STADIUMCOMPANY

Mission 6

Mise en place du Wi-Fi
pour les employés et les visiteurs

Authentification RADIUS / 802.1X

Projet	StadiumCompany - Infrastructure Réseau
Formation	BTS SIO option SISR - IRIS Paris
Année scolaire	2025 - 2026
Épreuve	E5 - Support et mise à disposition des services informatiques
Réalisation	Laurent HUSTIN, Ibrahim HAIDARA et Marcel OUTOU LASM

Sommaire

1. Introduction et contexte

Le stade de StadiumCompany accueille quotidiennement des employés permanents, des partenaires commerciaux et des visiteurs (supporters, journalistes, personnel VIP). Chacun de ces publics a besoin d'un accès Wi-Fi adapté à son niveau d'autorisation : les employés doivent pouvoir accéder au réseau interne de l'entreprise et à ses ressources (partages, applications métier, imprimantes), tandis que les visiteurs doivent disposer d'un accès limité à Internet uniquement, sans possibilité d'atteindre le réseau interne.

La direction de StadiumCompany impose une authentification sécurisée pour les salariés basée sur le standard WPA2/WPA3 Enterprise avec un serveur RADIUS. Ce mécanisme permet de vérifier l'identité de chaque utilisateur via son compte Active Directory avant de lui accorder l'accès au réseau Wi-Fi.

> **Objectif de la mission :** Mettre en place une solution Wi-Fi professionnelle avec deux réseaux distincts : un SSID "Employés" authentifié via RADIUS/802.1X relié au réseau interne, et un SSID "Visiteurs" isolé avec portail captif donnant accès uniquement à Internet. Le serveur RADIUS (NPS) s'appuie sur l'Active Directory et une infrastructure PKI (certificats) pour sécuriser l'authentification.

Le protocole RADIUS et le standard 802.1X

Le protocole **RADIUS** (Remote Authentication Dial-In User Service) est un protocole d'authentification, d'autorisation et de comptabilité (AAA). Dans le contexte Wi-Fi, il permet au point d'accès (qui agit comme client RADIUS) de déléguer la vérification des identifiants à un serveur centralisé. Le standard **IEEE 802.1X** définit le cadre d'authentification au niveau de la couche liaison, en utilisant le protocole EAP (Extensible Authentication Protocol).

Étape	Acteur	Action
1	Supplicant (PC/Mobile)	Demande de connexion au Wi-Fi
2	Authenticator (Borne Wi-Fi)	Transmet la demande au serveur RADIUS
3	Serveur RADIUS (NPS)	Vérifie les identifiants dans Active Directory
4	Active Directory	Confirme ou refuse l'identité de l'utilisateur
5	Serveur RADIUS (NPS)	Envoie Access-Accept ou Access-Reject
6	Authenticator (Borne Wi-Fi)	Autorise ou refuse la connexion

2. Architecture Wi-Fi de StadiumCompany

L'architecture Wi-Fi de StadiumCompany repose sur la séparation des flux via les VLAN existants et l'utilisation de deux SSID distincts. Le tableau ci-dessous synthétise la configuration cible.

Paramètre	SSID Employés	SSID Visiteurs
Nom du réseau	StadiumCompany-Corp	StadiumCompany-Guest
VLAN associé	VLAN WiFi - 172.20.3.0/24	VLAN DMZ - 172.20.4.0/24
Sécurité	WPA2 Enterprise (802.1X)	Portail captif / WPA2 PSK
Authentification	RADIUS via NPS + AD	Code d'accès temporaire
Accès réseau	Réseau interne + Internet	Internet uniquement
Isolement	Non	Oui (isolé du LAN)

Composant	Rôle	Adresse IP
Serveur AD / DNS / NPS	Contrôleur de domaine + RADIUS	172.20.1.14
Point d'accès Wi-Fi	Client RADIUS / Authenticator	172.20.3.5
pfSense (heimdall)	Pare-feu / Routeur inter-VLAN	172.20.1.250
Domaine AD	stadiumcompany.local	-

Prérequis : Avant de configurer le Wi-Fi avec authentification RADIUS, les éléments suivants doivent être en place : Active Directory opérationnel (Mission 2), serveur DNS fonctionnel, infrastructure réseau avec VLAN (Mission 1), et pare-feu pfSense configuré (Mission 5).

3. Installation de l'autorité de certification (AD CS)

L'authentification 802.1X avec la méthode PEAP (Protected EAP) nécessite un certificat numérique sur le serveur RADIUS. Ce certificat est émis par une autorité de certification (CA) interne intégrée à Active Directory. La première étape consiste donc à installer le rôle **Services de certificats Active Directory (AD CS)** sur le serveur.

3.1 Ajout du rôle Services de certificats AD

Depuis le Gestionnaire de serveur, le rôle "Services de certificats Active Directory" est ajouté via l'assistant d'ajout de rôles et fonctionnalités. Ce rôle permettra au serveur de fonctionner comme autorité de certification d'entreprise, émettant des certificats pour les services internes de StadiumCompany.

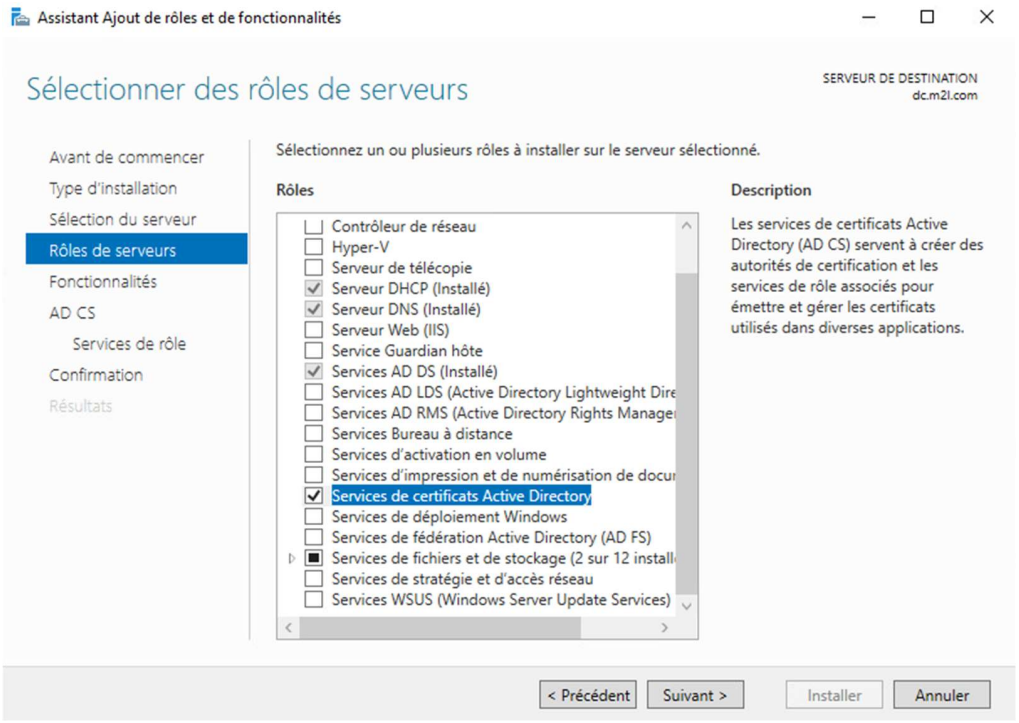

Figure 1 - Sélection du rôle Services de certificats Active Directory

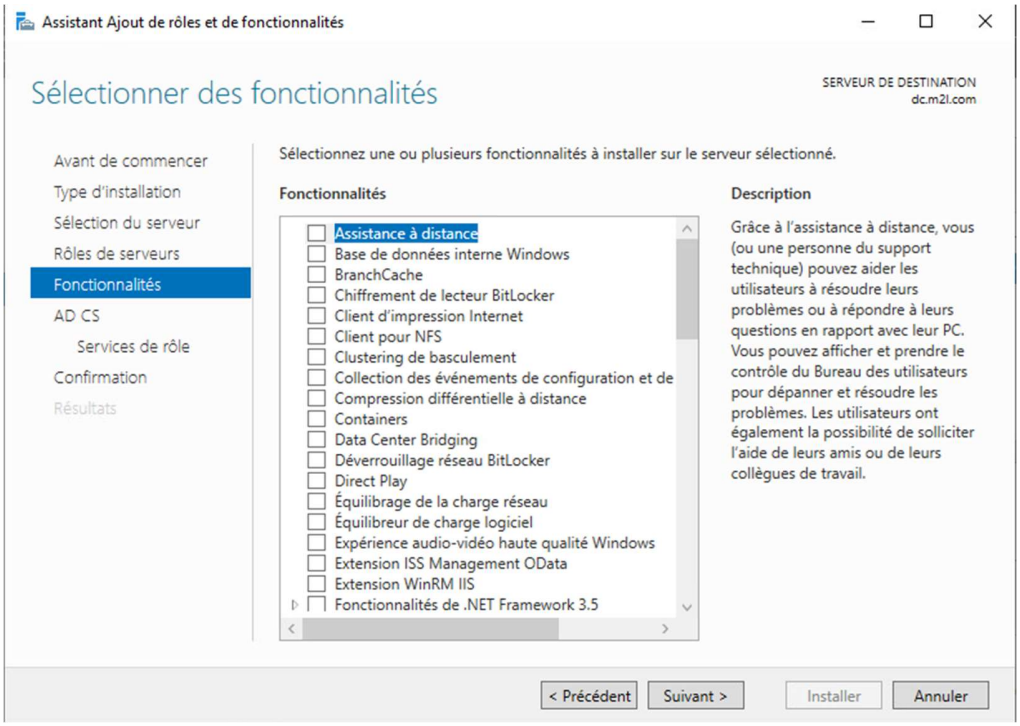

Figure 2 - Sélection des fonctionnalités complémentaires

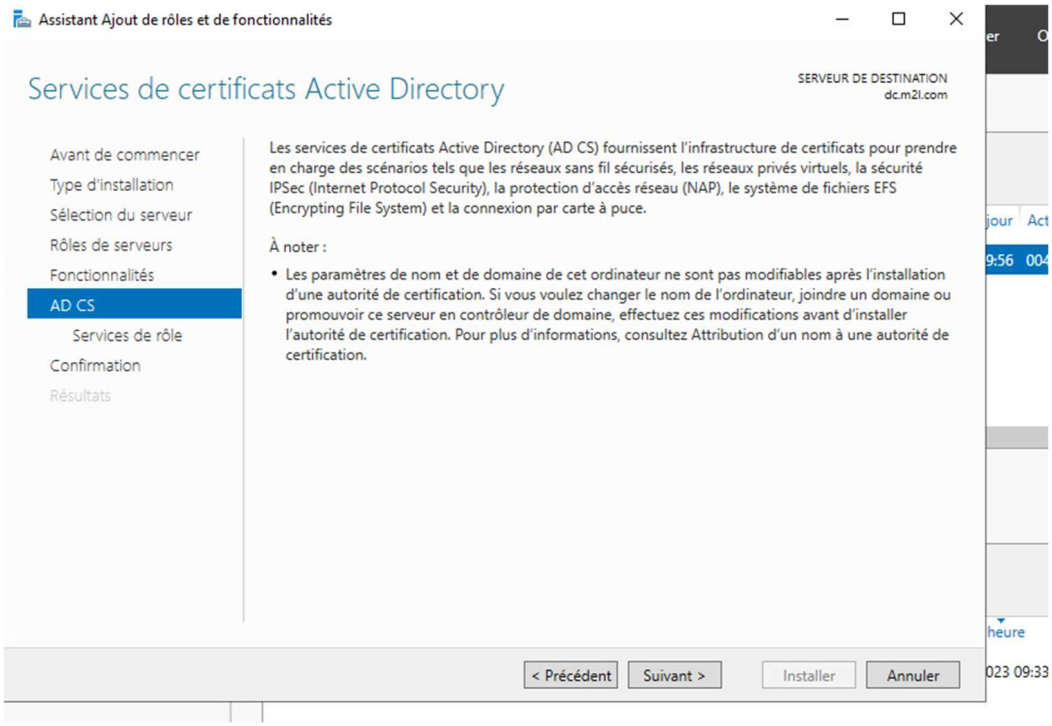

Figure 3 - Description des Services de certificats AD et avertissements

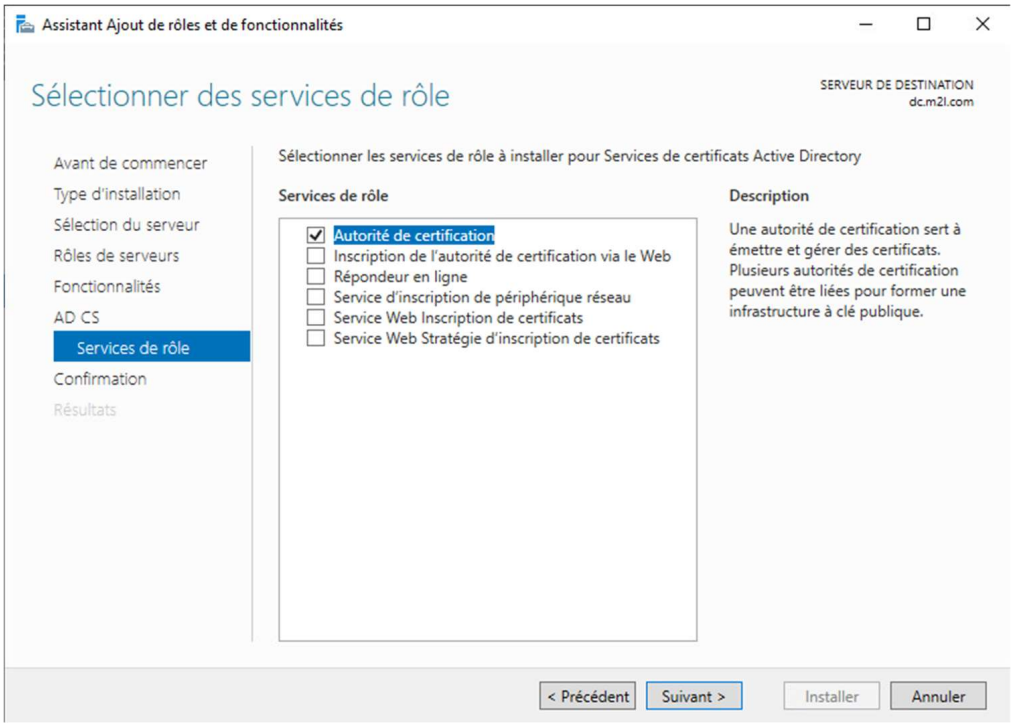

Figure 4 - Sélection du service Autorité de certification

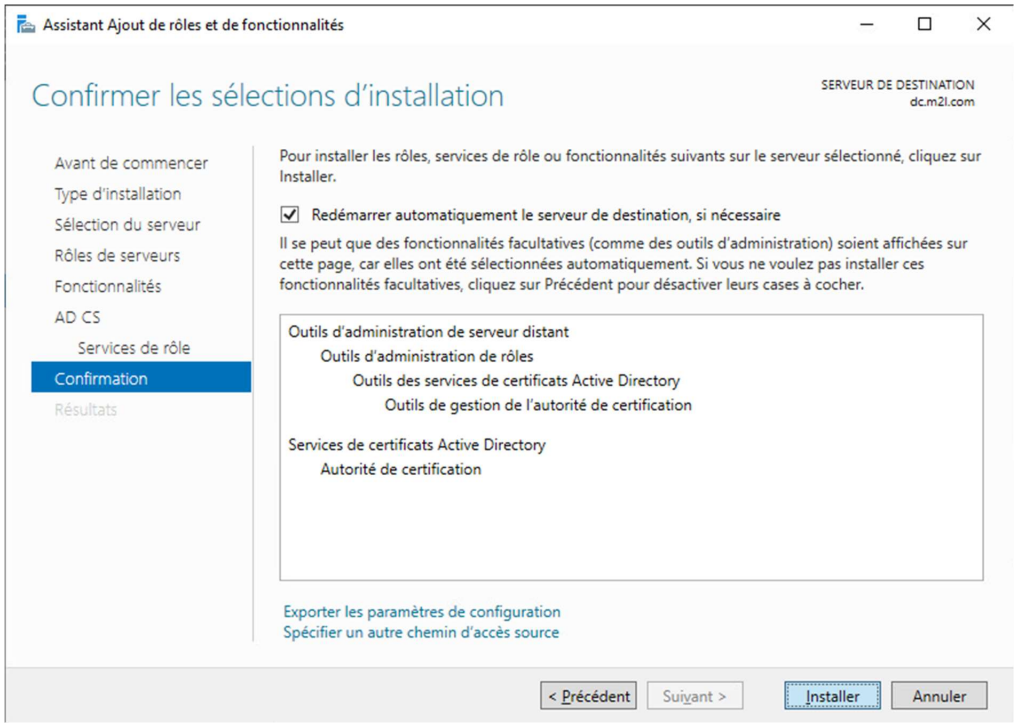

Figure 5 - Confirmation des rôles à installer

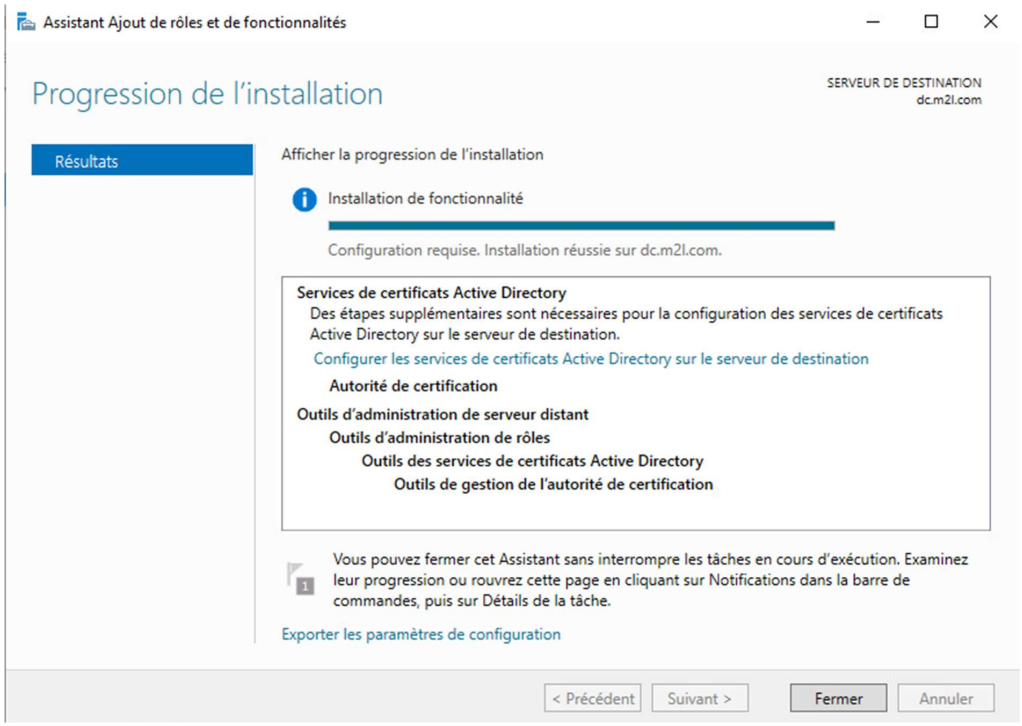

Figure 6 - Progression et résultat de l'installation (réussie)

3.2 Configuration de l'autorité de certification

Après l'installation du rôle, il est nécessaire de configurer l'autorité de certification. L'assistant de configuration post-déploiement guide l'administrateur à travers les étapes de paramétrage : type de CA, algorithme de chiffrement, nom, période de validité et emplacement de la base de données.

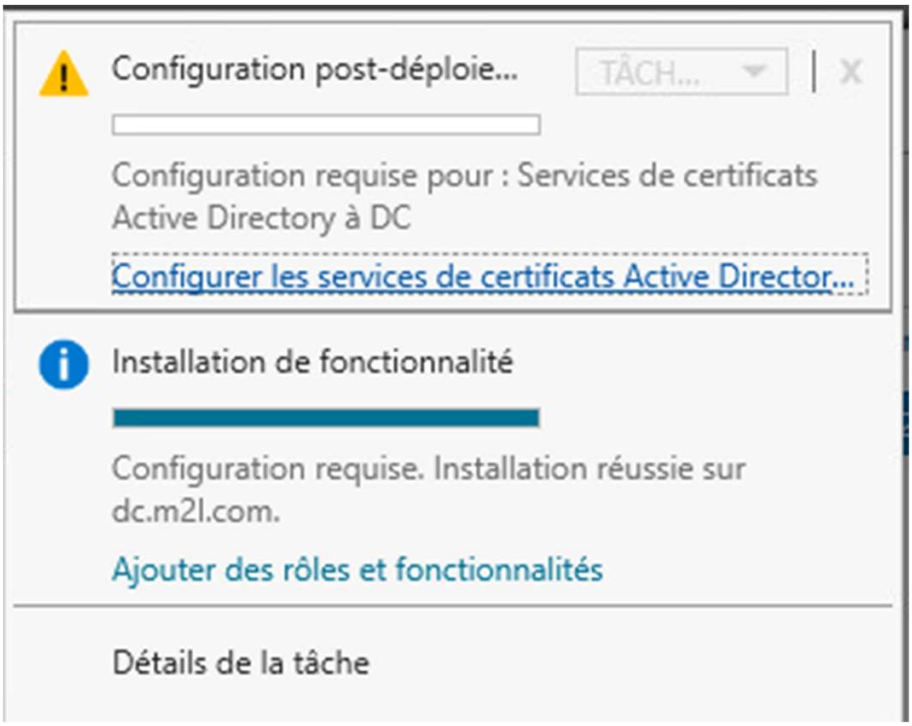

Figure 7 - Notification de configuration post-déploiement

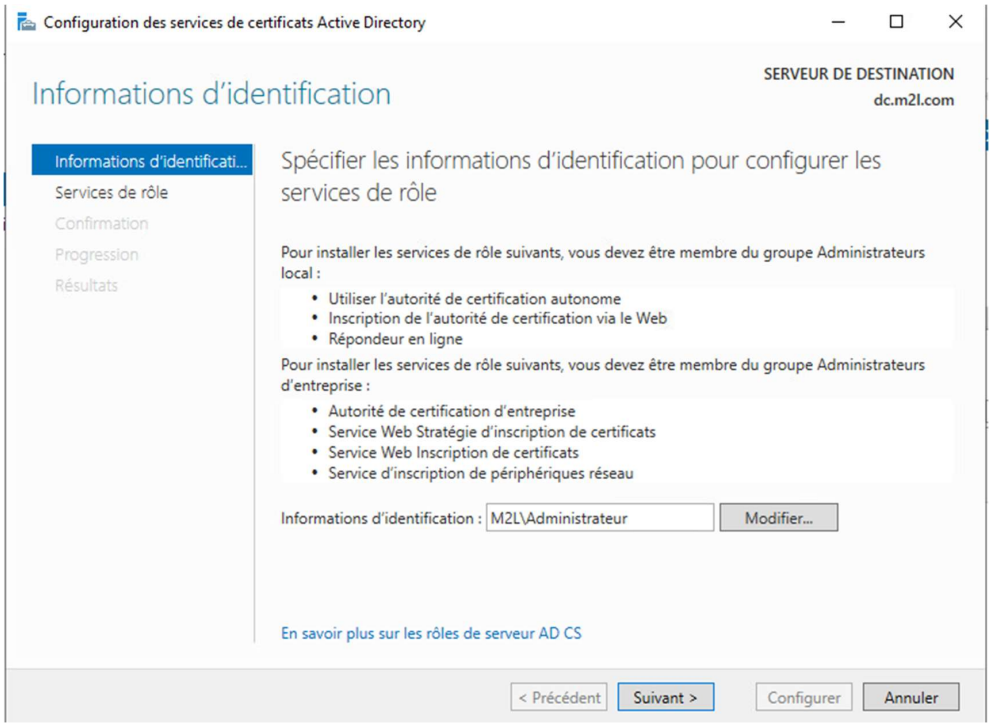

Figure 8 - Informations d'identification de l'administrateur

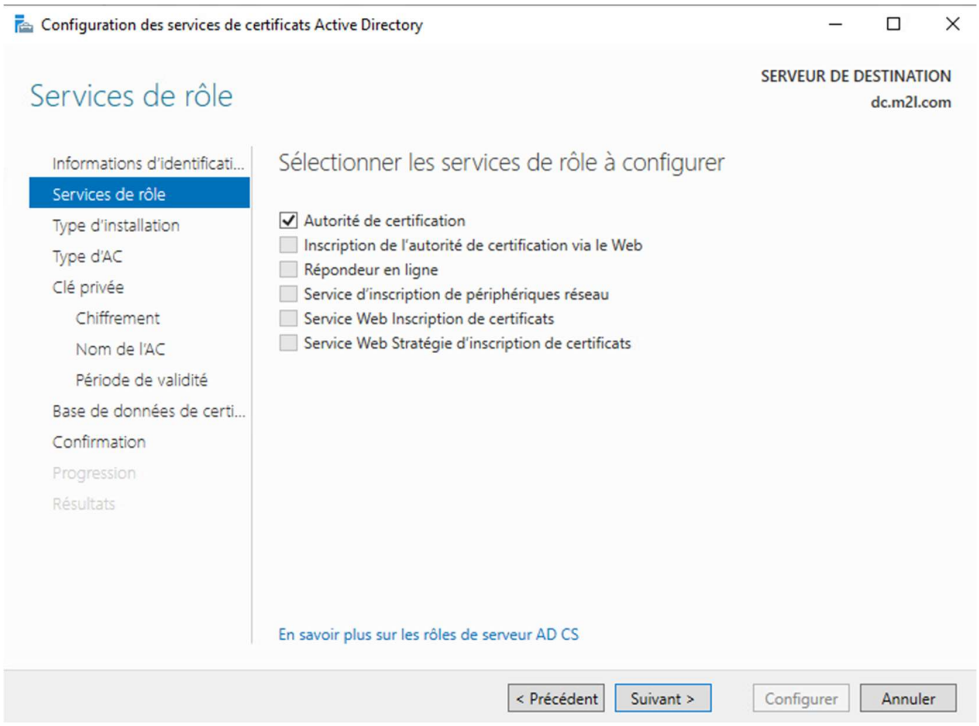

Figure 9 - Sélection du service Autorité de certification à configurer

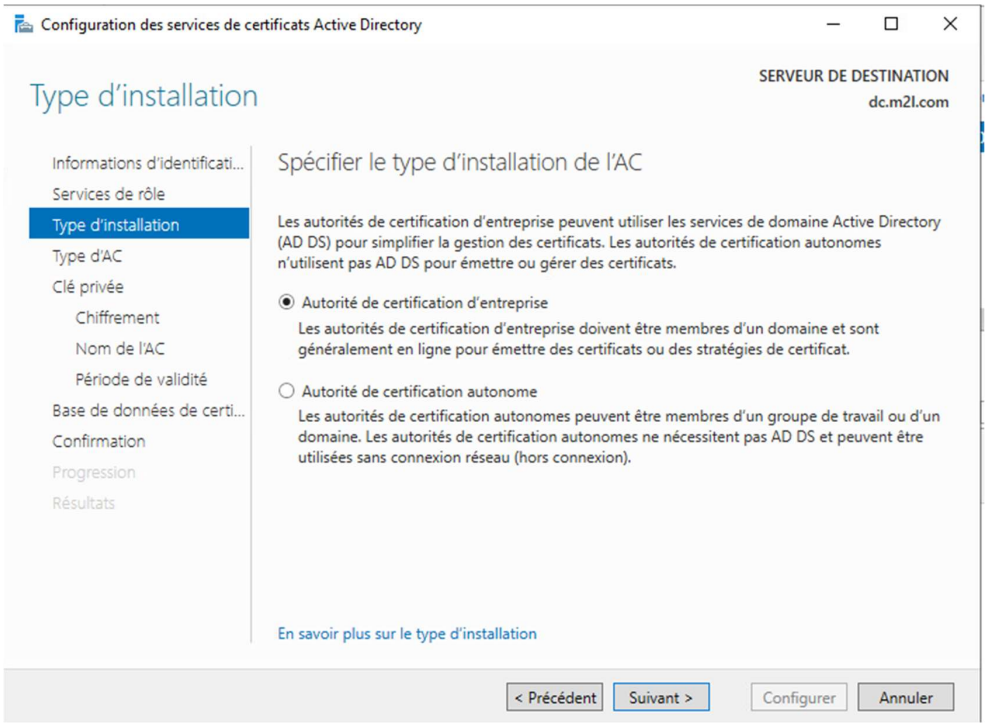

Figure 10 - Type d'installation : Autorité de certification d'entreprise

Le type **Autorité de certification d'entreprise** est sélectionné car le serveur est intégré au domaine Active Directory stadiumcompany.local. Ce type de CA utilise AD DS pour la gestion des certificats et l'inscription automatique.

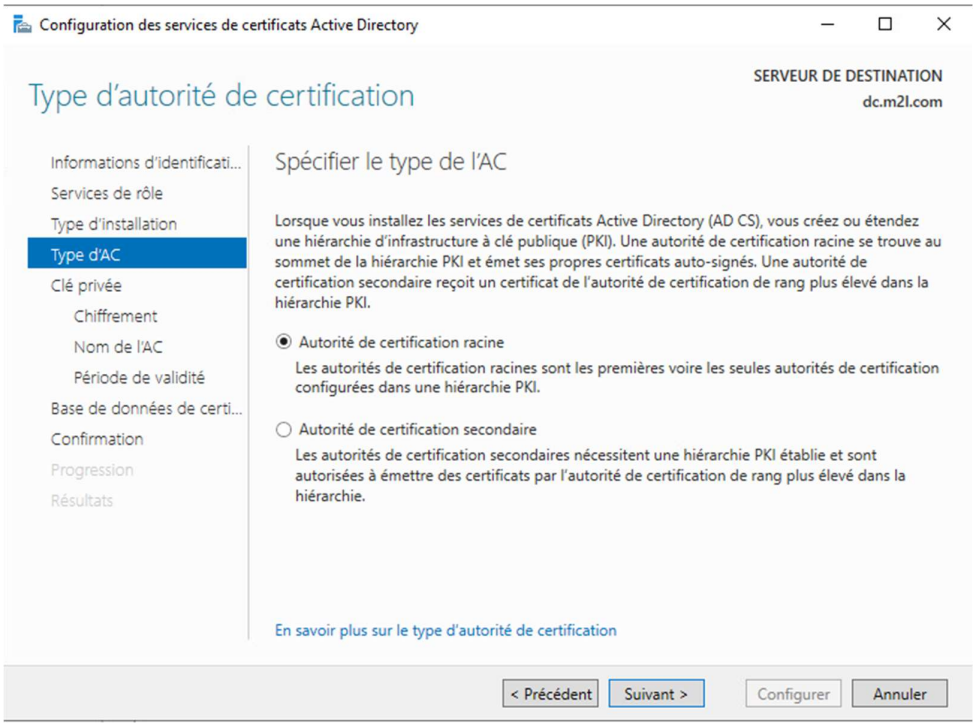

Figure 11 - Type d'AC : Autorité de certification racine

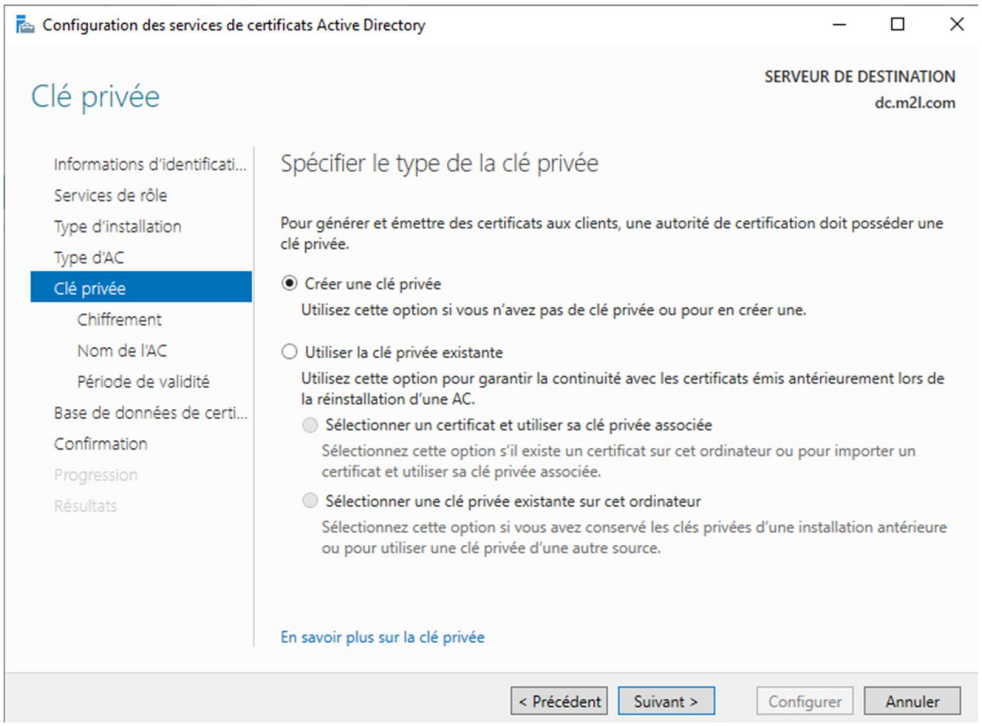

Figure 12 - Création d'une nouvelle clé privée pour la CA

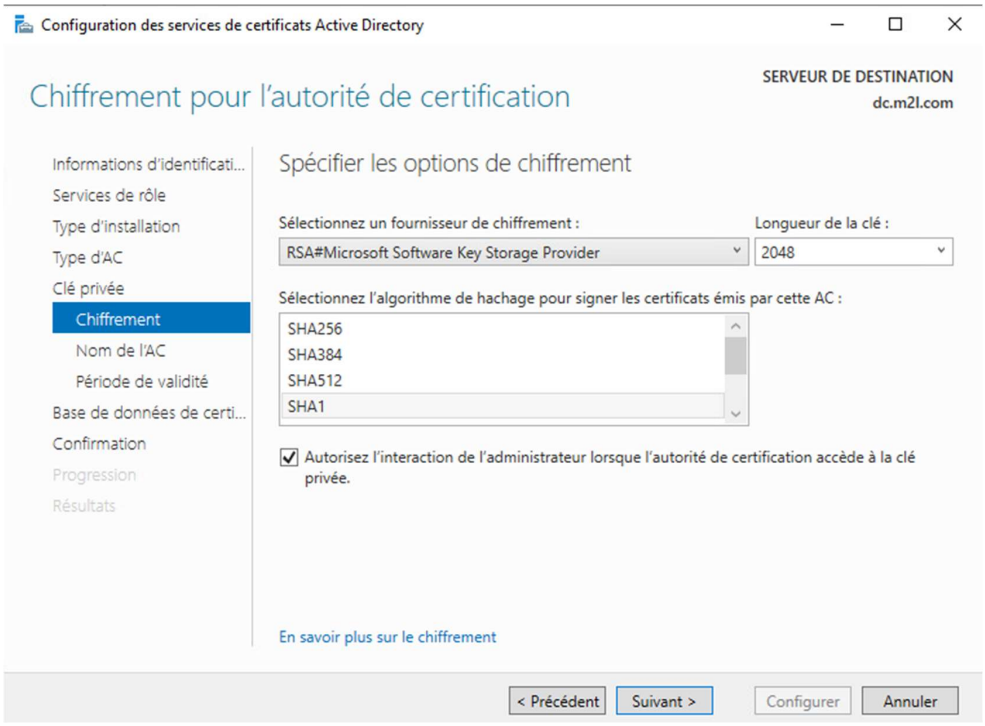

Figure 13 - Algorithme de chiffrement : RSA 2048 bits, SHA1

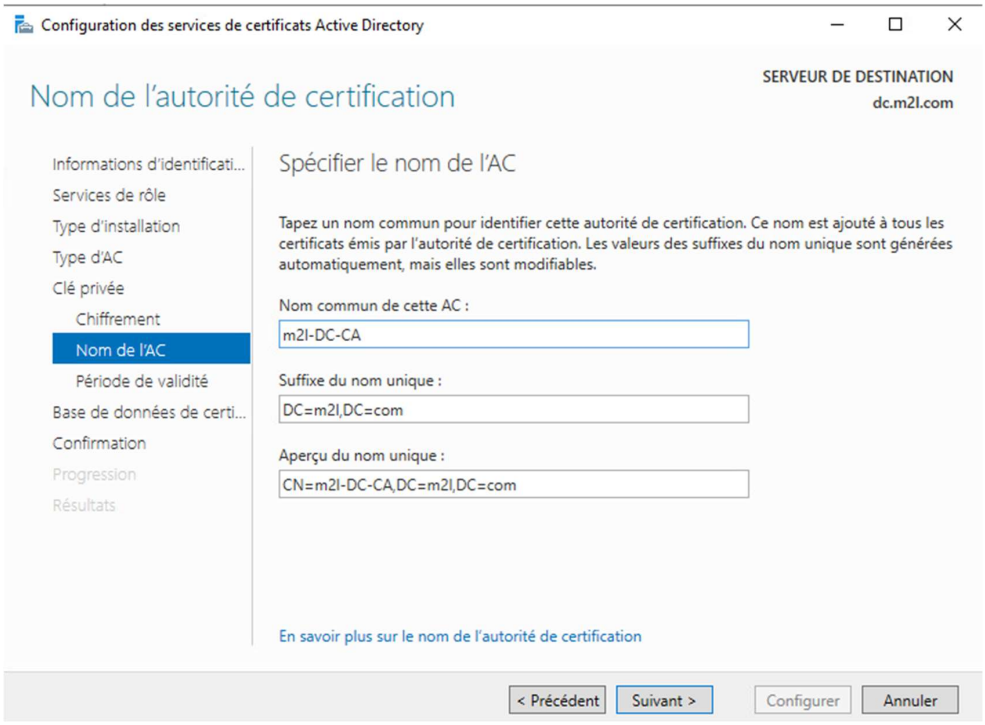

Figure 14 - Nom de l'autorité de certification (stadiumcompany-DC-CA)

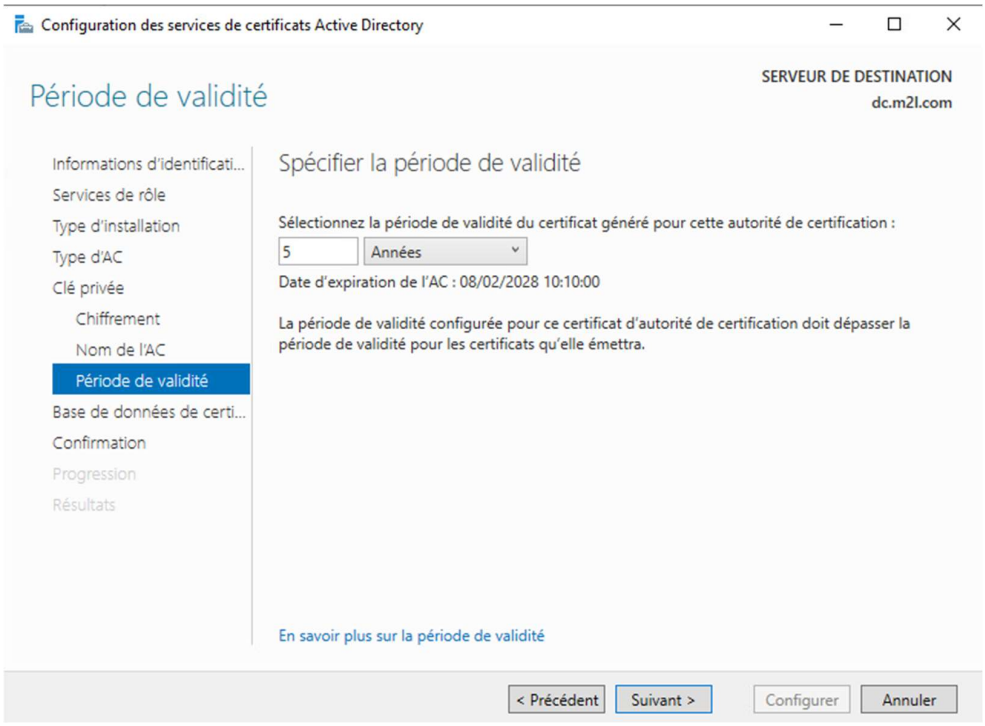

Figure 15 - Période de validité du certificat CA : 5 ans

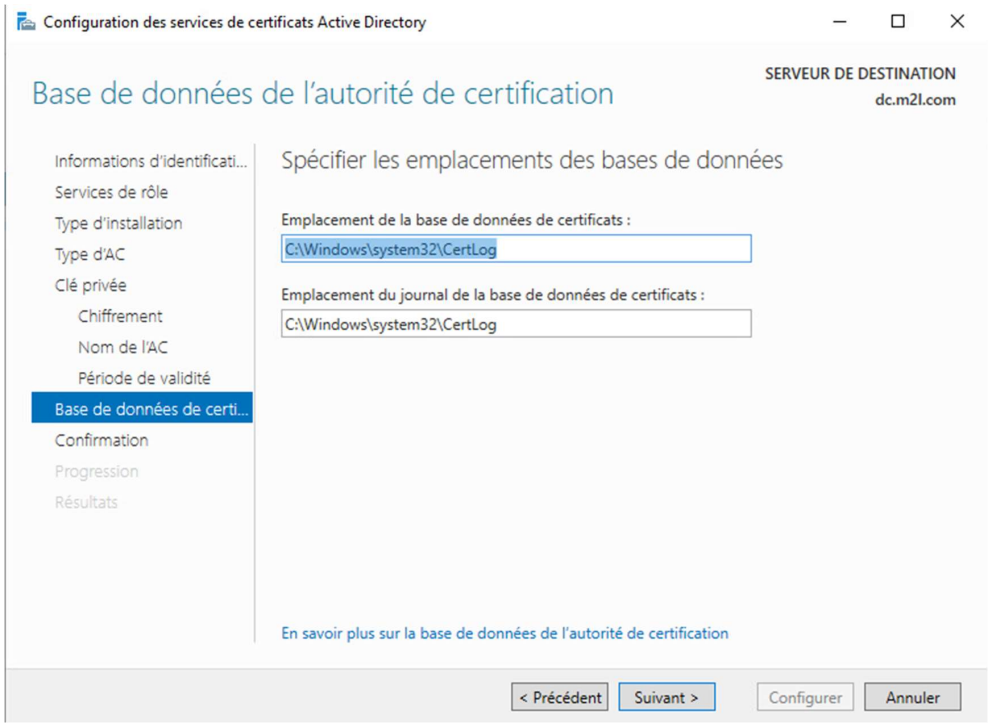

Figure 16 - Emplacement de la base de données des certificats

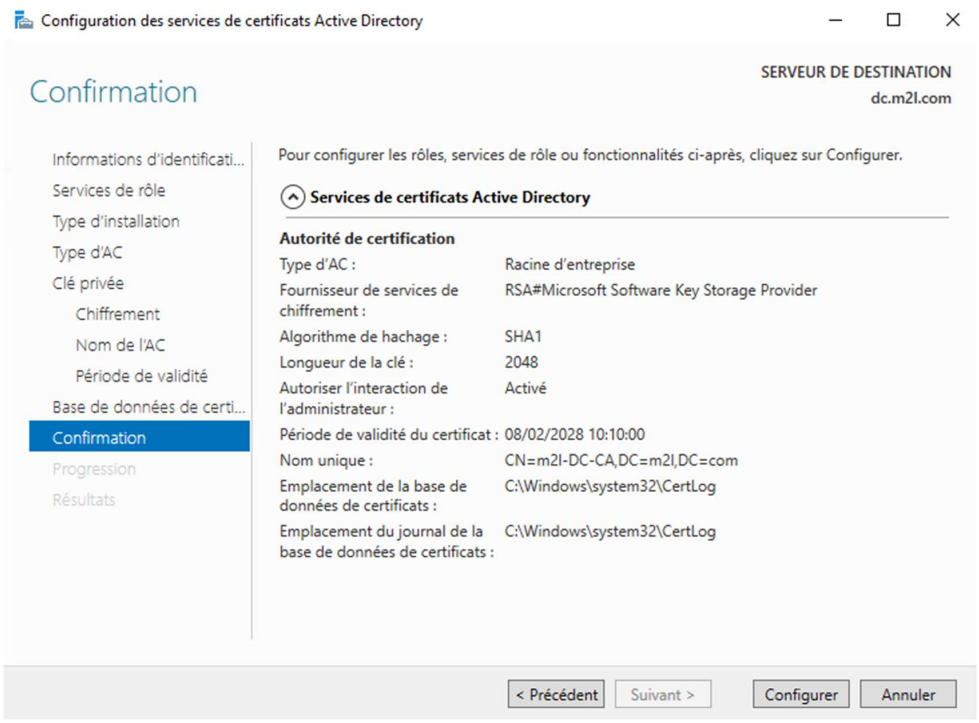

Figure 17 - Récapitulatif de la configuration avant validation

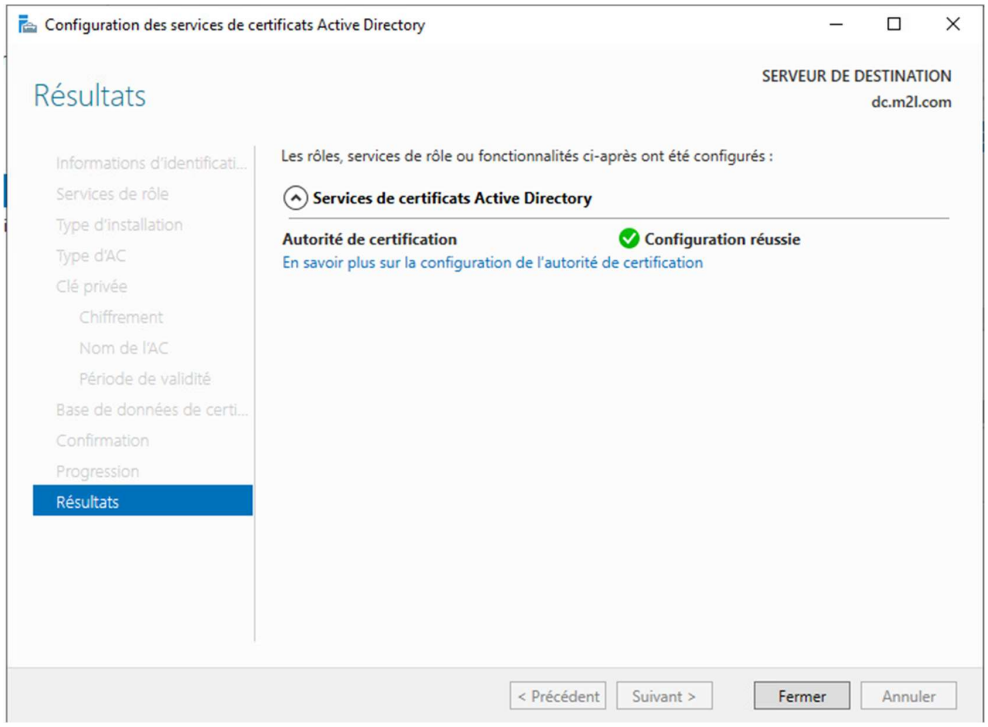

Figure 18 - Configuration réussie de l'autorité de certification

3.3 Inscription du certificat du contrôleur de domaine

Le serveur RADIUS (NPS) a besoin d'un certificat valide pour établir le tunnel TLS avec les clients lors de l'authentification PEAP. Il faut donc inscrire un certificat de type "Contrôleur de domaine" via la console MMC Certificats.

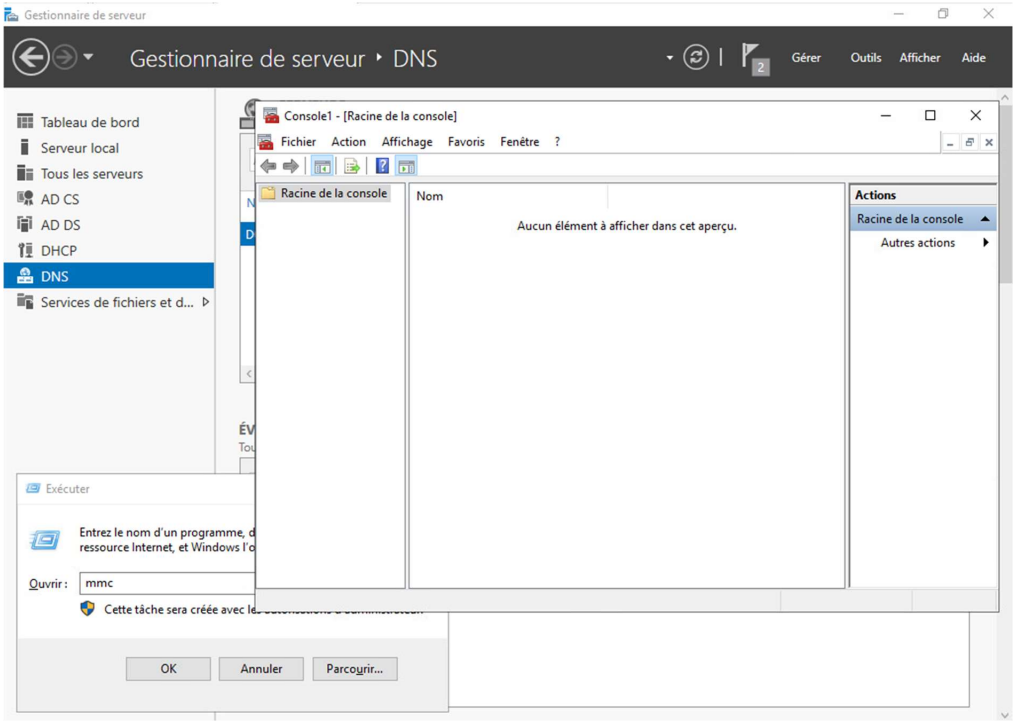

Figure 19 - Ouverture de la console MMC et ajout du composant Certificats

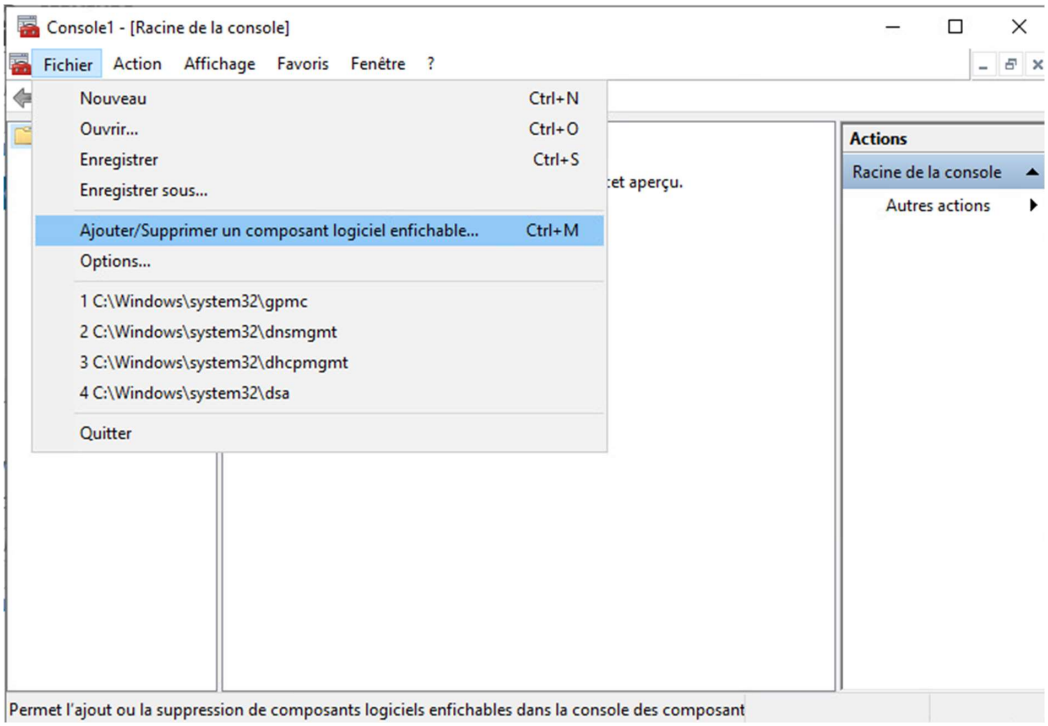

Figure 20 - Menu Fichier > Ajouter un composant logiciel enfichable

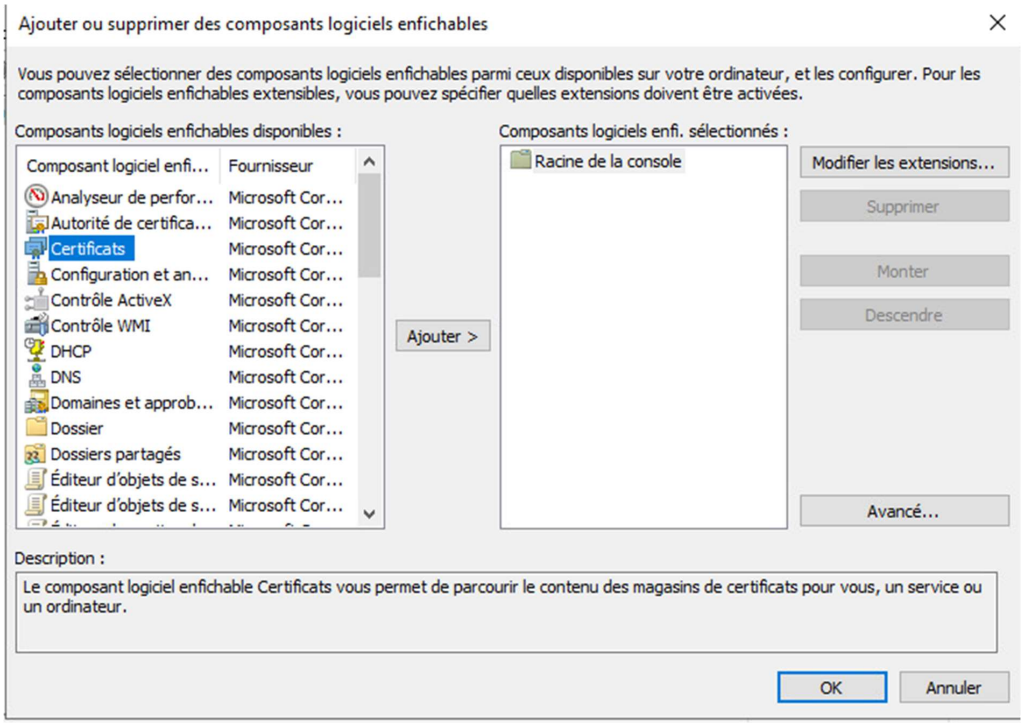

Figure 21 - Sélection du composant Certificats

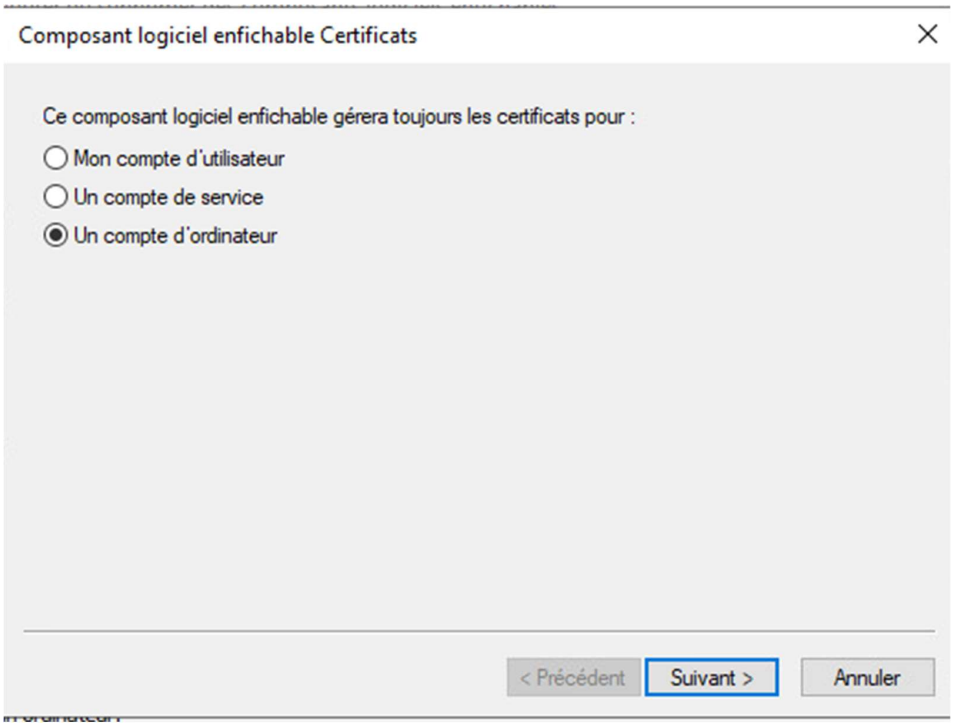

Figure 22 - Gestion des certificats pour un compte d'ordinateur

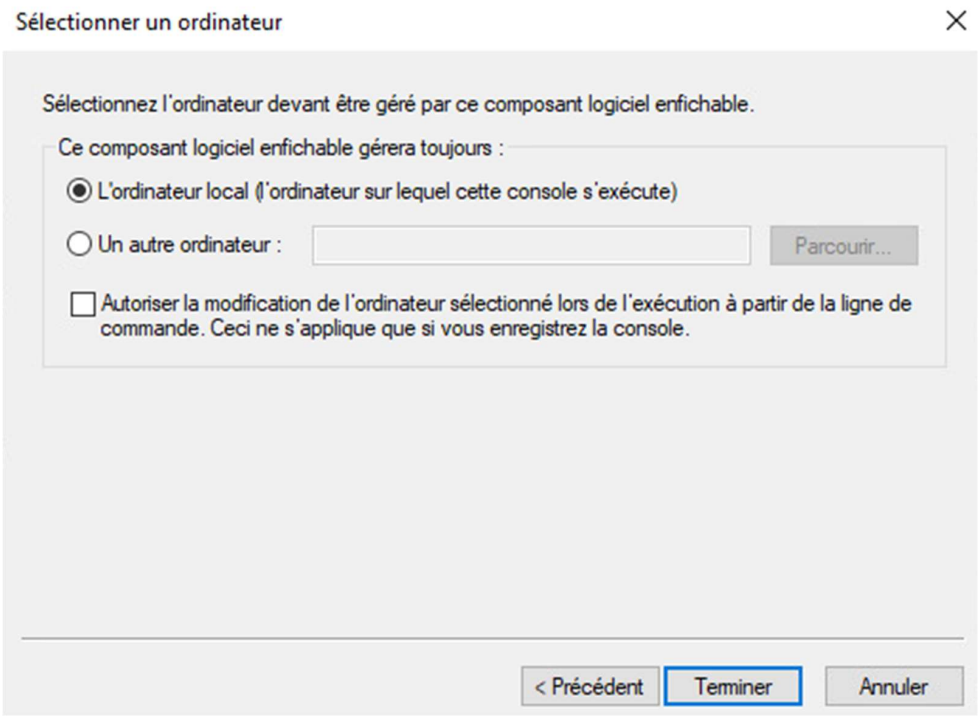

Figure 23 - Sélection de l'ordinateur local

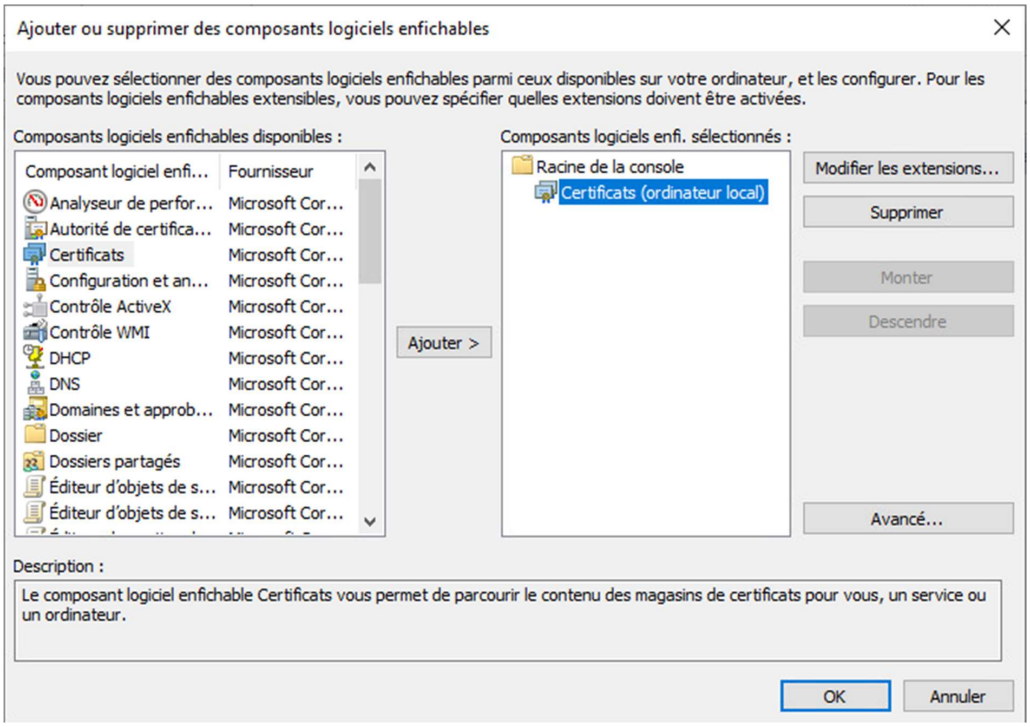

Figure 24 - Composant Certificats ajouté à la console

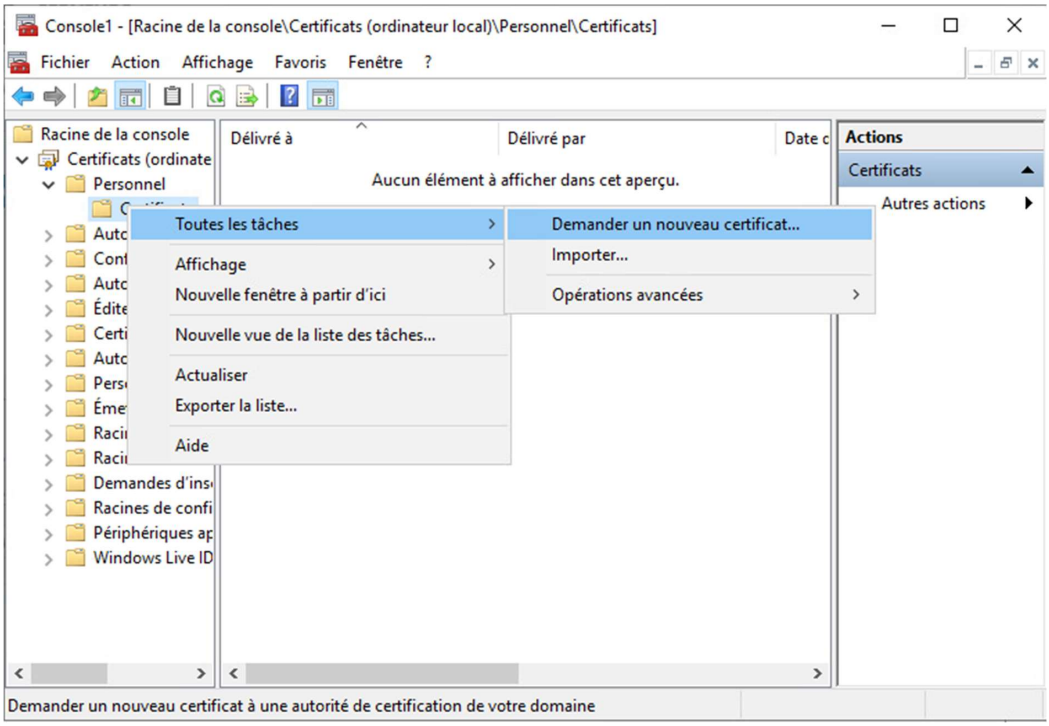

Figure 25 - Demande d'un nouveau certificat dans le magasin Personnel

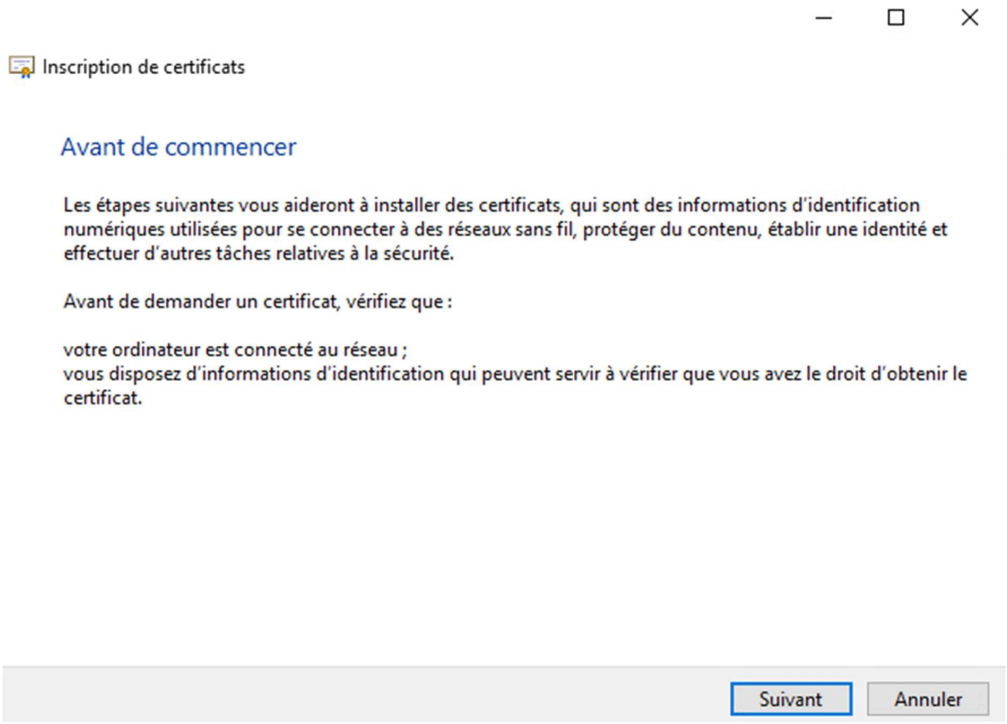

Figure 26 - Assistant d'inscription de certificats - Introduction

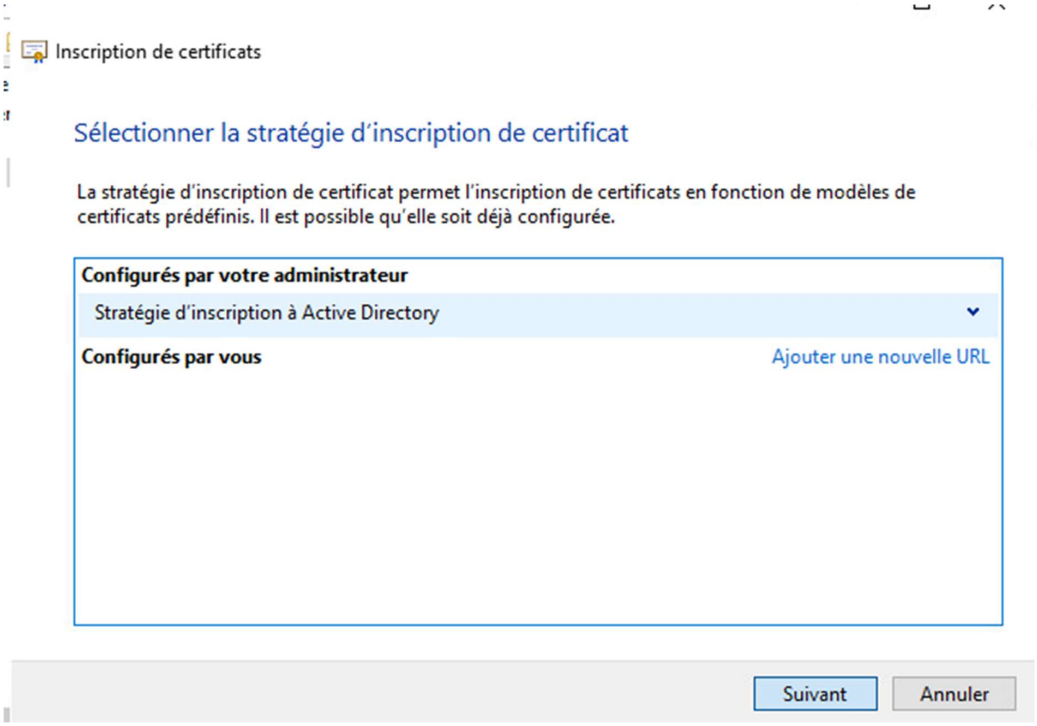

Figure 27 - Stratégie d'inscription à Active Directory

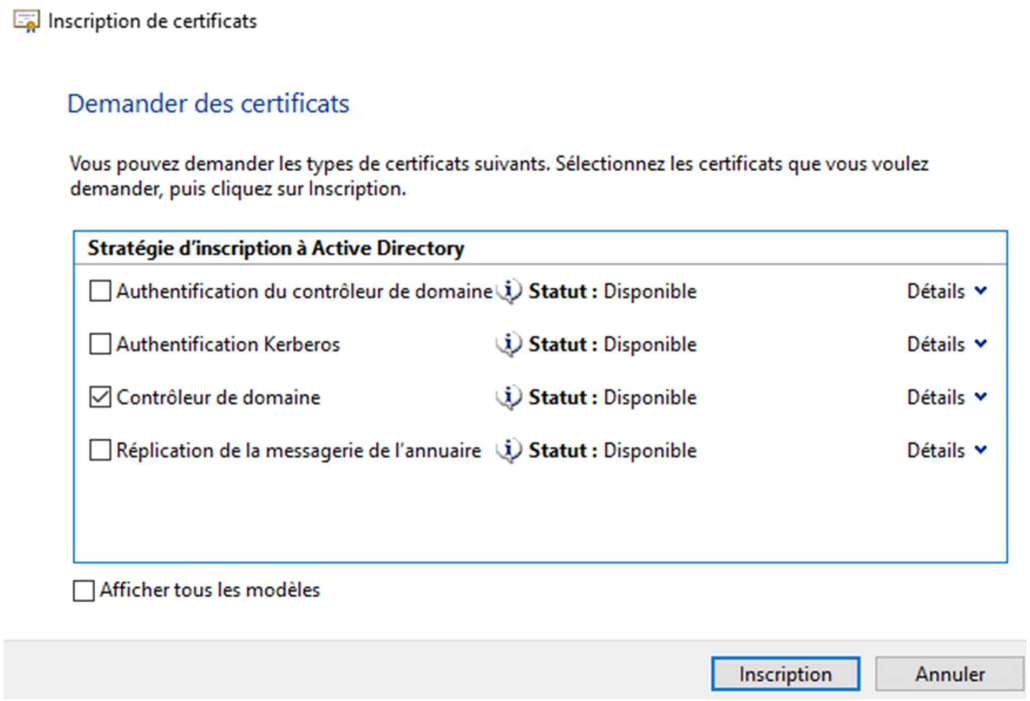

Figure 28 - Sélection du modèle "Contrôleur de domaine" puis Inscription

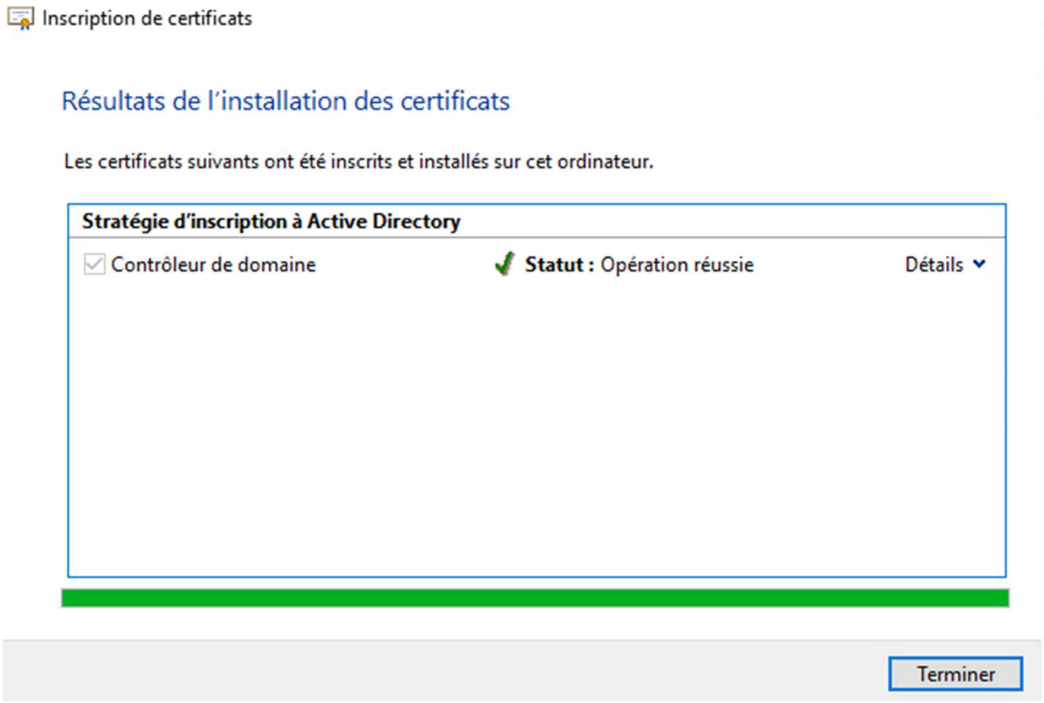

Figure 29 - Résultat : certificat de contrôleur de domaine installé avec succès

Figure 30 - Le certificat apparaît dans le magasin Personnel du serveur

Le certificat de contrôleur de domaine est maintenant installé. Il sera utilisé par le serveur NPS pour prouver son identité auprès des clients Wi-Fi lors de l'établissement du tunnel TLS dans le protocole PEAP.

4. Installation et configuration du serveur NPS (RADIUS)

Le serveur NPS (Network Policy Server) est l'implémentation Microsoft du protocole RADIUS. Il permet de centraliser l'authentification, l'autorisation et la comptabilité des connexions réseau. Dans notre cas, NPS authentifiera les employés de StadiumCompany qui se connectent au Wi-Fi via leurs identifiants Active Directory.

4.1 Ajout du rôle NPS

Le rôle "Services de stratégie et d'accès réseau" est ajouté depuis le Gestionnaire de serveur. Ce rôle inclut le serveur NPS qui servira de serveur RADIUS.

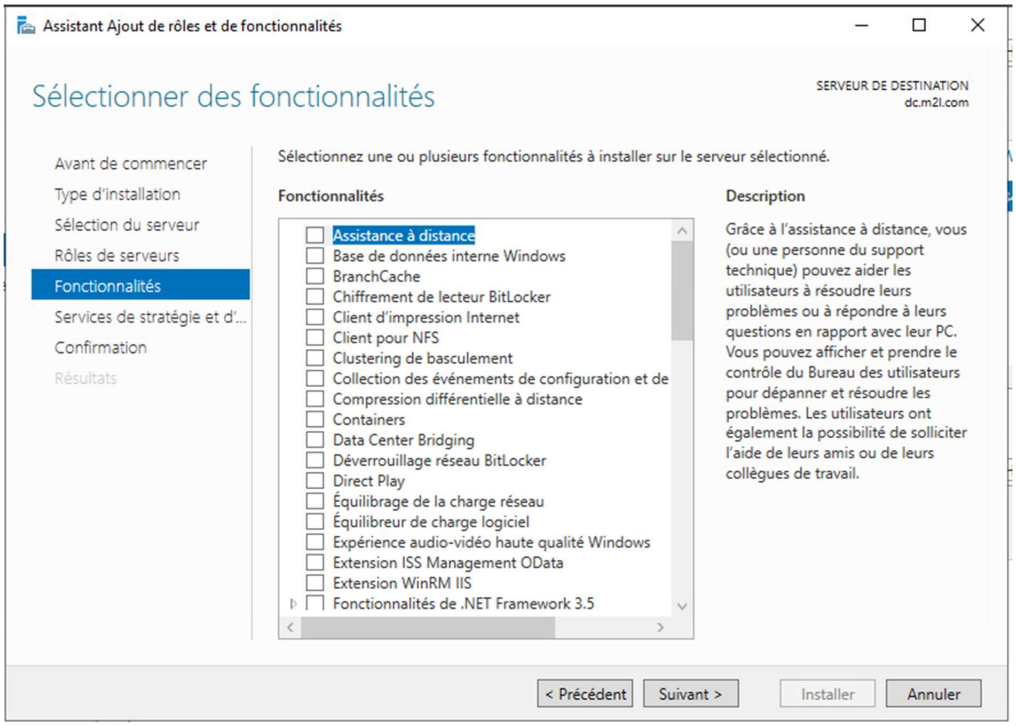

Figure 31 - Sélection du rôle Services de stratégie et d'accès réseau

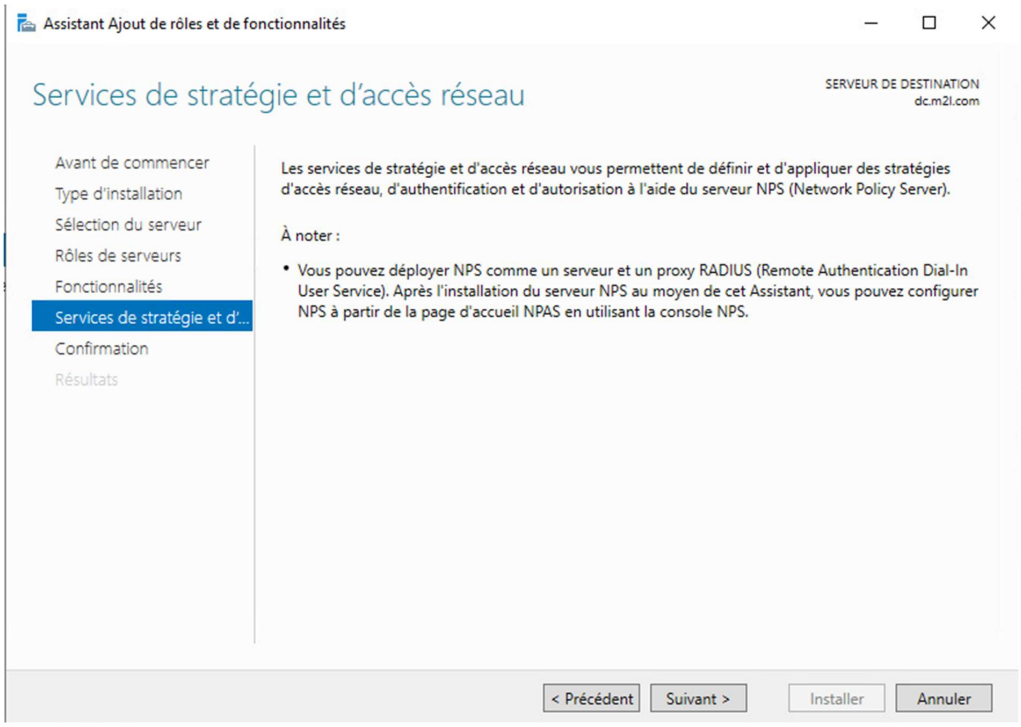

Figure 32 - Sélection des fonctionnalités complémentaires

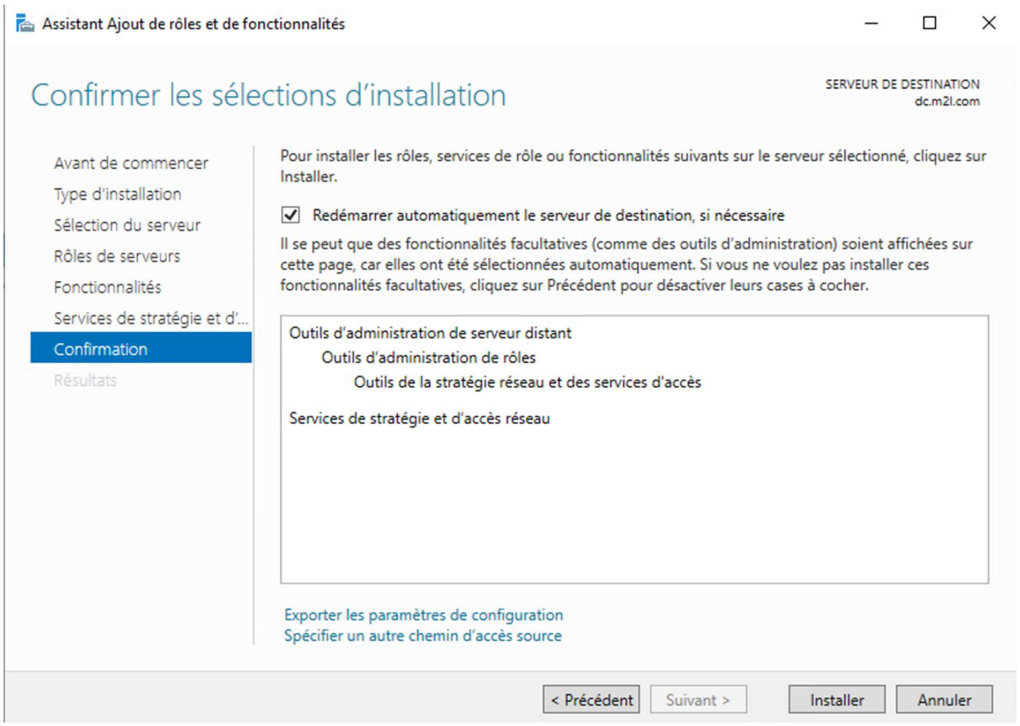

Figure 33 - Description du service NPS (Network Policy Server)

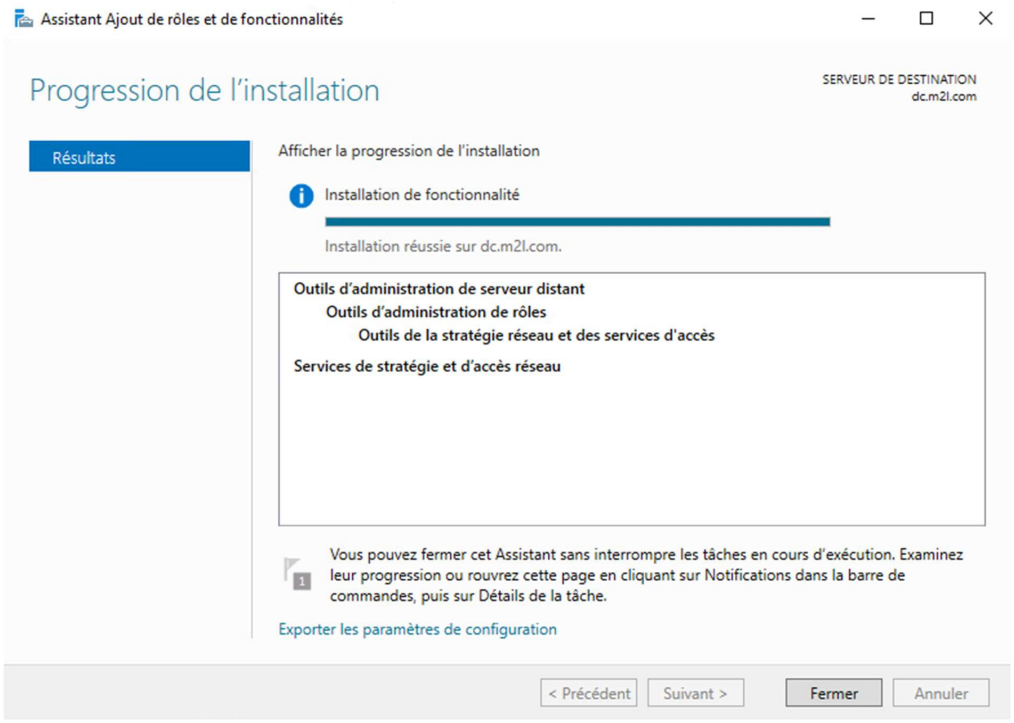

Figure 34 - Confirmation et lancement de l'installation

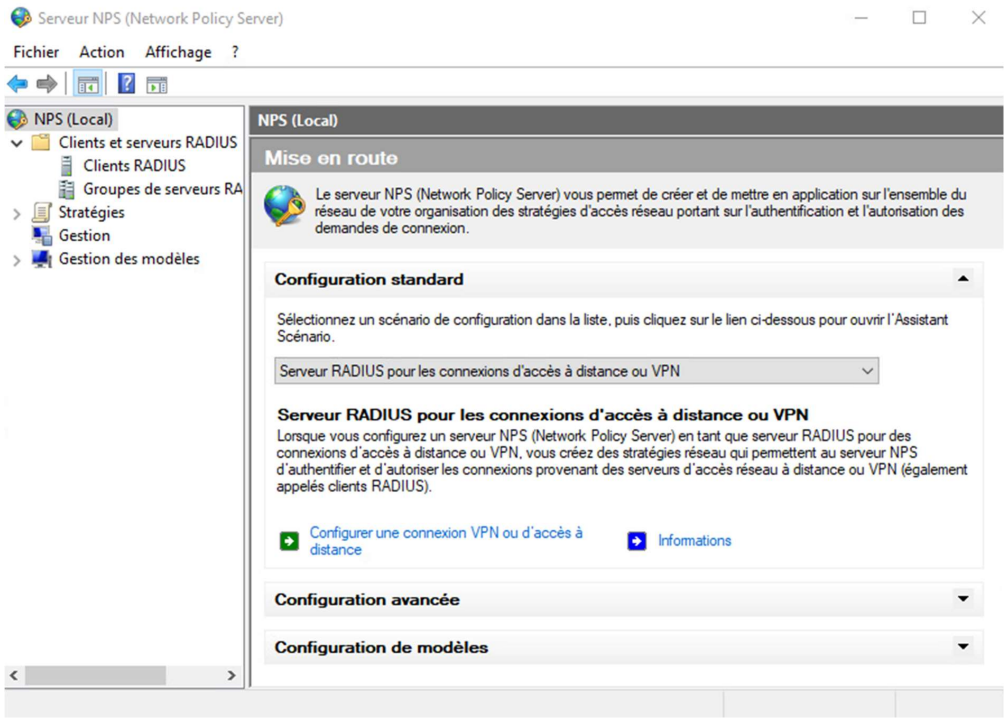

Figure 35 - Installation réussie du service NPS

Le service NPS est désormais installé. Il est accessible depuis le menu Outils du Gestionnaire de serveur, sous l'entrée "Serveur NPS (Network Policy Server)".

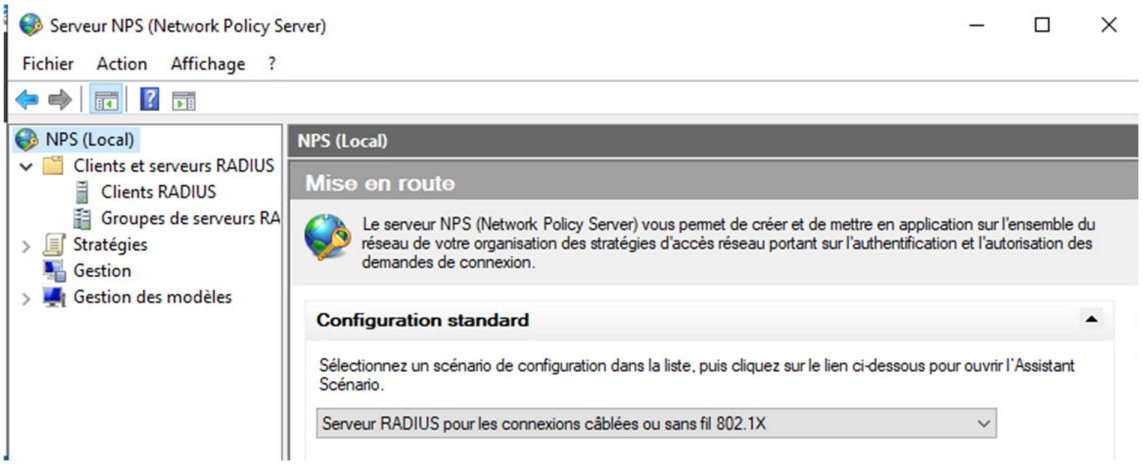

Figure 36 - Accès au serveur NPS depuis le menu Outils

4.2 Configuration du scénario 802.1X

Dans la console NPS, le scénario de configuration standard est modifié pour sélectionner "Serveur RADIUS pour les connexions câblées ou sans fil 802.1X". Ce scénario lance un assistant guidé pour configurer l'authentification Wi-Fi.

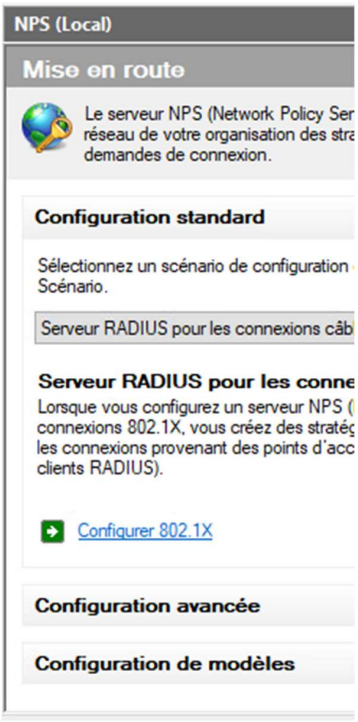

Figure 37 - Page d'accueil NPS - Configuration standard

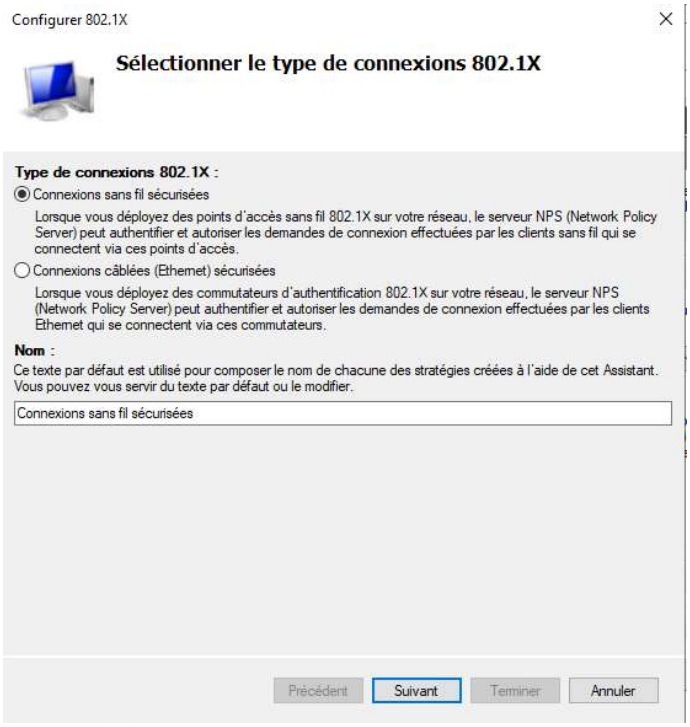

Figure 38 - Changement du scénario : connexions 802.1X

Lancement de l'assistant de configuration 802.1X

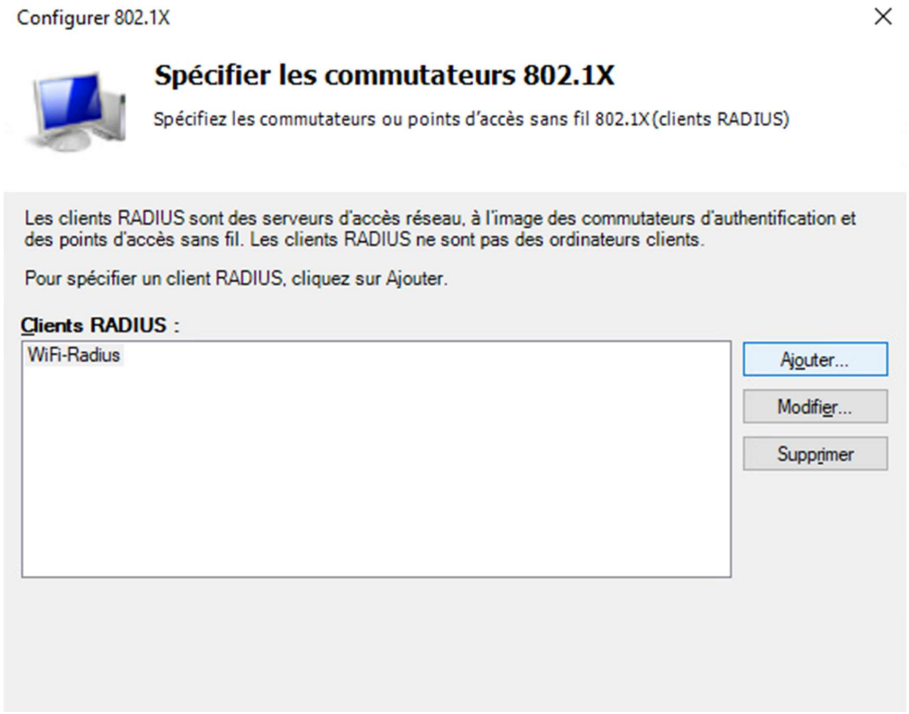

Figure 39 - Assistant 802.1X - Sélection du type de connexion : Sans fil sécurisées

Le type de connexion "Connexions sans fil sécurisées" est sélectionné. Le nom de la stratégie est conservé par défaut. L'assistant va maintenant demander de spécifier les clients RADIUS (points d'accès Wi-Fi) et la méthode d'authentification.

4.3 Ajout du client RADIUS (point d'accès Wi-Fi)

Un client RADIUS doit être déclaré pour chaque point d'accès Wi-Fi du stade. Le client est identifié par son nom convivial et son adresse IP. Un secret partagé est configuré pour sécuriser les échanges RADIUS entre la borne et le serveur NPS.

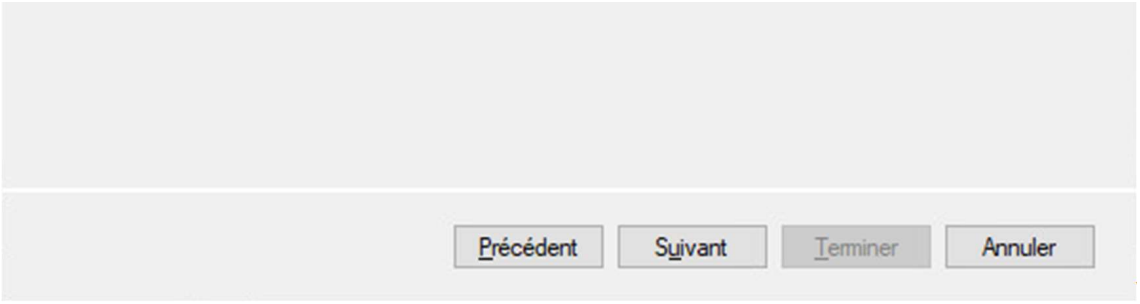

Figure 40 - Client RADIUS "WiFi-Radius" ajouté avec l'adresse IP du point d'accès

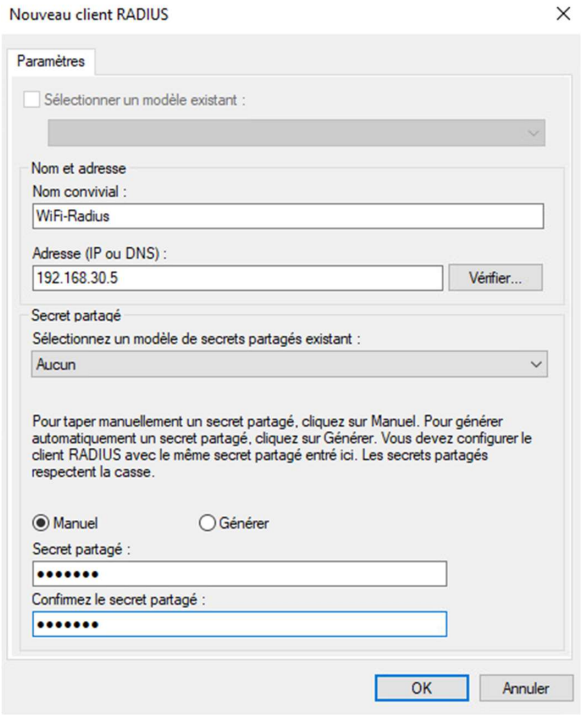

Figure 41 - Détails du client RADIUS : nom, adresse IP et secret partagé

Paramètre	Valeur
Nom convivial	WiFi-Radius
Adresse IP du point d'accès	172.20.3.5
Secret partagé	********** (identique sur la borne et NPS)
Type de client	Standard RADIUS

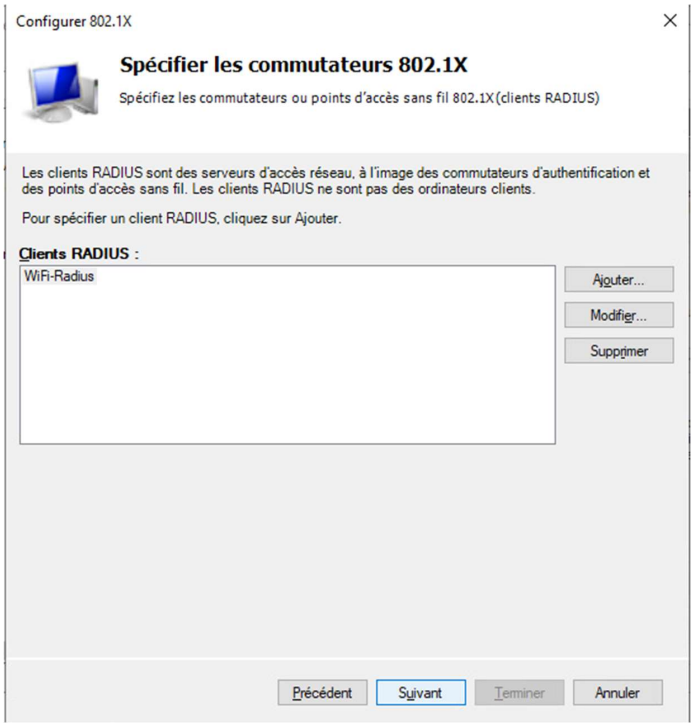

Figure 42 - Client RADIUS déclaré et visible dans la liste

4.4 Configuration de la méthode d'authentification (PEAP)

La méthode d'authentification sélectionnée est **Microsoft PEAP (Protected EAP)**. Ce protocole établit un tunnel TLS sécurisé entre le client Wi-Fi et le serveur RADIUS grâce au certificat du contrôleur de domaine installé précédemment. Les identifiants de l'utilisateur (login/mot de passe Active Directory) sont transmis à l'intérieur de ce tunnel chiffré via MSCHAPv2.

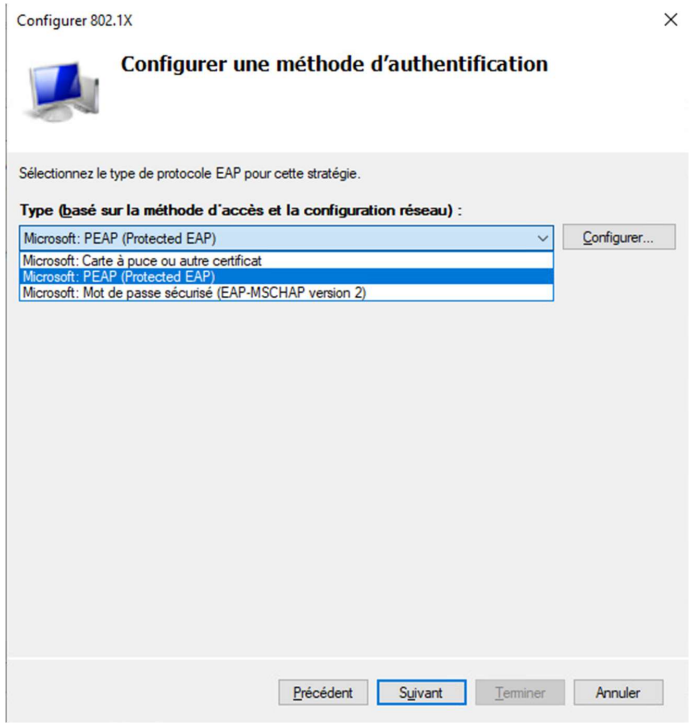

Figure 43 - Sélection de Microsoft PEAP (Protected EAP) comme méthode

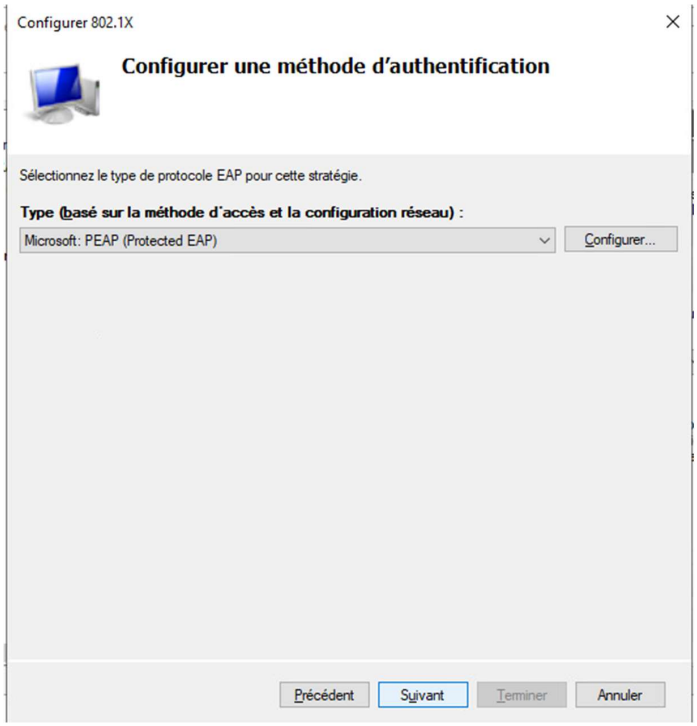

Figure 44 - Confirmation de la méthode PEAP avec MSCHAPv2

4.5 Spécification des groupes d'utilisateurs autorisés

L'accès au Wi-Fi est restreint aux membres du groupe Active Directory "Utilisateurs du domaine". Seuls les comptes présents dans ce groupe pourront s'authentifier via RADIUS et accéder au réseau Wi-Fi de StadiumCompany. Cette restriction garantit qu'aucun compte non autorisé ne pourra se connecter.

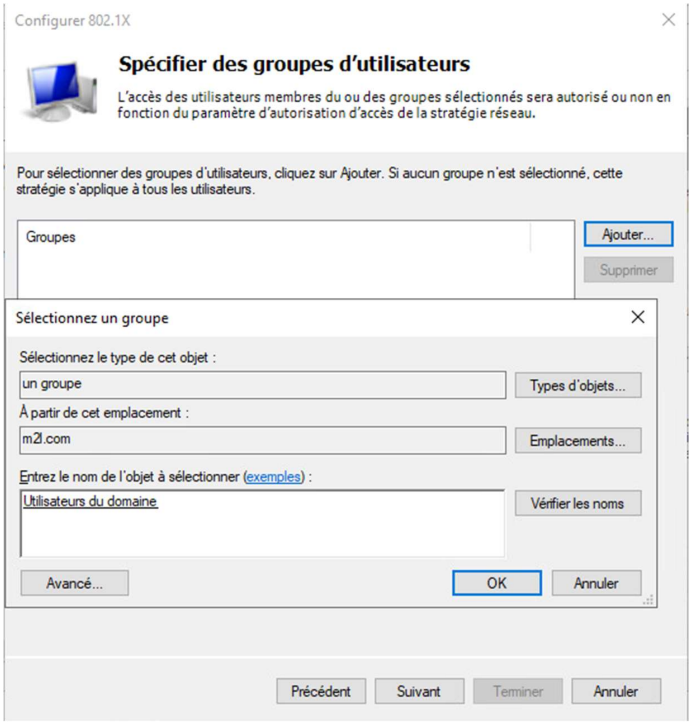

Figure 45 - Ajout du groupe "Utilisateurs du domaine" pour l'autorisation

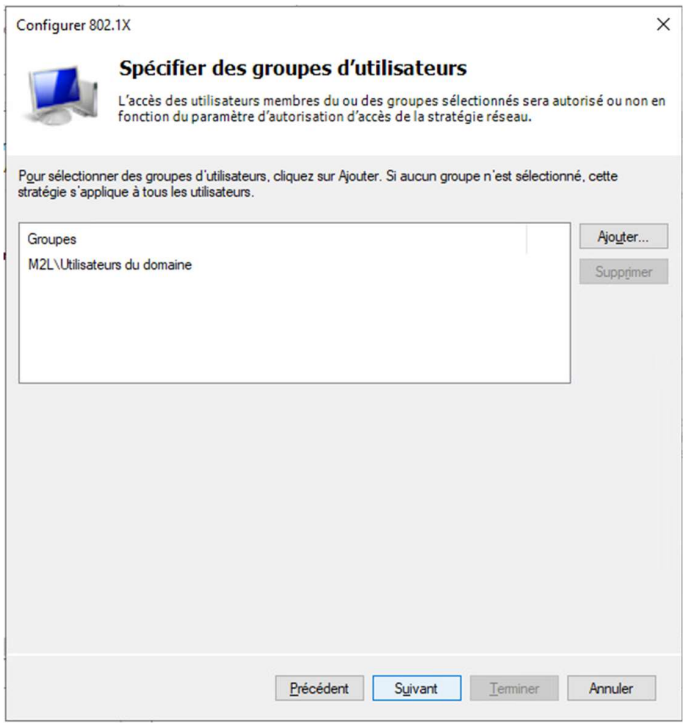

Figure 46 - Groupe sélectionné et validé dans la stratégie d'accès

4.6 Récapitulatif et finalisation

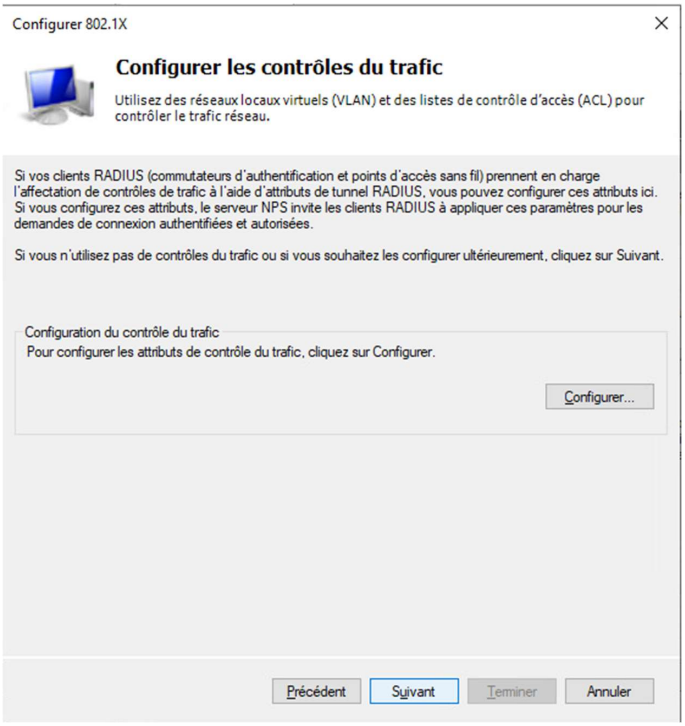

Figure 47 - Configuration des contrôles de trafic (VLAN et ACL optionnels)

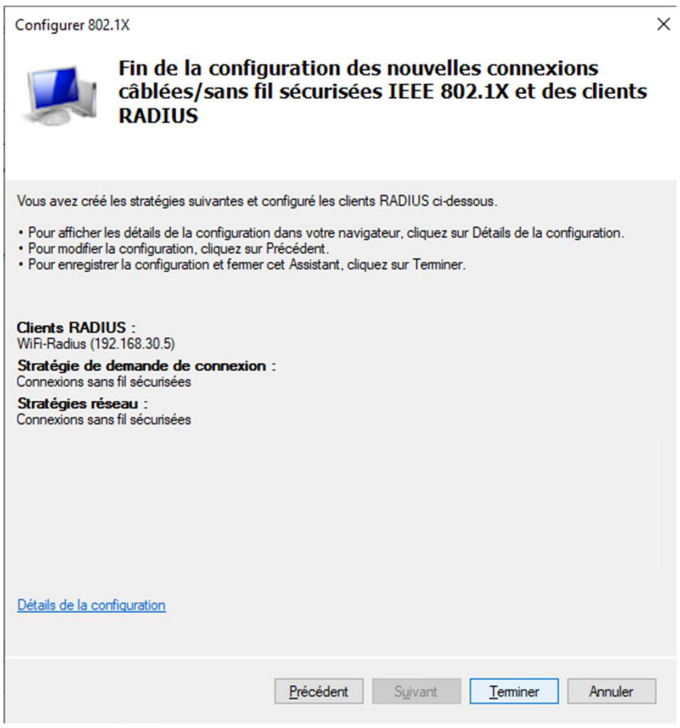

Figure 48 - Récapitulatif de la configuration 802.1X et des clients RADIUS

Le récapitulatif confirme la configuration : le client RADIUS "WiFi-Radius" est déclaré avec l'adresse IP 172.20.3.5, la stratégie de demande de connexion est "Connexions sans fil sécurisées", et la stratégie réseau autorise les utilisateurs du domaine stadiumcompany.local.

5. Tests et validation

5.1 Connexion Wi-Fi avec identifiants Active Directory

Après la configuration du serveur NPS et du point d'accès Wi-Fi, un test de connexion est réalisé depuis un poste client. L'utilisateur sélectionne le SSID "StadiumCompany-Corp" et saisit ses identifiants Active Directory (login et mot de passe du domaine). Le serveur NPS vérifie les informations et autorise la connexion.

Test réalisé	Résultat	Observation
Connexion SSID Employés avec compte AD valide	OK	Authentification réussie via RADIUS/PEAP
Connexion avec identifiants invalides	Refusé	Access-Reject envoyé par le serveur NPS
Connexion SSID Visiteurs (portail captif)	OK	Accès Internet uniquement réseau interne isolé
Accès ressources internes depuis SSID Employés	OK	Partages réseau et services accessibles
Accès réseau interne depuis SSID Visiteurs	Bloqué	Isolation VLAN respectée

5.2 Analyse du trafic RADIUS avec Wireshark

Pour valider le fonctionnement de l'authentification RADIUS, une capture de trafic réseau est réalisée avec Wireshark en appliquant le filtre "radius". La capture montre les échanges entre le point d'accès (client RADIUS) et le serveur NPS : requêtes Access-Request, challenges Access-Challenge, et réponse finale Access-Accept.

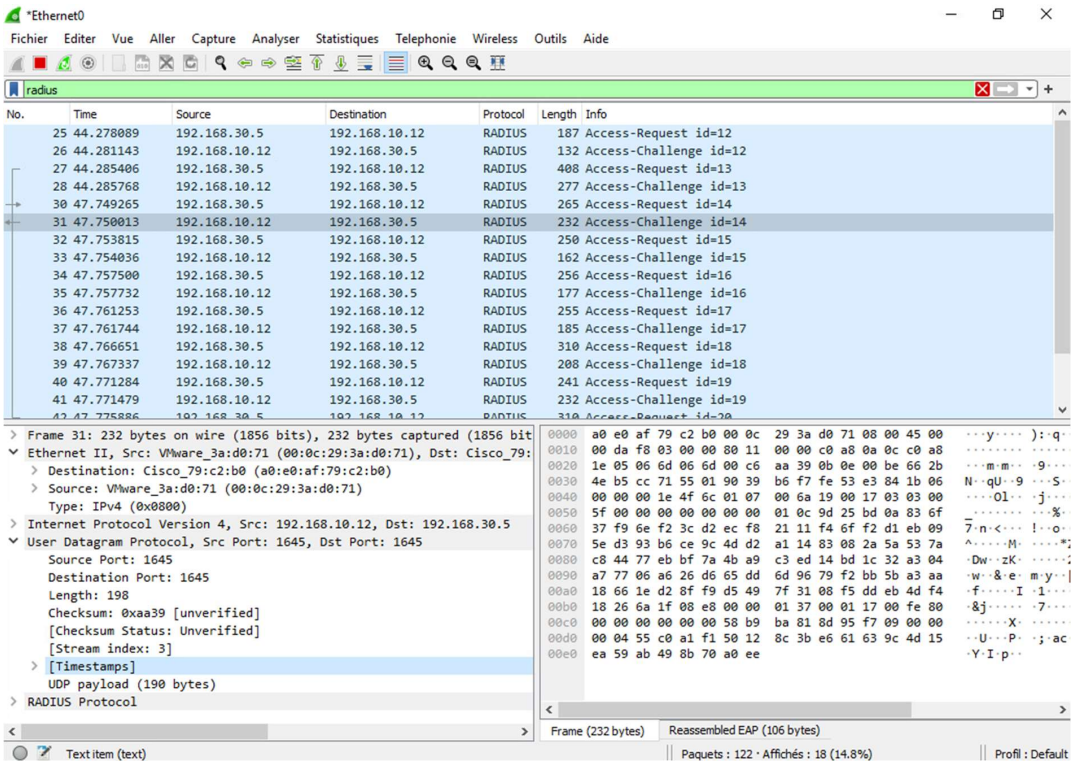

Figure 49 - Capture Wireshark du trafic RADIUS : séquence Access-Request / Access-Challenge / Access-Accept

La capture Wireshark confirme le bon fonctionnement de l'authentification 802.1X/RADIUS. On observe la séquence complète d'échanges EAP entre le client (172.20.3.5 - point d'accès) et le serveur NPS (172.20.1.14) sur les ports UDP 1645/1646. Les multiples échanges Access-Request / Access-Challenge correspondent aux étapes de négociation du tunnel TLS (PEAP), suivies de la vérification MSCHAPv2.

6. Procédure de connexion pour les utilisateurs

Procédure pour les employés (SSID StadiumCompany-Corp)

Étape 1 : Activez le Wi-Fi sur votre appareil (PC, tablette ou smartphone).

Étape 2 : Sélectionnez le réseau "StadiumCompany-Corp" dans la liste des réseaux disponibles.

Étape 3 : Saisissez votre identifiant Active Directory (ex : prenom.nom@stadiumcompany.local) et votre mot de passe habituel.

Étape 4 : Si un avertissement de certificat apparaît lors de la première connexion, acceptez le certificat du serveur (émis par l'autorité stadiumcompany-DC-CA).

Étape 5 : La connexion est établie. Vous avez accès au réseau interne et à Internet.

Procédure pour les visiteurs (SSID StadiumCompany-Guest)

Étape 1 : Activez le Wi-Fi et sélectionnez le réseau "StadiumCompany-Guest".

Étape 2 : Un portail captif s'affiche automatiquement dans votre navigateur.

Étape 3 : Saisissez le code d'accès temporaire fourni par l'accueil du stade.

Étape 4 : Vous avez accès à Internet uniquement. Le réseau interne est inaccessible.

7. Compétences E5 validées

Compétence E5	Mise en oeuvre dans cette mission
Mettre en place et vérifier les habilitations	Authentification RADIUS 802.1X basée sur AD, restriction d'accès par groupe d'utilisateurs, isolement du réseau visiteurs.
Mettre à disposition un service informatique	Déploiement du Wi-Fi professionnel avec deux SSID, configuration NPS/RADIUS, mise en service de l'infrastructure PKI.
Accompagner les utilisateurs	Rédaction de la procédure de connexion pour les employés et les visiteurs, guide utilisateur clair et accessible.
Gérer le patrimoine informatique	Documentation de l'architecture Wi-Fi, inventaire des certificats et des clients RADIUS, procédures d'administration.

8. Conclusion

La mission 6 a permis de déployer une solution Wi-Fi complète et sécurisée pour StadiumCompany, répondant aux besoins distincts des employés et des visiteurs du stade. L'infrastructure mise en place repose sur des standards éprouvés et offre un niveau de sécurité conforme aux exigences de la direction.

Pour les employés, l'authentification WPA2 Enterprise avec RADIUS/802.1X garantit que seuls les utilisateurs disposant d'un compte Active Directory valide peuvent accéder au réseau Wi-Fi de l'entreprise. Le protocole PEAP assure le chiffrement des identifiants grâce au tunnel TLS établi avec le certificat du serveur. La centralisation de l'authentification via NPS simplifie la gestion des accès : l'ajout ou la suppression d'un employé dans Active Directory se répercute automatiquement sur ses droits Wi-Fi.

Pour les visiteurs, un SSID dédié et isolé du réseau interne permet un accès Internet contrôlé via un portail captif, conformément aux bonnes pratiques de sécurité. L'isolation par VLAN garantit qu'aucun visiteur ne peut atteindre les ressources internes.

L'ensemble de la solution a été validé par des tests fonctionnels (connexion avec identifiants AD, refus des identifiants invalides, isolation des visiteurs) et par une analyse du trafic RADIUS avec Wireshark, confirmant les échanges d'authentification Access-Request / Access-Challenge / Access-Accept entre le point d'accès et le serveur NPS.