Ecole IRIS

Implémentation d'un Réseau Wi-Fi pour les Employés et les Visiteurs au Stade

Borne Wi-Fi Cisco

Projet Personnalisé Encadré

Implémentation d'un solution Wi-Fi

I - Contexte :

1.1 Présentation de l'entreprise :

Stadium gère un grand stade et avait initialement mis en place un réseau de communication avancé lors de la construction. Cependant, au fil du temps, l'entreprise a ajouté de nouveaux équipements et augmenté les connexions sans tenir compte de ses objectifs commerciaux à long terme ni de la conception de son infrastructure réseau. Cela a conduit à des problèmes de bande passante et de gestion du trafic, limitant la capacité de la société à offrir des services de qualité.

Maintenant, la direction de Stadium souhaite améliorer la satisfaction de ses clients en introduisant de nouvelles technologies et en permettant l'organisation de concerts, mais le réseau actuel ne le permet pas. Sachant qu'elle ne possède pas l'expertise nécessaire en matière de réseau, la direction a décidé de faire appel à des consultants réseau pour concevoir, gérer et mettre en œuvre ce projet en trois phases.

La première phase consiste à planifier le projet et à préparer une conception réseau de haut niveau. Pour cela, Stadium a engagé NetworkingCompany, une société spécialisée en conception de réseaux, qui a interrogé le personnel du stade pour comprendre l'organisation et les installations.

StadiumCompany emploie 170 personnes à temps plein :

- 35 dirigeants et responsables
- 135 employés

Environ 80 intérimaires sont embauchés en fonction des besoins, pour des événements spéciaux dans les services installations et sécurité.

Tous les employés, à l'exception des préposés au terrain et des gardiens, utilisent des PC et des téléphones connectés à un PABX vocal numérique.

1.2 Présentation du prestataire informatique :

StadiumCompany a engagé NetworkingCompany, une société locale spécialisée dans la conception de réseaux et le conseil, de la phase 1, la conception de haut niveau. NetworkingCompany est une société partenaire Cisco Premier Partner. Elle emploie 20 ingénieurs réseau qui disposent de diverses certifications et d'une grande expérience dans ce secteur.
Pour créer la conception de haut niveau, NetworkingCompany a tout d'abord interrogé le personnel du stade et décrit un profil de l'organisation et des installations.

Créée en 1989, NetworkingCompany est une société spécialiste en infrastructures systèmes et vente de matériel informatique pour professionnels de la vidéo.

Employant aujourd'hui 20 ingénieurs réseau, l'activité de NetworkingCompany s'établit à 1,8 millions d'euros de chiffre d'affaires. Son cœur de métier se situe au niveau de l'infrastructure informatique afin de garantir les besoins des activités « métiers ». NetworkingCompany est l'une des seules sociétés de services informatique qui accompagne réellement et jusqu'au bout ses clients dans le choix et la mise en œuvre de solutions.

NetworkingCompany intervient en mode Projet (Engagement de résultats), Régie (Engagement de moyens) et Infogérance des environnements Windows. Son outil de compétitivité et de productivité réside dans la capitalisation de son savoir-faire, le haut niveau de certification de ses partenariats ainsi qu'une veille technologique active.

NetworkingCompany a développé une expertise forte dans les domaines de la virtualisation, les infrastructures d'accès (Application delivery), l'industrialisation du poste de travail (Itil, Supervision, Télédistribution), les annuaires et la gestion de l'identité.

Reconnu depuis 25 ans comme une entreprise innovante, et avec aujourd'hui plus de 300 collaborateurs, cette société répond avec flexibilité et efficacité à tous les besoins, qu'ils émanent de PME ou de grands comptes. Enfin, NetworkingCompany est en partenariat avec de nombreux gros groupes du monde de l'informatique, tout comme Microsoft, CISCO, HP, Huawei ou encore DELL, pour ne citer que les plus importants.

II - Cahier des charges :

Cette année, vous allez intégrer la division du stade de StadiumCompany. Vous serez chargé de la maintenance des systèmes et réseaux informatiques.

StadiumCompany est composé de plusieurs sites :
Site 1 : Stade (hébergement informatique, siège social et centre administratif)
Site 2 : Billetterie (vente des billets)
Site 3 : Magasin (la vente d'articles souvenirs)

Les différentes solutions retenues pour l'étude du projet d'un point de vue général de StadiumCompany pourront faire l'objet de documentations techniques suivant la complexité de la mise en œuvre.

Mission 6 : Restructuration de l'Infrastructure de Stadium

Actuellement, le stade possède un accès aux différentes ressources de StadiumCompagny (fichiers, impression, internet, bases de données,). Mais cet accès n'est possible qu'à travers une liaison filaire. La direction du stade souhaite étendre aux services équipés d'un terminal Wifi.
StadimCompagny a fait l'acquisition de plusieurs Switchs compatibles PoE et des AP Cisco.
Vous êtes chargé d'implémenter une solution d'accès sans fil pour les salariés du stade ainsi qu'aux visiteurs. Ces derniers n'auront accès qu'à la ressource internet mais d'une façon sécurisée (obligation légale).
Éléments du cahier des charges concernant les accès Wifi.
A chaque service est disposé d'un point d'accès 802.11 b/g/n PoE. Il y a un SSID non diffusé par VLAN sauf le Vlan visiteur.
La confidentialité est assurée par la norme WPA2 Enterprise sauf pour le dernier dans première temps, puis un renforcement de l'authentification dans un deuxième temps.
Prérequis :

- Le système d'information d'AP est opérationnel.
- Modification à opérer :
- Proposer une solution d'accès Wifi pour le Vlan Wifi (stade-wifi)
- Proposer une solution d'accès Wifi pour les visiteurs
- Intégrer et configurer le ou les switchs PoE
- Intégrer et configurer les AP Wifi
- Authentification des salariés via le réseau sans fils
- Accès des visiteurs à internet seulement.

Phase 1 :

- Proposer une solution d'infrastructure réseau et système permettant d'assurer l'accès sans fils aux salariés et aux visiteurs dans tous les locaux sans interruption de service.
- Proposer un schéma réseau logique et physique et la démarche à mettre en œuvre avec l'ordonnancement des tâches pour assurer cette extension sans fils.

Phase 2 :

- Configurer le matériel et les systèmes nécessaires pour mener à bien cette extension d'accès sans fil

- Proposer la batterie de tests nécessaires pour valider votre infrastructure.
- Documentation technique sur les switchs et les AP
- Documentation technique sur le cryptage des données

III - Solution :

Test et comparaison des solutions :

Pour assurer la sécurité du réseau nous allons utiliser le Wi-Fi Protected Access 2 (WPA2 – IEEE 802.11i), en implémentant différents protocoles qui permettront de répondre aux exigences de sécurité et de transparence auprès des utilisateurs.

Authentification des utilisateurs:

Pour le réseau des visiteurs médicaux, nous allons utiliser un serveur Radius.

Radius (Remote Authentifiacation Dial-in User Service) est un protocole client-serveur permettant de centraliser les données d'authentification.

Pour s'authentifier, le poste utilisateur transmet une requête d'accès à un client RADIUS pour entrer sur le réseau, ce dernier se charge de demander les informations identifiant l'utilisateur (utilisateur & mot de passe). Le client RADIUS génère une requête d'accès qu'il transmet au serveur RADIUS, ce dernier préalablement couplé avec le service d'annuaire va pouvoir aller vérifier les informations envoyées par le client et ainsi valider ou bien refusé l'accès.

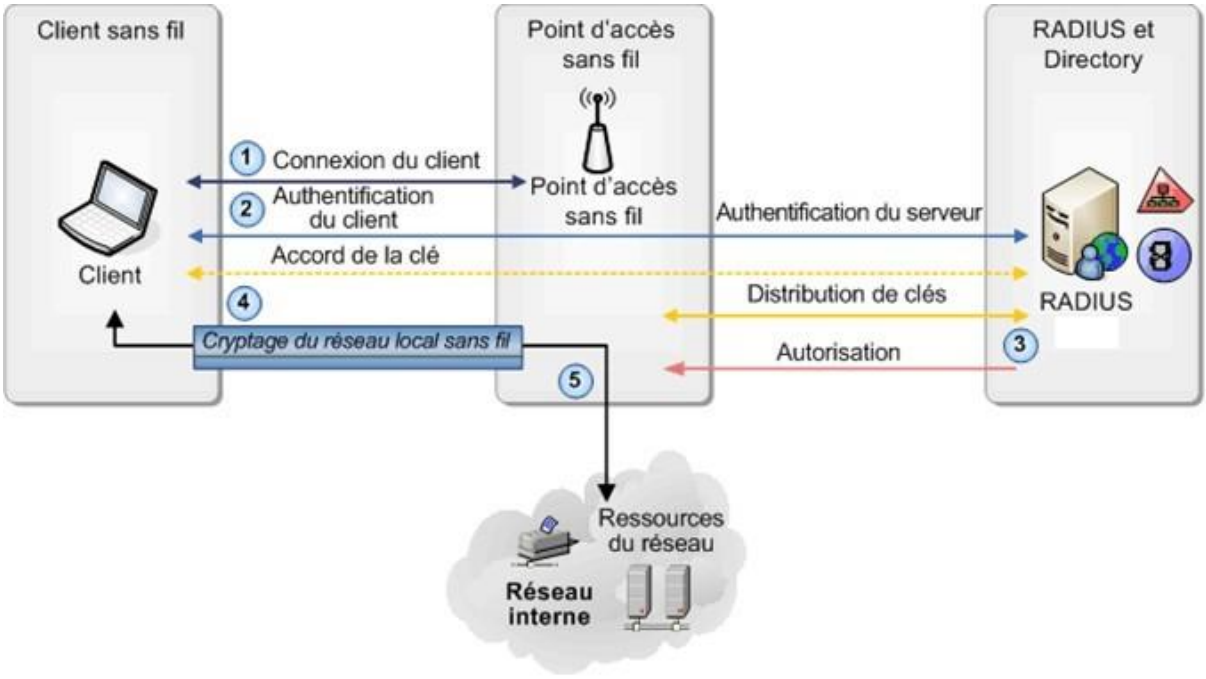
Sécurité des communications:

Pour sécuriser les communications sur le réseau WPA2 offre deux types de chiffrements :

- Temporal Key Integrity Protocol (TKIP) : il permet l'authentification et la protection des données transitant sur le réseau. C'est une méthode de cryptage. Qui génère une clé de paquets, mélange les paquets du message, puis remet les paquets dans l'ordre pour retrouver l'intégrité du message grâce à un mécanisme de triage.

- Advanced Encryption Standard (AES) : c'est une méthode de chiffrement symétrique (chiffrement avec une clé secrète). TKIP est donc initialement mis en place pour pallier aux différents problèmes du chiffrage WEP, il repose sur la même base de chiffrement qui a révélé ses limites. AES quant à lui est une méthode de chiffrement complètement à part qui n'a pour l'instant pas été cassé. De plus TKIP générant dynamiquement (quelques minutes d'intervalle entre chaque génération de clés) des clés de chiffrement peuvent diminuer les performances alors que l'AES n'a besoin que de très peu de ressources.

Le réseau Wi-Fi utilisera donc la sécurité suivante : WPA2 Enterprise AES. Les bornes Wi-Fi devront être référencées sur le serveur d'authentification afin d'assurer la provenance des connexions. On renseigne un code secret qui ne sera connu que par le point d'accès et le serveur.



Étude du matériel :

Pour la mise en place du réseau Wi-Fi nous avons sélectionné la borne Cisco :

CISCO Aironet 1042 N		- Interface de gestion sécurisée - Ligne de commande (telnet et SSH) - WPA2 AES - Filtre MAC - RADIUS - SSID Caché - Multi-SSID - PoE - 802.11a/b/g/n - VLAN 802.1Q

IV/ Mise en œuvre :

Choix de solutions:

Suite cette comparaison nous avons choisi le point d'accès Aironet de Cisco qui est le plus adaptés à nos besoins. Elle est compatible avec toutes les contraintes de sécurisation besoin, son avantage par rapport aux autres points d'accès et la garantie matérielle à vie. De plus notre réseau étant essentiellement formé de matériel du constructeur Cisco, cette borne respectera l'homogénéité matérielle.

V/Conclusion

L'objectif de ce projet est la mise en place d'une architecture sans fil accessible et propre à chaque vlan avec un accès visiteur. Cette architecture doit avoir StadiumCompany veut proposer une solution d'accès Wifi pour le Vlan Wifi (stade- wifi) et pour les visiteurs du stade. Le groupe souhaite que les point d'accès sans fil soient compatible avec la technologie PoE pour des raisons esthétiques et éviter des pertes des chargeurs électriques. L'architecture wifi doit permettre une authentification des salariés via le réseau sans fil grâce à la mise en place d'un serveur d'authentification de type Radius. Le plan de sécurité de l'architecture doit permettre l'accès des visiteurs uniquement à internet.

Annexe :

Procédure :

Configuration de l'AP :

Activation du pont entre les interfaces wifi et le FastEthernet :

```
AP#configure terminal
AP(config)#bridge irb
Procedure :
```

Configuration de l'adresse IP de l'AP :

```
AP#configure terminal
AP(config)#interface BVI 1
AP(config-if)#ip address 172.20.2.10 255.255.255.128
AP(config-if)#no shutdown
AP(config-if)#end
```

Activation de l'interface graphique :

```
AP(config)#ip http secure-server
AP(config)#end
```

Configuration de la passerelle par défaut :

```
AP(config)#ip default-gateway 172.20.0.1
```

Configuration des différents SSID :

```
AP(config)#dot11 vlan-name administration vlan
10 AP(config)#dot11 vlan-name equipes vlan 20
AP(config)#dot11 vlan-name vlan 20
AP(config)#dot11 vlan-name VIP-Presse vlan 30
AP(config)#dot11 vlan-name fournisseur vlan 40
AP(config)#dot11 vlan-name restaurant vlan 50
AP(config)#dot11 vlan-name wifi vlan 100
AP(config)#dot11 vlan-name  camera vlan 200
```

```
AP(config)#dot11 ssid administration
AP(config-ssid)#vlan 10
AP(config-ssid)#authentication
open AP(config-ssid)#exit

AP(config-ssid)#dot11 ssid equipes
AP(config-ssid)#vlan 20
AP(config-ssid)#authentication
open AP(config-ssid)#exit

AP(config-ssid)#dot11 ssid VIP-Presse
AP(config-ssid)#vlan 30
AP(config-ssid)#authentication
open AP(config-ssid)#exit

AP(config-ssid)#dot11 ssid fournisseur
AP(config-ssid)#vlan 40
AP(config-ssid)#authentication
open AP(config-ssid)#exit

AP(config-ssid)#dot11 ssid
restaurant AP(config-ssid)#vlan 50
AP(config-ssid)#authentication
open AP(config-ssid)#exit

AP(config-ssid)#dot11 ssid wifi
AP(config-ssid)#vlan 100 AP(config-
ssid)#authentication open
AP(config-ssid)#mbssid guest-mode
AP(config-ssid)#exit

AP(config-ssid)#dot11 ssid camera
AP(config-ssid)#vlan 200
```

```
AP(config-ssid)#authentication
open AP(config-ssid)#exit
```

Configuration de l'interface radio :

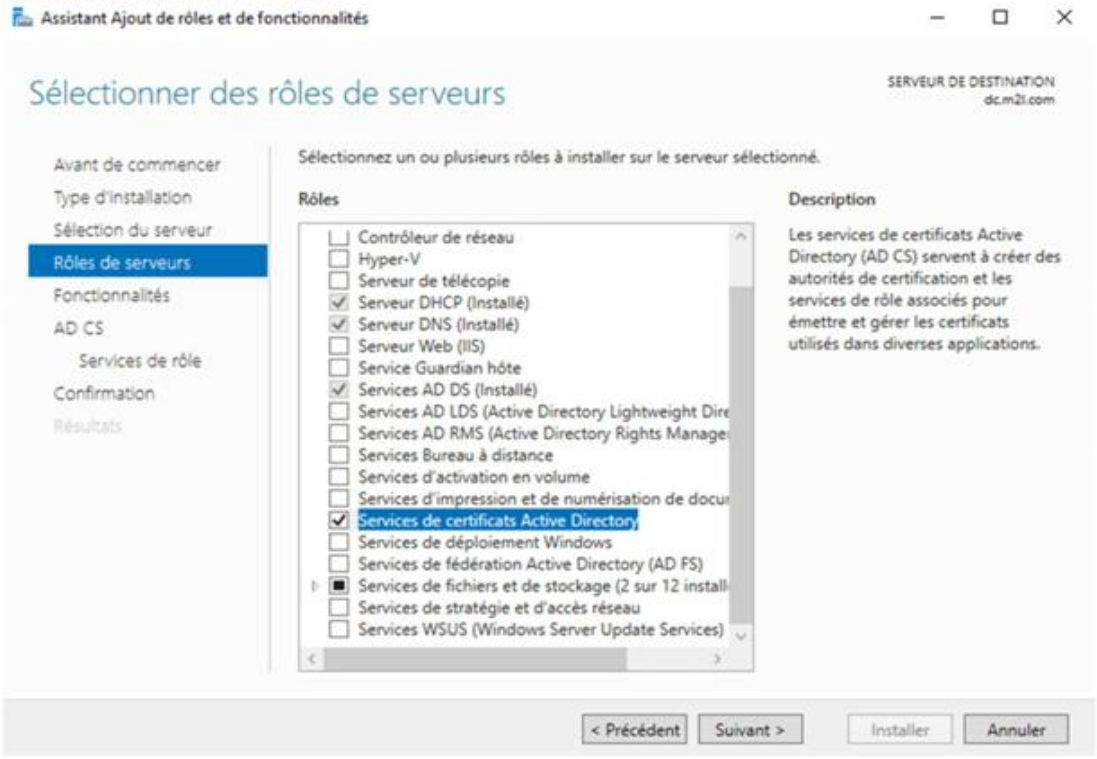
```
AP(config)#interface Dot11Radio0 AP(config-if)#mbssid
AP(config-if)#encryption vlan 10 mode wep mandatory AP(config-if)#encryption vlan 10 key 1 size 128bit 7
01234567890123456789abcdef
AP(config-if)#encryption vlan 20 mode wep mandatory AP(config-if)#encryption vlan 20 key 1 size 128bit 7
01234567890123456789abcdef
AP(config-if)#encryption vlan 30 mode wep mandatory AP(config-if)#encryption vlan 30 key 1 size 128bit 7
01234567890123456789abcdef
AP(config-if)#encryption vlan 40 mode wep mandatory AP(config-if)#encryption vlan 40 key 1 size 128bit 7
01234567890123456789abcdef
AP(config-if)#encryption vlan 50 mode wep mandatory AP(config-if)#encryption vlan 50 key 1 size 128bit 7
01234567890123456789abcdef
AP(config-if)#encryption vlan 100 mode wep mandatory AP(config-if)#encryption vlan 100 key 1 size 128bit 7
01234567890123456789abcdef
AP(config-if)#encryption vlan 200 mode wep mandatory AP(config-if)#encryption vlan 200 key 1 size 128bit 7
01234567890123456789abcdef

AP(config-if)#ssid administration AP(config-if)#ssid equipes AP(config-if)#ssid VIP-Presse AP(config-if)#ssid
fournisseur AP(config-if)#ssid restaurant AP(config-if)#ssid wifi AP(config-if)#ssid camera AP(config-if)#no
shutdown AP(config-if)#exit
```

```
AP#conf terminal
AP(config)#interface Dot11Radio0.10
```

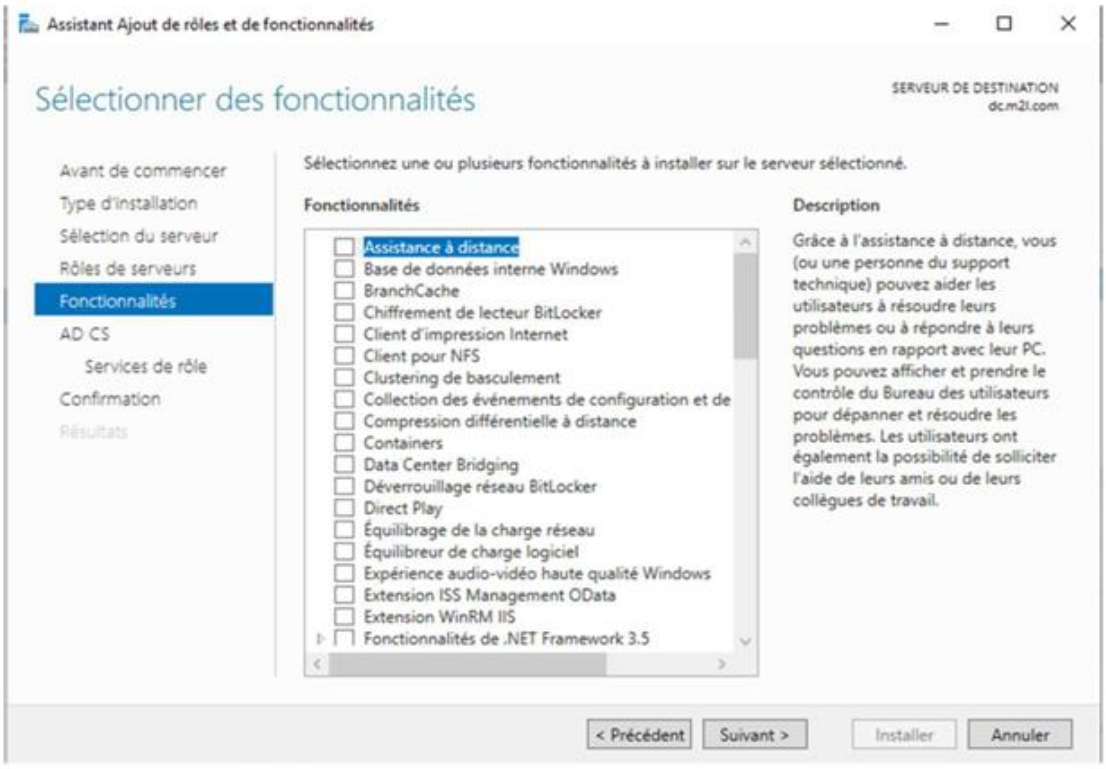
```
AP(config-subif)#encapsulation dot1Q 10
AP(config-subif)#bridge-group
10 AP(config-subif)#no sh
AP(config-if)#exit
AP(config-subif)#encapsulation dot1Q 20
AP(config-subif)#bridge-group
20 AP(config-subif)#no sh
AP(config-if)#exit
AP(config-subif)#encapsulation dot1Q 30
AP(config-subif)#bridge-group
30 AP(config-subif)#no sh
AP(config-if)#exit
AP(config-subif)#encapsulation dot1Q 40
AP(config-subif)#bridge-group
40 AP(config-subif)#no sh
AP(config-if)#exit
AP(config-subif)#encapsulation dot1Q 50
AP(config-subif)#bridge-group
50 AP(config-subif)#no sh
AP(config-if)#exit
AP(config-subif)#encapsulation dot1Q 100
AP(config-subif)#bridge-group
100 AP(config-subif)#no sh
AP(config-if)#exit
AP(config-subif)#encapsulation dot1Q 200
AP(config-subif)#bridge-group
200 AP(config-subif)#no sh
AP(config-if)#exit
```

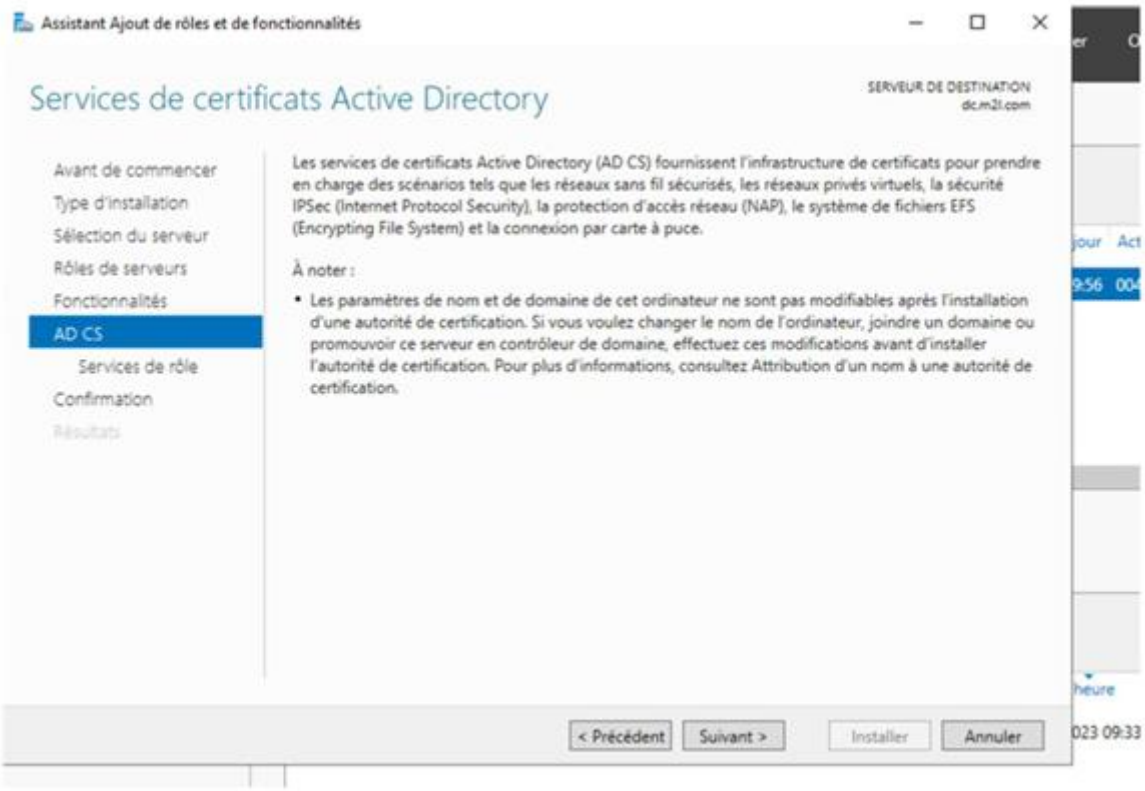
Configuration du serveur Radius :

Installation du rôle CA :

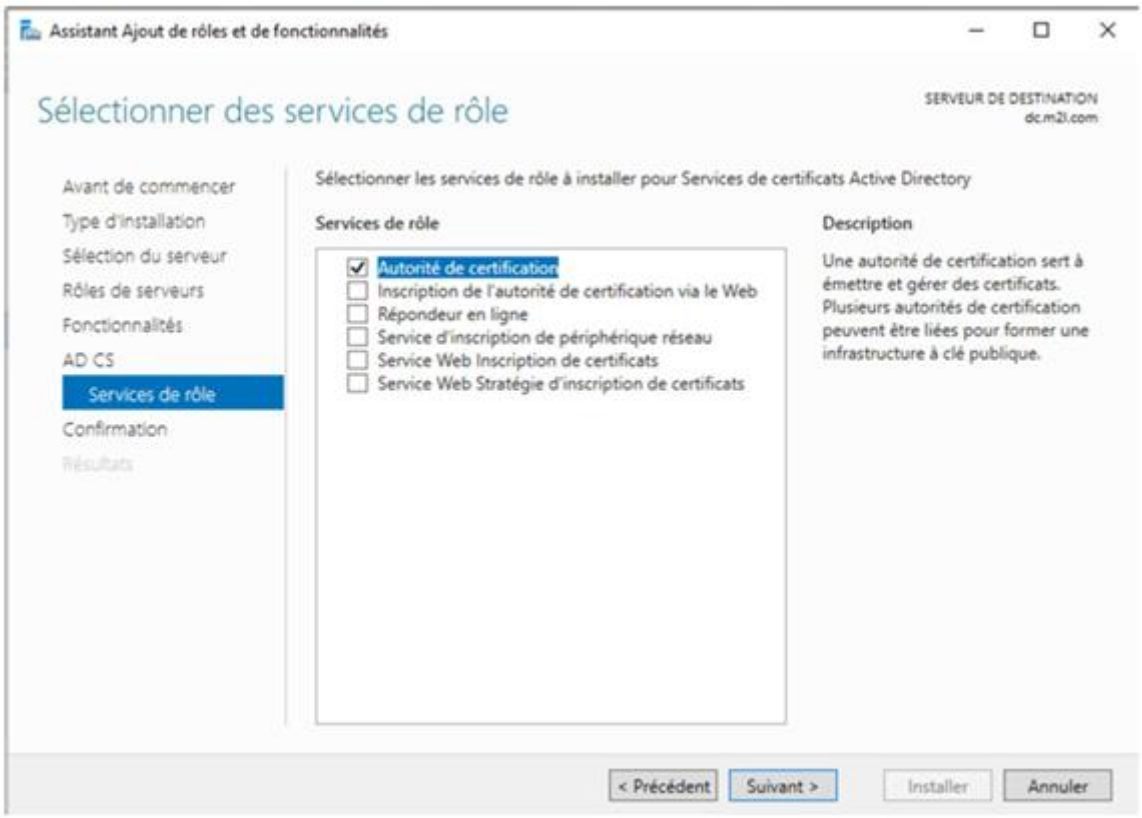


Puis suivant

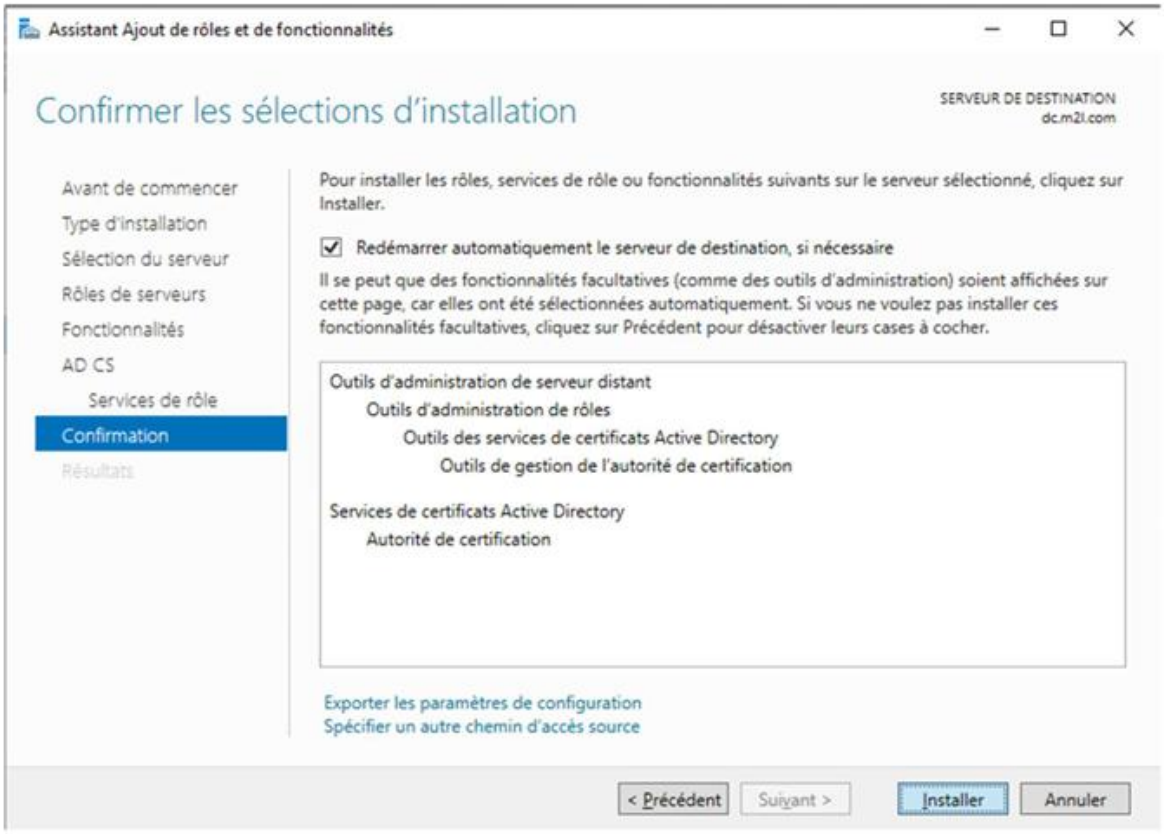



Assistant Ajout de rôles et de fonctionnalités
Services de certificats Active Directory
SERVEUR DE DESTINATION
dc.m2i.com
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
AD CS
Services de rôle
Confirmation
Résultats
Les services de certificats Active Directory (AD CS) fournissent l'infrastructure de certificats pour prendre en charge des scénarios tels que les réseaux sans fil sécurisés, les réseaux privés virtuels, la sécurité IPSec (Internet Protocol Security), la protection d'accès réseau (NAP), le système de fichiers EFS (Encrypting File System) et la connexion par carte à puce.
À noter :
Les paramètres de nom et de domaine de cet ordinateur ne sont pas modifiables après l'installation d'une autorité de certification. Si vous voulez changer le nom de l'ordinateur, joindre un domaine ou promouvoir ce serveur en contrôleur de domaine, effectuez ces modifications avant d'installer l'autorité de certification. Pour plus d'informations, consultez Attribution d'un nom à une autorité de certification.
< Précédent
Suivant >
Installer
Annuler

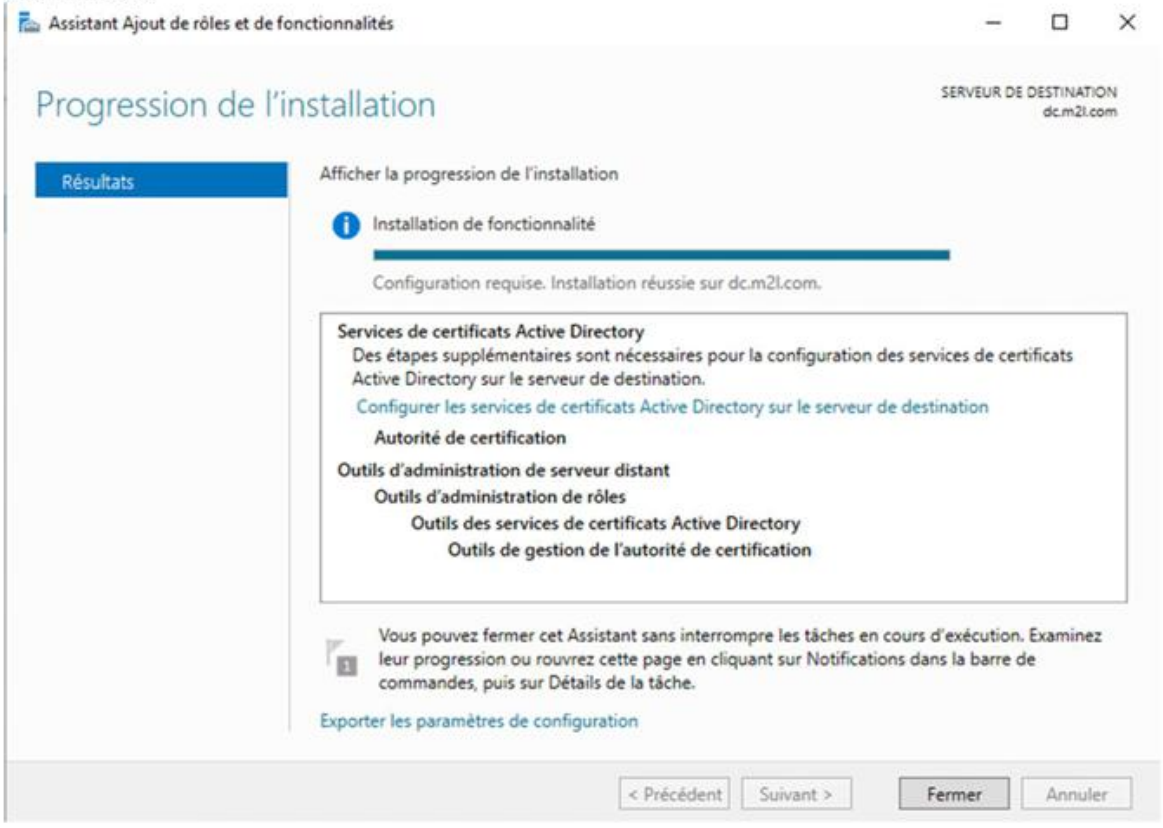
Suivant


Assistant Ajout de rôles et de fonctionnalités
Sélectionner des services de rôle
SERVEUR DE DESTINATION
dc.m2i.com
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
AD CS
Services de rôle
Confirmation
Résultats
Sélectionner les services de rôle à installer pour Services de certificats Active Directory
Services de rôle
Autorité de certification
Inscription de l'autorité de certification via le Web
Répondeur en ligne
Service d'inscription de périphérique réseau
Service Web Inscription de certificats
Service Web Stratégie d'inscription de certificats
Description
Une autorité de certification sert à émettre et gérer des certificats. Plusieurs autorités de certification peuvent être liées pour former une infrastructure à clé publique.
< Précédent
Suivant >
Installer
Annuler

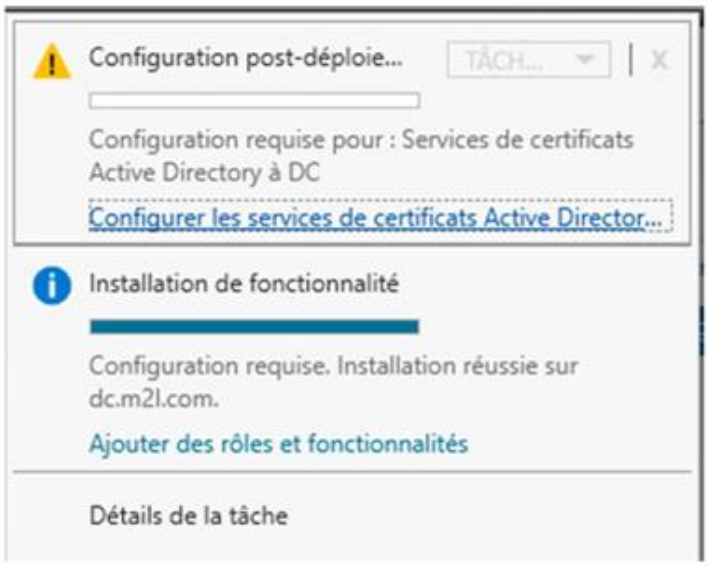
Et installer



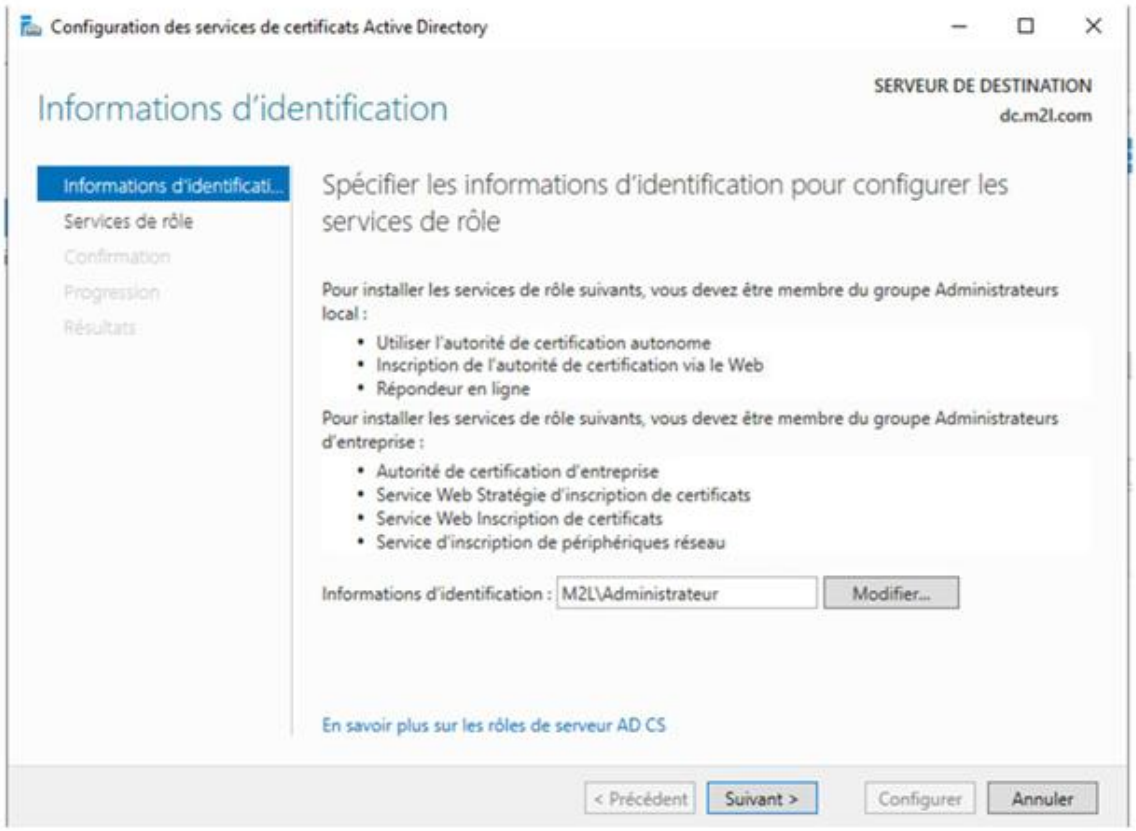
Confirmation



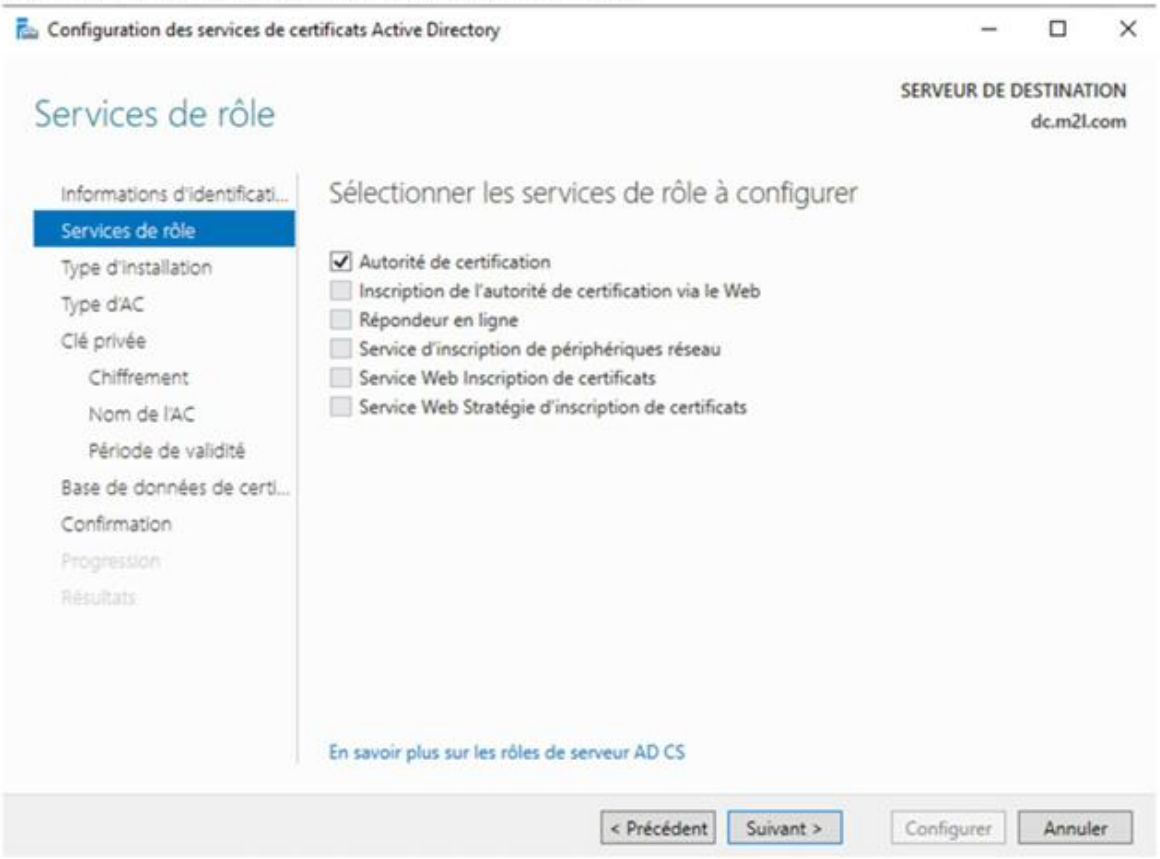
Cliquez sur « Configurer les services »



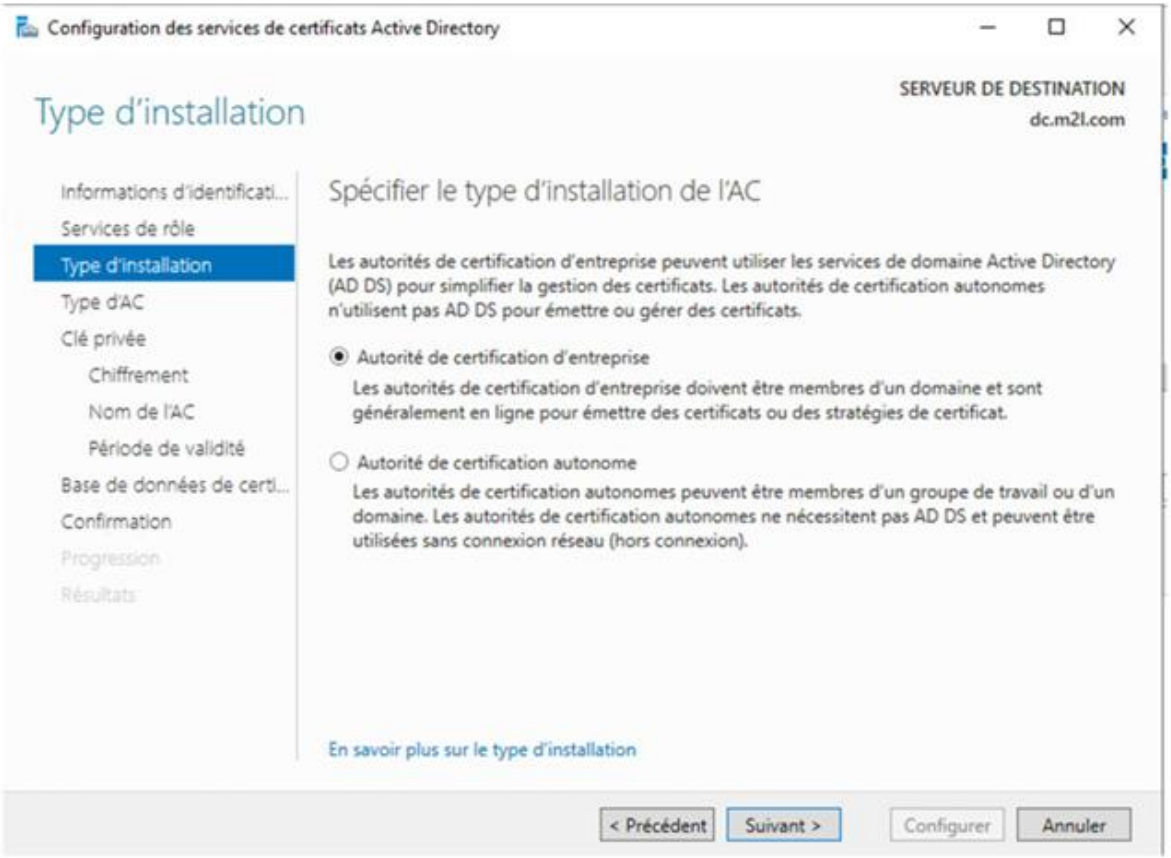
Cliquez sur Suivant



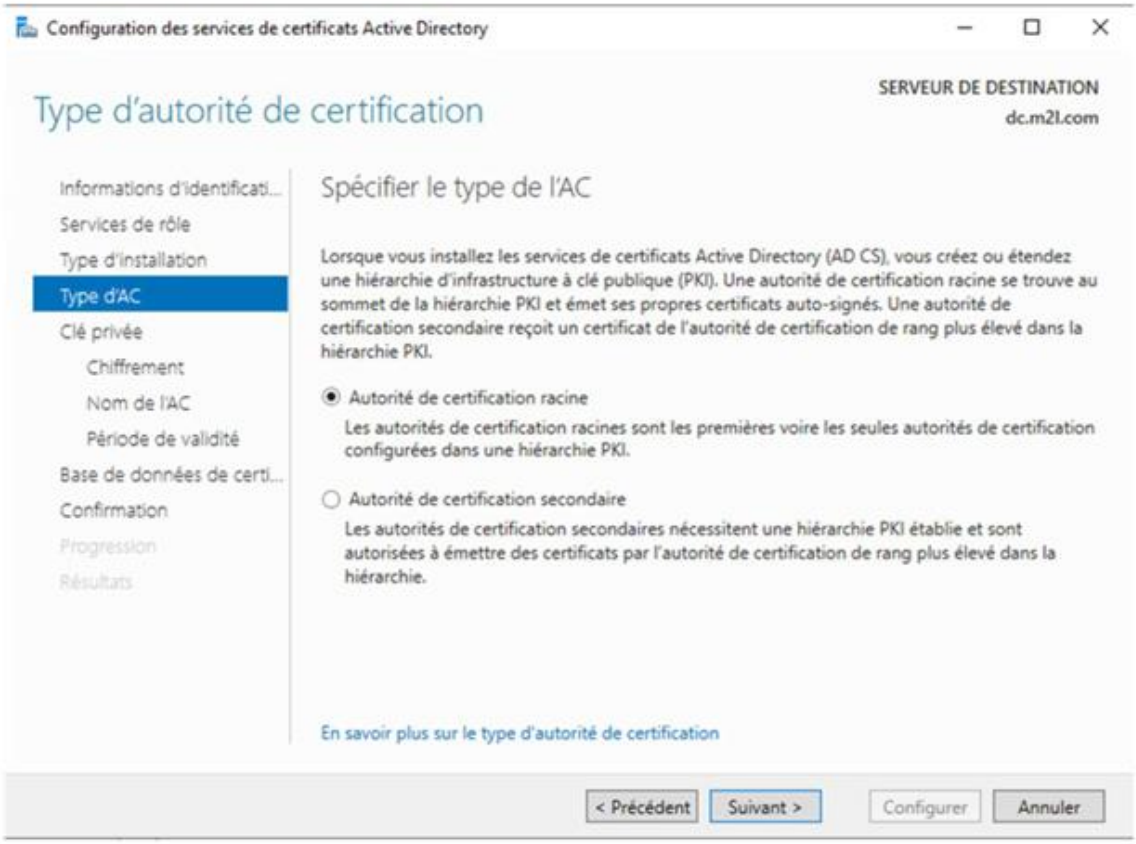
Cochez « Autorité de Certification » puis suivant :



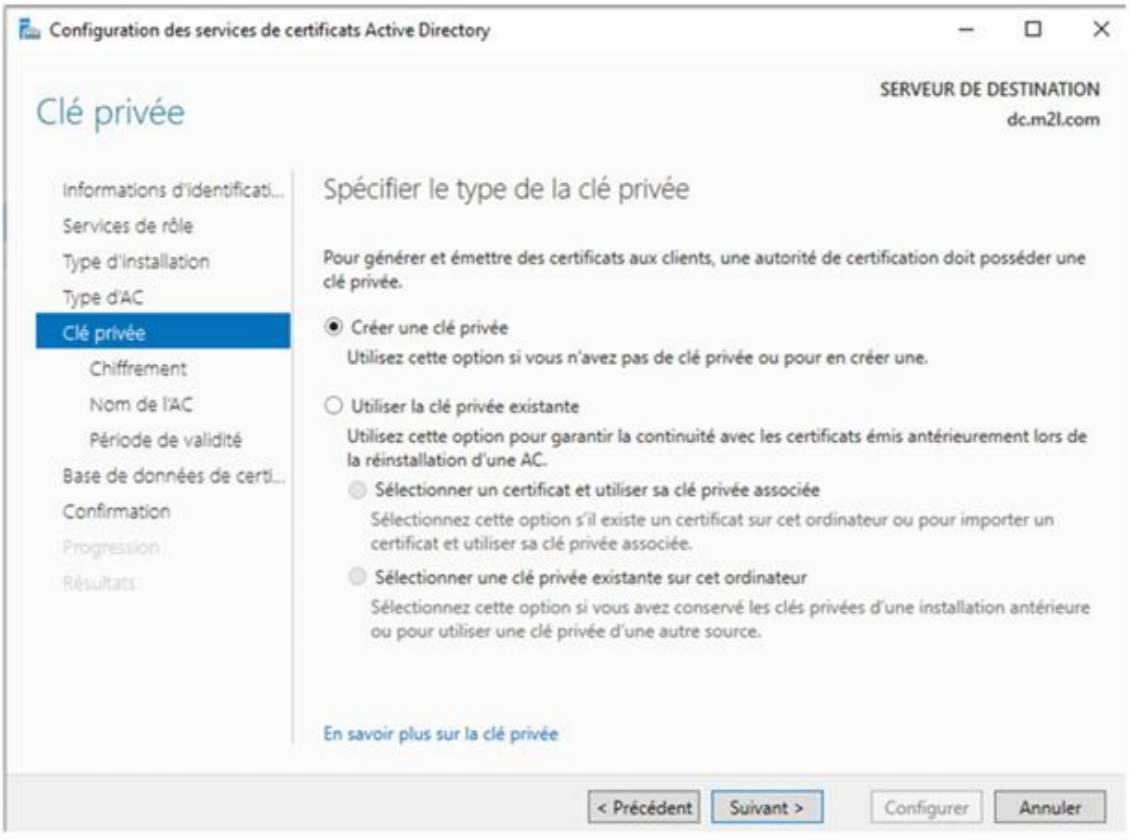
Suivant



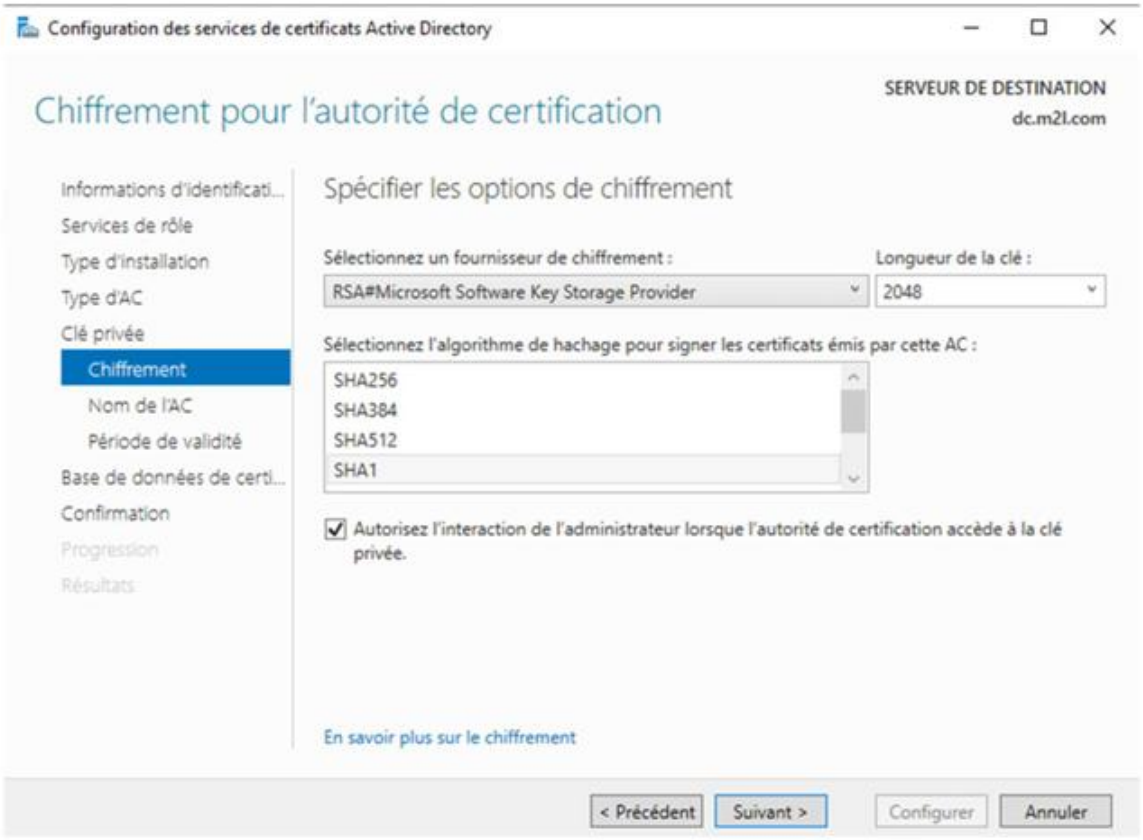
Suivant



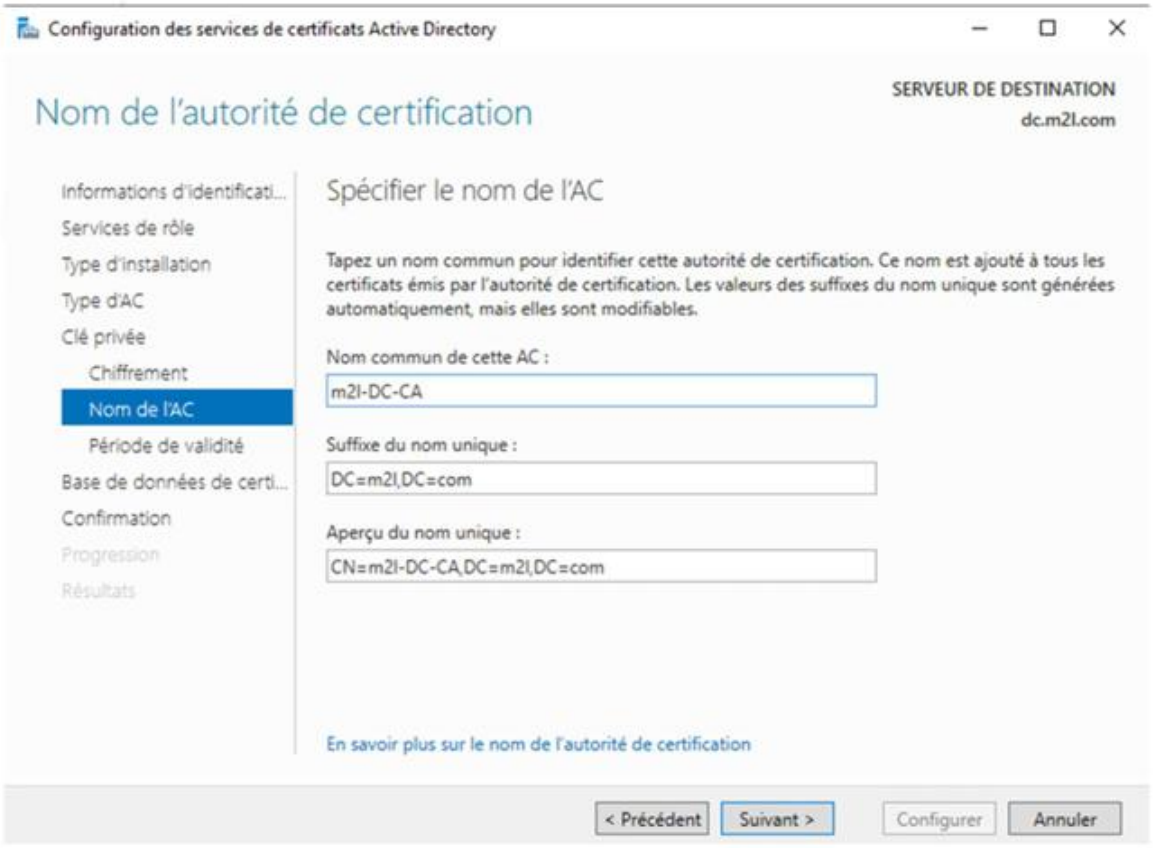
Suivant



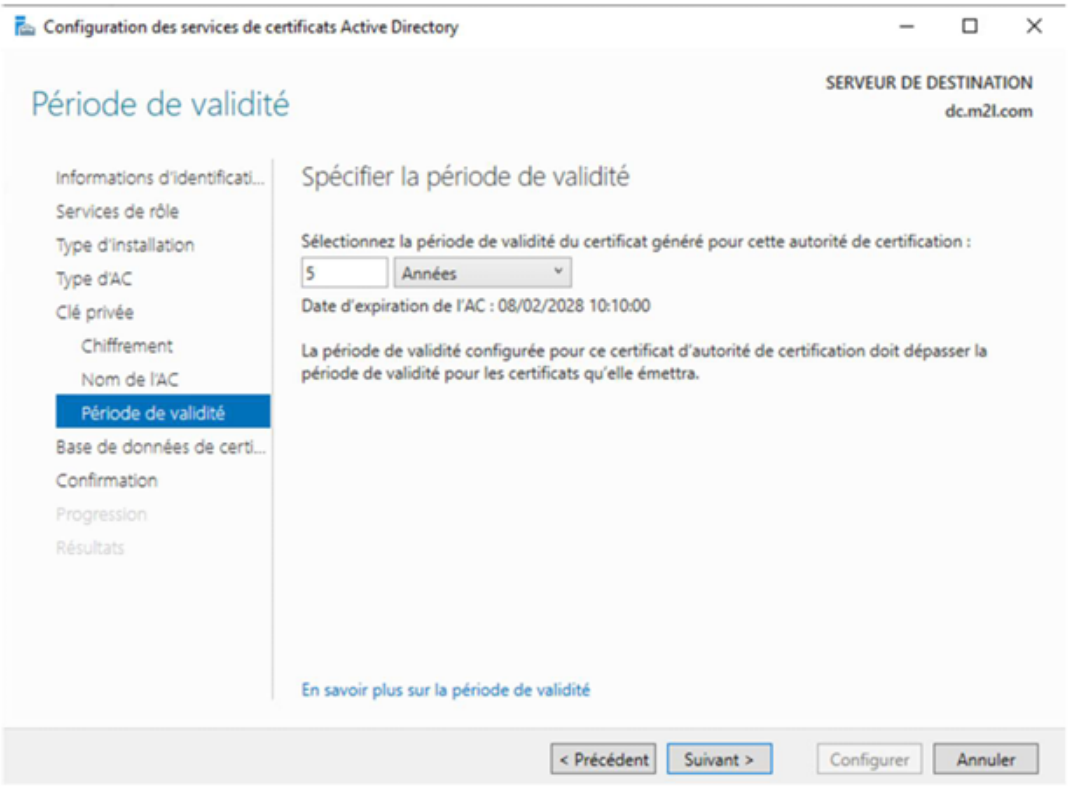
Sélectionner l'algorithme de hachage : SHA1



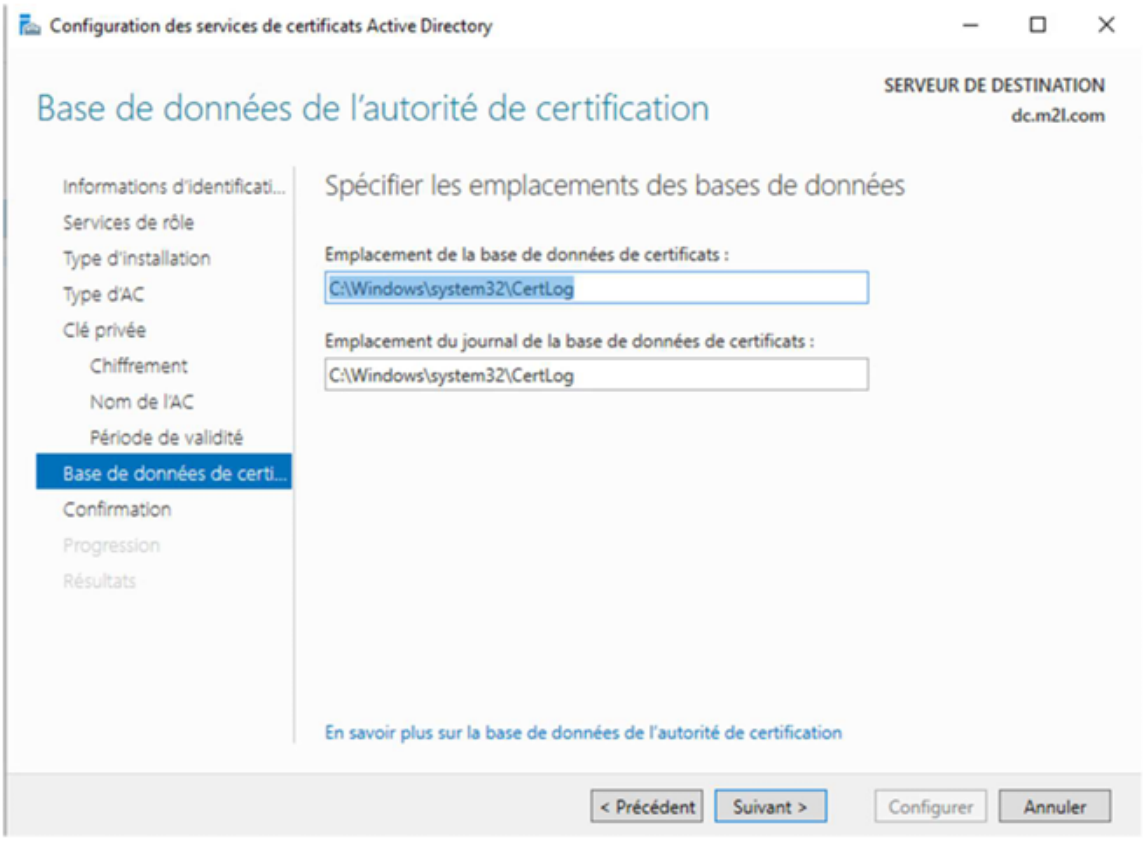
Suivant



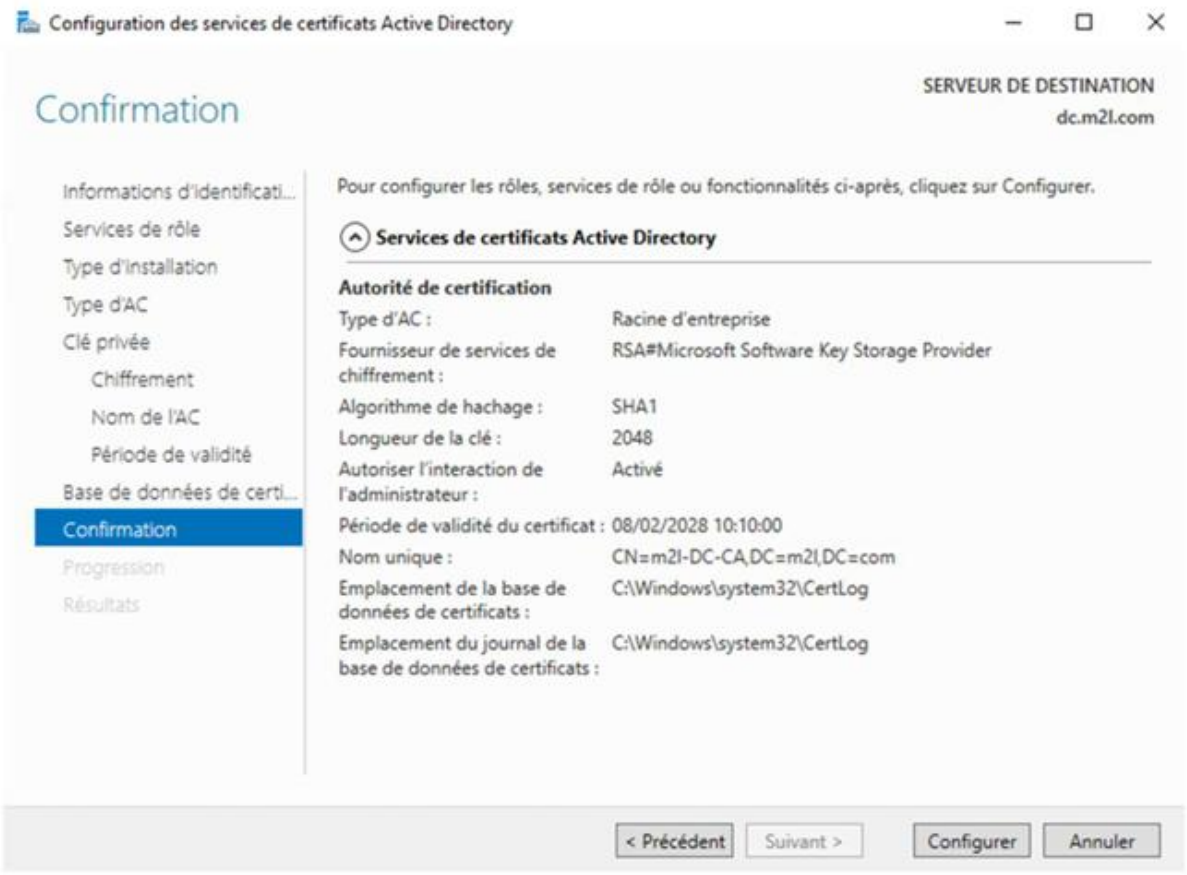
Suivant



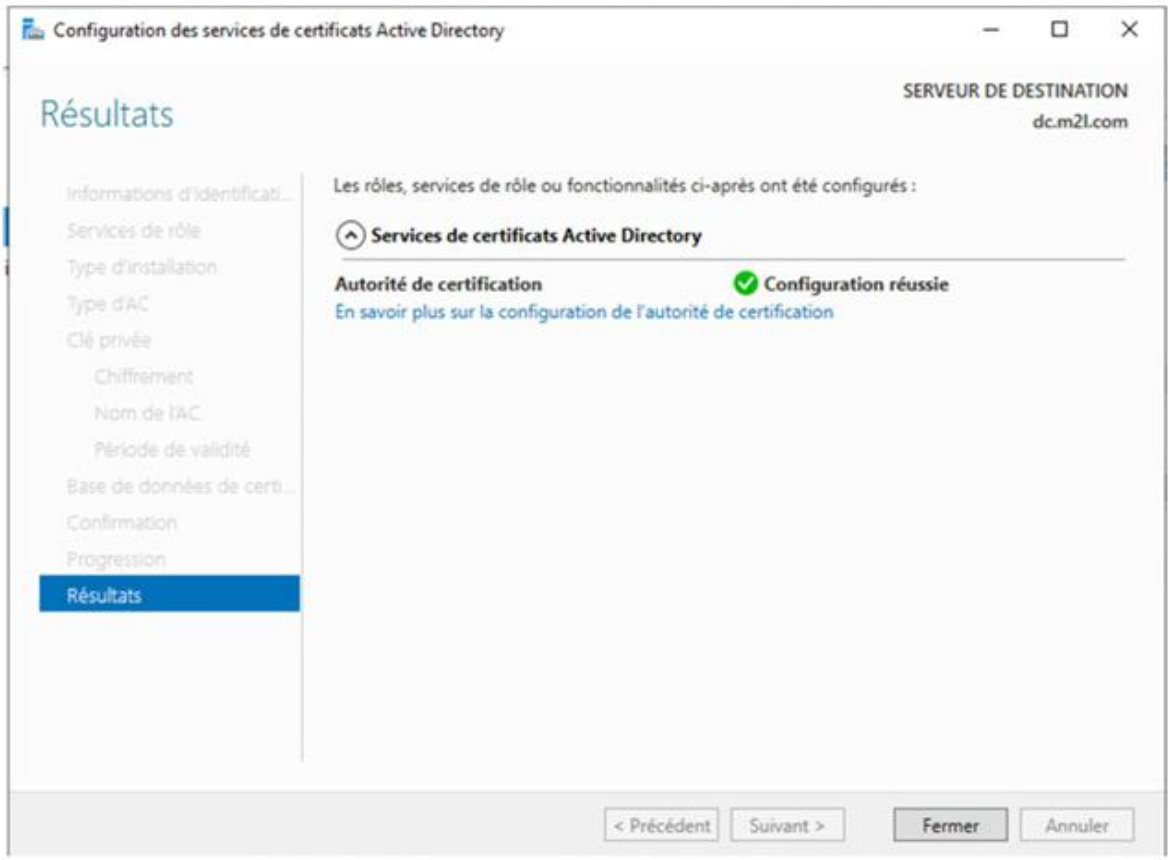
Suivant



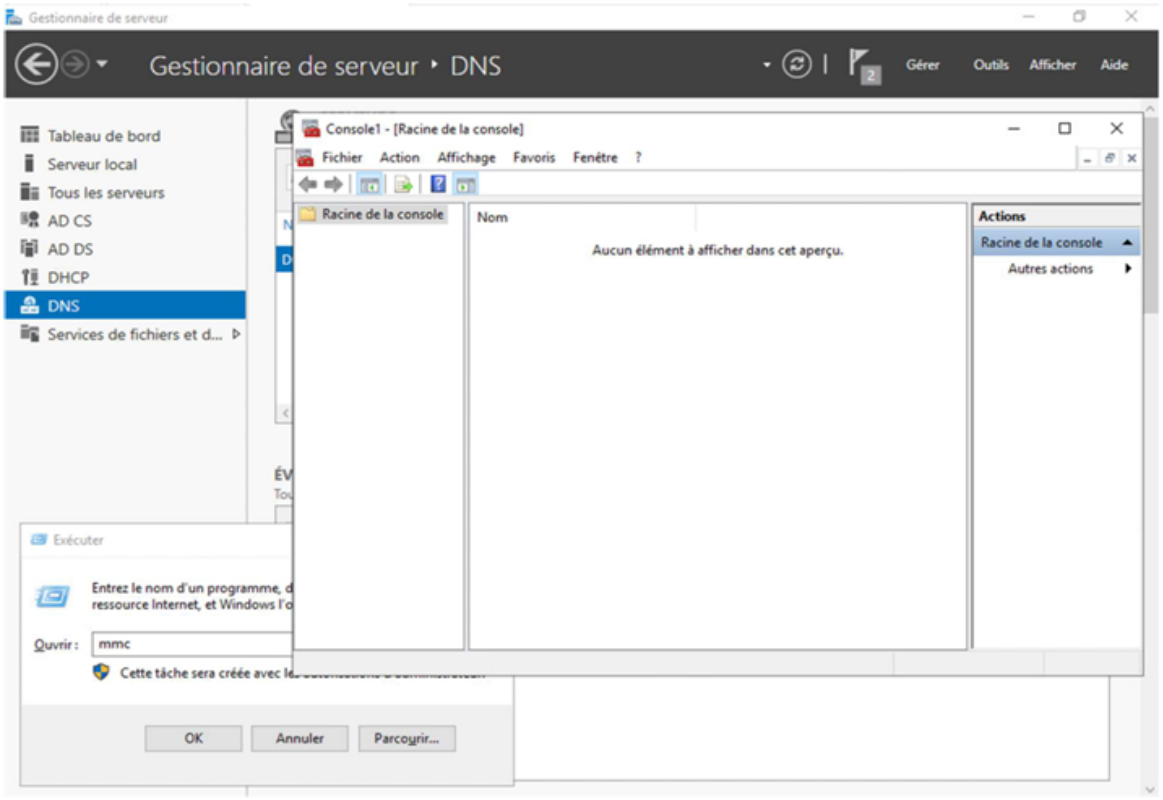
Cliquez sur « Configurer »



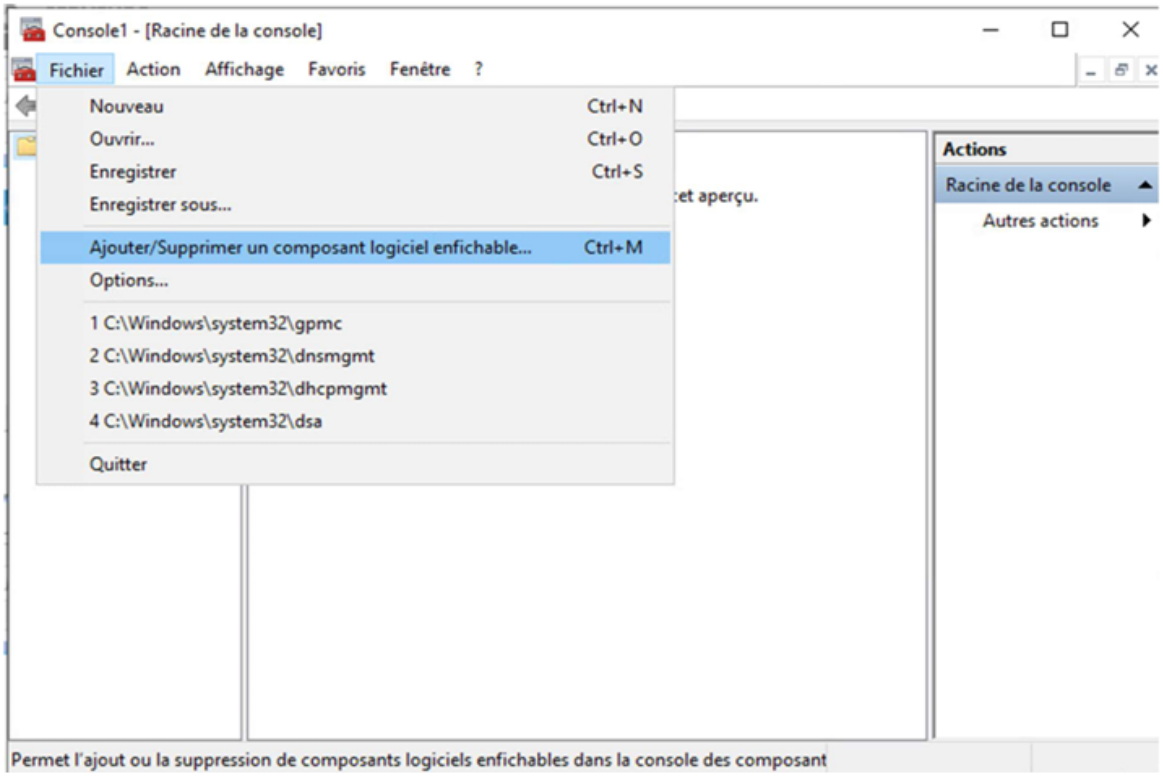
Voici le résultat



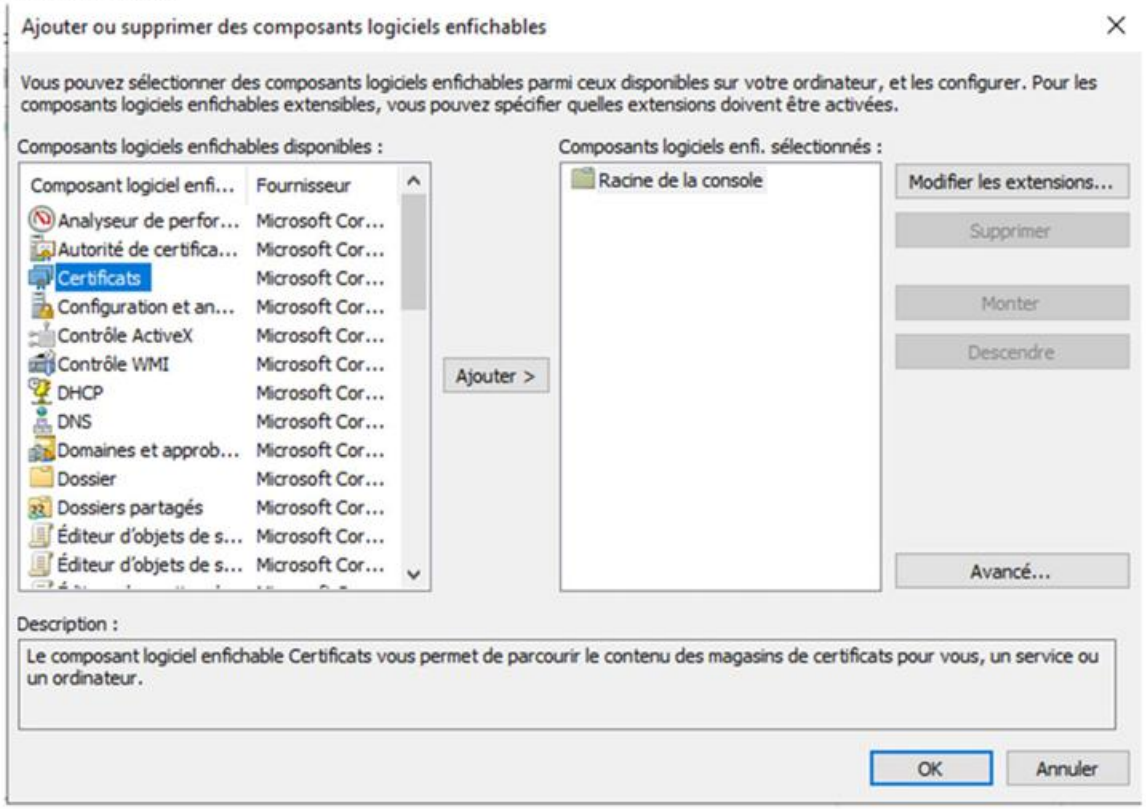
Il faut maintenant ajouter le certificat : dans la fenêtre ‘exécuter’, taper « mmc »



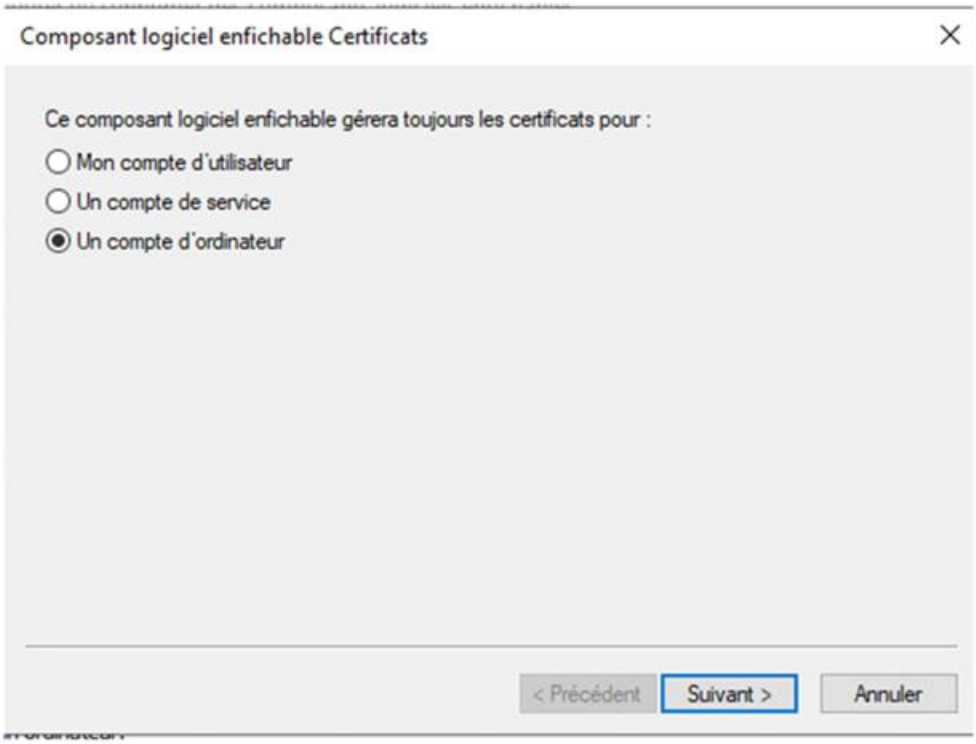
Puis fichier



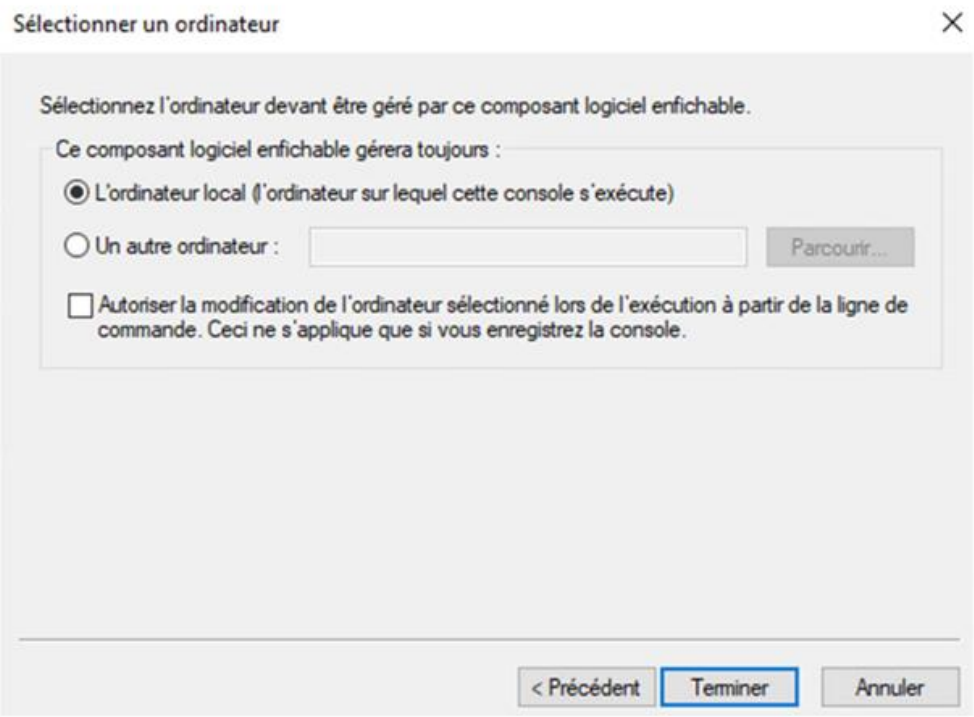
Puis certificat :



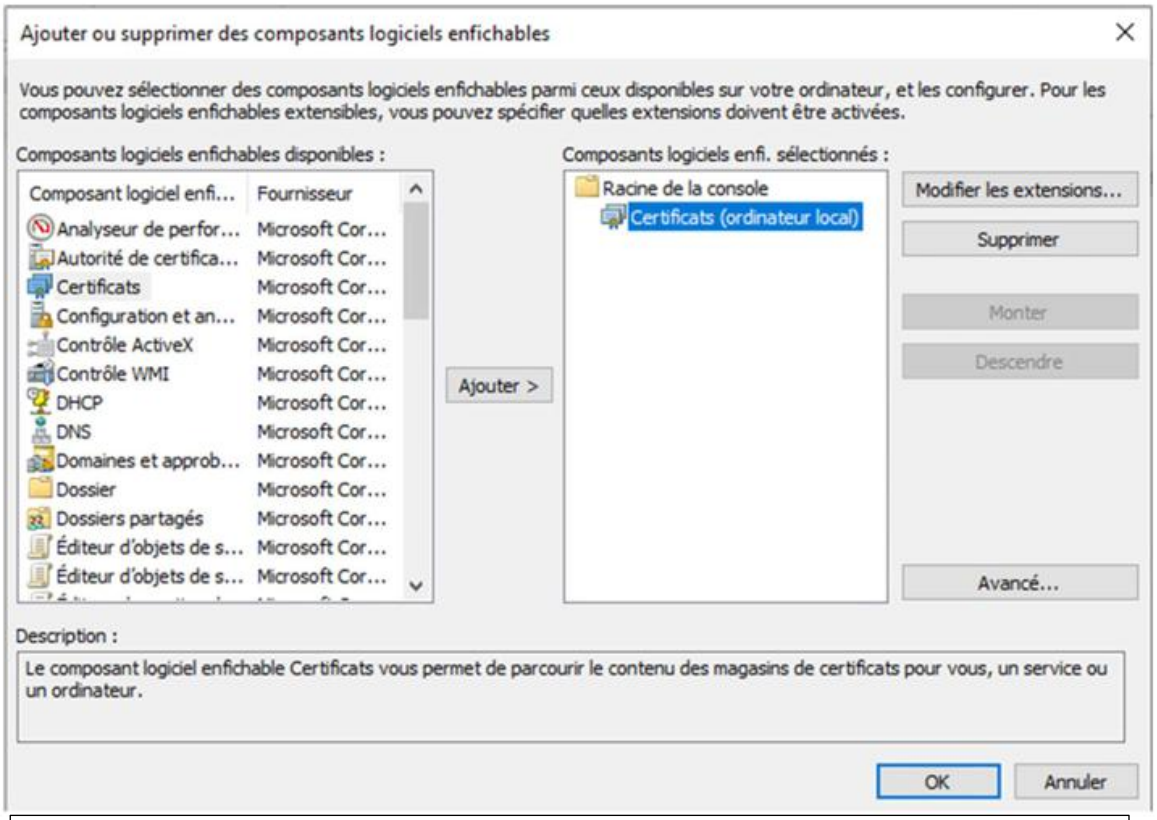
Sur « un compte d'ordinateur »



Puis sur l'ordinateur local

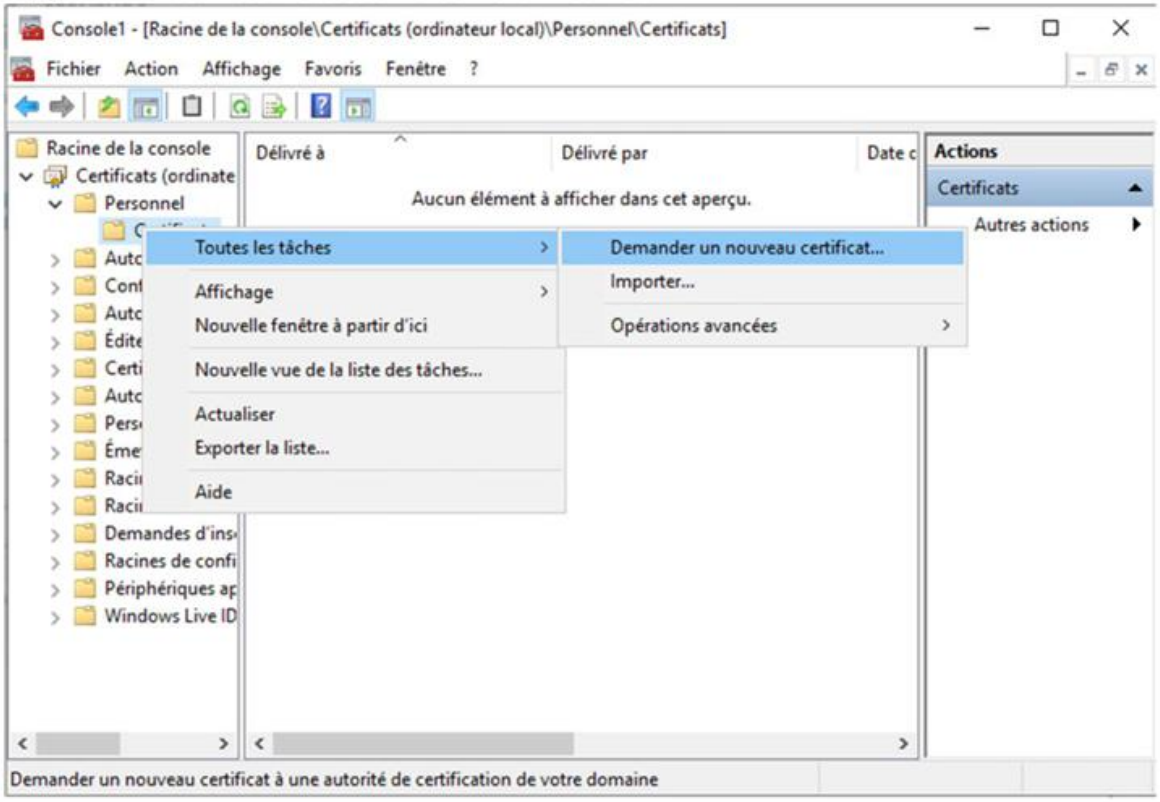


Cliquez sur « ok »

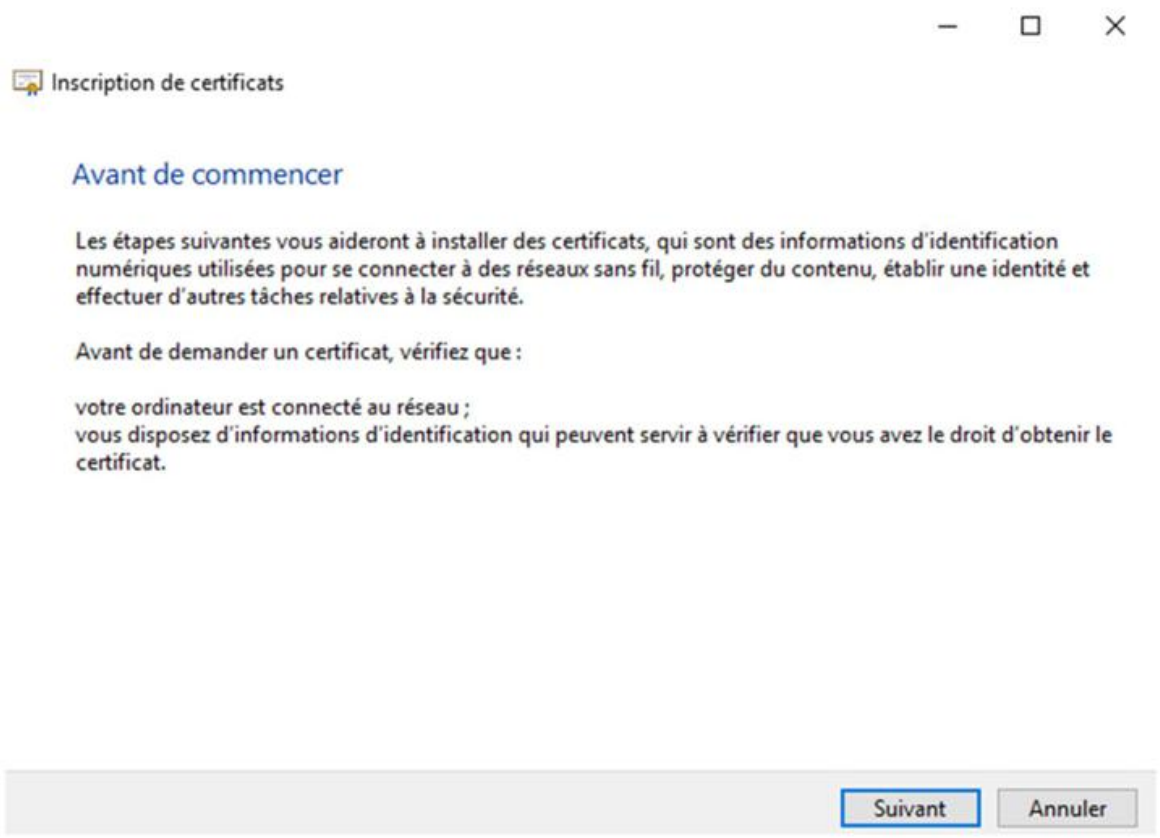


IL FAUT SUPPRIMER LE CERTIFICAT DEJA PRESENT

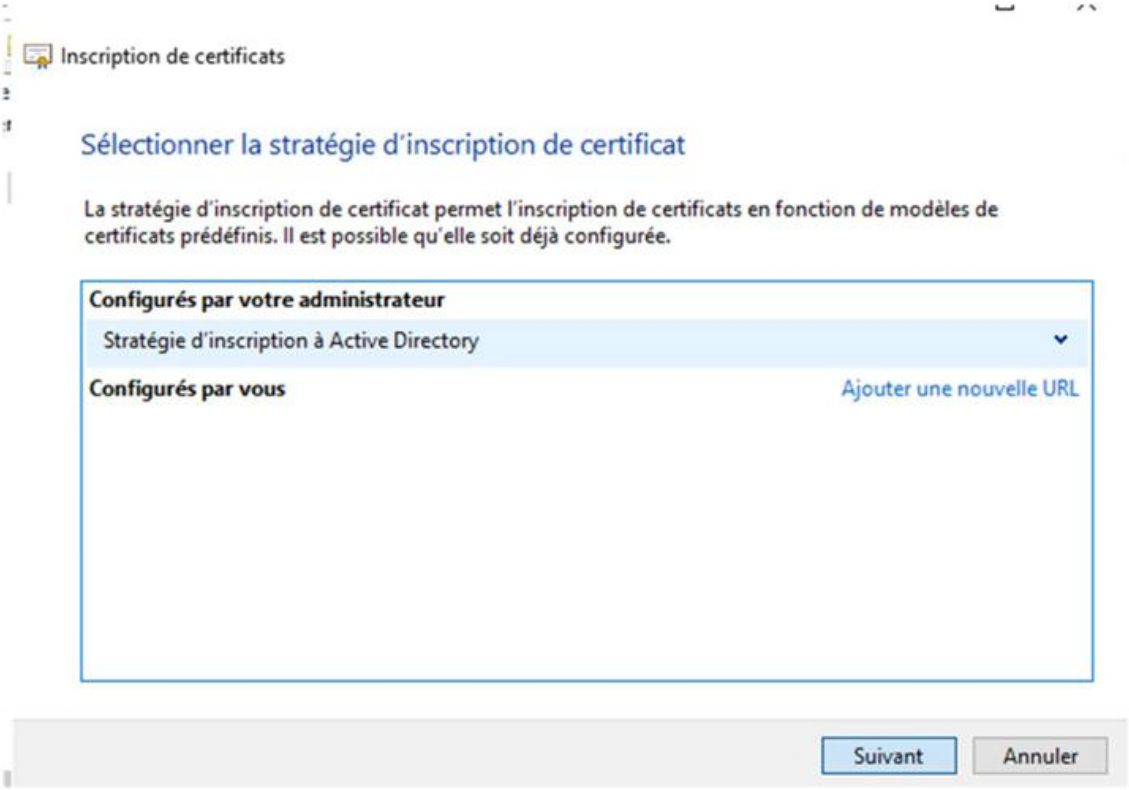
Supprimez l'ancien certificat et demandez en un nouveau :



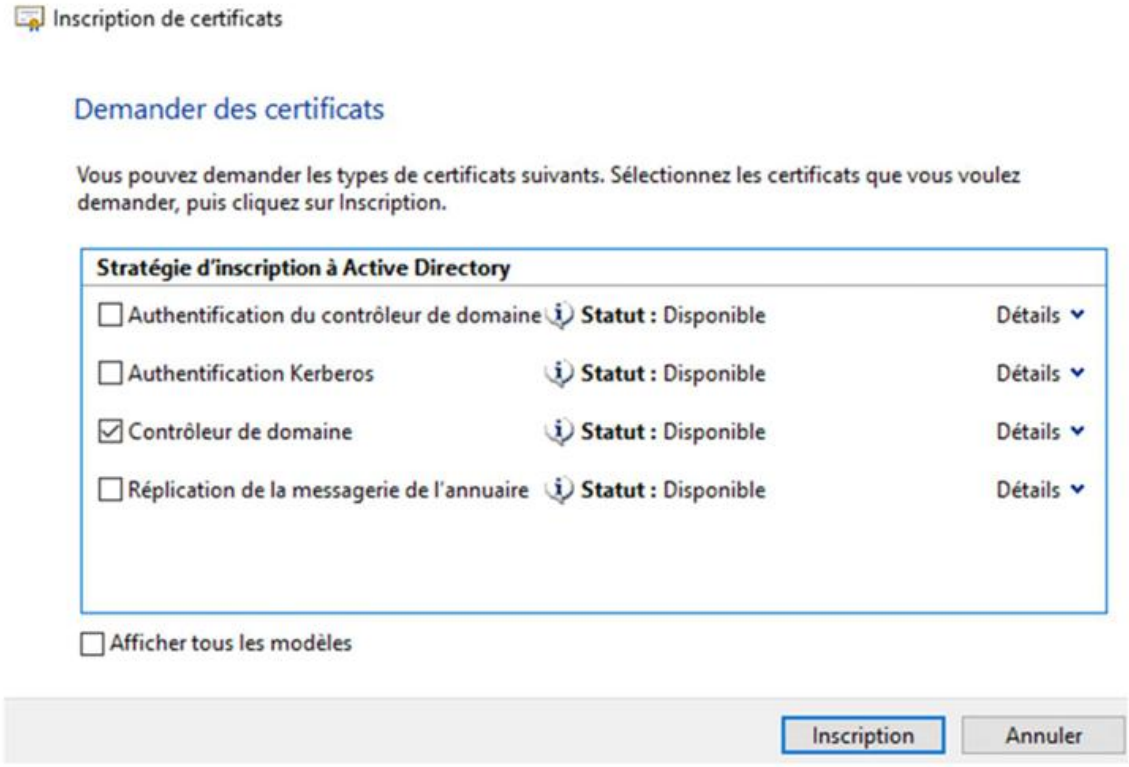
Suivant



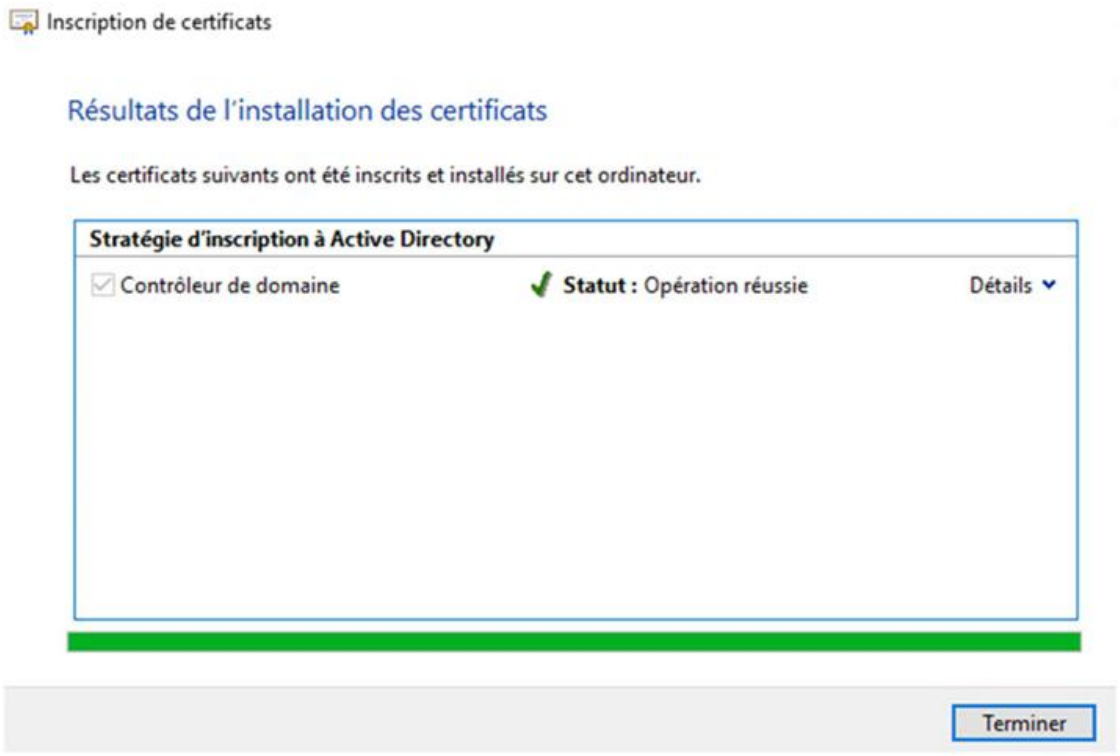
Suivant



Demander un certificat pour le contrôleur de domaine puis cliquez sur « Inscription » :

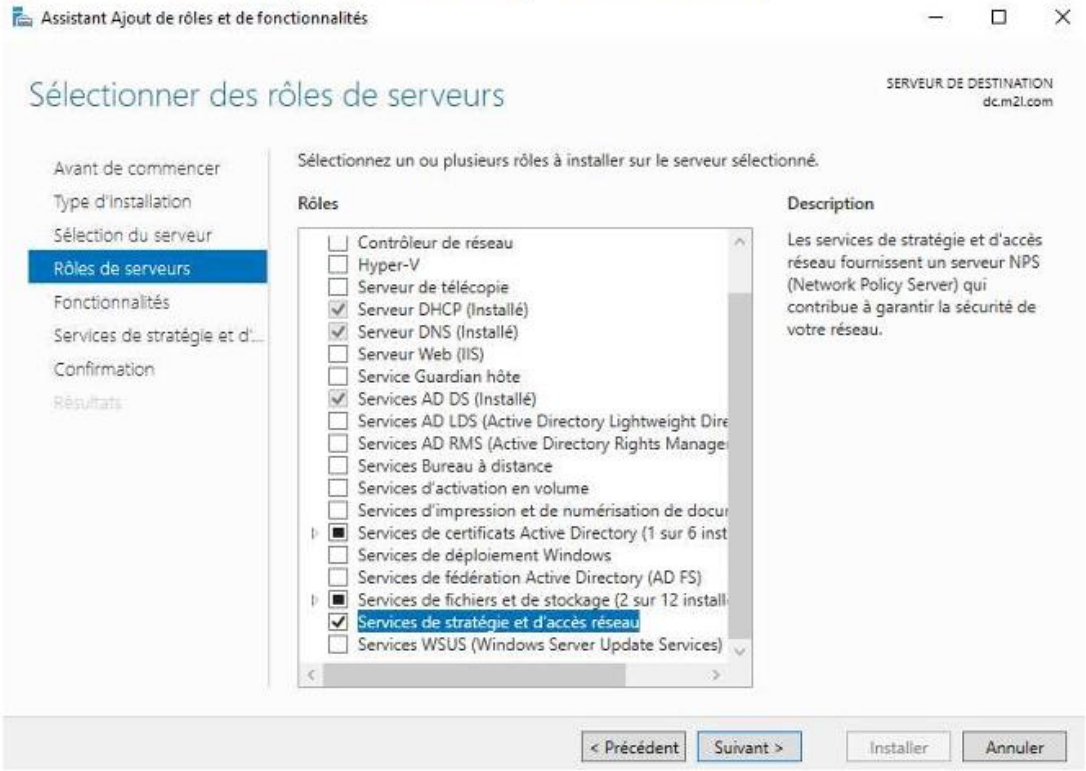


Le certificat est installé :

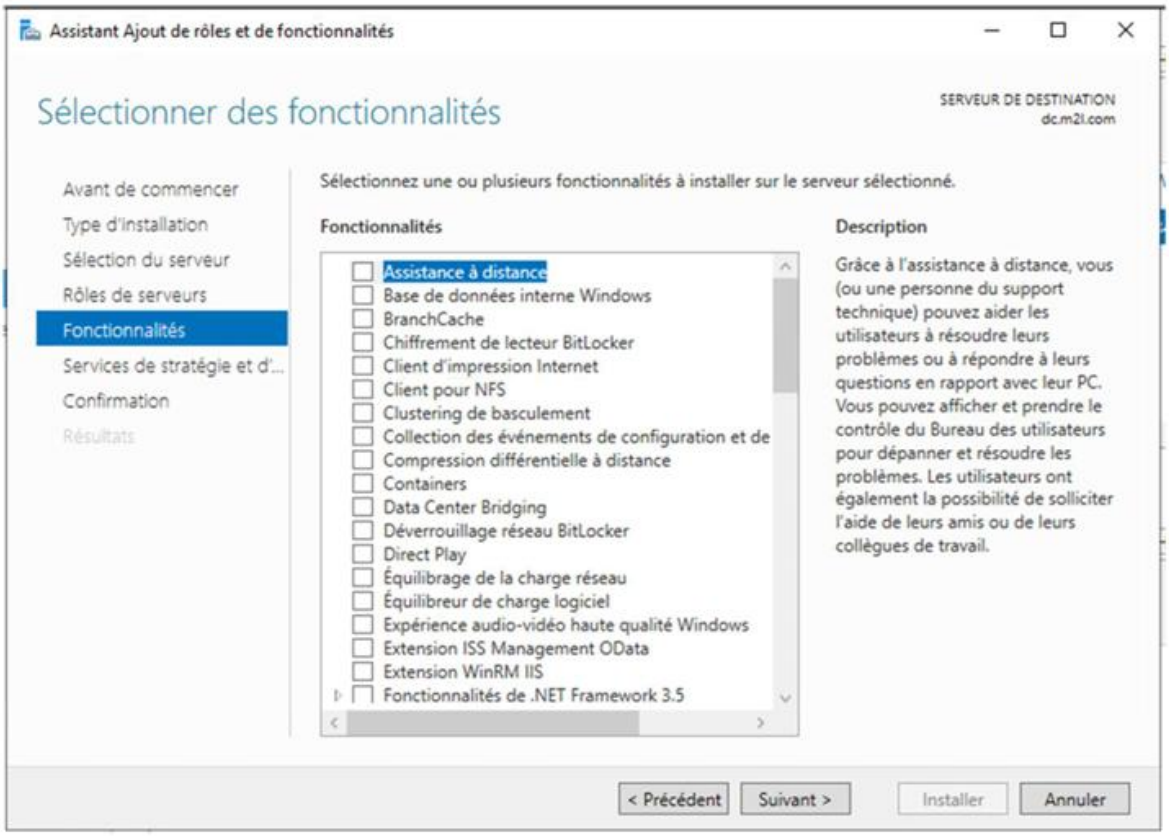


Il apparait :

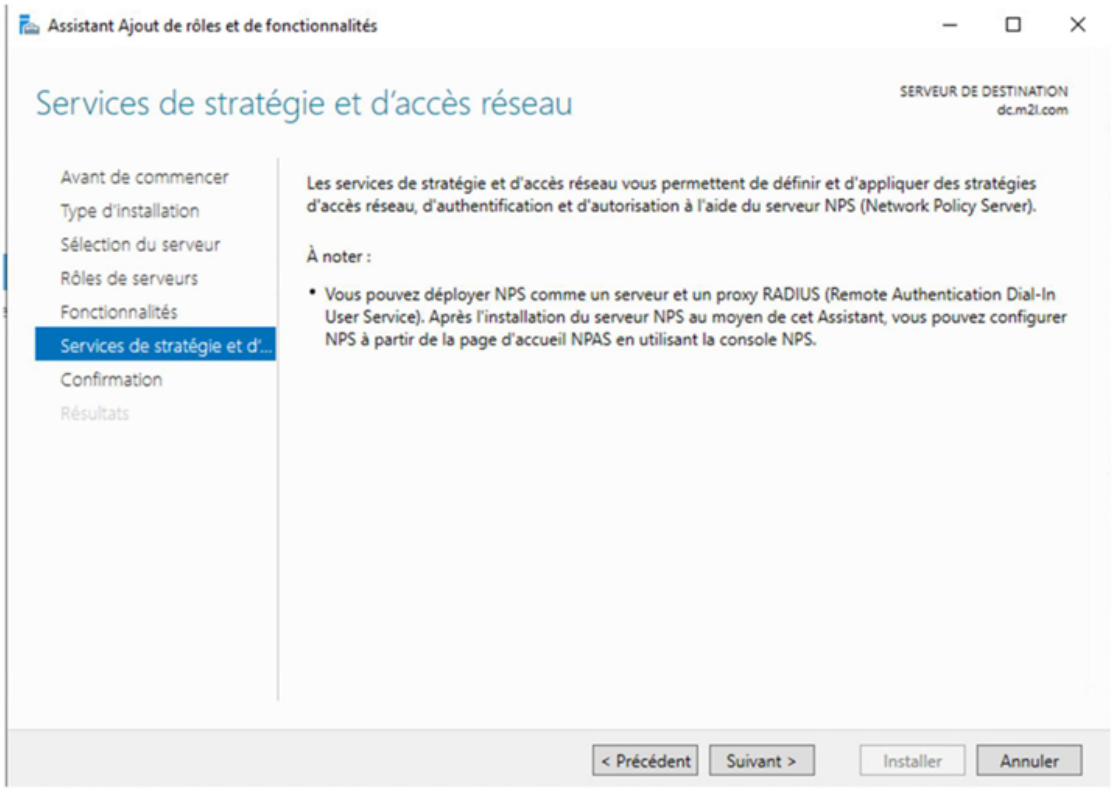
Ajout du service NPS (Service de stratégie d'accès réseau) :



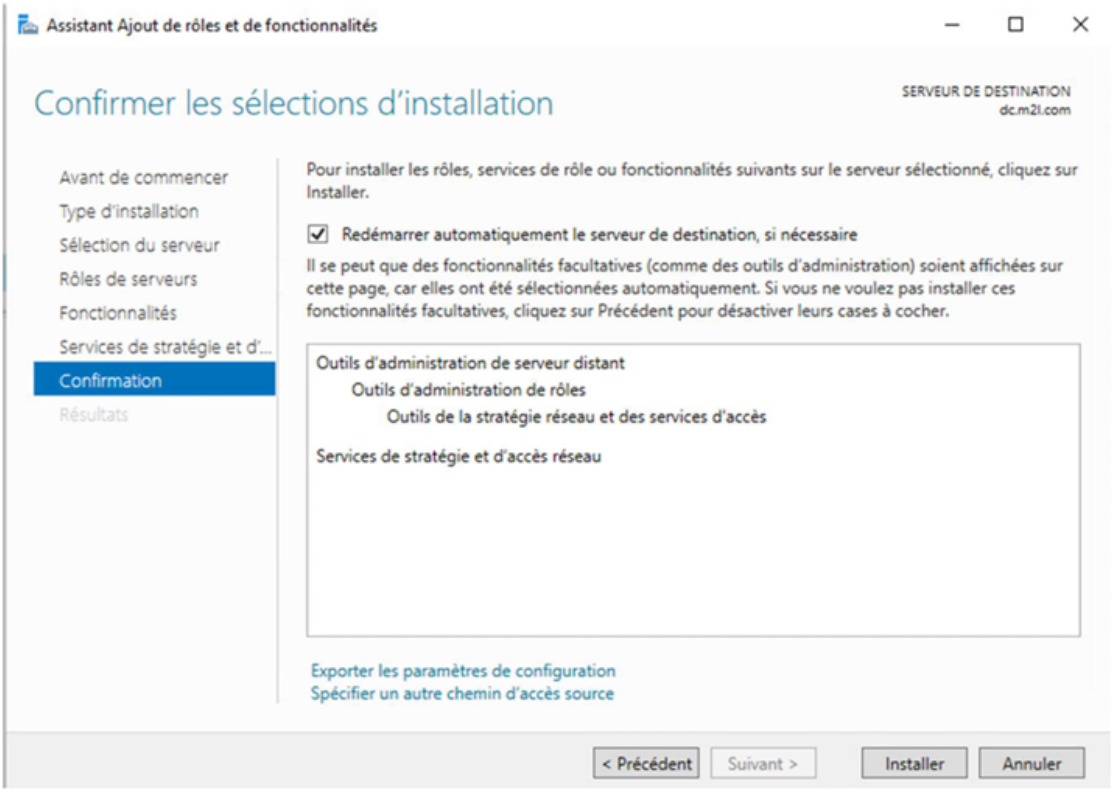
Suivant



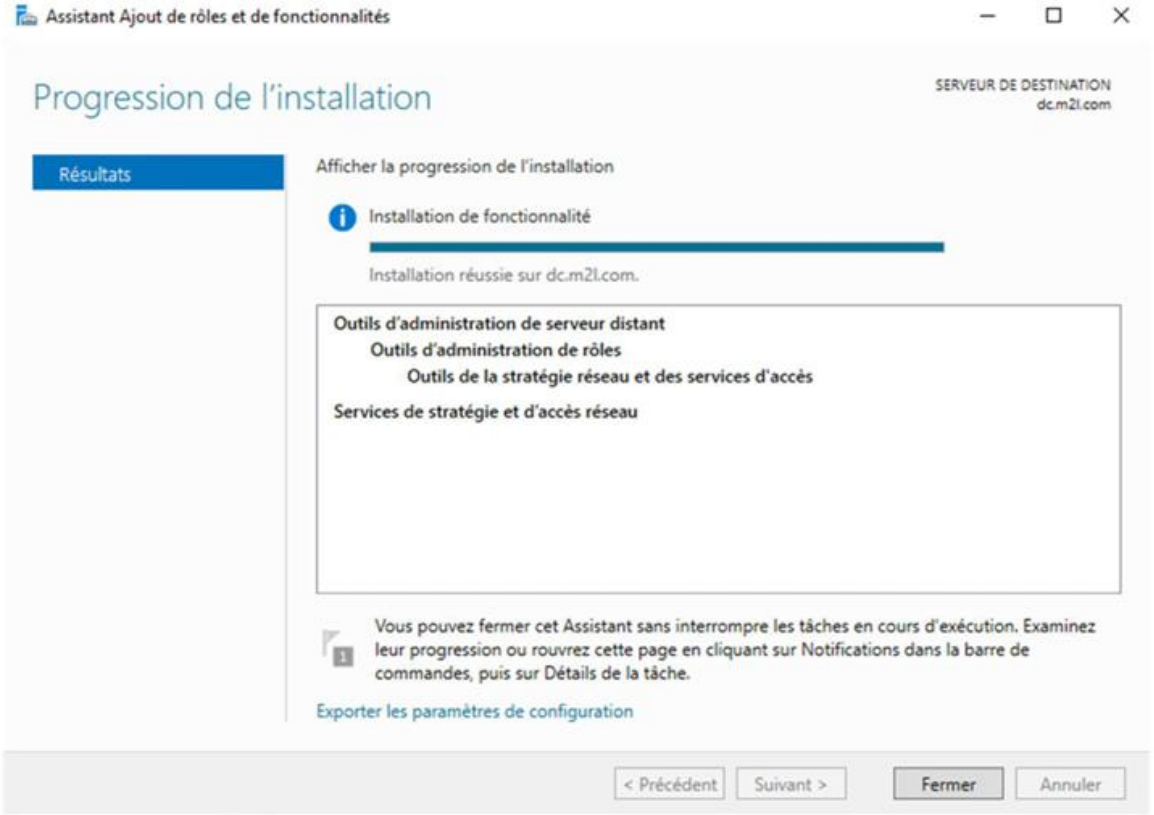
Suivant



Puis « installer »

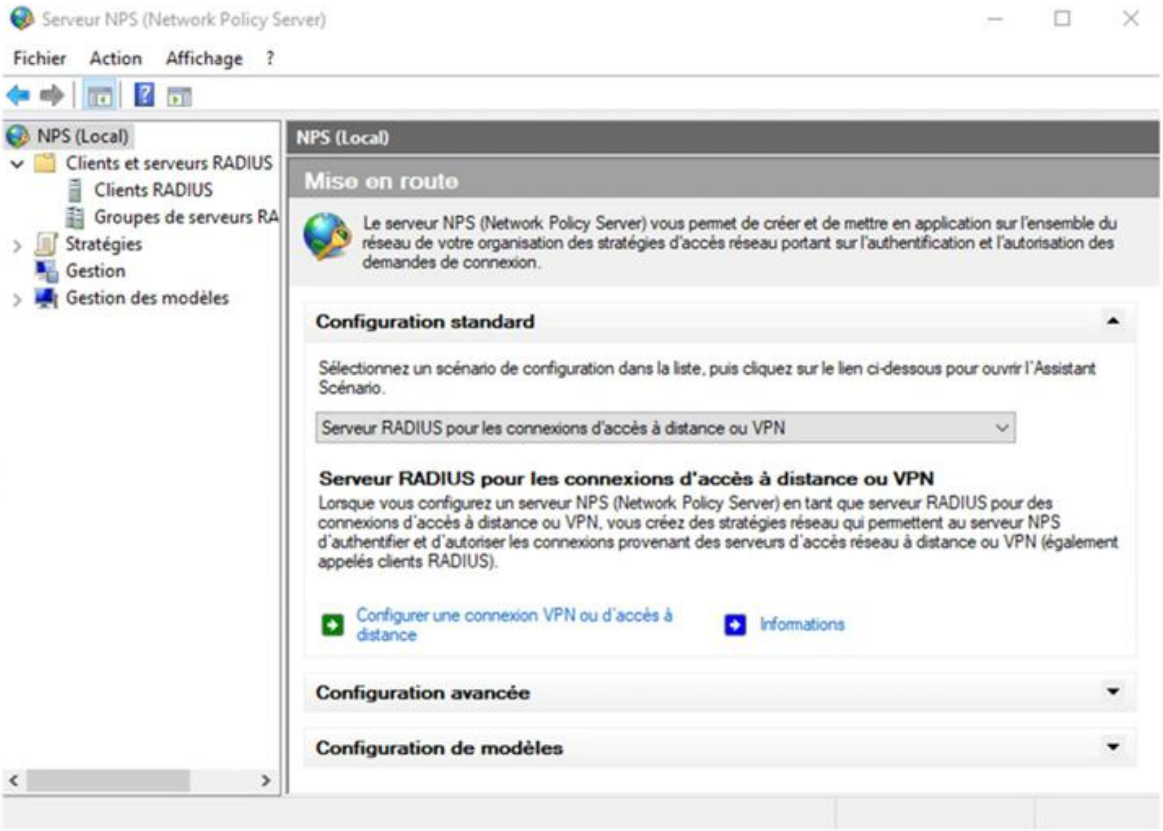


Voici la confirmation :



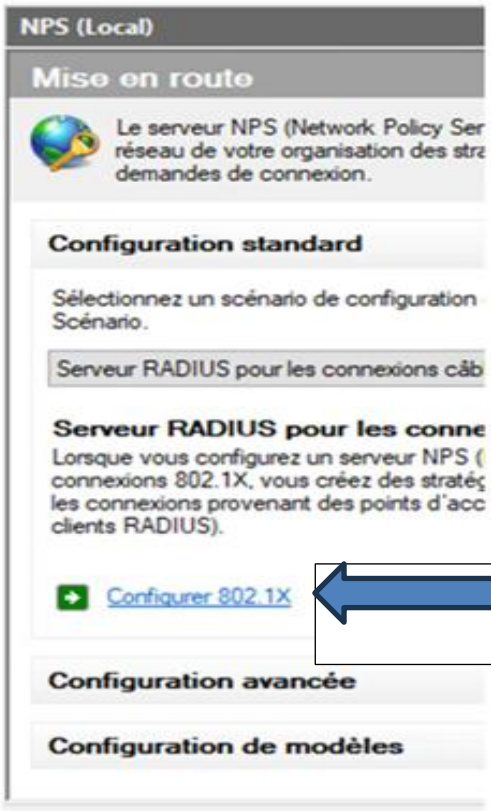
Il faut maintenant configurer le service NPS :

Voici la page de configuration :



Changer le scénario de configuration :

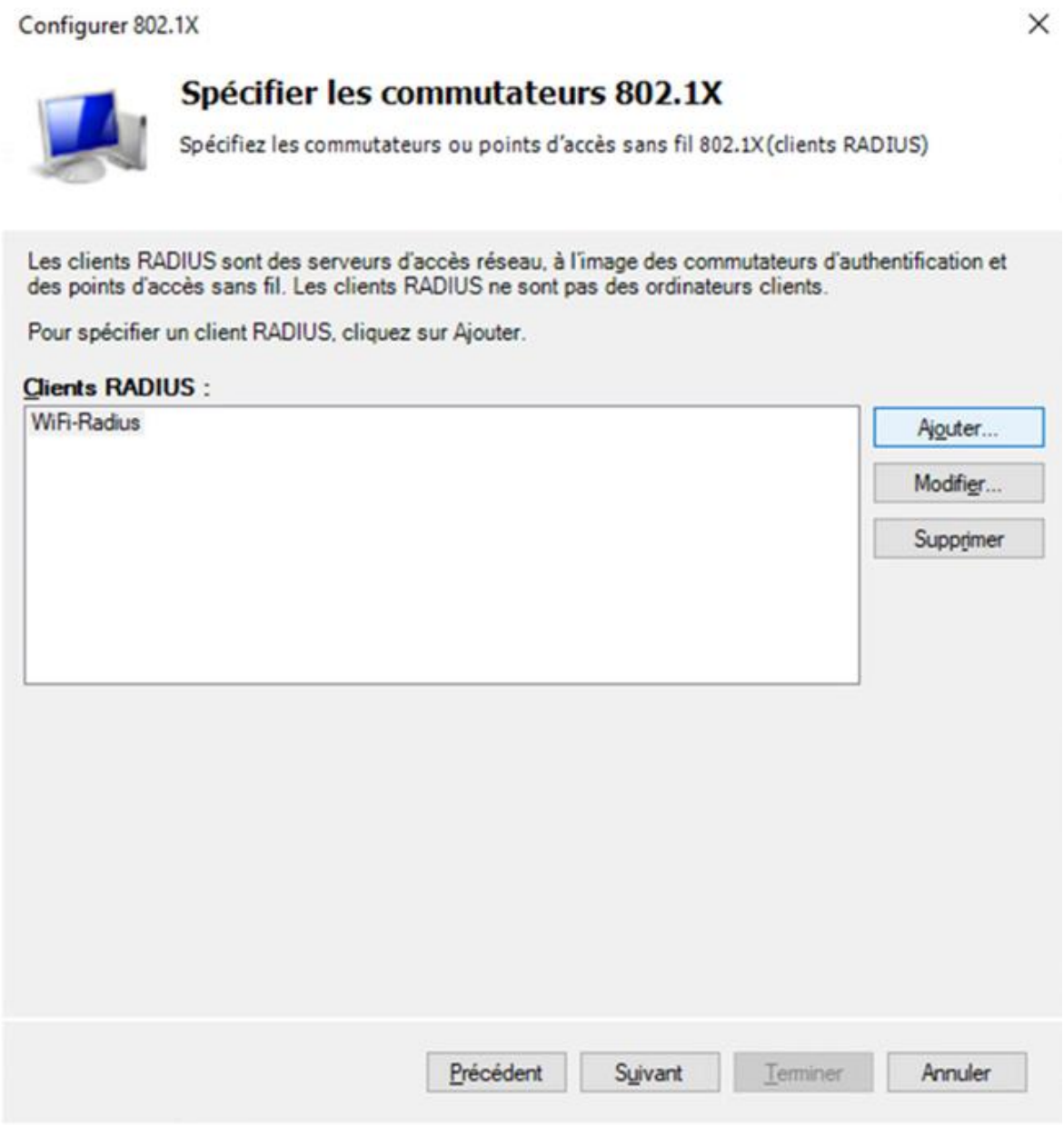
Configurer 802.1X :

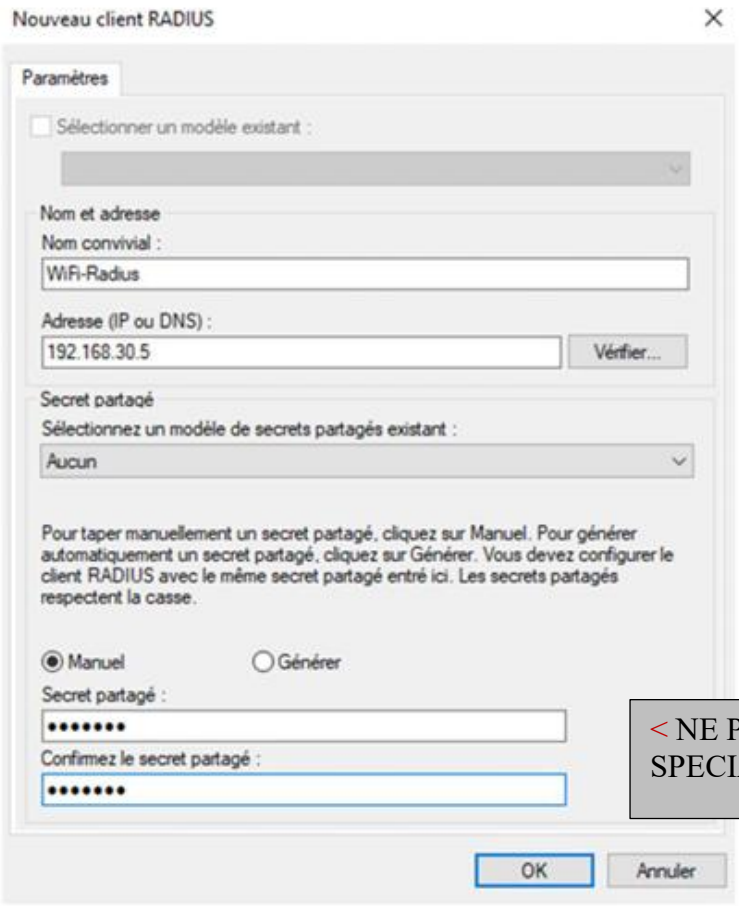


CLIQUER SUR CONFIGURER 802.1X

Donnez un nom à la connexion

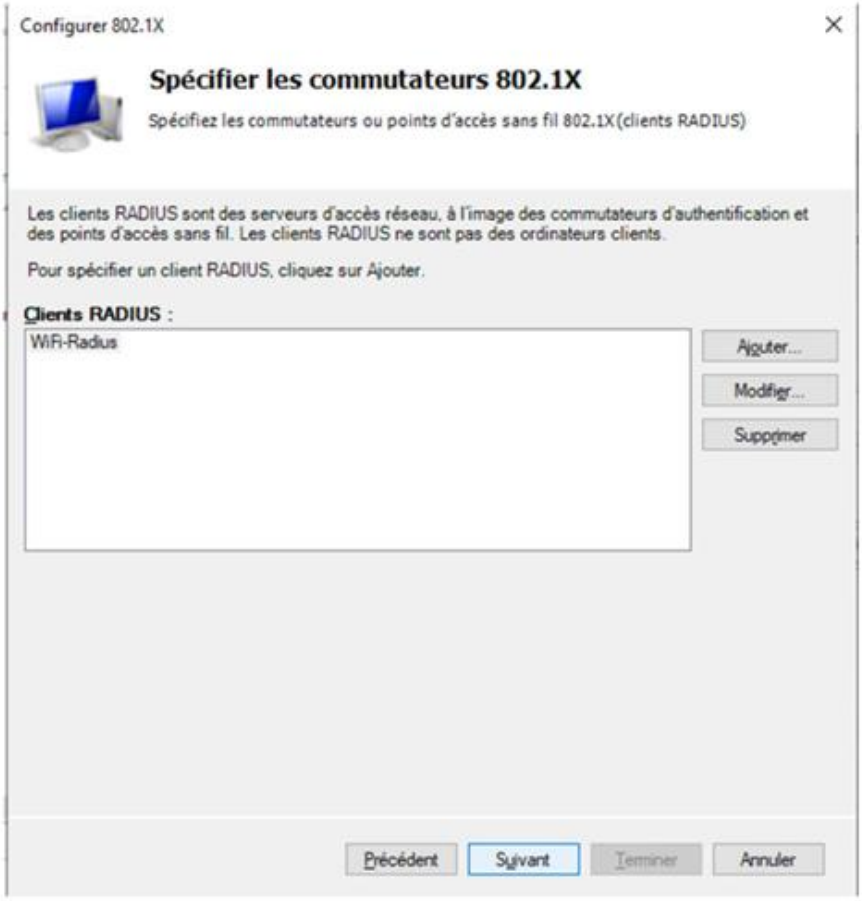
Ajouter un client Radius :



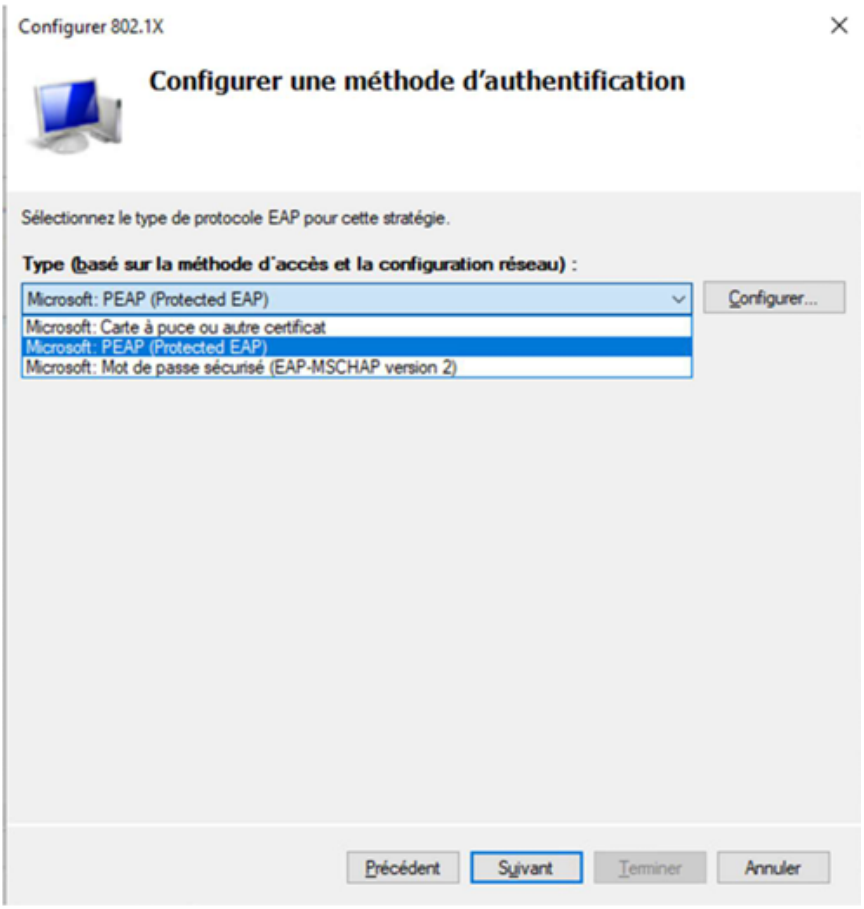


< NE PAS METTRE DE CARACTERE SPECIAUX COMME @/ !

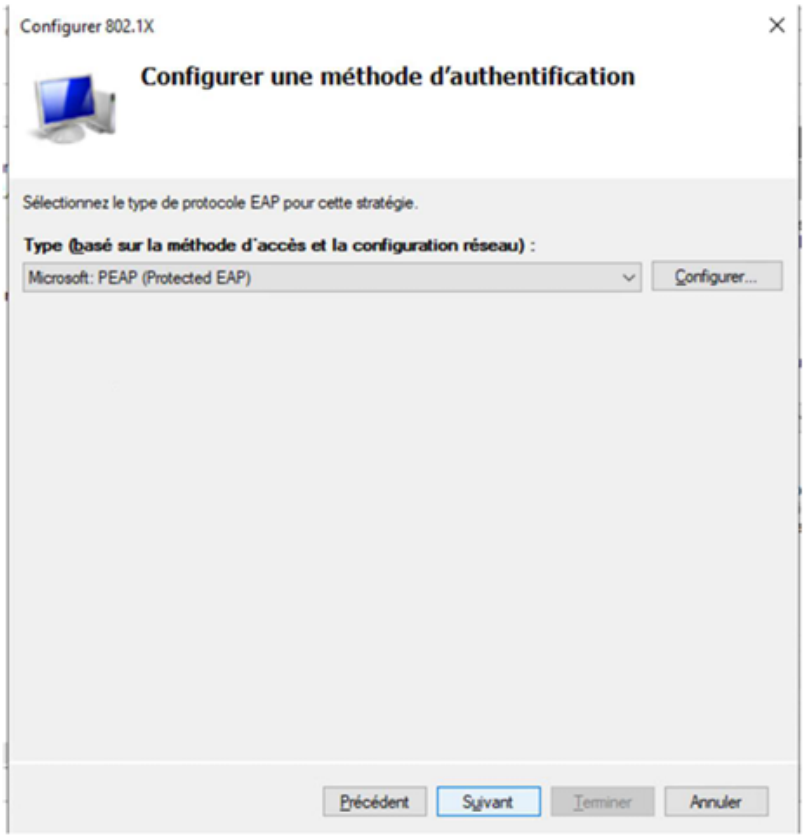
Puis Suivant



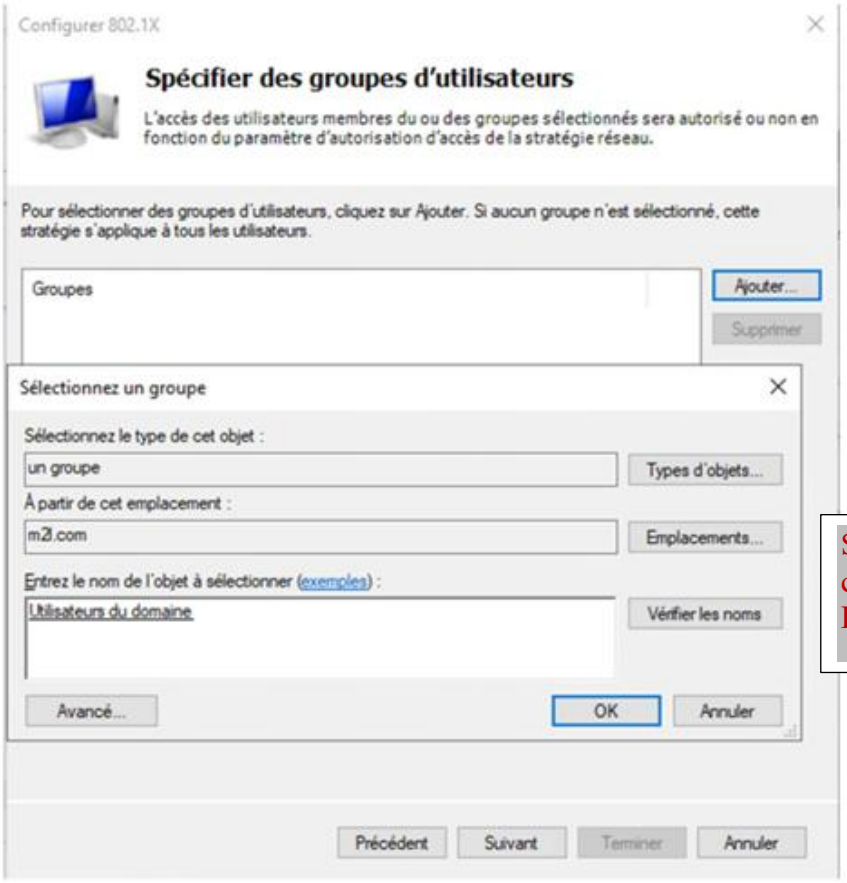
Sélectionner « Microsoft PEAP (EAP)



Suivant

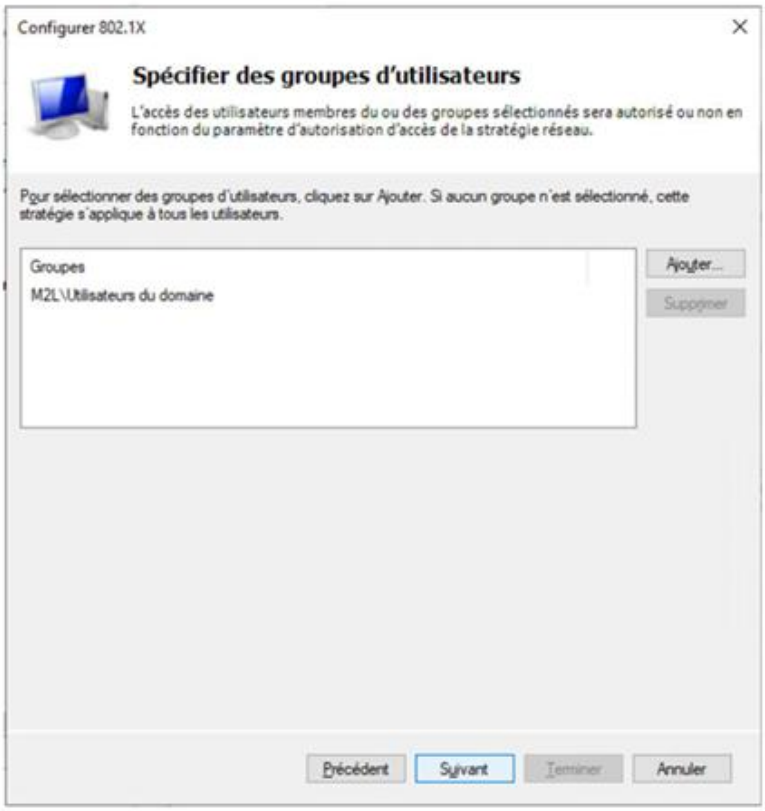


Ajouter les groupes d'utilisateurs :

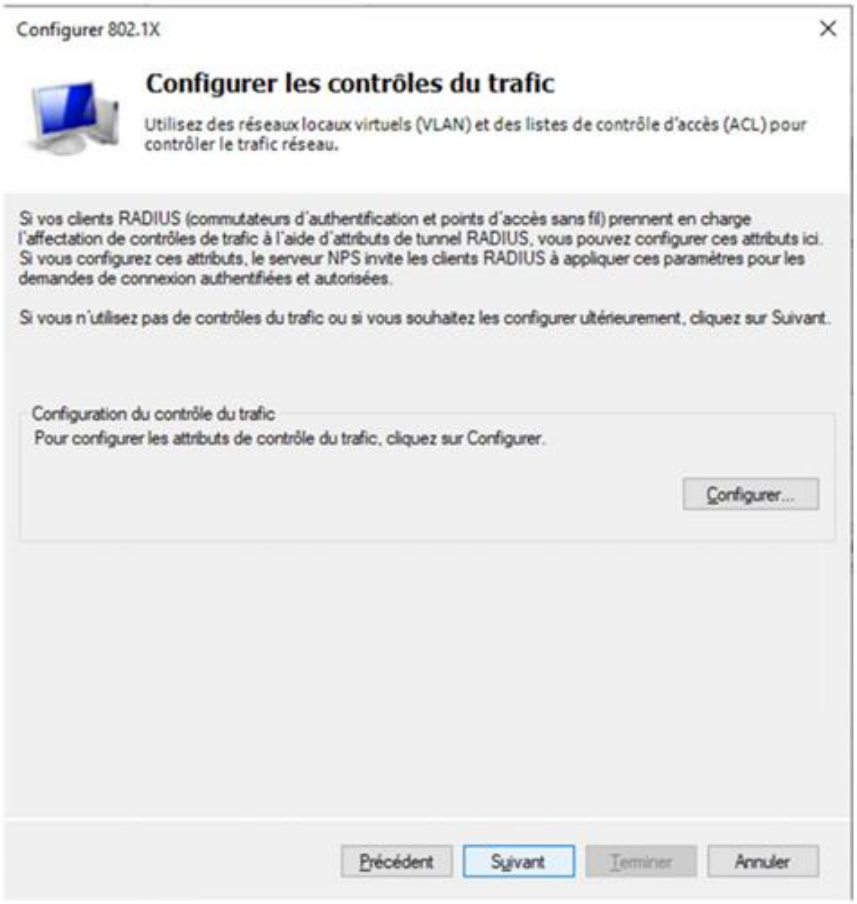


Spécifier un utilisateur du domaine crée, ou un groupe dans l'Active Directory

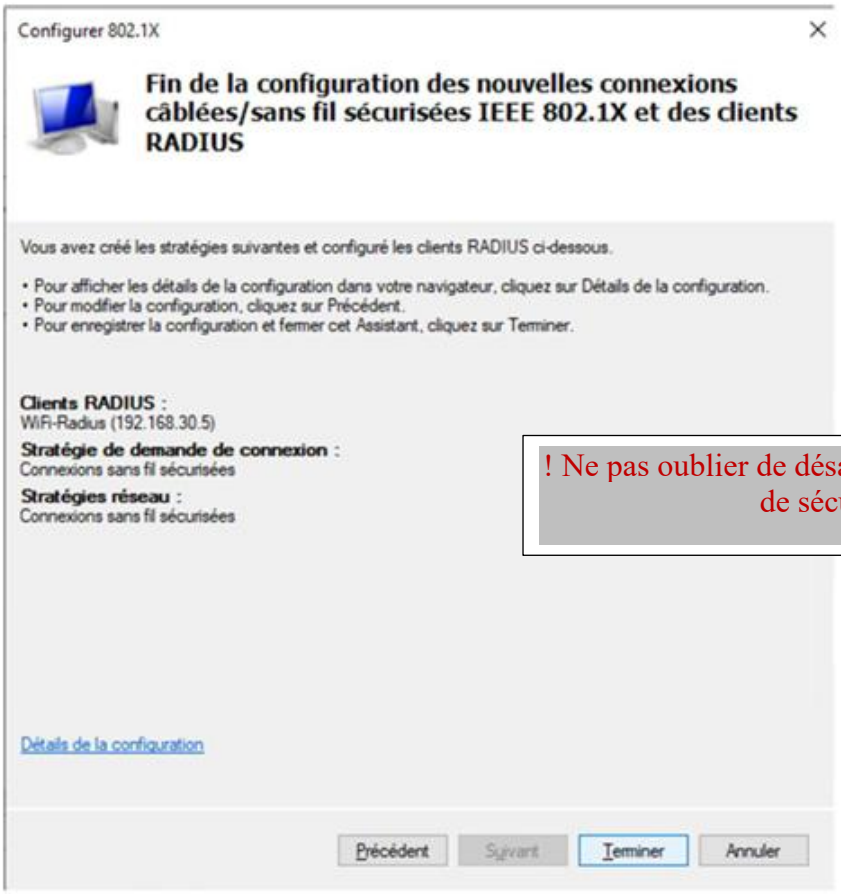
Puis suivant



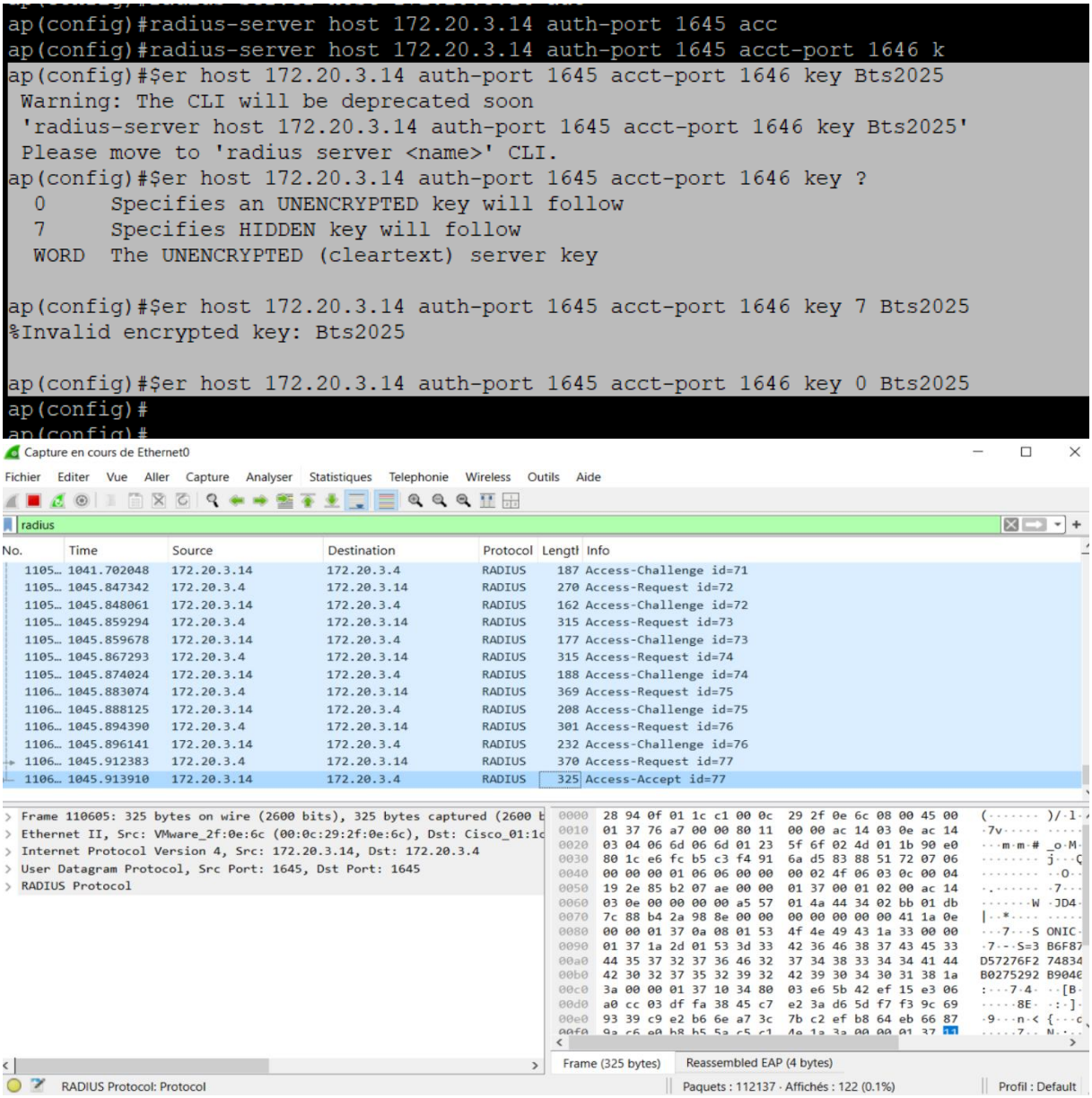
Suivant



Récapitulatif de la configuration



! Ne pas oublier de désactiver tous les pare-feu ou outils de sécurité Windows !



Dans ces captures d'écrans, nous voyons qu'un ordinateur invité avec l'adresse ip en 172.20.3.14 demande au serveur Radius (dans l'AD) en 172.20.3.4 un accès au WiFi. Celui-ci lui envoie un "challenge" sous forme d'authentification. En rentrant les identifiants d'un utilisateur de l'AD (autorisé à accéder au WiFi), le challenge est passé et l'accès est accepté.

Conclusion :

La mise en place d'une solution Wi-Fi sécurisée pour les employés et les visiteurs du stade, basée sur des points d'accès PoE et la norme WPA2 Enterprise, assure un accès sans fil fiable et sécurisé. L'intégration du protocole RADIUS pour l'authentification des employés et la création d'un réseau Wi-Fi distinct pour les visiteurs permettent de répondre aux exigences de sécurité et aux obligations légales. Avec une configuration adaptée des switchs PoE, des points d'accès et des SSID, cette solution garantit une gestion fluide et sécurisée des connexions Wi-Fi, tout en préparant la phase de renforcement de l'authentification