

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 StadiumCompany (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.

StadiumCompany 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 Authentification Dial-in User Service) est un protocole client-serveur permettant de centraliser les données d'authentification.

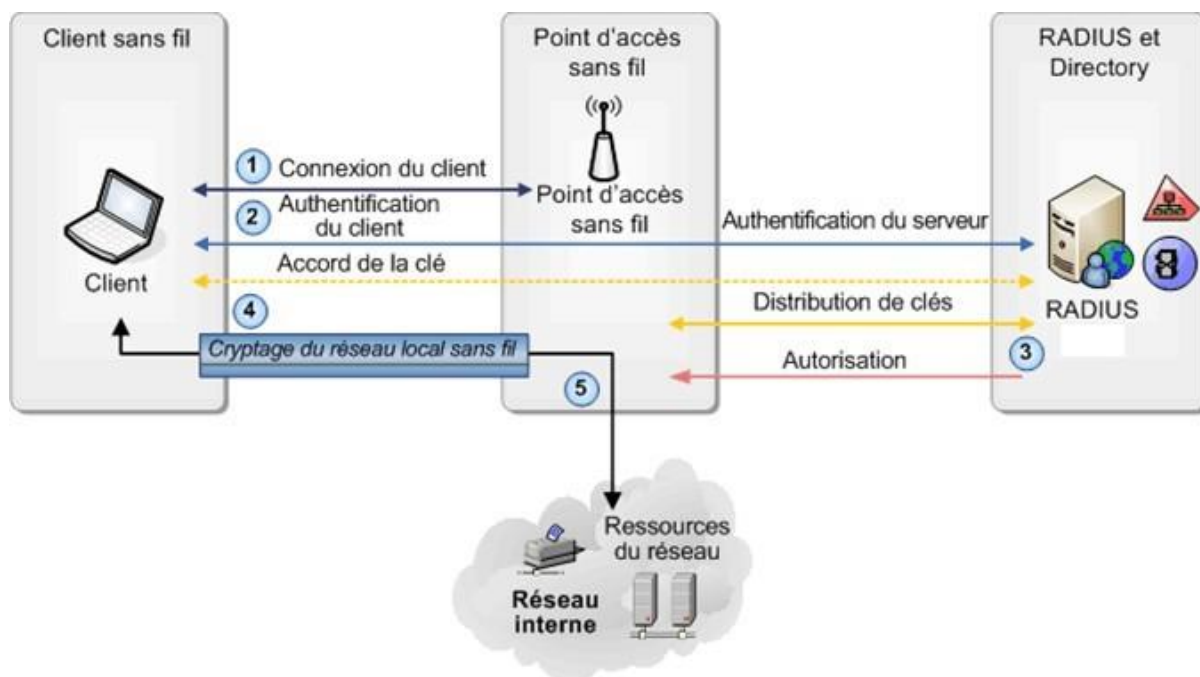
Pour s'authentifier, le poste utilisateur transmet une requête d'accès à un client RADIUS pour entrer sur le réseau, ce dernier se charge de demander les informations identifiant l'utilisateur (utilisateur & mot de passe). Le client RADIUS génère une requête d'accès qu'il transmet au serveur RADIUS,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

<p>CISCO Aironet 1042 N</p>		<ul style="list-style-type: none"> <li>- Interface de gestion sécurisée</li> <li>- Ligne de commande (telnet et SSH)</li> <li>- WPA2 AES</li> <li>- Filtre MAC</li> <li>- RADIUS</li> <li>- SSID Caché</li> <li>- Multi-SSID</li> <li>- PoE</li> <li>- 802.11a/b/g/n</li> <li>- VLAN 802.1Q</li> </ul>
-----------------------------	--------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## 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
Procédure :
```

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-Presses 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-Pressé
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-Press 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 :

Assistant Ajout de rôles et de fonctionnalités

SÉLECTIONNER DES RÔLES DE SERVEURS

SERVEUR DE DESTINATION  
dc.m2i.com

Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.

Rôles	Description
<input type="checkbox"/> Contrôleur de réseau	
<input type="checkbox"/> Hyper-V	
<input type="checkbox"/> Serveur de télécopie	
<input checked="" type="checkbox"/> Serveur DHCP (Installé)	
<input checked="" type="checkbox"/> Serveur DNS (Installé)	
<input type="checkbox"/> Serveur Web (IIS)	
<input type="checkbox"/> Service Guardian hôte	
<input checked="" type="checkbox"/> Services AD DS (Installé)	
<input type="checkbox"/> Services AD LDS (Active Directory Lightweight Directory Services)	
<input type="checkbox"/> Services AD RMS (Active Directory Rights Management Services)	
<input type="checkbox"/> Services Bureau à distance	
<input type="checkbox"/> Services d'activation en volume	
<input type="checkbox"/> Services d'impression et de numérisation de documents	
<input checked="" type="checkbox"/> Services de certificats Active Directory	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.
<input type="checkbox"/> Services de déploiement Windows	
<input type="checkbox"/> Services de fédération Active Directory (AD FS)	
<input type="checkbox"/> Services de fichiers et de stockage (2 sur 12 installés)	
<input type="checkbox"/> Services de stratégie et d'accès réseau	
<input type="checkbox"/> Services WSUS (Windows Server Update Services)	

< Précédent   Suivant >   Installer   Annuler

### Puis suivant

Assistant Ajout de rôles et de fonctionnalités

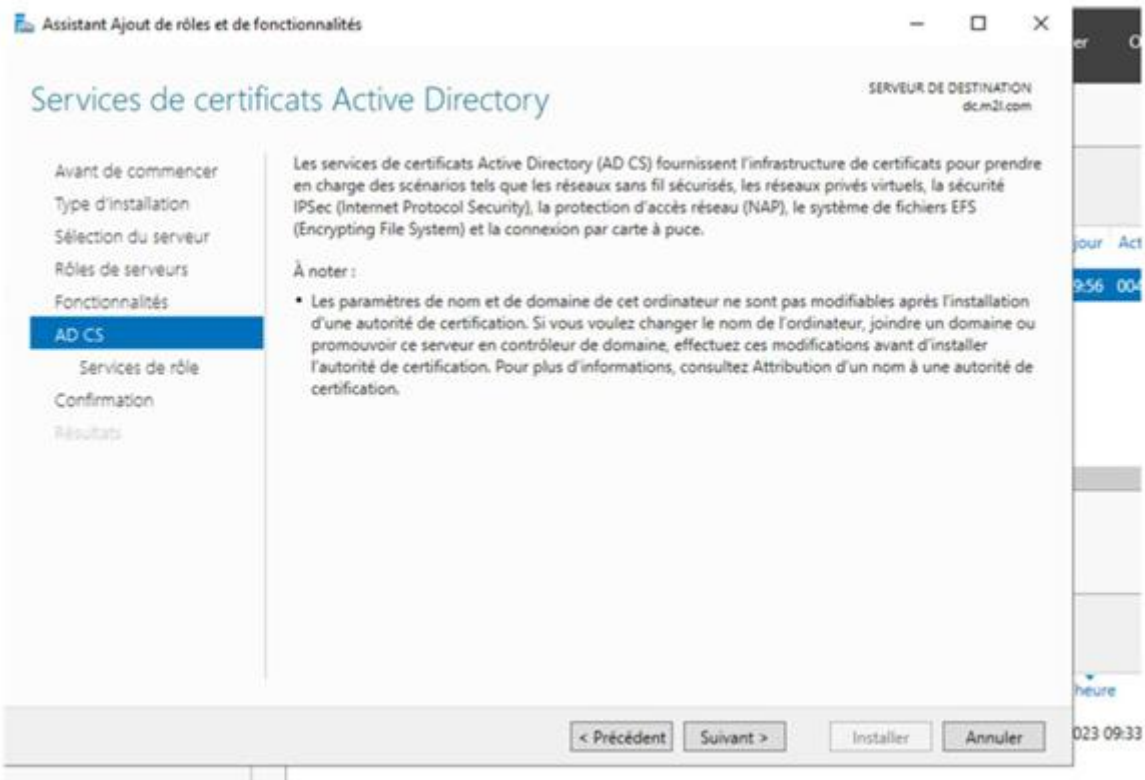
SÉLECTIONNER DES FONCTIONNALITÉS

SERVEUR DE DESTINATION  
dc.m2i.com

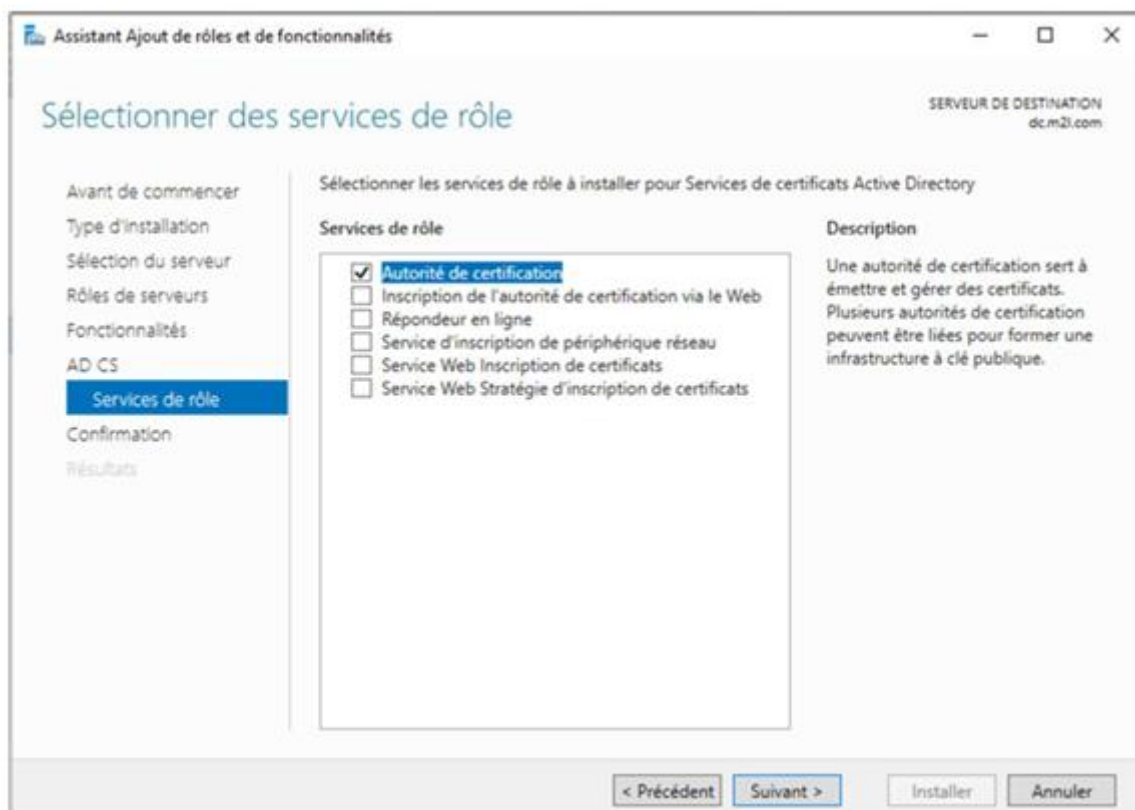
Sélectionnez une ou plusieurs fonctionnalités à installer sur le serveur sélectionné.

Fonctionnalités	Description
<input checked="" type="checkbox"/> Assistance à distance	Grâce à l'assistance à distance, vous (ou une personne du support technique) pouvez aider les utilisateurs à résoudre leurs problèmes ou à répondre à leurs questions en rapport avec leur PC. Vous pouvez afficher et prendre le contrôle du Bureau des utilisateurs pour dépanner et résoudre les problèmes. Les utilisateurs ont également la possibilité de solliciter l'aide de leurs amis ou de leurs collègues de travail.
<input type="checkbox"/> Base de données interne Windows	
<input type="checkbox"/> BranchCache	
<input type="checkbox"/> Chiffrement de lecteur BitLocker	
<input type="checkbox"/> Client d'impression Internet	
<input type="checkbox"/> Client pour NFS	
<input type="checkbox"/> Clustering de basculement	
<input type="checkbox"/> Collection des événements de configuration et de diagnostic	
<input type="checkbox"/> Compression différentielle à distance	
<input type="checkbox"/> Containers	
<input type="checkbox"/> Data Center Bridging	
<input type="checkbox"/> Déverrouillage réseau BitLocker	
<input type="checkbox"/> Direct Play	
<input type="checkbox"/> Équilibrage de la charge réseau	
<input type="checkbox"/> Équilibreur de charge logiciel	
<input type="checkbox"/> Expérience audio-vidéo haute qualité Windows	
<input type="checkbox"/> Extension ISS Management OData	
<input type="checkbox"/> Extension WinRM IIS	
<input type="checkbox"/> Fonctionnalités de .NET Framework 3.5	

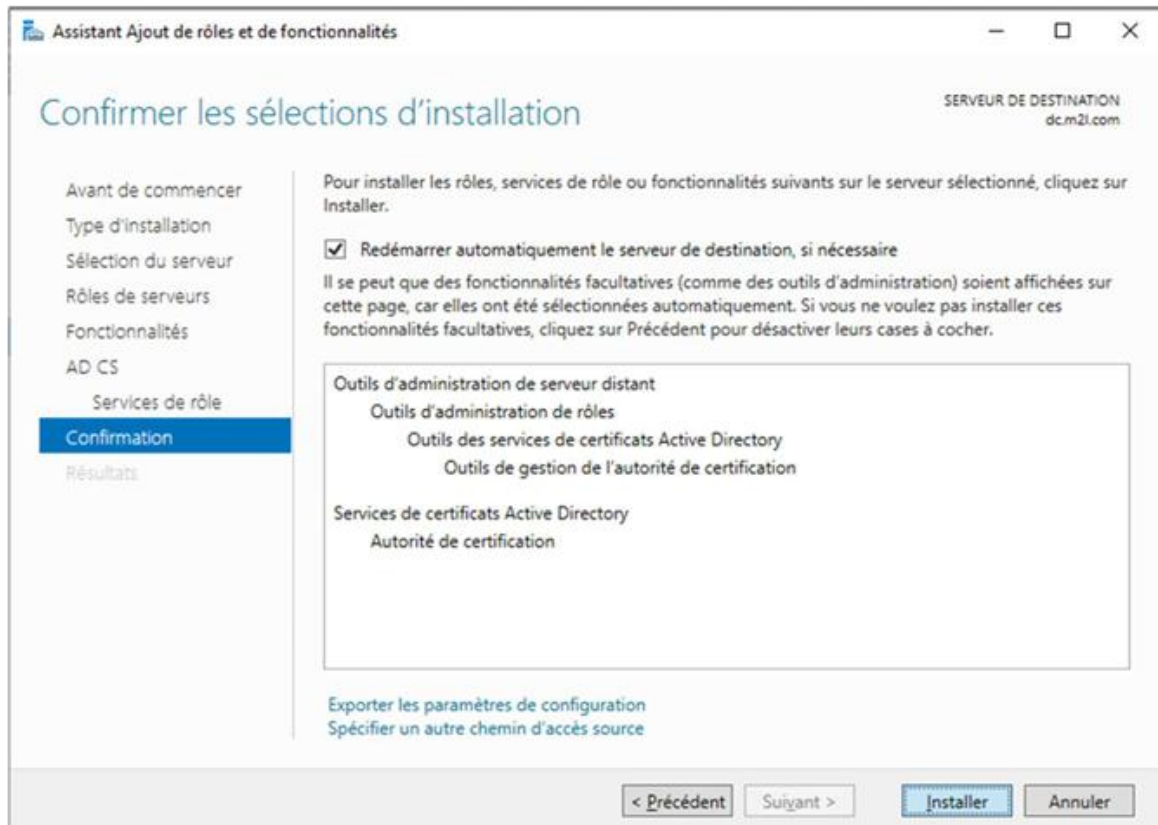
< Précédent   Suivant >   Installer   Annuler



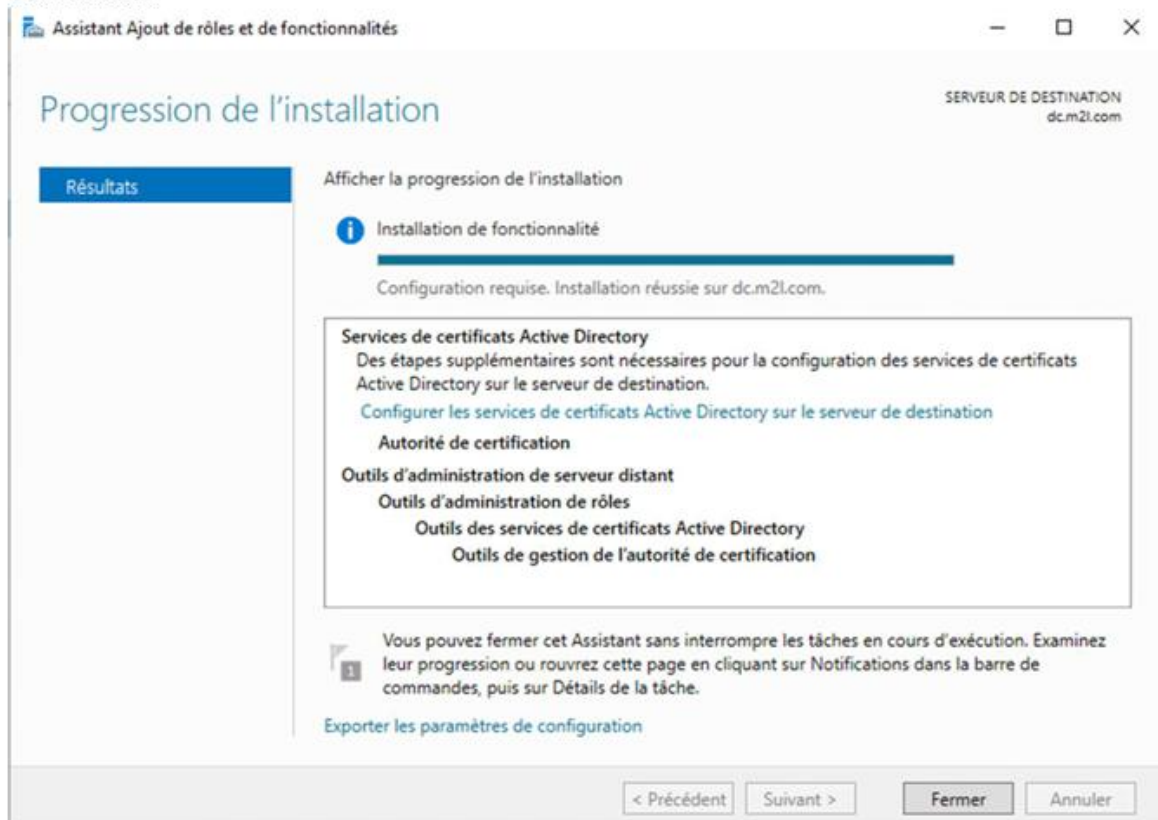
## Suivant



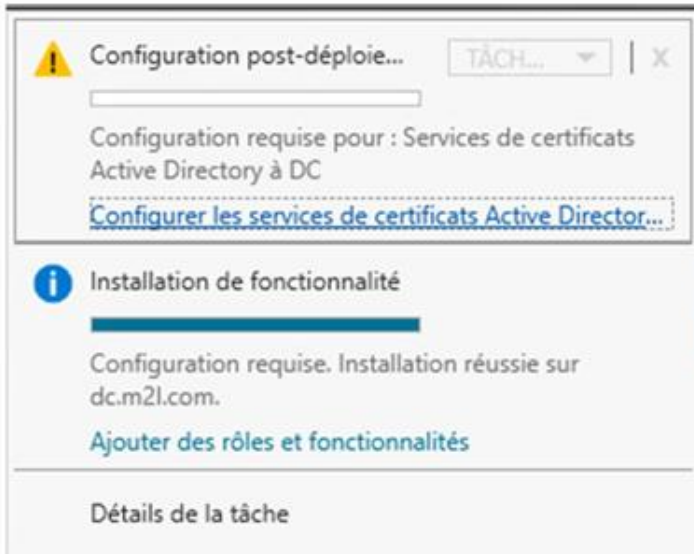
## Et installer



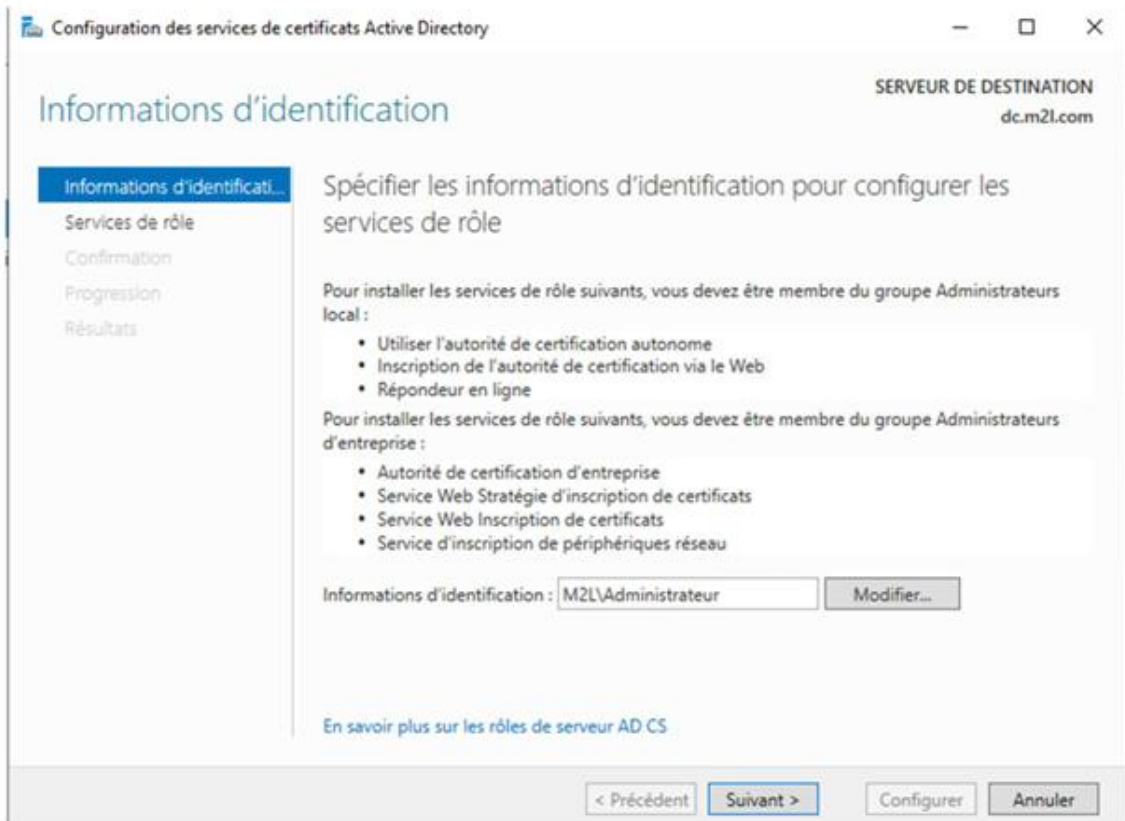
## Confirmation



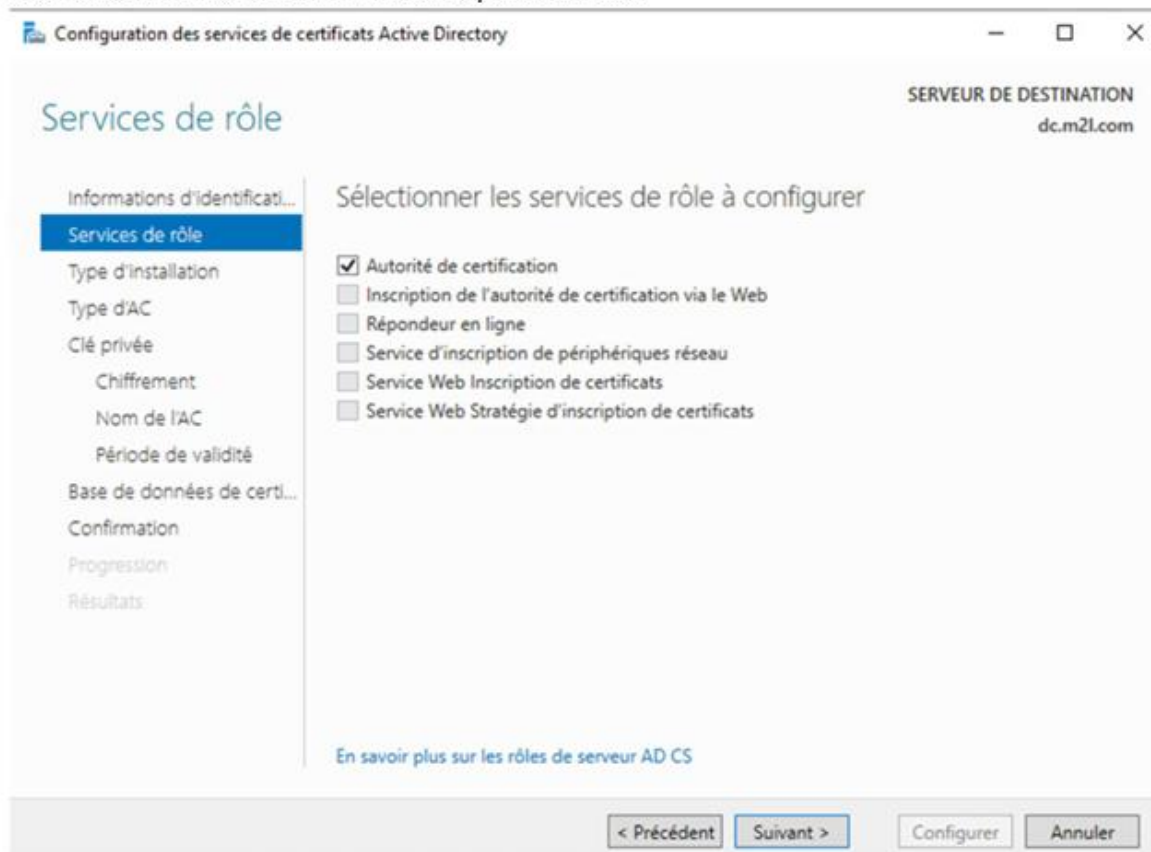
Cliquez sur « Configurer les services »



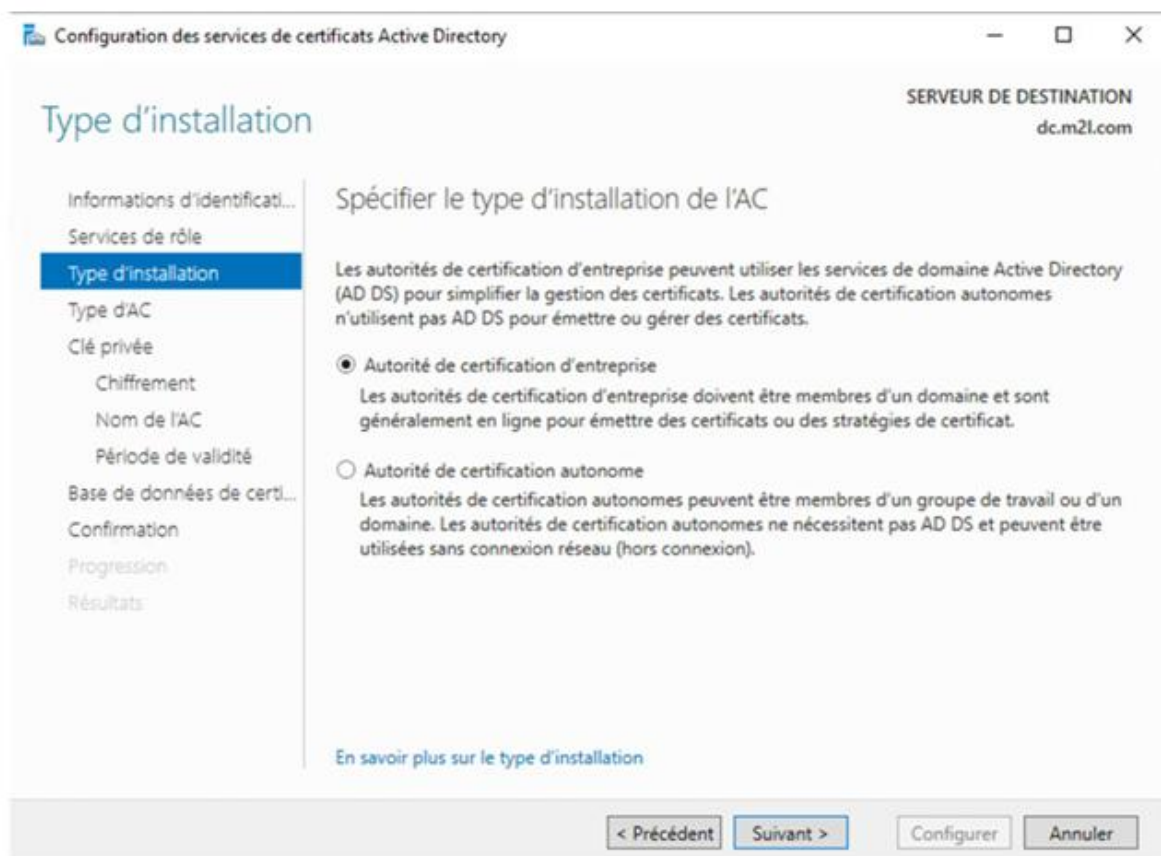
Cliquez sur Suivant



Cochez « Autorité de Certification » puis suivant :



Suivant



## Suivant

Configuration des services de certificats Active Directory

— □ ×

SERVERE DE DESTINATION  
dc.m2l.com

### Type d'autorité de certification

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

## Suivant

Configuration des services de certificats Active Directory

— □ ×

SERVERE DE DESTINATION  
dc.m2l.com

### Clé privée

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

## Sélectionner l'algorithme de hachage : SHA1

Configuration des services de certificats Active Directory

Chiffrement pour l'autorité de certification

SERVEUR DE DESTINATION  
dc.m2l.com

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 :  
2048

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

## Suivant

Configuration des services de certificats Active Directory

Nom de l'autorité de certification

SERVEUR DE DESTINATION  
dc.m2l.com

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 :  
m2l-DC-CA

Suffixe du nom unique :  
DC=m2l,DC=com

Aperçu du nom unique :  
CN=m2l-DC-CA,DC=m2l,DC=com

[En savoir plus sur le nom de l'autorité de certification](#)

< Précédent Suivant > Configurer Annuler

## Suivant

Configuration des services de certificats Active Directory

SERVEUR DE DESTINATION  
dc.m2l.com

### Période de validité

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 :

Date d'expiration de l'AC : 08/02/2028 10:10:00

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

## Suivant

Configuration des services de certificats Active Directory

SERVEUR DE DESTINATION  
dc.m2l.com

### Base de données de l'autorité de certification

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 emplacements des bases de données

Emplacement de la base de données de certificats :

Emplacement du journal de la base de données de certificats :

[En savoir plus sur la base de données de l'autorité de certification](#)

< Précédent   Suivant >   Configurer   Annuler

Cliquez sur « Configurer »

The screenshot shows the 'Confirmation' step of the 'Configuration des services de certificats Active Directory' wizard. The window title is 'Configuration des services de certificats Active Directory' and the server name is 'SERVEUR DE DESTINATION dc.m2l.com'. On the left, a navigation pane lists steps: 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 (highlighted), Progression, and Résultats. The main area contains the text: 'Pour configurer les rôles, services de rôle ou fonctionnalités ci-après, cliquez sur Configurer.' Below this is a section titled 'Services de certificats Active Directory' with a sub-section 'Autorité de certification'. The configuration details are as follows:

Type d'AC :	Racine d'entreprise
Fournisseur de services de chiffrement :	RSA#Microsoft Software Key Storage Provider
Algorithme de hachage :	SHA1
Longueur de la clé :	2048
Autoriser l'interaction de l'administrateur :	Activé
Période de validité du certificat :	08/02/2028 10:10:00
Nom unique :	CN=m2l-DC-CA,DC=m2l,DC=com
Emplacement de la base de données de certificats :	C:\Windows\system32\CertLog
Emplacement du journal de la base de données de certificats :	C:\Windows\system32\CertLog

At the bottom, there are four buttons: '< Précédent', 'Suivant >', 'Configurer', and 'Annuler'.

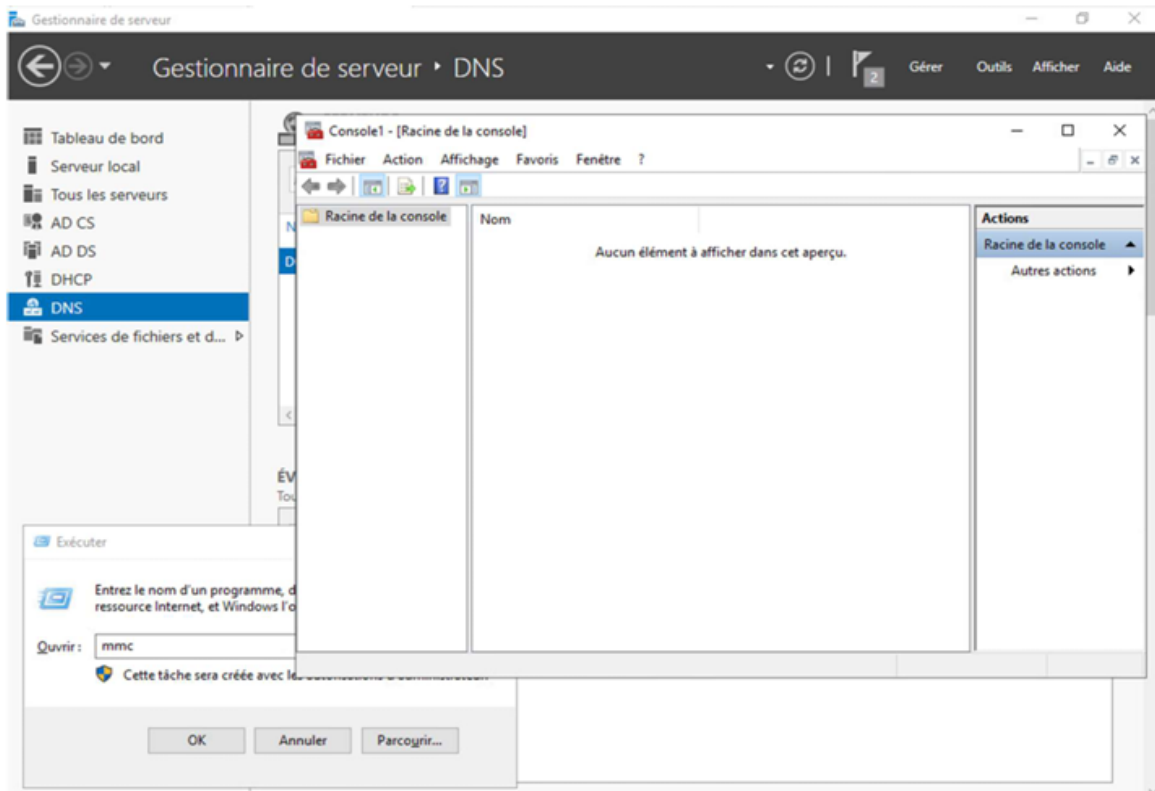
Voici le résultat

The screenshot shows the 'Résultats' step of the 'Configuration des services de certificats Active Directory' wizard. The window title is 'Configuration des services de certificats Active Directory' and the server name is 'SERVEUR DE DESTINATION dc.m2l.com'. On the left, the navigation pane lists steps: 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, and Résultats (highlighted). The main area contains the text: 'Les rôles, services de rôle ou fonctionnalités ci-après ont été configurés :'. Below this is a section titled 'Services de certificats Active Directory' with a sub-section 'Autorité de certification'. The configuration details are as follows:

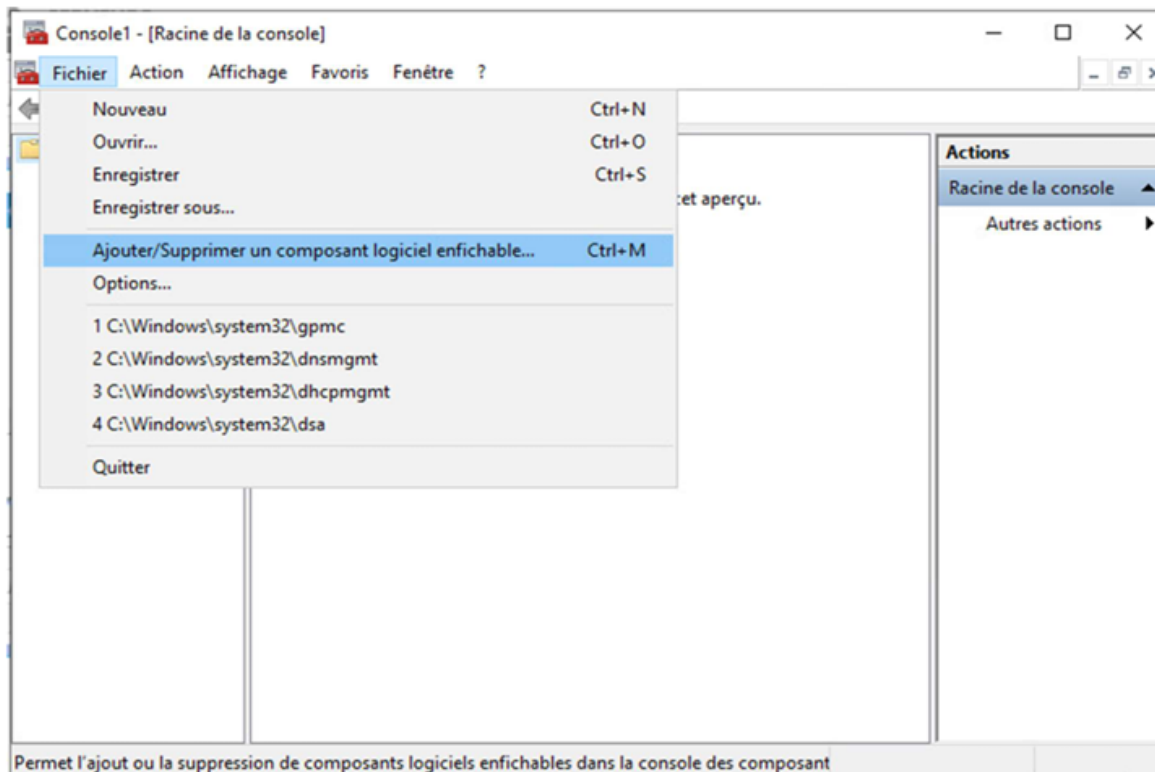
Autorité de certification	Configuration réussie
---------------------------	-----------------------

Below the table, there is a link: 'En savoir plus sur la configuration de l'autorité de certification'. At the bottom, there are four buttons: '< Précédent', 'Suivant >', 'Fermer', and 'Annuler'.

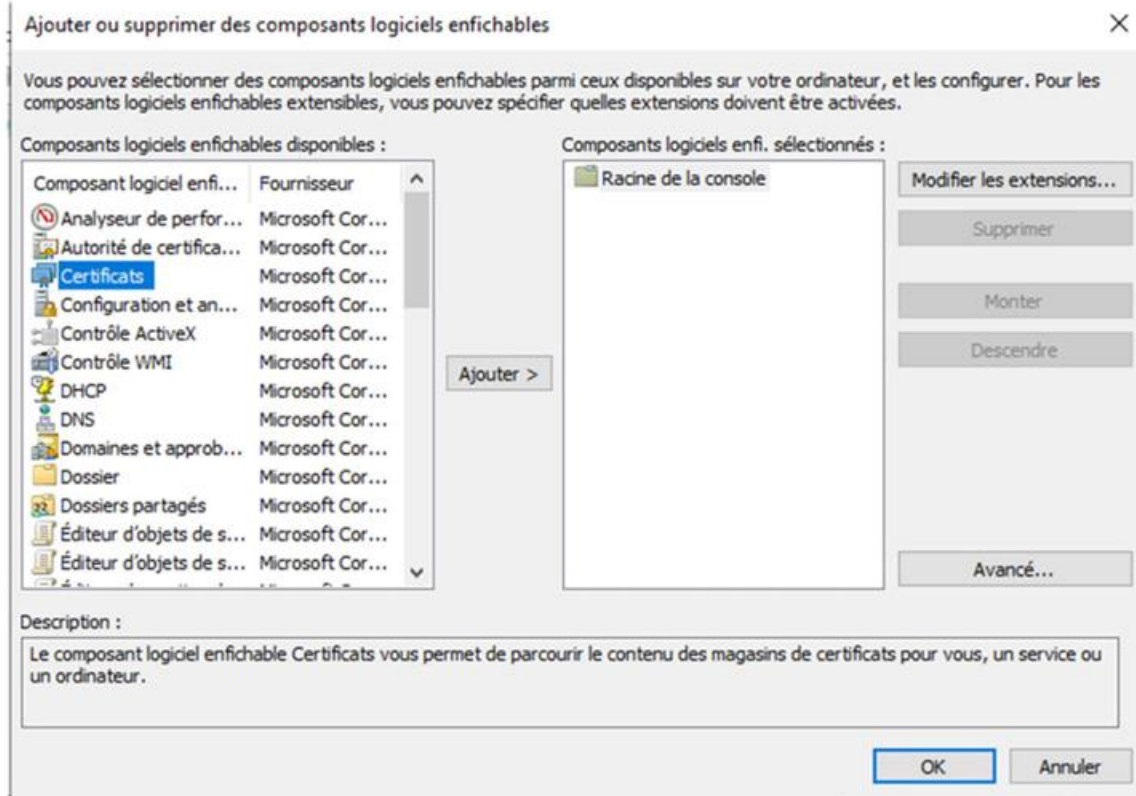
Il faut maintenant ajouter le certificat : dans la fenêtre 'exécuter', taper « mmc »



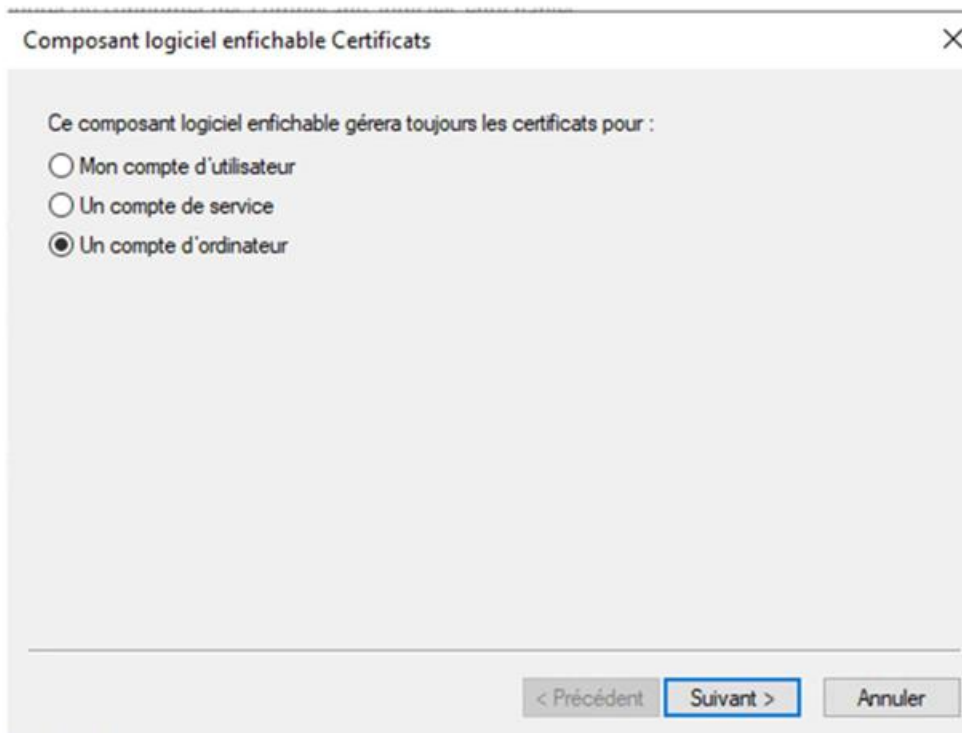
Puis fichier



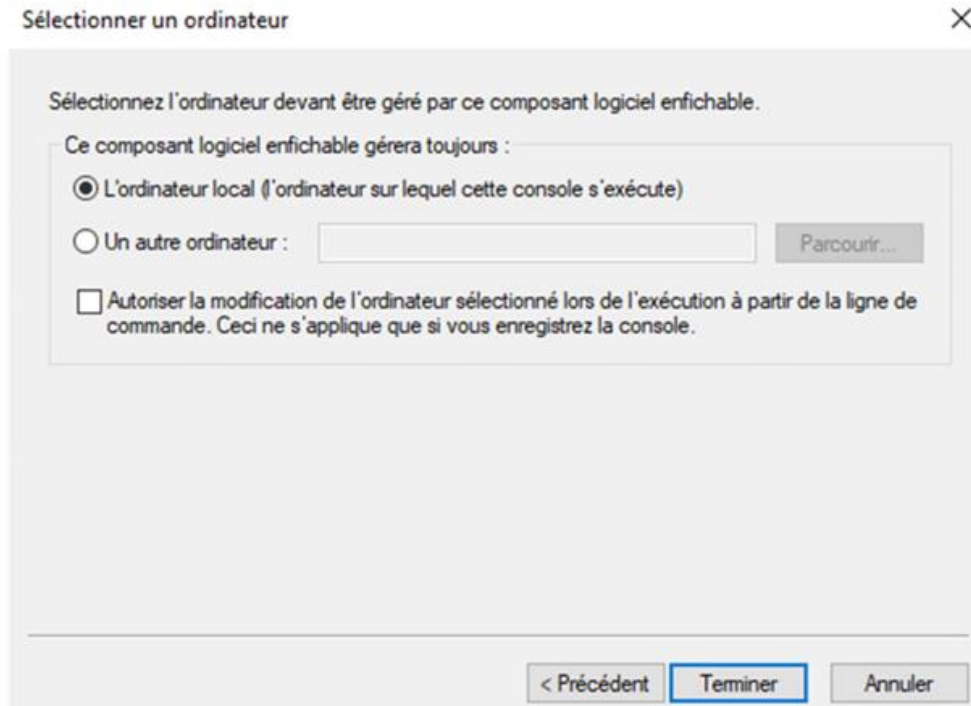
Puis certificat :



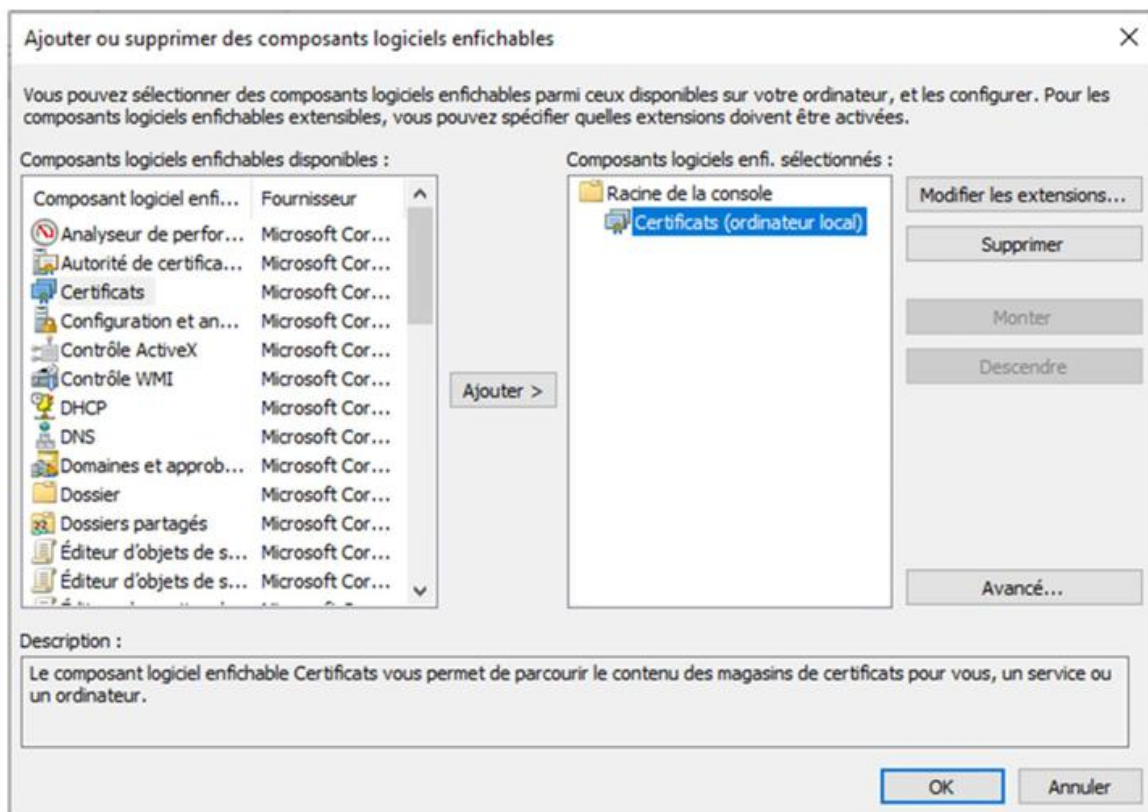
Sur « un compte d'ordinateur »



Puis sur l'ordinateur local

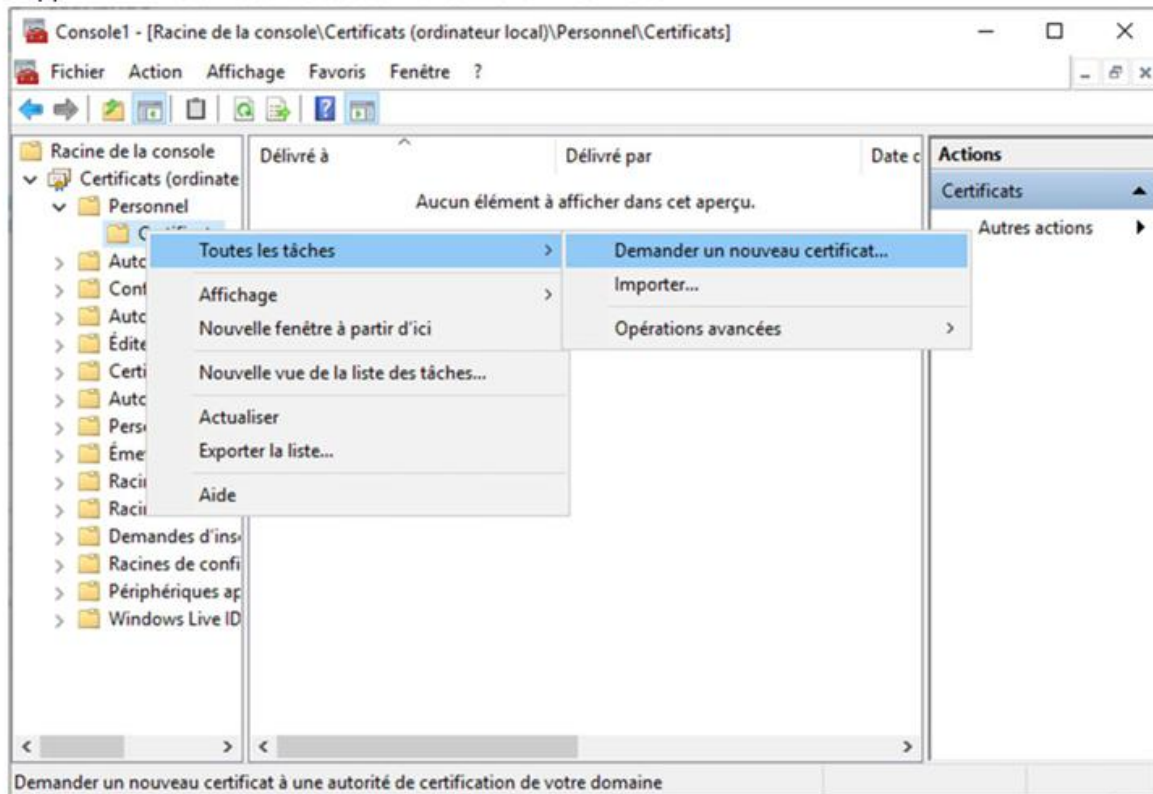


Cliquez sur « ok »

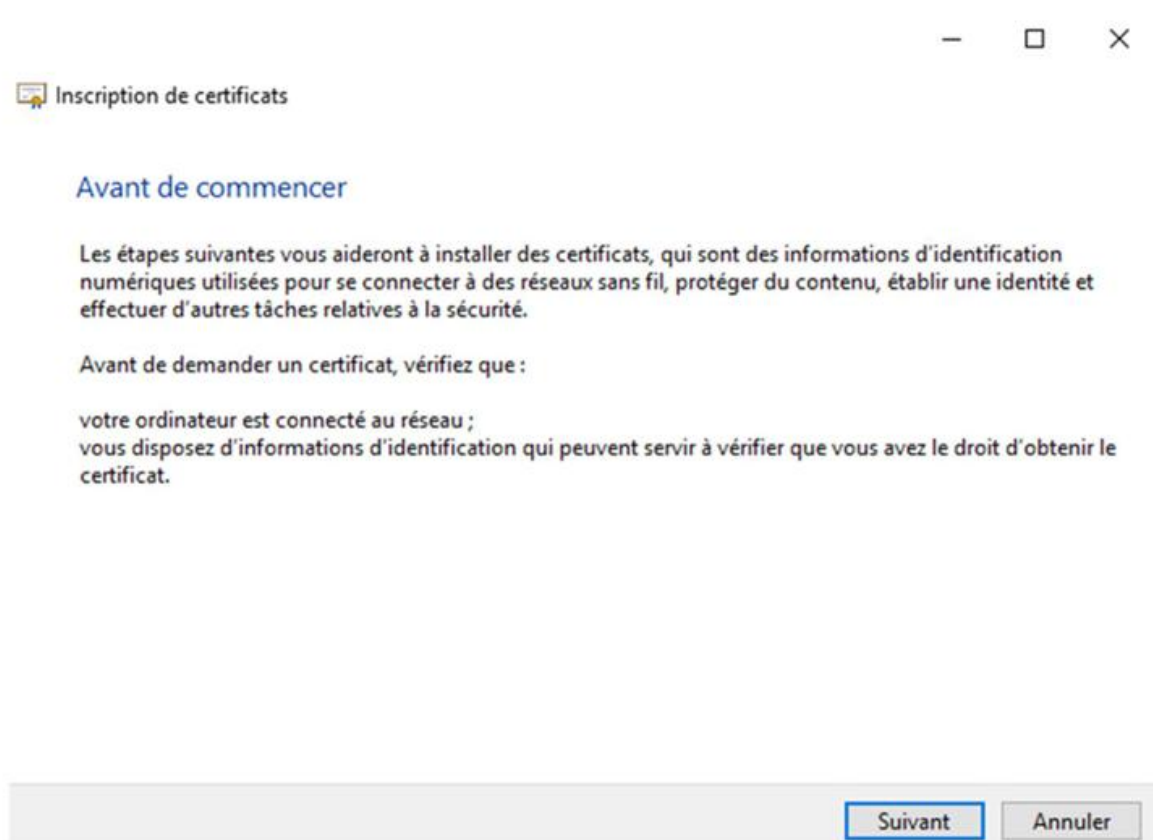


**IL FAUT SUPPRIMER LE CERTIFICAT DEJA PRESENT**

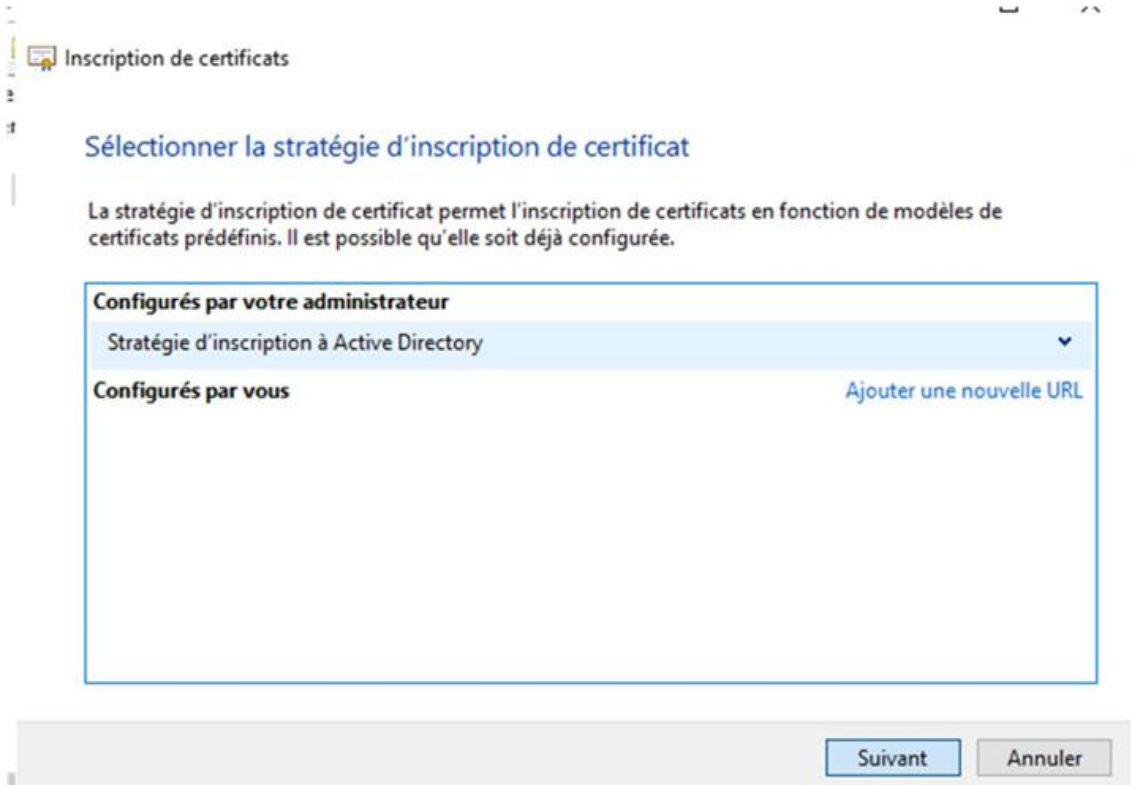
Supprimez l'ancien certificat et demandez en un nouveau :



Suivant



Suivant



Inscription de certificats

### Sélectionner la stratégie d'inscription de certificat

La stratégie d'inscription de certificat permet l'inscription de certificats en fonction de modèles de certificats prédéfinis. Il est possible qu'elle soit déjà configurée.

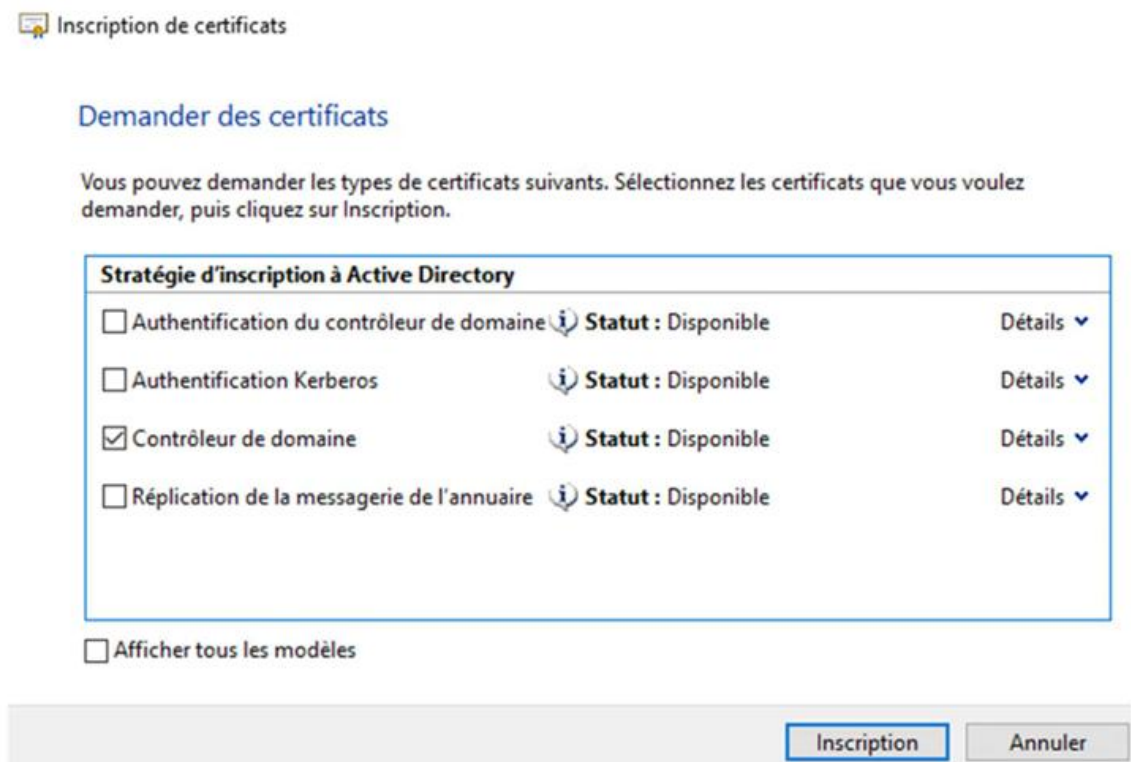
**Configurés par votre administrateur**

- Stratégie d'inscription à Active Directory

**Configurés par vous** [Ajouter une nouvelle URL](#)

Suivant Annuler

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



Inscription de certificats

### Demander des certificats

Vous pouvez demander les types de certificats suivants. Sélectionnez les certificats que vous voulez demander, puis cliquez sur Inscription.

Stratégie d'inscription à Active Directory				
<input type="checkbox"/>	Authentification du contrôleur de domaine		Statut : Disponible	Détails ▼
<input type="checkbox"/>	Authentification Kerberos		Statut : Disponible	Détails ▼
<input checked="" type="checkbox"/>	Contrôleur de domaine		Statut : Disponible	Détails ▼
<input type="checkbox"/>	Réplication de la messagerie de l'annuaire		Statut : Disponible	Détails ▼

Afficher tous les modèles

Inscription Annuler

Le certificat est installé :

 Inscription de certificats

### Résultats de l'installation des certificats

Les certificats suivants ont été inscrits et installés sur cet ordinateur.

Stratégie d'inscription à Active Directory		
<input checked="" type="checkbox"/> Contrôleur de domaine	✓ Statut : Opération réussie	Détails ▾

Terminer

Il apparaît :

Délivré à	Délivré par	Date d'expirati...	Rôles prévus	Nom convivial
 SRV-WIN.m2l.com	m2l-DC-CA	02/04/2024	Authentification du...	<Aucun>

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

Assistant Ajout de rôles et de fonctionnalités

SÉLECTIONNER DES RÔLES DE SERVEURS

SERVEUR DE DESTINATION  
dc.m2l.com

Avant de commencer  
Type d'installation  
Sélection du serveur  
**Rôles de serveurs**  
Fonctionnalités  
Services de stratégie et d'...  
Confirmation  
Résultats

Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.

Rôles	Description
<input type="checkbox"/> Contrôleur de réseau	
<input type="checkbox"/> Hyper-V	
<input type="checkbox"/> Serveur de télécopie	
<input checked="" type="checkbox"/> Serveur DHCP (Installé)	
<input checked="" type="checkbox"/> Serveur DNS (Installé)	
<input type="checkbox"/> Serveur Web (IIS)	
<input type="checkbox"/> Service Guardian hôte	
<input checked="" type="checkbox"/> Services AD DS (Installé)	
<input type="checkbox"/> Services AD LDS (Active Directory Lightweight Dire...	
<input type="checkbox"/> Services AD RMS (Active Directory Rights Manage...	
<input type="checkbox"/> Services Bureau à distance	
<input type="checkbox"/> Services d'activation en volume	
<input type="checkbox"/> Services d'impression et de numérisation de docu...	
<input checked="" type="checkbox"/> Services de certificats Active Directory (1 sur 6 inst...	
<input type="checkbox"/> Services de déploiement Windows	
<input type="checkbox"/> Services de fédération Active Directory (AD FS)	
<input checked="" type="checkbox"/> Services de fichiers et de stockage (2 sur 12 install...	
<input checked="" type="checkbox"/> Services de stratégie et d'accès réseau	
<input type="checkbox"/> Services WSUS (Windows Server Update Services)	

Les services de stratégie et d'accès réseau fournissent un serveur NPS (Network Policy Server) qui contribue à garantir la sécurité de votre réseau.

< Précédent   Suivant >   Installer   Annuler

## Suivant

Assistant Ajout de rôles et de fonctionnalités

SÉLECTIONNER DES FONCTIONNALITÉS

SERVEUR DE DESTINATION  
dc.m2l.com

Avant de commencer  
Type d'installation  
Sélection du serveur  
Rôles de serveurs  
**Fonctionnalités**  
Services de stratégie et d'...  
Confirmation  
Résultats

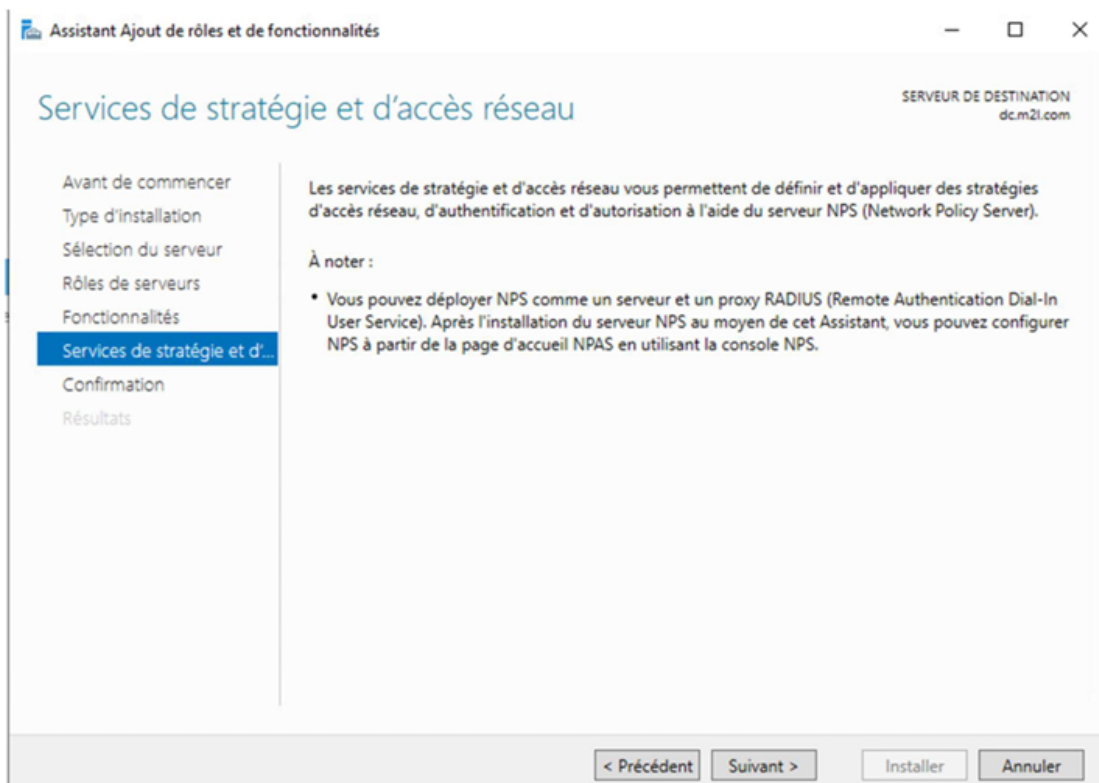
Sélectionnez une ou plusieurs fonctionnalités à installer sur le serveur sélectionné.

Fonctionnalités	Description
<input checked="" type="checkbox"/> Assistance à distance	
<input type="checkbox"/> Base de données interne Windows	
<input type="checkbox"/> BranchCache	
<input type="checkbox"/> Chiffrement de lecteur BitLocker	
<input type="checkbox"/> Client d'impression Internet	
<input type="checkbox"/> Client pour NFS	
<input type="checkbox"/> Clustering de basculement	
<input type="checkbox"/> Collection des événements de configuration et de...	
<input type="checkbox"/> Compression différentielle à distance	
<input type="checkbox"/> Containers	
<input type="checkbox"/> Data Center Bridging	
<input type="checkbox"/> Déverrouillage réseau BitLocker	
<input type="checkbox"/> Direct Play	
<input type="checkbox"/> Équilibrage de la charge réseau	
<input type="checkbox"/> Équilibreur de charge logiciel	
<input type="checkbox"/> Expérience audio-vidéo haute qualité Windows	
<input type="checkbox"/> Extension ISS Management OData	
<input type="checkbox"/> Extension WinRM IIS	
<input type="checkbox"/> Fonctionnalités de .NET Framework 3.5	

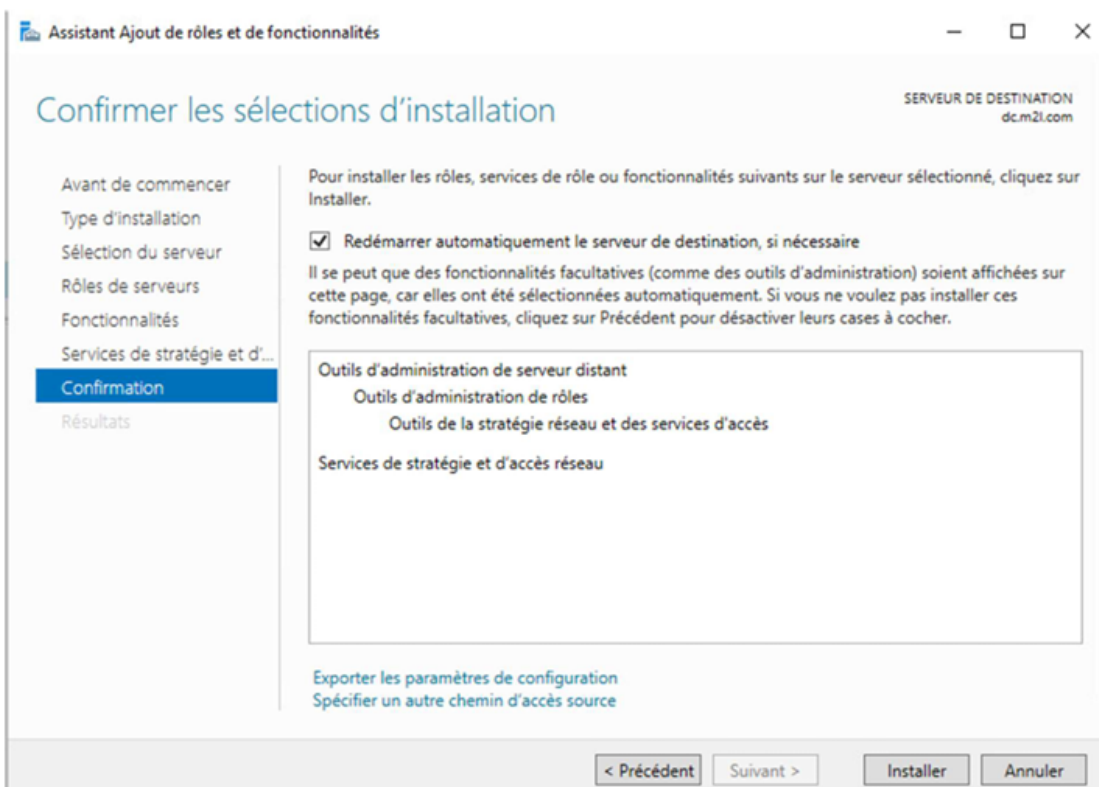
Grâce à l'assistance à distance, vous (ou une personne du support technique) pouvez aider les utilisateurs à résoudre leurs problèmes ou à répondre à leurs questions en rapport avec leur PC. Vous pouvez afficher et prendre le contrôle du Bureau des utilisateurs pour dépanner et résoudre les problèmes. Les utilisateurs ont également la possibilité de solliciter l'aide de leurs amis ou de leurs collègues de travail.

< Précédent   Suivant >   Installer   Annuler

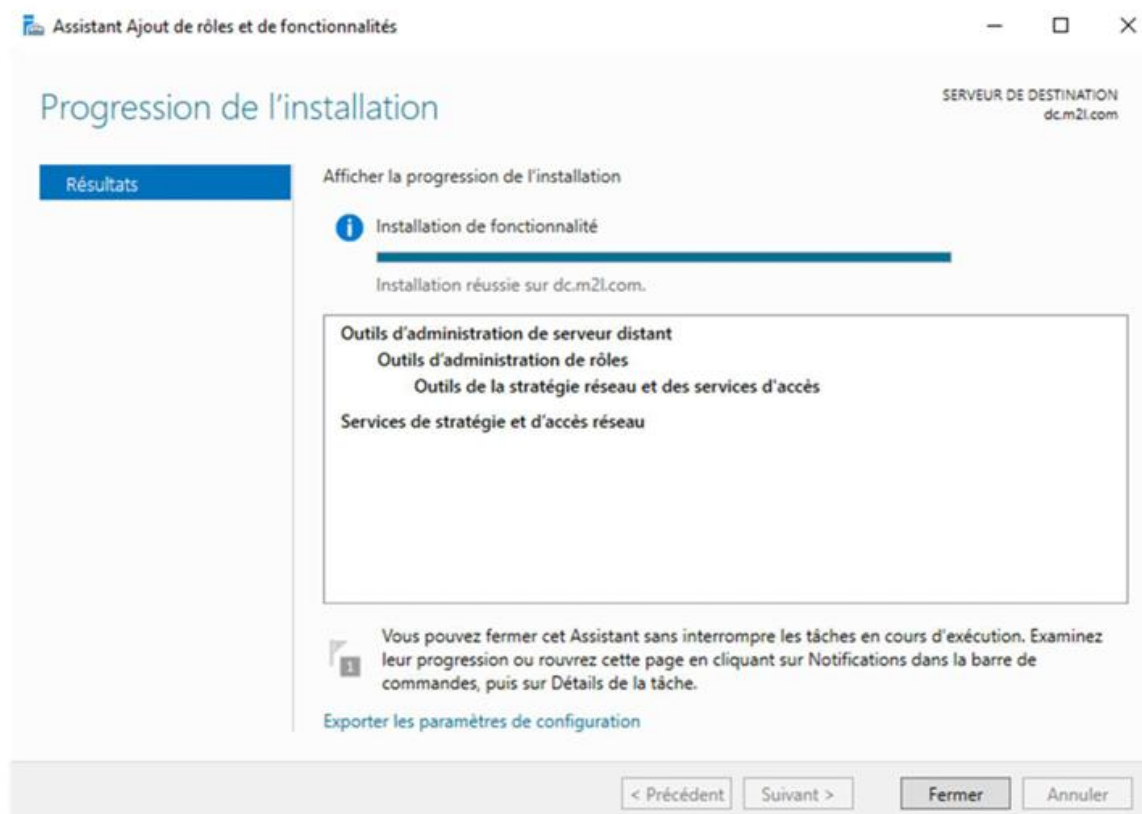
Suivant



Puis « installer »



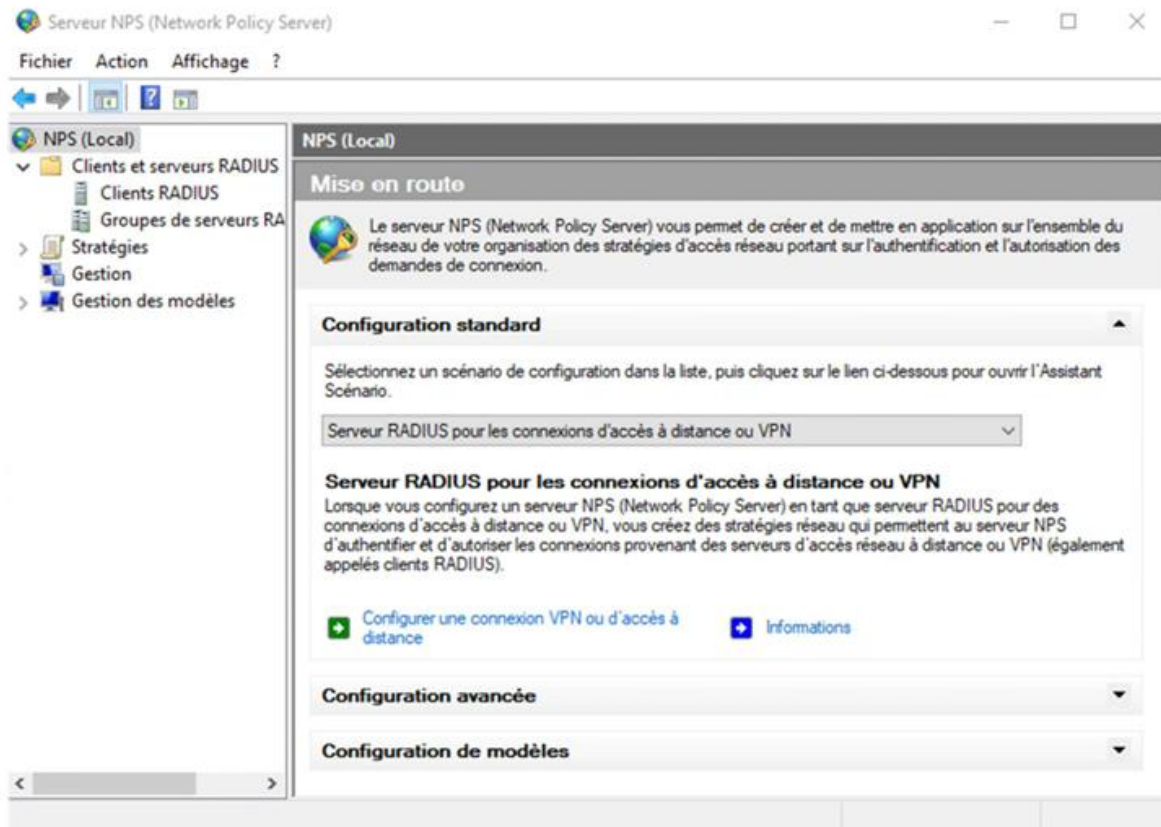
Voici la confirmation :



Il faut maintenant configurer le service NPS :



Voici la page de configuration :



Changer le scénario de configuration :







Ajouter un client Radius :

Configurer 802.1X



## Spécifier les commutateurs 802.1X

Spécifiez les commutateurs ou points d'accès sans fil 802.1X (clients RADIUS)

Les clients RADIUS sont des serveurs d'accès réseau, à l'image des commutateurs d'authentification et des points d'accès sans fil. Les clients RADIUS ne sont pas des ordinateurs clients.

Pour spécifier un client RADIUS, cliquez sur Ajouter.

### Clients RADIUS :

WiFi-Radius

Ajouter...

Modifier...

Supprimer

Précédent

Suivant

Terminer

Annuler

## Nouveau client RADIUS



**Paramètres**

Sélectionner un modèle existant :

Nom et adresse

Nom convivial :  
WiFi-Radius

Adresse (IP ou DNS) :  
192.168.30.5

Secret partagé

Sélectionnez un modèle de secrets partagés existant :  
Aucun

Pour taper manuellement un secret partagé, cliquez sur Manuel. Pour générer automatiquement un secret partagé, cliquez sur Générer. Vous devez configurer le client RADIUS avec le même secret partagé entré ici. Les secrets partagés respectent la casse.

Manuel  Générer

Secret partagé :  
.....

Confirmez le secret partagé :  
.....

< NE PAS METTRE DE CARACTERE SPECIAUX COMME @/ !

## Puis Suivant

Configurer 802.1X

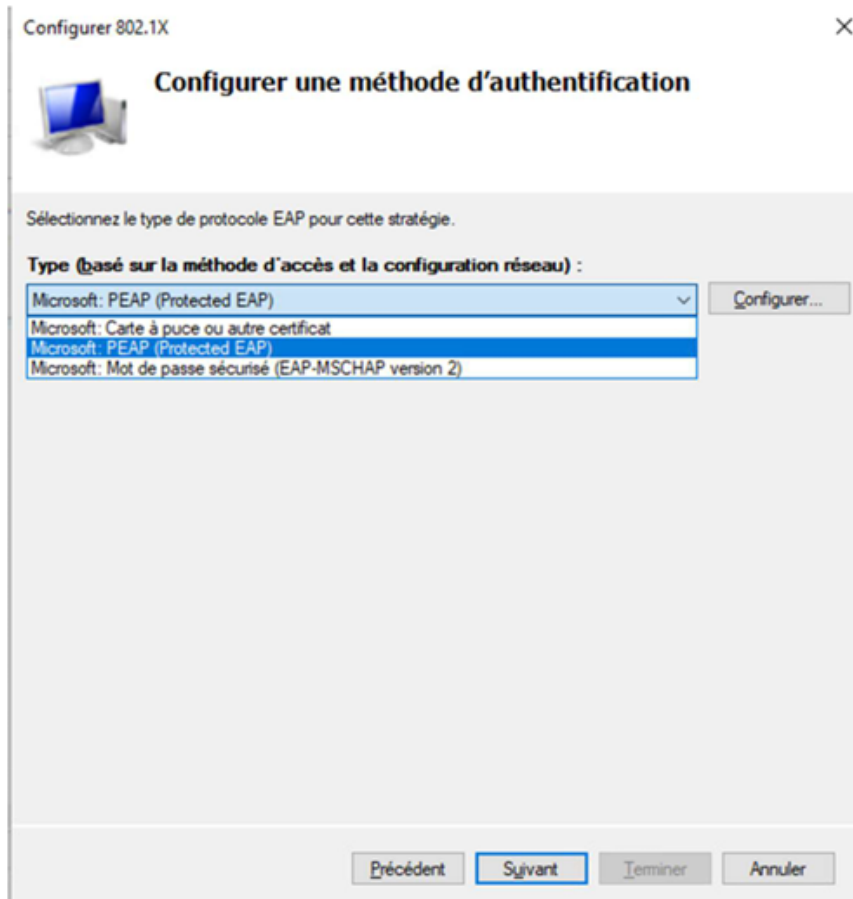
**Spécifier les commutateurs 802.1X**  
Spécifiez les commutateurs ou points d'accès sans fil 802.1X (clients RADIUS)

Les clients RADIUS sont des serveurs d'accès réseau, à l'image des commutateurs d'authentification et des points d'accès sans fil. Les clients RADIUS ne sont pas des ordinateurs clients.  
Pour spécifier un client RADIUS, cliquez sur Ajouter.

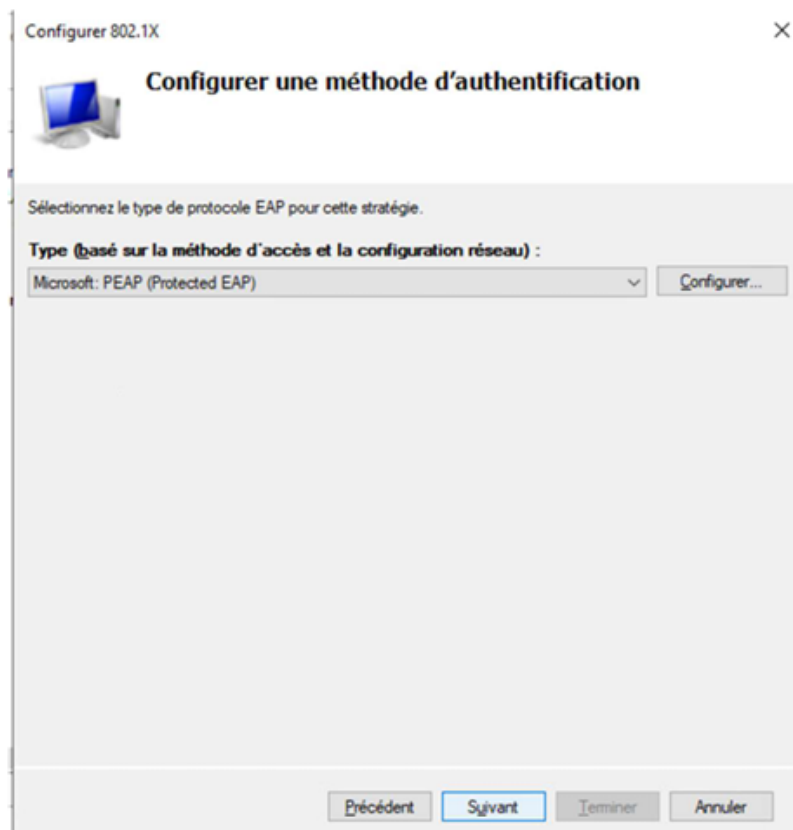
**Clients RADIUS :**

WiFi-Radius

Sélectionner « Microsoft PEAP (EAP) »



Suivant



Ajouter les groupes d'utilisateurs :

Configurer 802.1X

### Spécifier des groupes d'utilisateurs

L'accès des utilisateurs membres du ou des groupes sélectionnés sera autorisé ou non en fonction du paramètre d'autorisation d'accès de la stratégie réseau.

Pour sélectionner des groupes d'utilisateurs, cliquez sur **Ajouter**. Si aucun groupe n'est sélectionné, cette stratégie s'applique à tous les utilisateurs.

Groupes

**Ajouter...**  
Supprimer

Sélectionnez un groupe

Sélectionnez le type de cet objet :

un groupe

Types d'objets...

À partir de cet emplacement :

m2l.com

Emplacements...

Entrez le nom de l'objet à sélectionner (exemples) :

Utilisateurs du domaine

Vérifier les noms

Avancé... OK Annuler

Précédent Suivant Terminer Annuler

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

Puis suivant

Configurer 802.1X

### Spécifier des groupes d'utilisateurs

L'accès des utilisateurs membres du ou des groupes sélectionnés sera autorisé ou non en fonction du paramètre d'autorisation d'accès de la stratégie réseau.

Pour sélectionner des groupes d'utilisateurs, cliquez sur **Ajouter**. Si aucun groupe n'est sélectionné, cette stratégie s'applique à tous les utilisateurs.

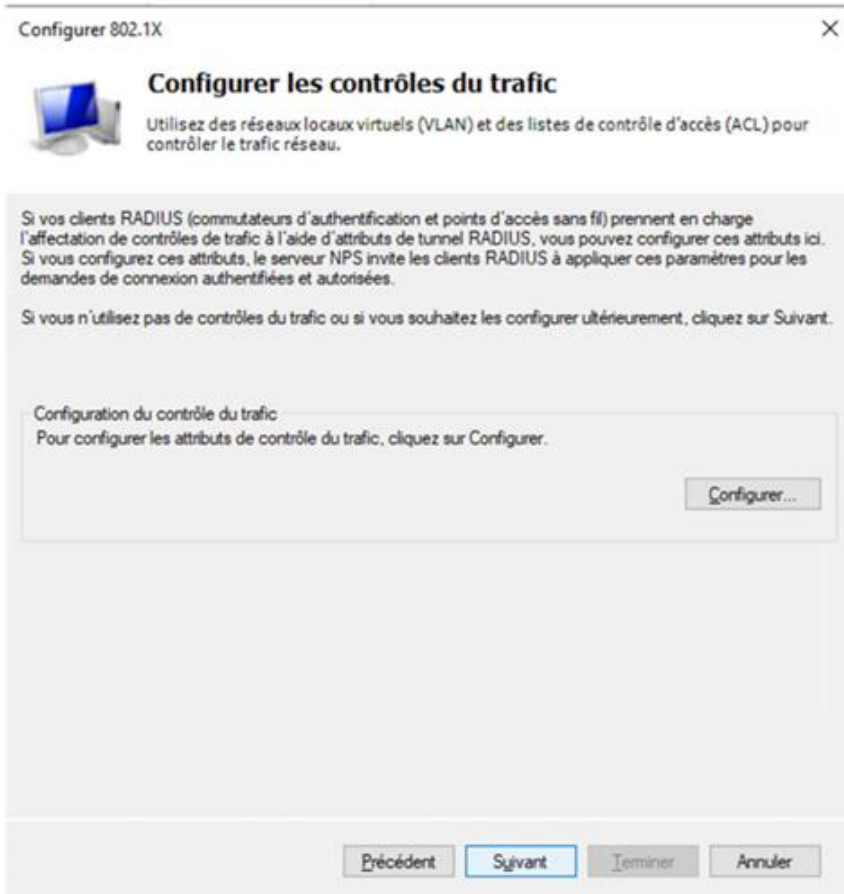
Groupes

M2L\Utilisateurs du domaine

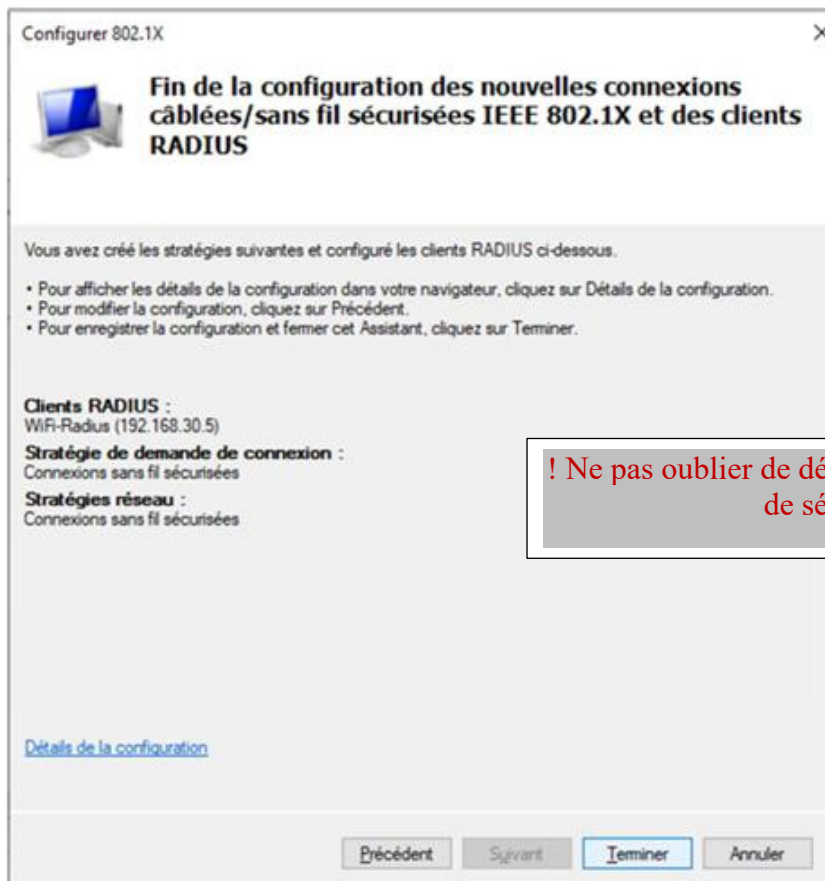
**Ajouter...**  
Supprimer

Précédent **Suivant** Terminer Annuler

## Suivant



## Récapitulatif de la configuration



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

```

ap(config)#radius-server host 172.20.3.14 auth-port 1645 acc
ap(config)#radius-server host 172.20.3.14 auth-port 1645 acct-port 1646 k
ap(config)#$er host 172.20.3.14 auth-port 1645 acct-port 1646 key Bts2025
Warning: The CLI will be deprecated soon
'radius-server host 172.20.3.14 auth-port 1645 acct-port 1646 key Bts2025'
Please move to 'radius server <name>' CLI.
ap(config)#$er host 172.20.3.14 auth-port 1645 acct-port 1646 key ?
 0 Specifies an UNENCRYPTED key will follow
 7 Specifies HIDDEN key will follow
WORD The UNENCRYPTED (cleartext) server key

ap(config)#$er host 172.20.3.14 auth-port 1645 acct-port 1646 key 7 Bts2025
%Invalid encrypted key: Bts2025

ap(config)#$er host 172.20.3.14 auth-port 1645 acct-port 1646 key 0 Bts2025
ap(config)#
ap(config)#

```

Capture en cours de Ethernet0

Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

radius

No.	Time	Source	Destination	Protocol	Length	Info
1105...	1041.702048	172.20.3.14	172.20.3.4	RADIUS	187	Access-Challenge id=71
1105...	1045.847342	172.20.3.4	172.20.3.14	RADIUS	270	Access-Request id=72
1105...	1045.848061	172.20.3.14	172.20.3.4	RADIUS	162	Access-Challenge id=72
1105...	1045.859294	172.20.3.4	172.20.3.14	RADIUS	315	Access-Request id=73
1105...	1045.859678	172.20.3.14	172.20.3.4	RADIUS	177	Access-Challenge id=73
1105...	1045.867293	172.20.3.4	172.20.3.14	RADIUS	315	Access-Request id=74
1105...	1045.874024	172.20.3.14	172.20.3.4	RADIUS	188	Access-Challenge id=74
1106...	1045.883074	172.20.3.4	172.20.3.14	RADIUS	369	Access-Request id=75
1106...	1045.888125	172.20.3.14	172.20.3.4	RADIUS	208	Access-Challenge id=75
1106...	1045.894390	172.20.3.4	172.20.3.14	RADIUS	301	Access-Request id=76
1106...	1045.896141	172.20.3.14	172.20.3.4	RADIUS	232	Access-Challenge id=76
1106...	1045.912383	172.20.3.4	172.20.3.14	RADIUS	370	Access-Request id=77
1106...	1045.913910	172.20.3.14	172.20.3.4	RADIUS	325	Access-Accept id=77

> Frame 110605: 325 bytes on wire (2600 bits), 325 bytes captured (2600 b...  
 > Ethernet II, Src: VMware\_2f:0e:6c (00:0c:29:2f:0e:6c), Dst: Cisco\_01:1c...  
 > Internet Protocol Version 4, Src: 172.20.3.14, Dst: 172.20.3.4  
 > User Datagram Protocol, Src Port: 1645, Dst Port: 1645  
 > RADIUS Protocol

0000 28 94 0f 01 1c c1 00 0c 29 2f 0e 6c 08 00 45 00 (... ..) /1...  
 0010 01 37 76 a7 00 00 80 11 00 00 ac 14 03 0e ac 14 -7v... ..  
 0020 03 04 06 6d 06 6d 01 23 5f 6f 02 4d 01 1b 90 e0 ...m-m-#...o-M...  
 0030 80 1c e6 fc b5 c3 f4 91 6a d5 83 88 51 72 07 06 ...j...C...  
 0040 00 00 00 01 06 06 00 00 00 02 4f 06 03 0c 00 04 ...-O... ..  
 0050 19 2e 85 b2 07 ae 00 00 01 37 00 01 02 00 ac 14 ...-7... ..  
 0060 03 0e 00 00 00 00 a5 57 01 4a 44 34 02 bb 01 db ...W...J04...  
 0070 7c 88 b4 2a 98 8e 00 00 00 00 00 00 41 1a 0e |...\*... ..  
 0080 00 00 01 37 0a 08 01 53 4f 4e 49 43 1a 33 00 00 ...7...S=3 ONIC...  
 0090 01 37 1a 2d 01 53 3d 33 42 36 46 38 37 43 45 33 -7--S=3 B6F87...  
 00a0 44 35 37 32 37 36 46 32 37 34 38 33 34 34 41 44 D57276F2 74834...  
 00b0 42 30 32 37 35 32 39 32 42 39 30 34 30 31 38 1a B0275292 B904E...  
 00c0 3a 00 00 01 37 10 34 80 03 e6 5b 42 ef 15 e3 06 ...-7-4-...[B...  
 00d0 a0 cc 03 df fa 38 45 c7 e2 3a d6 5d f7 f3 9c 69 ...-8E-...:]...  
 00e0 93 39 c9 e2 b6 6e a7 3c 7b c2 ef b8 64 eb 66 87 -9--n-< {...c...  
 00fa 0a c6 e0 b8 5a c5 c1 4e 1a 3a 00 00 01 37 |...7... M...>

< Frame (325 bytes) Reassembled EAP (4 bytes)

RADIUS Protocol: Protocol Paquets: 112137 · Affichés: 122 (0.1%) Profil: Default

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**