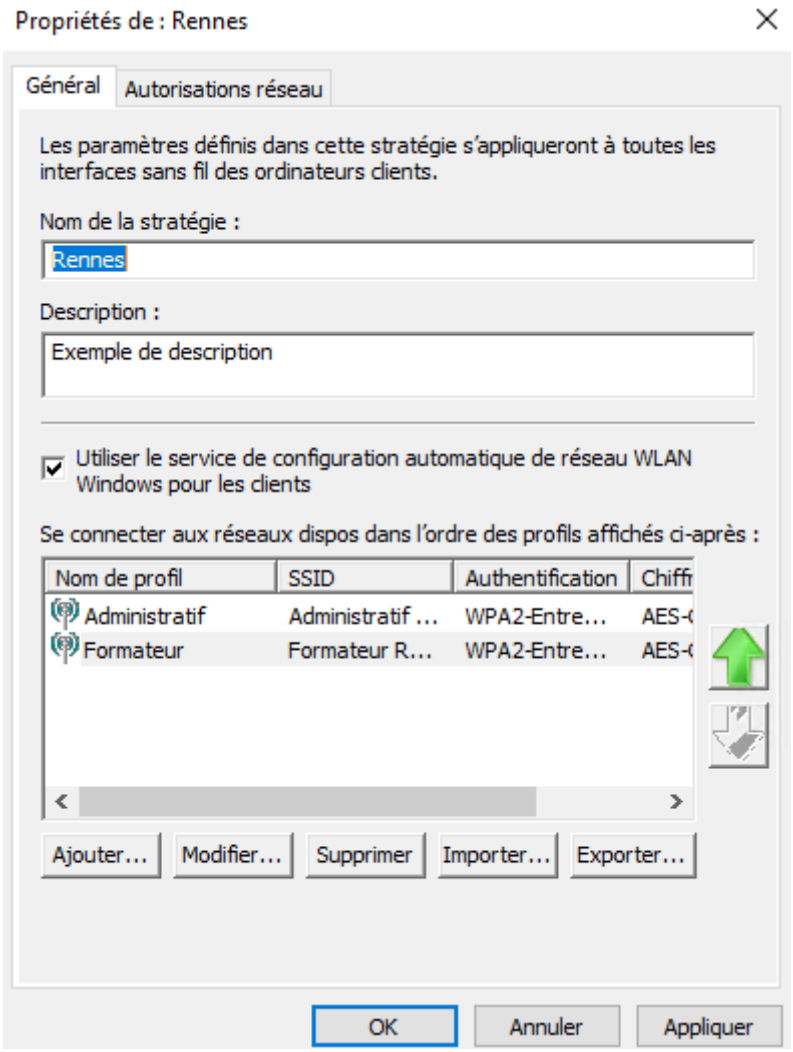
Déploiement du wifi 802.1x PEAP-TLS par GPO

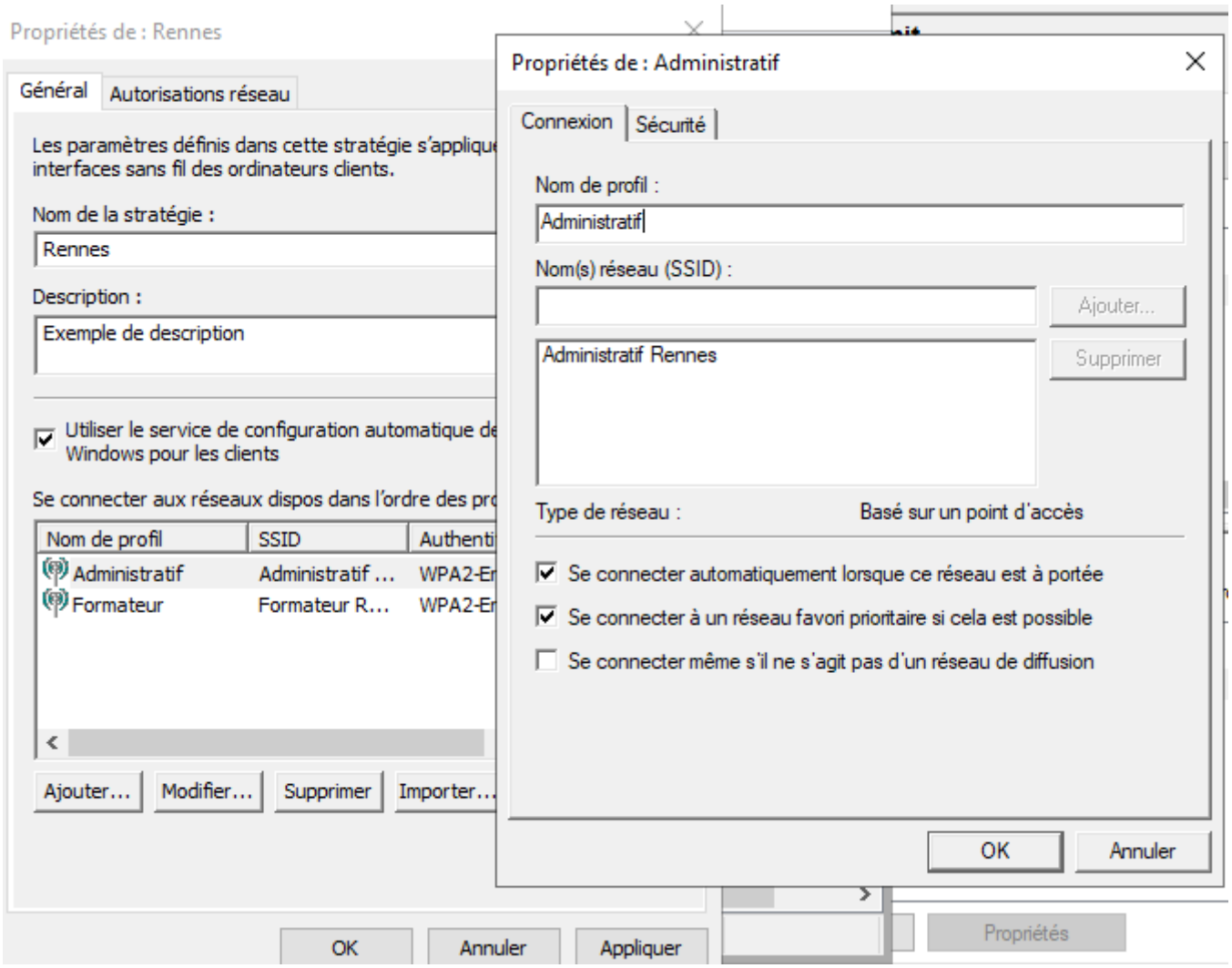
On peut connecter les ordinateurs aux réseaux Wifi par GPO automatiquement.

On crée et lie une GPO à une OU Ordinateurs puis on la modifie.

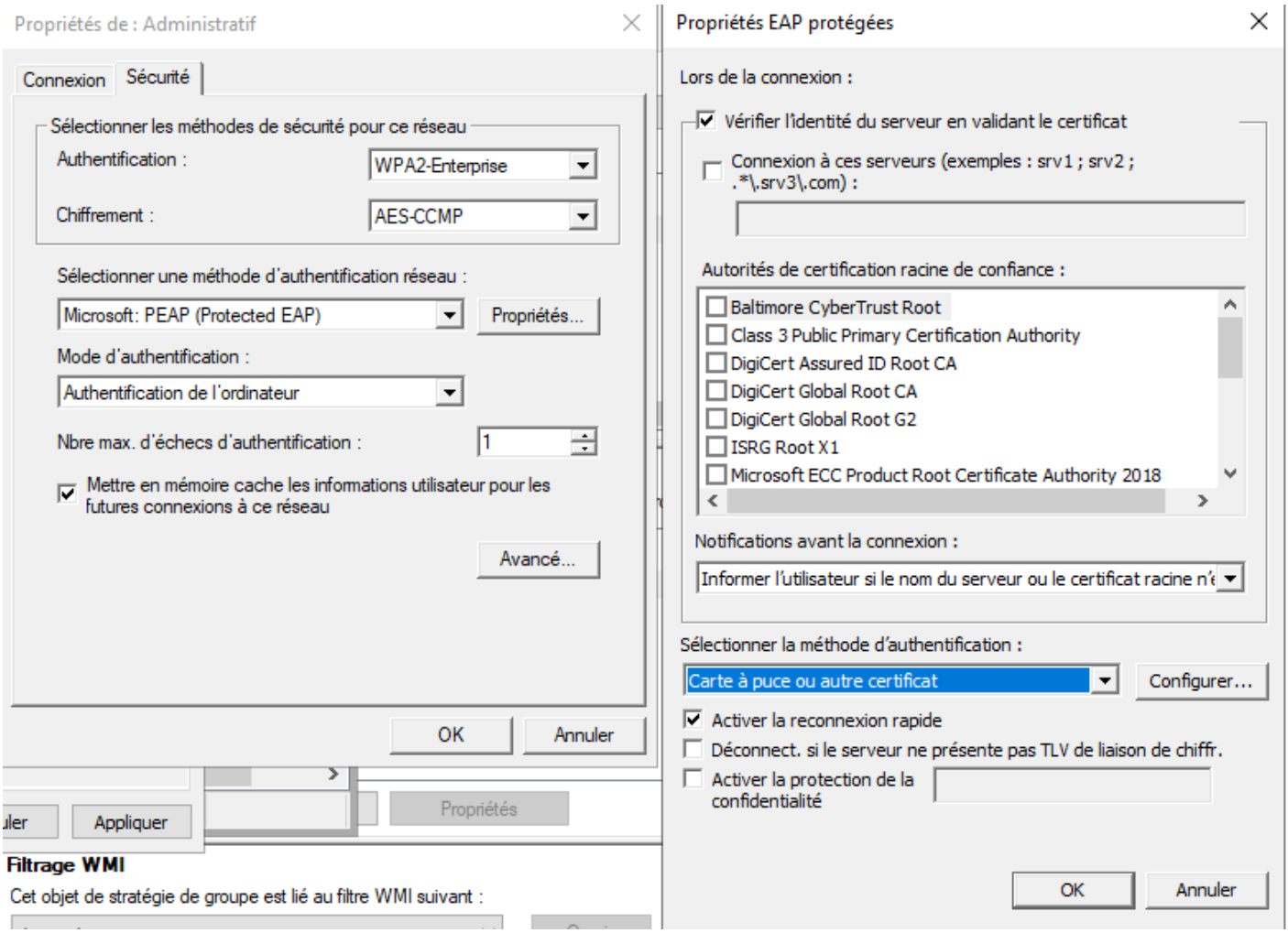
Sous "Configuration ordinateurs" > "Stratégies" > "Paramètres Windows" > "Paramètres de sécurité" > "Stratégies de réseau sans fil (IEEE 802.11)", on y crée une stratégie.

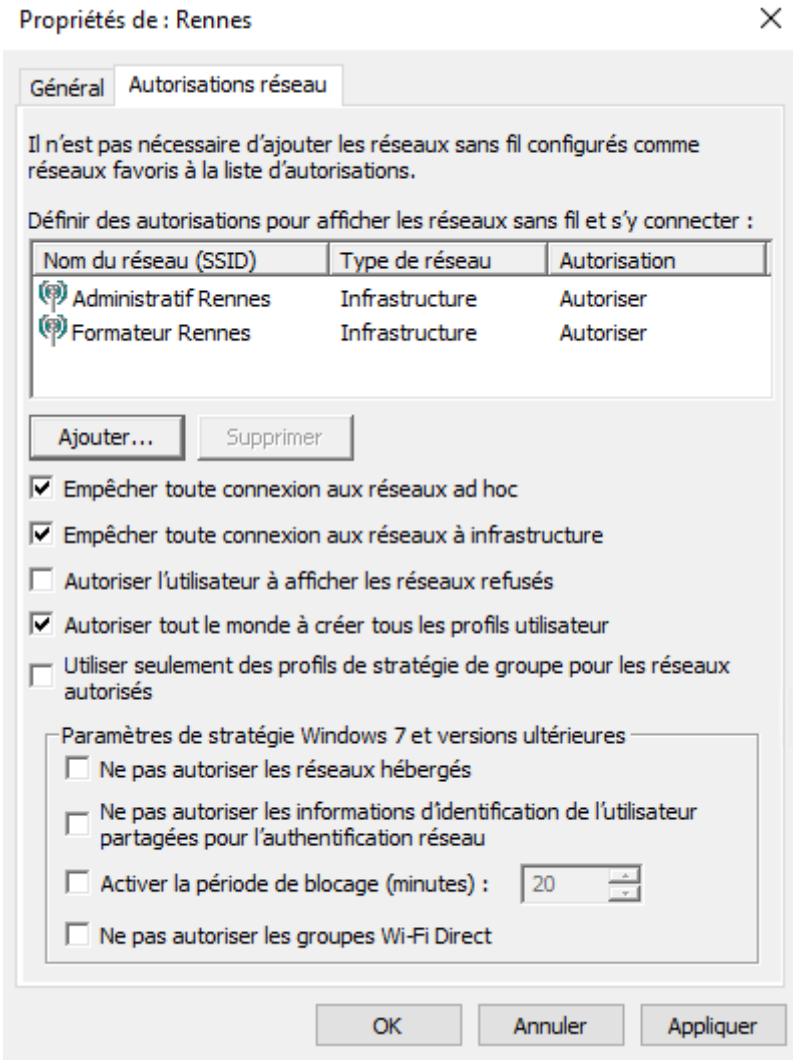
On ajoute nos réseaux wifi :





On choisit "Microsoft: PEAP (Protected EAP)" puis dans ses propriétés "Carte à puce ou autre certificat".


Propriétés de : Administratif
Connexion
Sécurité
Sélectionner les méthodes de sécurité pour ce réseau
Authentification :
WPA2-Enterprise
Chiffrement :
AES-CCMP
Sélectionner une méthode d'authentification réseau :
Microsoft: PEAP (Protected EAP)
Propriétés...
Mode d'authentification :
Authentification de l'ordinateur
Nbre max. d'échecs d'authentification :
1
Mettre en mémoire cache les informations utilisateur pour les futures connexions à ce réseau
Avancé...
OK
Annuler
Propriétés EAP protégées
Lors de la connexion :
Vérifier l'identité du serveur en validant le certificat
Connexion à ces serveurs (exemples : srv1 ; srv2 ; .*\.srv3\.com) :
Autorités de certification racine de confiance :
Baltimore CyberTrust Root
Class 3 Public Primary Certification Authority
DigiCert Assured ID Root CA
DigiCert Global Root CA
DigiCert Global Root G2
ISRG Root X1
Microsoft ECC Product Root Certificate Authority 2018
Notifications avant la connexion :
Informer l'utilisateur si le nom du serveur ou le certificat racine n'
Sélectionner la méthode d'authentification :
Carte à puce ou autre certificat
Configurer...
Activer la reconnexion rapide
Déconnect. si le serveur ne présente pas TLV de liaison de chiffr.
Activer la protection de la confidentialité
OK
Annuler
Appliquer
Propriétés
Filtrage WMI
Cet objet de stratégie de groupe est lié au filtre WMI suivant :


Propriétés de : Rennes
Général
Autorisations réseau
Il n'est pas nécessaire d'ajouter les réseaux sans fil configurés comme réseaux favoris à la liste d'autorisations.
Définir des autorisations pour afficher les réseaux sans fil et s'y connecter :
Nom du réseau (SSID)
Type de réseau
Autorisation
Administratif Rennes
Infrastructure
Autoriser
Formateur Rennes
Infrastructure
Autoriser
Ajouter...
Supprimer
Empêcher toute connexion aux réseaux ad hoc
Empêcher toute connexion aux réseaux à infrastructure
Autoriser l'utilisateur à afficher les réseaux refusés
Autoriser tout le monde à créer tous les profils utilisateur
Utiliser seulement des profils de stratégie de groupe pour les réseaux autorisés
Paramètres de stratégie Windows 7 et versions ultérieures
Ne pas autoriser les réseaux hébergés
Ne pas autoriser les informations d'identification de l'utilisateur partagées pour l'authentification réseau
Activer la période de blocage (minutes) :
20
Ne pas autoriser les groupes Wi-Fi Direct
OK
Annuler
Appliquer

Audit et sécurisation (hardening) d'AD CS

Il est important que notre PKI soit sécurisée. Il existe différents outils permettant de l'auditer : Certipy, Exegol, PSPKIAudit ou encore Locksmith.

Exemple de Certify et Certipy :

```
C:\>certify find /vulnerable


   _____          _   _  __
  / ____|        | | (_)/ _|
 | |     ___ _ __| |_ _| |_ _   _
 | |    / _ \ '__| __| |  _| | | |
 | |___|  __/ |  | |_| | | | |_| |
  \_____\___|_|   \__|_|_|  \__, |
                             __/ |
                            |___./
  v1.0.0

[*] Action: Find certificate templates
[*] Using the search base 'CN=Configuration,DC=ad,DC=khroners,DC=fr'

[*] Listing info about the Enterprise CA 'Khroners Labs Enterprise CA'

    Enterprise CA Name            : Khroners Labs Enterprise CA
    DNS Hostname                  : SRV-CA35-01.ad.khroners.fr
    FullName                      : SRV-CA35-01.ad.khroners.fr\Khroners Labs Enterprise CA
    Flags                         : SUPPORTS_NT_AUTHENTICATION, CA_SERVERTYPE_ADVANCED
    Cert SubjectName              : CN=Khroners Labs Enterprise CA, DC=ad, DC=khroners, DC=fr
    Cert Thumbprint               : 8FD1AEAF57EE974EB726D884775133B4D4C9D270
    Cert Serial                   : 1500000004A03185E3D30CA7C3000000000004
    Cert Start Date               : 02/10/2023 08:09:54
    Cert End Date                 : 02/10/2028 08:19:54
    Cert Chain                    : CN=KhronersLabsCertificateAuthority ->
```

```
CN=KhronersLabsEnterpriseCA,DC=ad,DC=khroners,DC=fr
    UserSpecifiedSAN              : Disabled
    CA Permissions                :
      Owner: BUILTIN\Administrateurs       S-1-5-32-544

      Access Rights                                       Principal

      Allow  Enroll                                       AUTORITE NT\Utilisateurs
authentifiésS-1-5-11
      Allow  ManageCA, ManageCertificates                 BUILTIN\Administrateurs       S-1-5-
32-544
      Allow  ManageCA, ManageCertificates                 AD\Admins du domaine          S-1-5-
21-1812995439-3560927909-1751902240-512
      Allow  ManageCA, ManageCertificates                 AD\Administrateurs de l'entrepriseS-1-
5-21-1812995439-3560927909-1751902240-519
    Enrollment Agent Restrictions : None

[+] No Vulnerable Certificates Templates found!



Certify completed in 00:00:00.5455163
```

```
certipy find -u gilles.besson@ad.khroners.fr -password Password -scheme ldap

Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Finding certificate templates
[*] Found 36 certificate templates
[*] Finding certificate authorities
[*] Found 1 certificate authority
[*] Found 14 enabled certificate templates
[*] Trying to get CA configuration for 'Khroners Labs Enterprise CA' via CSRA
[!] Got error while trying to get CA configuration for 'Khroners Labs Enterprise CA' via CSRA:
CASessionError: code: 0x80070005 - E_ACCESSDENIED - General access denied error.
[*] Trying to get CA configuration for 'Khroners Labs Enterprise CA' via RRP
[!] Failed to connect to remote registry. Service should be starting now. Trying again...
[*] Got CA configuration for 'Khroners Labs Enterprise CA'
[*] Saved BloodHound data to '20231007001536_Certipy.zip'. Drag and drop the file into the
BloodHound GUI from @ly4k
```

```
[*] Saved text output to '20231007001536_Certipy.txt'
[*] Saved JSON output to '20231007001536_Certipy.json'
```

3 fichiers sont ensuite générés. On peut analyser nous même le txt ou importer dans BloodHound GUI le .zip.