Mission 5 & 6 : Sécurisation de l'accès à Internet et mise en place d'une DMZ & Implémentation d'un Réseau Wi-Fi pour les Employés et les Visiteurs au Stade

Kevin Roussel
Chloe Houivet
Ajay Muthu Kumar
Ecole IRIS

SOMMAIRE

PARTIE 2 : MISSION 6

1. INTRODUCTION

Pour commencer, le WiFi est un réseau local sans fil (WLAN) qui est un type de réseau sans fil beaucoup utilisé dans les foyers ainsi que les bureaux et les campus. En effet, c'est dû au fait qu'il permet une connectivité réseau sans l'utilisation de câbles physiques.

Le WiFi a plusieurs avantages dont ses principaux sont les suivants :

- La mobilité car il permet aux appareils de se déplacer librement dans la zone de couverture.
- La flexibilité dû à son adaptation rapide aux besoins et aux technologies en évolution.
- L'évolutivité car il peut facilement être étendu ou mis à jour sans avoir de refonte complète à effectuer.

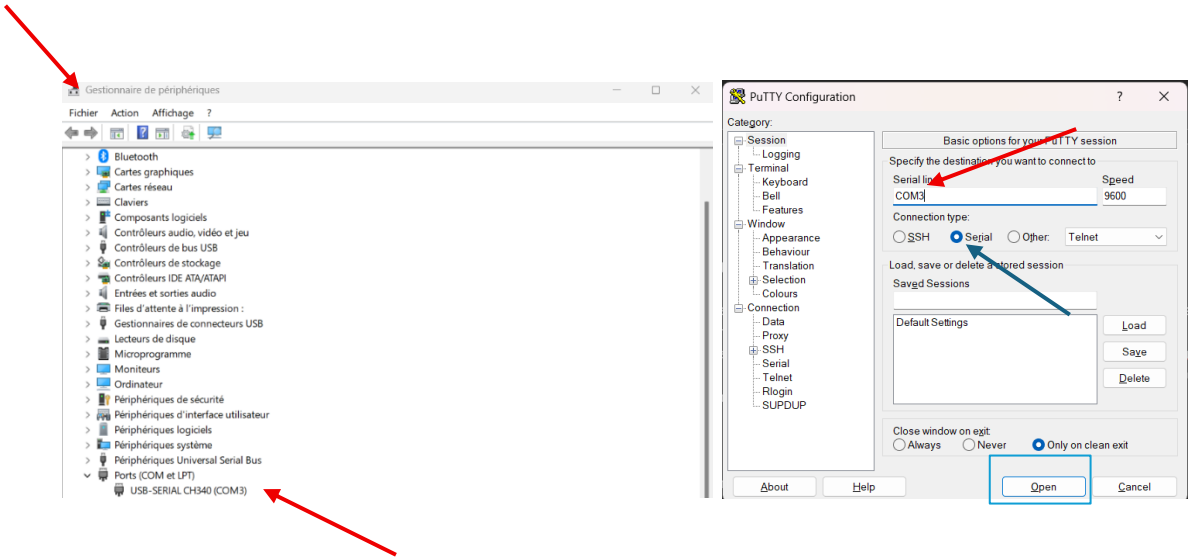
Le WiFi a un rôle dans l'écosystème des réseaux sans fil. En effet, il s'inscrit dans un écosystème plus large de technologies sans fil, chacune adaptée à des besoins spécifiques en termes de portée et de consommation d'énergie.

Il existe différents types de réseaux sans fil :

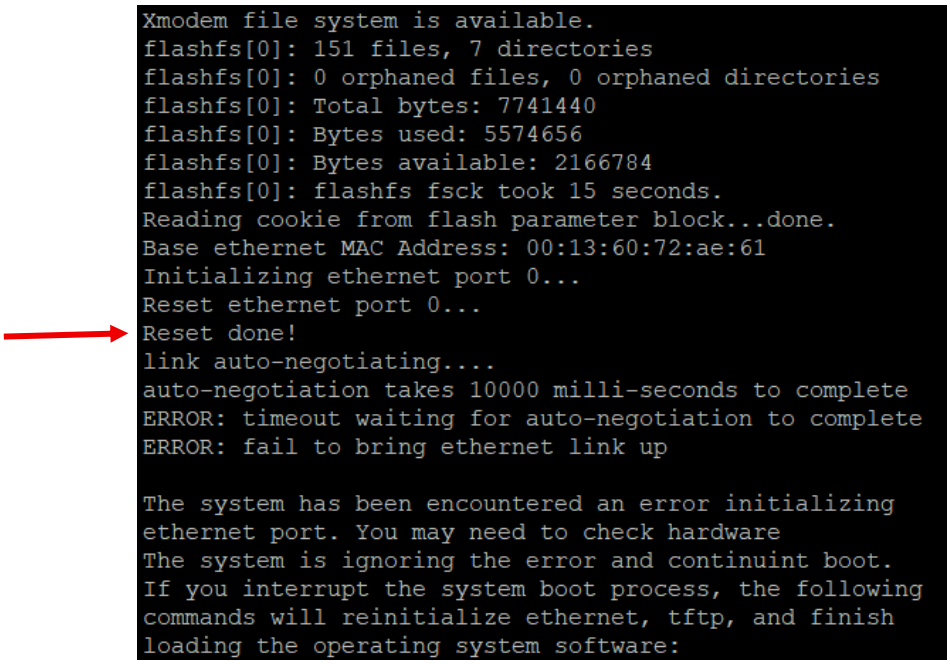
- Le WPAN est un réseau personnel sans fil comme le Bluetooth. Il a une faible portée de 6 à 9 mètres ainsi qu'une faible consommation dû à son utilisation sur de petits appareils.
- Le WLAN est un réseau local sans fil ayant une portée jusqu'à 90 mètres et ait une moyenne consommation. Il est principalement utilisé en réseau domestique.
- Le WMAN est un réseau métropolitain sans fil comme WIMAX. Il a une haute portée, jusqu'à 50 kilomètres pouvant ainsi recouvrir toute une ville ou un quartier. Il n'a qu'une consommation moyenne malgré sa haute portée.
- Le WWAN est un réseau étendu sans fil comme la 4G ou la 5G. Ainsi, il a une portée nationale voire mondiale venant d'un haut débit satellite et se focalisant la téléphonie cellulaire. Du fait de sa haute portée, il a une consommation élevée.

2. REINITIALISATION DE LA BORNE WIFI

1°) Pour procéder à la réinitialisation d'une borne WiFi, il faut débrancher l'alimentation, maintenir le bouton « MODE » durant 15 secondes. A la suite de cela, rebrancher l'alimentation à la borne WiFi.
Ensuite, brancher la borne WiFi à un PC grâce à un câble console, ouvrir l'application « Putty », renseigner le port USB du PC utilisé (COM*), cocher la case « Serial » et ensuite cliquer sur « Open » pour ouvrir la connexion.



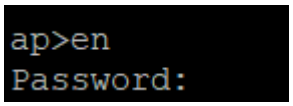
2°) On voit bien que la réinitialisation a fonctionné en voyant la phrase « Reset done ! »



Kevin Roussel
Chloe Houivet
Ajay Muthu Kumar
Ecole IRIS

3°) Ensuite, vous allez vous connecter avec cet identifiant et le mot de passe suivant :

Nom par défaut de la borne : ap
Login : en
Mot de passe : Cisco



Kevin Roussel
Chloe Houivet
Ajay Muthu Kumar
Ecole IRIS

3. CONFIGURATION DE L'INTERFACE EN DHCP

1°) Concernant la configuration de l'interface en DHCP, il faut taper plusieurs commandes qui vont permettre de configurer plus précisément le BVI. En effet, le BVI signifie Bridge Virtual Interface, c'est un pont qui permet de faire passer internet de l'antenne WIFI vers le trafic Ethernet.

Pour cela, il faut d'abord entrer en phase de configuration du terminal en tapant « conf t ».
Puis, choisir l'interface que l'on souhaite justement configurer qui est le BVI 1 en écrivant « interface BVI 1 ».
Enfin, on met une adresse IP en DHCP et on active l'interface avec les commandes « ip address DHCP » et « no shutdown ».

```
ap#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ap(config)#interface BVI 1
ap(config-if)#ip address DHCP
ap(config-if)#no shutdown
ap(config-if)#
*Mar 10 18:06:39.499: %DHCP-6-ADDRESS_ASSIGN: Interface BVI1 assigned DHCP address 10.0.228.51, mask 255.255.254.0, hostname ap
```

Ensuite, exécutez la commande « *exit* » afin de sortir du mode configuration d'interface (config-if).

4. CREATION DU RESEAU WIFI ET DE SON SSID

1°) Pour la création du réseau Wi-Fi et de son SSID (nom du réseau), il faut commencer par choisir l'interface où l'on souhaite créer notre réseau.
Pour cela, on tape la commande « interface dot11Radio 0 ». La radio 0 correspond au 2,4Ghz et dot11 correspond à la spécification 802.11.
A la suite, on créer notre nom de réseau avec la commande « ssid WiFi-Stade_GRACK ».
Enfin, il faut exécuter la commande « exit » afin de sortir du mode configuration d'interface (config-if).

```
ap(config)#interface dot11Radio 0
ap(config-if)#ssid WiFi-Stade_GRACK
ap(config-if-ssid)#exit
```

2°) Ensuite, on va activer le mode d'encryptage de la clé sécurisé WPA2 via aes-ccm. Tkip est un autre standard moins sécurisé mais plus compatible (vis-à-vis de l'ancienneté du matériel).
Pour activer le mode d'encryptage, il faut utiliser la commande « encryption mode ciphers aes-ccm tkip ».
Ensuite il faut activer l'interface avec la commande « no shutdown ».

```
ap(config-if)#encryption mode ciphers aes-ccm tkip
ap(config-if)#no shutdown
ap(config-if)#
*Mar 10 18:10:08.727: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to reset
*Mar 10 18:10:08.738: %DOT11-6-FREQ_SCAN: Interface Dot11Radio0, Scanning frequencies for 39 seconds
*Mar 10 18:10:47.503: %DOT11-6-FREQ_USED: Interface Dot11Radio0, frequency 2417 selected
*Mar 10 18:10:47.505: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Mar 10 18:10:48.505: %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio0, changed state to up
```

Ensuite, exécutez la commande « *exit* » afin de sortir du mode configuration d'interface (config-if).

5. CONFIGURATION DU RESEAU WIFI AVEC MOT DE PASSE

1°) Maintenant, nous allons créer un nouvel identifiant de réseau SSID qui se nommera WiFi-Stade_GRACK avec la commande suivante : « dot11 ssid Wifi-Stade_GRACK ».
C'est le nom que verront les utilisateurs sur les ordinateurs ou téléphones par exemple.

Ensuite, la commande « authentication open » permet à un appareil de s'associer au point d'accès sans passer par une vérification initiale complexe.

```
ap(config)#dot11 ssid WiFi-Stade_GRACK
ap(config-ssid)#authentication open
ap(config-ssid)#
*Mar 10 18:11:46.550: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to reset
*Mar 10 18:11:46.560: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
```

2°) Par la suite, pour que le réseau soit visible, il faut activer sa diffusion dans les trames « Beacon » du point d'accès avec la commande « guest-mode ».

```
ap(config-ssid)#guest-mode
ap(config-ssid)#
*Mar 10 18:12:14.702: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to reset
*Mar 10 18:12:14.712: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
```

3°) De plus, il faut indiquer que le point d'accès de ce réseau est sécurisé et nécessite une méthode de chiffrement. Pour cela, il faut activer la gestion des clés de sécurité via le protocole WPA avec la commande « authentication key-management wpa ».
Automatiquement, ça choisira la version 2 du WPA.

Ainsi, il faut configurer une clé pré-partagée à l'aide de la commande « wpa-psk ascii Bts2026@ ». Le ascii indique que le mot de passe est une chaîne de caractères lisible comme du texte et Bts2026@ correspond au mot de passe choisi.

```
ap(config-ssid)#authentication key-management wpa
ap(config-ssid)#
*Mar 10 18:18:12.304: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to reset
*Mar 10 18:18:12.314: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
ap(config-ssid)#wpa-psk ascii Bts2026@
ap(config-ssid)#
*Mar 10 18:19:00.043: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to reset
*Mar 10 18:19:00.053: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
```

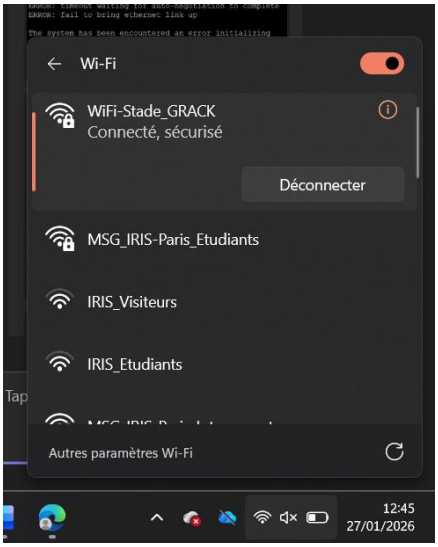
Ensuite, exécutez la commande « *exit* » afin de sortir du mode configuration d'interface (config-ssid).

6. TEST

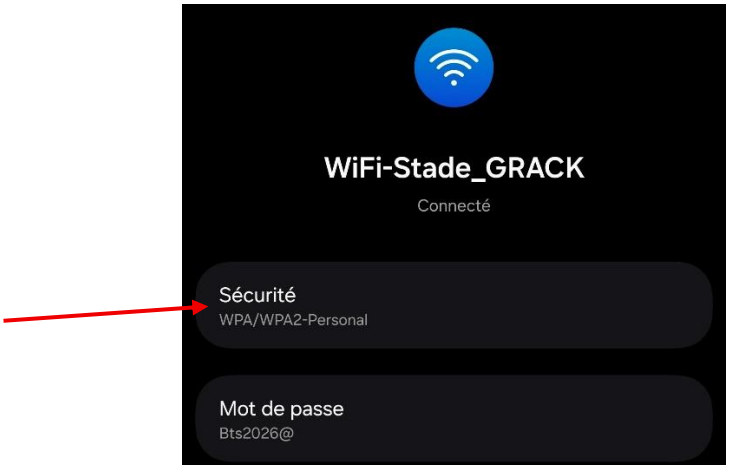
Comme vous pouvez remarquer, on peut se connecter au réseau WIFI (WiFi-Stade_GRACK) selon différentes plateformes, comme le PC :

1

2

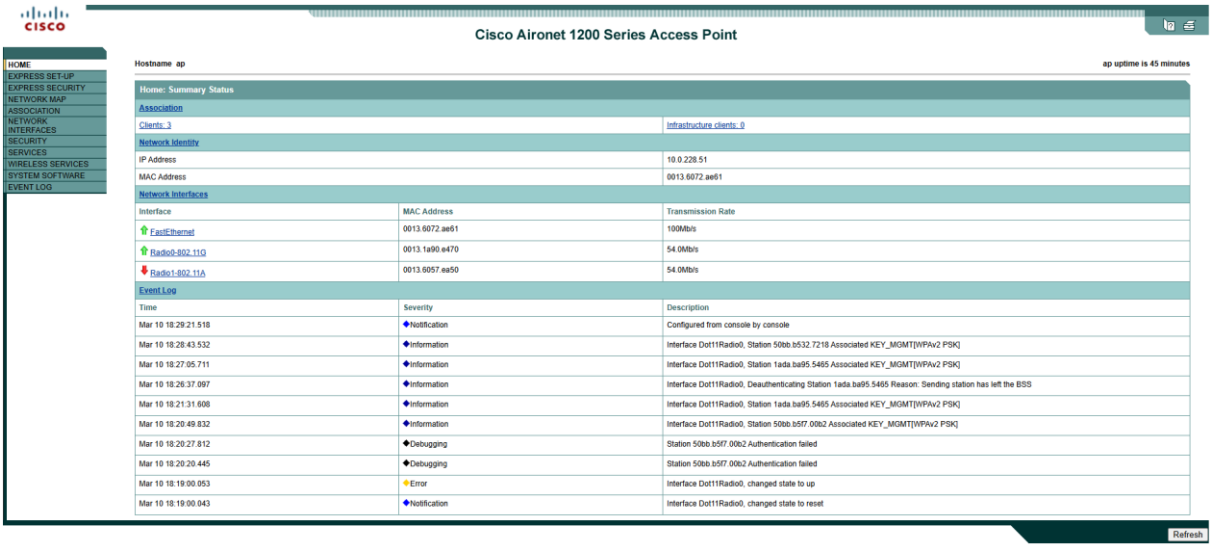


Mais aussi sur un téléphone, que le réseau utilise une sécurité de type WPA/WPA2. De plus, on retrouve l'information du mot de passe qui a été ajouté (Bts2026@).



Kevin Roussel
Chloe Houivet
Ajay Muthu Kumar
Ecole IRIS

Lorsque vous ouvrez le navigateur et saisissez l'adresse IP (10.0.228.51) du point d'accès WiFi, vous pouvez accéder à l'interface de configuration suivante :



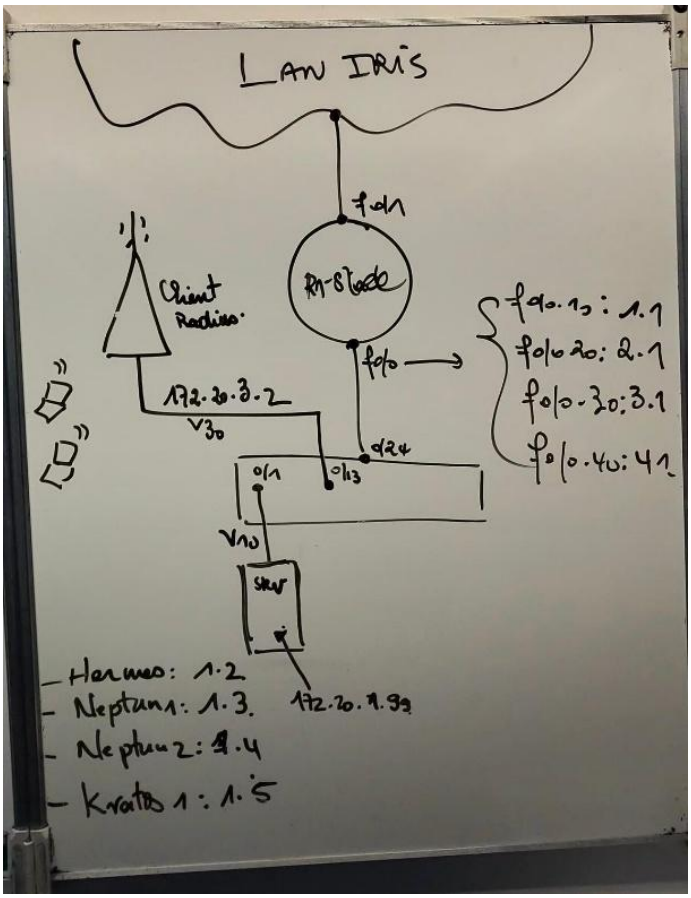
Kevin Roussel
Chloe Houivet
Ajay Muthu Kumar
Ecole IRIS

PARTIE 2 : MISSION 6

1. Introduction

Dans le cadre de l'infrastructure StadiumCompany, nous mettons en place une architecture réseau sécurisée reposant sur le protocole RADIUS.

Cette solution permet de centraliser l'authentification des utilisateurs (Hermes, Neptune, Kratos) via un serveur dédié. L'infrastructure s'appuie sur une segmentation par VLANs et un routage inter-VLAN assuré par le routeur R1-Stade, garantissant ainsi une gestion des accès à la fois souple, évolutive et hautement sécurisée.

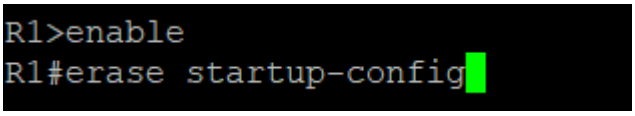


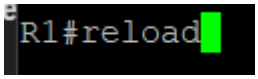
Kevin Roussel
Chloe Houivet
Ajay Muthu Kumar
Ecole IRIS

2. Préparation du matériel (réinitialisation du switch, routeur, borne wifi)

1°) Pour commencer, il faut réinitialiser tous les équipements avec l'utilisation de plusieurs commandes, en fonction de chaque équipements :
Pour cela, il faut tout d'abord taper la commande « enable » qui permet de passer du mode utilisateur au mode privilège.
Switch : "erase startup-config" qui supprime le fichier de configuration sauvegardé en NVRAM.
Mais aussi la commande « delete flash :vlan.dat » qui est spécifique au switch et supprime la base de données des VLANs.
Enfin, « reload » qui redémarre l'équipement pour appliquer la réinitialisation.

Concernant les routeurs, il y a la commande « erase startup-config » comme pour le switch ainsi que « reload ».





2°) Pour procéder à la réinitialisation d'une borne WiFi, il faut débrancher l'alimentation, maintenir le bouton « MODE » durant 15 secondes. A la suite de cela, rebrancher l'alimentation à la borne WiFi.

3. Configuration du routeur

1°) Maintenant, il faut nommer chacun des équipements pour mieux se repérer concernant leur configuration. Pour cela, il faut tout d'abord taper la commande « enable » qui permet de passer du mode utilisateur au mode privilège.
Après cela, un # apparaît et il faut taper « conf t » pour accéder au mode configuration globale.
Enfin, on choisit le nom qu'on veut donner à l'équipement comme là dans notre cas ce sera R1-Stade, cela donne « hostname R1-Stade ».

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1-Stade
R1-Stade(config)#
```

2°) Pour que le routeur agit comme une passerelle pour chaque VLAN, il faut procéder à un routage inter-vlan.
Ainsi, il faut créer une « sous-interface » virtuelle sur le port physique de notre choix comme là c'est fastEthernet 0/0 pour le VLAN 10 avec la commande « interface fastEthernet 0/0.10 ».
Taper « no shutdown » permet d'activer le port.
La commande « encapsulation dot1q 10 » indique au routeur qu'il doit lire les étiquettes du VLAN 10 arrivant sur ce câble.
Enfin, on lui définit une adresse IP qui servira de passerelle par défaut du VLAN 10 en utilisant la commande « ip address 172.20.1.1 255.255.255.0 ».

On procède à la même chose pour les 3 autres VLANs en changeant le numéro de sous interface, celui de l'encapsulation ainsi que l'adresse IP qui est différente et le masque.

VLAN 10

```
R1-Stade(config)#interface fastEthernet 0/0
R1-Stade(config-if)#no shutdown
R1-Stade(config-if)#
*Feb  3 12:14:12.883: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Feb  3 12:14:13.883: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R1-Stade(config-if)#interface fastEthernet 0/0.10
R1-Stade(config-subif)#encapsulation dot1q 10
R1-Stade(config-subif)#ip address 172.20.1.1 255.255.255.0
R1-Stade(config-subif)#exit
```

VLAN 20

```
R1-Stade(config)#interface fastEthernet 0/0.20
R1-Stade(config-subif)#encapsulation dot1q 20
R1-Stade(config-subif)#ip address 172.20.2.1 255.255.255.0
R1-Stade(config-subif)#exit
```


Kevin Roussel
Chloe Houivet
Ajay Muthu Kumar
Ecole IRIS

VLAN 30

```
R1-Stade(config)#interface fastEthernet 0/0.30
R1-Stade(config-subif)#encapsulation dot1q 30
R1-Stade(config-subif)#ip address 172.20.3.1 255.255.255.0
R1-Stade(config-subif)#exit
```

VLAN 40

```
R1-Stade(config)#interface fastEthernet 0/0.40
R1-Stade(config-subif)#encapsulation dot1q 40
R1-Stade(config-subif)#ip address 172.20.4.1 255.255.255.0
R1-Stade(config-subif)#exit
```

3°) Concernant le NAT, qui est un mécanisme essentiel qui agit comme un traducteur entre vos réseau privé et le réseau public.
Pour pouvoir le configurer, il faut sélectionner une interface physique qui est relié vers l'extérieur, c'est-à-dire vers Internet. Dans notre cas, « interface fastEthernet 0/1 ».
Ensuite, on ne va pas lui attribuer une adresse IP, on va demander au routeur de demander une adresse automatiquement au réseau de l'école en utilisant « ip address dhcp ».
Enfin, on spécifie que cette interface est celle étant l'extérieur du réseau et donc que c'est ici que les paquets sortiront après avoir été traduits.
Pour cela, on utilise la commande « ip nat outside ».

```
R1-Stade(config)#interface fastEthernet 0/1
R1-Stade(config-if)#ip address dhcp
R1-Stade(config-if)#no shut
*Feb  3 12:23:09.491: %DHCP-6-ADDRESS_ASSIGN: Interface FastEthernet0/1 assigned DHCP address 10.0.228.42, mask 255.255.254.0, hostname R1-Stade

R1-Stade(config-if)#no shut
R1-Stade(config-if)#ip nat outside
R1-Stade(config-if)#exit
```

4°) Après avoir configurer l'interface de sortie, il faut maintenant configurer les interfaces internes. De ce fait, pour que le NAT fonctionne, le routeur doit savoir d'où proviennent les paquets à traduire.

Donc pour chaque sous-interfaces créées pour les VLANs, on va appliquer la commande suivante : « ip nat inside » qui marque que ces interfaces sont comme étant l'intérieur du réseau après être retournés sur chacune avec la commande « interface fastEthernet 0/0.10 » par exemple.

```
R1-Stade(config)#interface fastEthernet 0/0.10
R1-Stade(config-subif)#ip nat inside
R1-Stade(config-subif)#exit
R1-Stade(config)#interface fastEthernet 0/0.20
R1-Stade(config-subif)#ip nat inside
R1-Stade(config-subif)#exit
R1-Stade(config)#interface fastEthernet 0/0.30
R1-Stade(config-subif)#ip nat inside
R1-Stade(config-subif)#exit
R1-Stade(config)#interface fastEthernet 0/0.40
R1-Stade(config-subif)#ip nat inside
R1-Stade(config-subif)#exit
```

5°) De plus, le NAT permet aux adresses privées de sortir sur Internet via une adresse publique. Pour ce faire, on va créer une liste d'autorisation qui dira par exemple « le réseau 172.20.0.0 est autorisé à être traduit ».

On utilise alors la commande « access-list 10 permit 172.20.0.0 0.0.0.255 ».

On procède à la même chose pour les 3 autres VLANs en changeant certaines informations qui leurs seront spécifiques.

```
R1-Stade(config)#access-list 10 permit 172.20.1.0 0.0.0.255
R1-Stade(config)#access-list 20 permit 172.20.2.0 0.0.0.255
R1-Stade(config)#access-list 30 permit 172.20.3.0 0.0.0.255
R1-Stade(config)#access-list 40 permit 172.20.4.0 0.0.0.255
```

6°) Maintenant, en utilisant la commande « ip nat inside source list 10 interface fastEthernet 0/1 overload », on va prendre tout ce qui correspond par exemple à l'ACL 10 et le traduire en utilisant l'adresse IP de l'interface de sortie (f0/1). Et le terme « overload » permet à plusieurs PC d'utiliser une seule adresse publique.

On réplique cela sur chacun des VLANs.

```
R1-Stade(config)#$de source list 10 interface fastEthernet 0/1 overload

R1-Stade(config)#$de source list 20 interface fastEthernet 0/1 overload

R1-Stade(config)#$de source list 30 interface fastEthernet 0/1 overload

R1-Stade(config)#$de source list 40 interface fastEthernet 0/1 overload
```

4. Configuration du switch

1°) Maintenant, il faut nommer chacun des équipements pour mieux se repérer concernant leur configuration. Pour cela, il faut tout d'abord taper la commande « enable » qui permet de passer du mode utilisateur au mode privilège.
Après cela, un # apparaît et il faut taper « conf t » pour accéder au mode configuration globale.
Enfin, on choisit le nom qu'on veut donner à l'équipement comme là dans notre cas ce sera SW1, cela donne « hostname SW1 ».

```
Switch>   enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SW1
SW1(config)#
```

2°) Pour procéder à la configuration des ports trunk du Switch à notre disposition. Cela permet de configurer le port afin qu'il laisse passer plusieurs VLANs simultanément.
Il faut utiliser la commande « interface fastEthernet 0/24 », cela nous permet de sélectionner le port physique.
Et ensuite, « switchport mode trunk » qui configure le port.

```
SW1(config)#interface fastEthernet 0/24
SW1(config-if)#switchport mode tr
SW1(config-if)#switchport mode trunk
SW1(config-if)#exi
*Mar  1 01:22:07.610: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
*Mar  1 01:22:08.600: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to downt
SW1(config)#
*Mar  1 01:22:11.620: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to up
*Mar  1 01:22:40.645: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
SW1(config)#
```

3°) Pour créer un VLAN sur le switch il faut être en mode configuration « conf t », puis sélectionner le VLAN que nous voulons créer ou modifier. Par exemple « vlan 10 » et on indiquera le nom que l'on souhaite pour ce VLAN avec la commande « name ».
Ainsi, les commandes qu'il faut utiliser : « Vlan ** » et ensuite « name ** ».
Dans notre cas, c'est « Vlan 10 » par exemple et à la suite « name LAN_SERVEUR » et on reproduit la même chose pour les 3 autres VLANs.

```
SW1(config)#vlan 10
SW1(config-vlan)#name LAN_SERVEUR
SW1(config-vlan)#exit
SW1(config)#vlan 20
SW1(config-vlan)#name LAN_EQUIPE
SW1(config-vlan)#exit
SW1(config)#vlan 30
SW1(config-vlan)#name LAN_WIFI
SW1(config-vlan)#exit
SW1(config)#vlan 40
SW1(config-vlan)#name LAN_DMZ
SW1(config-vlan)#exit
```

4°) Après avoir créé nos VLANs en leur fournissant un numéro ainsi qu'un nom, il faut procéder à l'attribution des ports à chaque VLANs sur les 2 switch.
Pour cela, on sélectionne les ports destinés aux PC avec la commande « interface range fastEthernet 0/1 – 6 ». Cela fait qu'on sélectionne les ports de 1 à 6.
Ensuite, on tape la commande « switchport access vlan 10 » qui permet de regrouper ces ports physiquement dans le réseau virtuel 10.
On reproduit la même chose avec les 3 autres VLANs en leur attribuant des ports.

```
SW1(config)#interface range fastEthernet 0/1 - 6
SW1(config-if-range)#switchport access vlan 10
SW1(config-if-range)#exit
SW1(config)#interface range fastEthernet 0/7 - 12
SW1(config-if-range)#switchport access vlan 20
SW1(config-if-range)#exit
SW1(config)#interface range fastEthernet 0/13 - 14
SW1(config-if-range)#switchport access vlan 30
SW1(config-if-range)#exit
SW1(config)#interface range fastEthernet 0/16 - 20
SW1(config-if-range)#switchport access vlan 40
SW1(config-if-range)#exit
```

5. Configuration de la borne wifi

1°) Nom par défaut de la borne : ap>
Login : en
Mot de passe : Cisco

```
ap>en
Password:
```

2°) Pour la création du réseau Wi-Fi et de son SSID (nom du réseau), il faut commencer par choisir l'interface où l'on souhaite créer notre réseau.
Pour cela, on tape la commande « interface dot11Radio 0 ». La radio 0 correspond au 2,4Ghz et dot11 correspond à la spécification 802.11.
A la suite, on créer notre nom de réseau avec la commande « ssid WiFi-Stade_GRACK ».
Enfin, il faut exécuter la commande « exit » afin de sortir du mode configuration d'interface (config-if).

```
ap(config)#interface dot11Radio 0
ap(config-if)#ssid WiFi-Stade_GRACK
ap(config-if-ssid)#exit
```

3°) Maintenant, On allume le point d'accès et on lui dit de trouver tout seul son adresse sur le réseau grâce à cette commande qui suivent :

- « interface BVI 1 » : On sélectionne le menu de réglages du point d'accès Wi-Fi.
- « ip address DHCP » : On demande au point d'accès de récupérer automatiquement son adresse IP (comme un téléphone qui se connecte au Wi-Fi).
- « no shutdown » : On allume l'appareil pour qu'il commence à fonctionner.

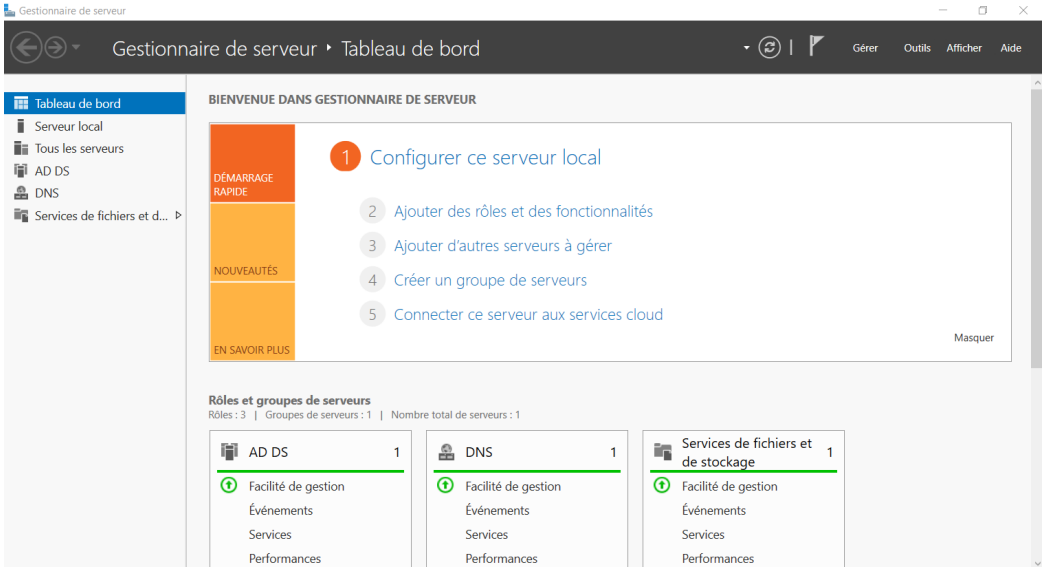
```
ap#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ap(config)#interface BVI 1
ap(config-if)#ip address DHCP
ap(config-if)#no shutdown
ap(config-if)#
*Mar 10 18:06:39.499: %DHCP-6-ADDRESS_ASSIGN: Interface BVI1 assigned DHCP address 10.0.228.51, mask 255.255.254.0, hostname ap
```

6. Mise en place d'une authentification RADIUS

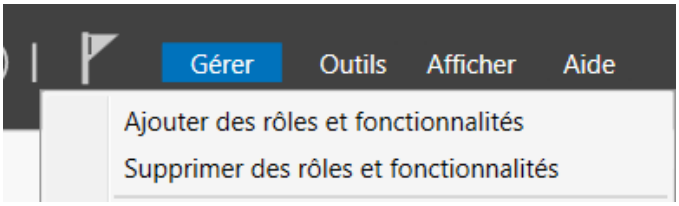
L'objectif de l'authentification RADIUS est de sécuriser l'accès au Wi-Fi en imposant une authentification via RADIUS / 802.1X, avec des identifiants provenant de l'Active Directory (AD).

Installation du service de certificats Active Directory

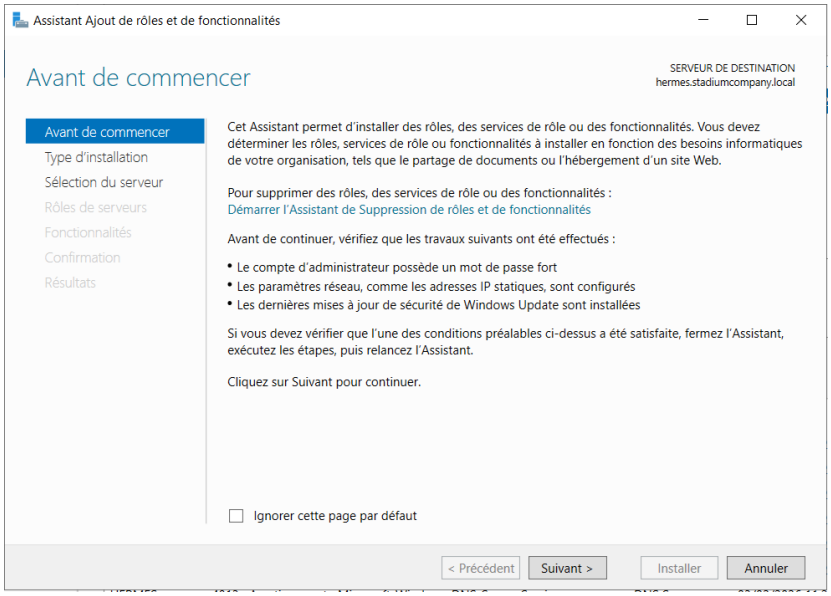
Sur le tableau de bord du gestionnaire de serveur Windows.



On ajoute un nouveau rôle, « gérer » puis ajouter des rôles et fonctionnalités.

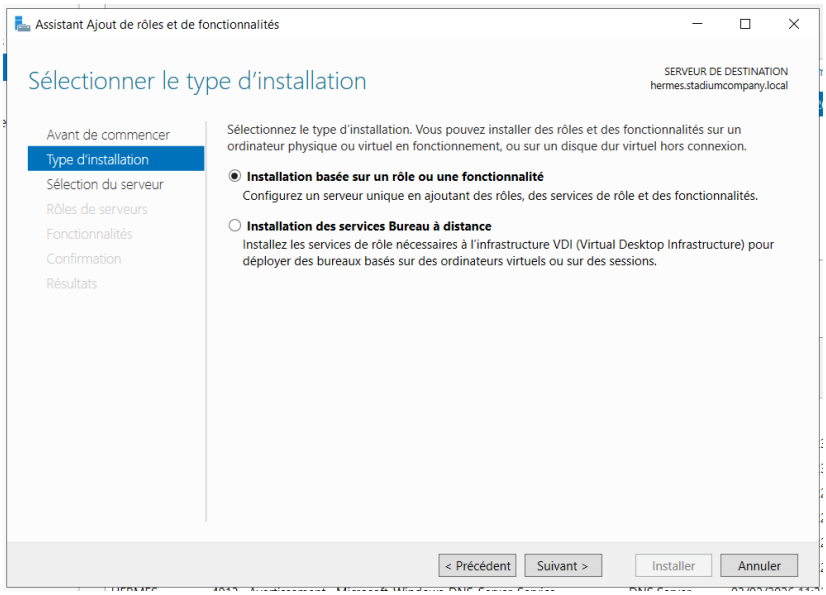


Suivant jusqu'à avoir le choix du rôle de serveurs qu'on souhaite mettre en place.

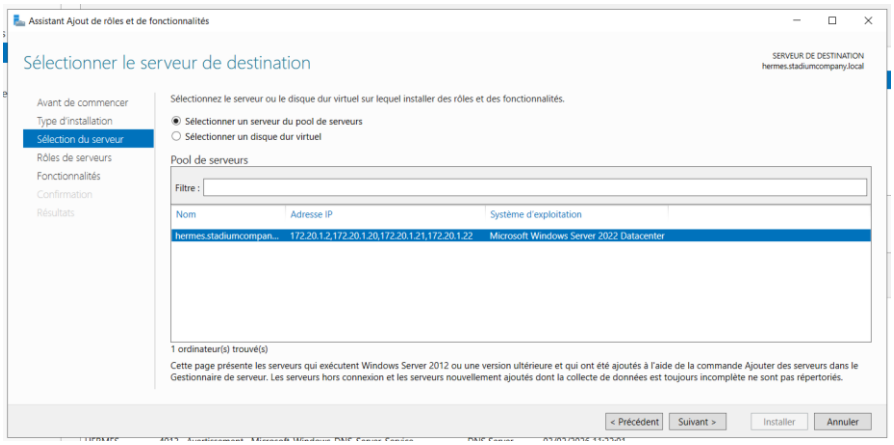


Kevin Roussel
Chloe Houivet
Ajay Muthu Kumar
Ecole IRIS

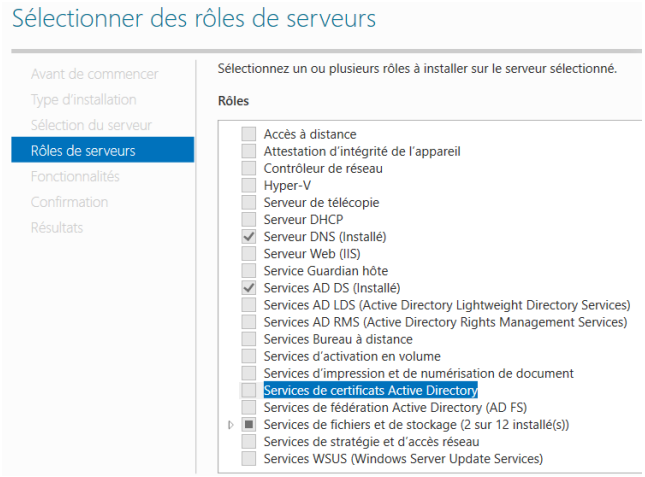
On effectue l'installation d'une fonctionnalité, et non d'un services Bureau à distance « Suivant ».



Ici, on valide que le service sera installé sur le serveur de notre choix, « Suivant ».

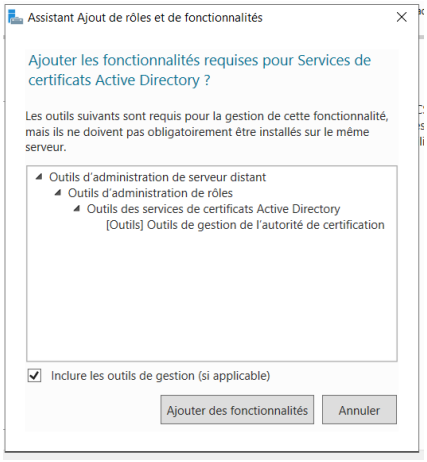


On sélectionne les services de certificats Active Directory.

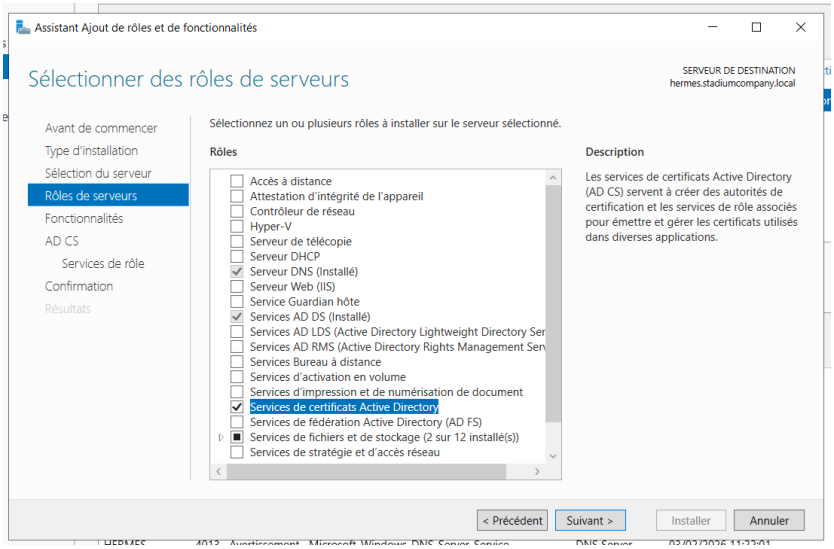


Kevin Roussel
Chloe Houivet
Ajay Muthu Kumar
Ecole IRIS

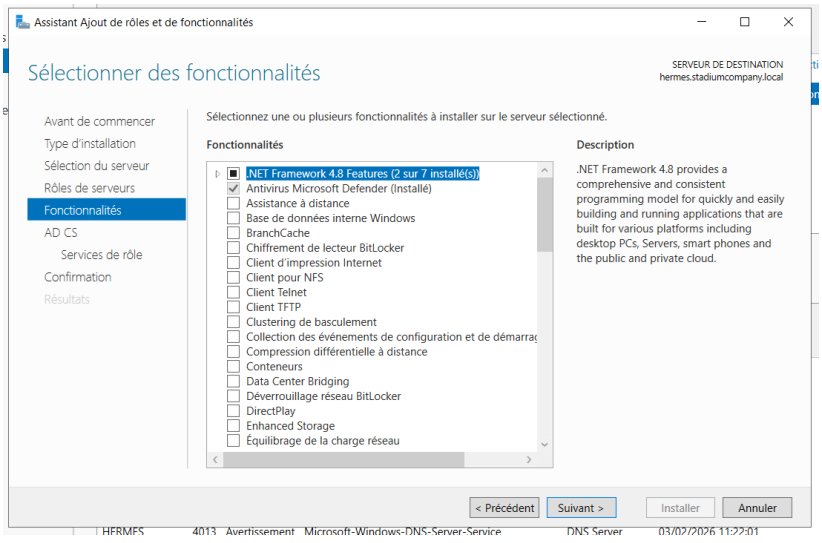
On ajoute la fonctionnalité sélectionnée.



Une fois validé, la case est cochée, ce qui nous permet de faire suivant pour valider.

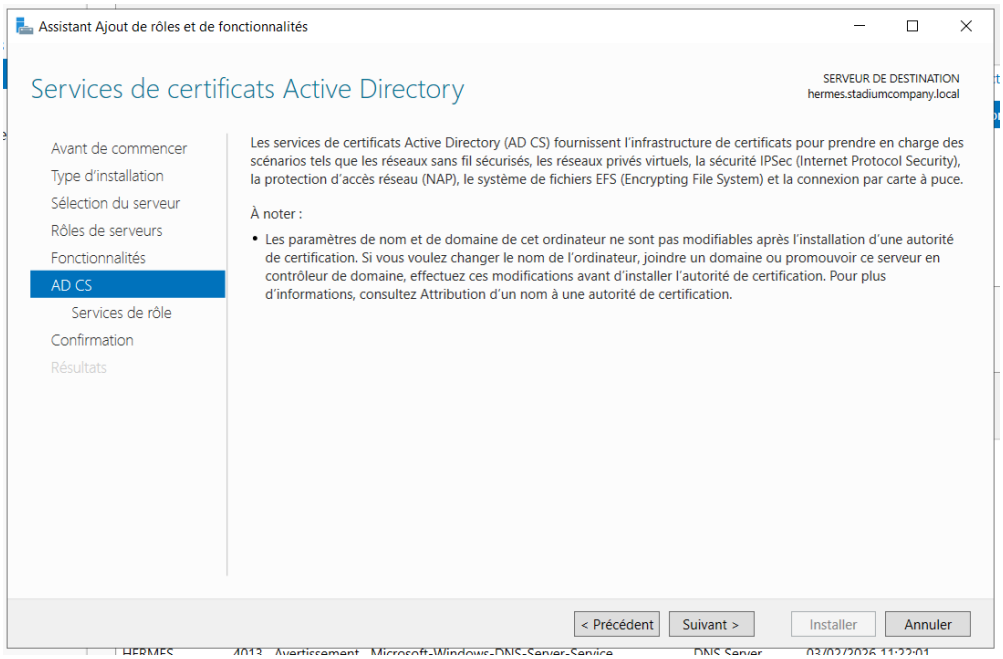


Ici, on laisse par défaut puis « Suivant ».

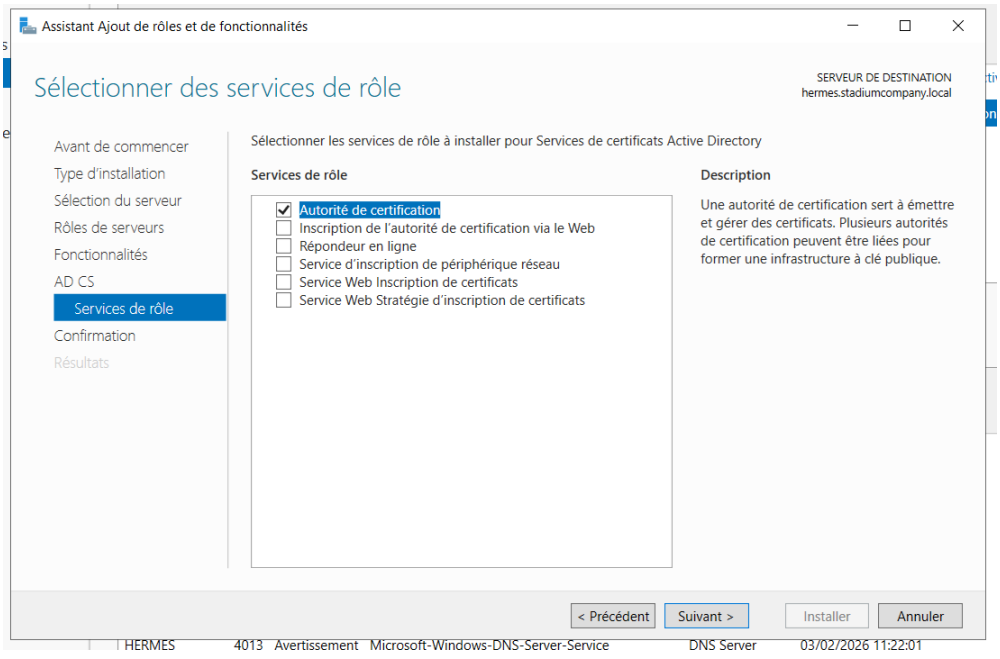


Kevin Roussel
Chloe Houivet
Ajay Muthu Kumar
Ecole IRIS

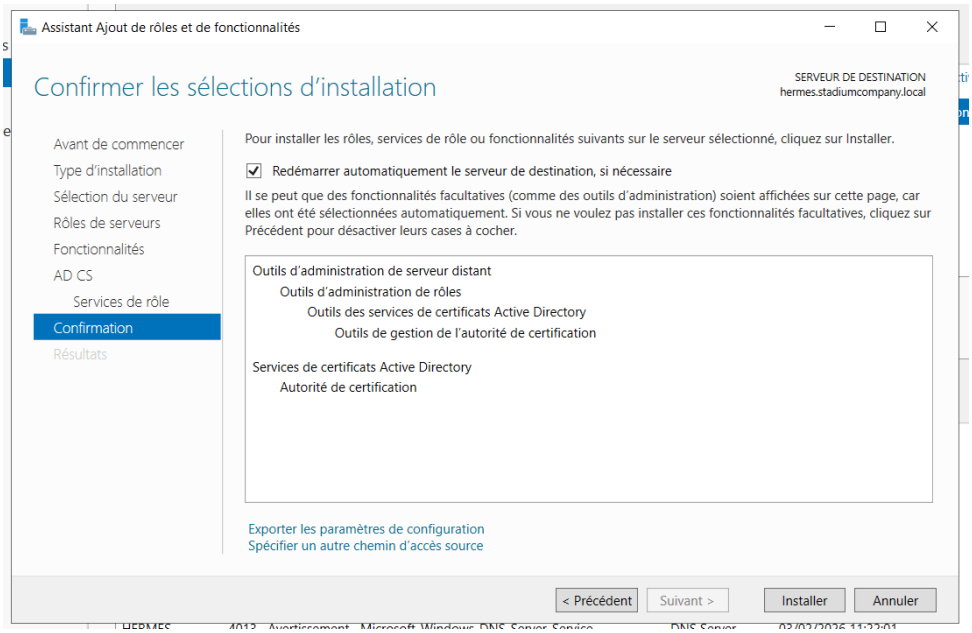
Information par rapport à l'autorité de certification, « Suivant ».



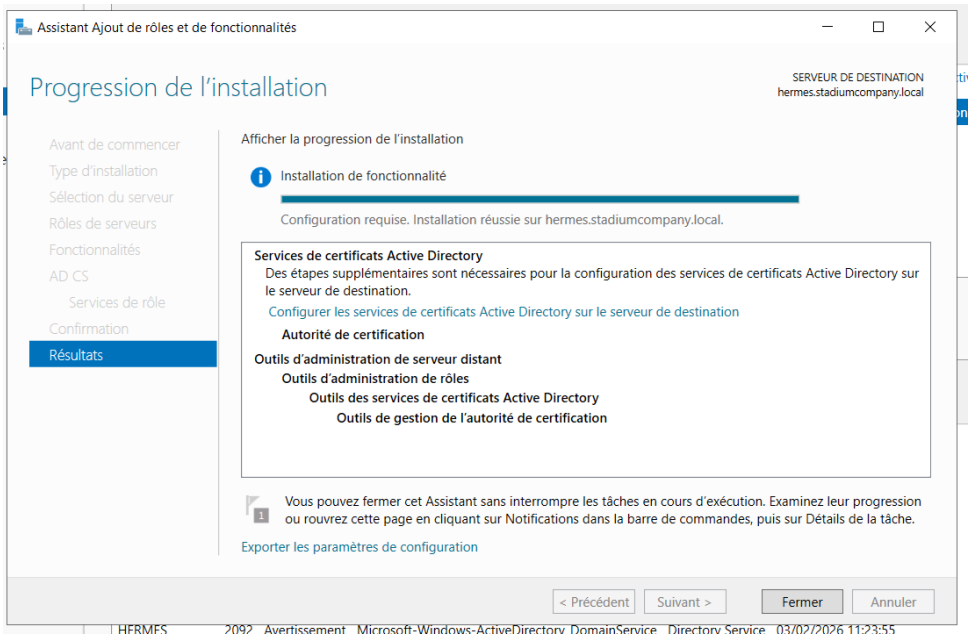
On sélectionne le rôle « Autorité de certification » puis « Suivant ».



Et on lance l'installation avec « Installer ».

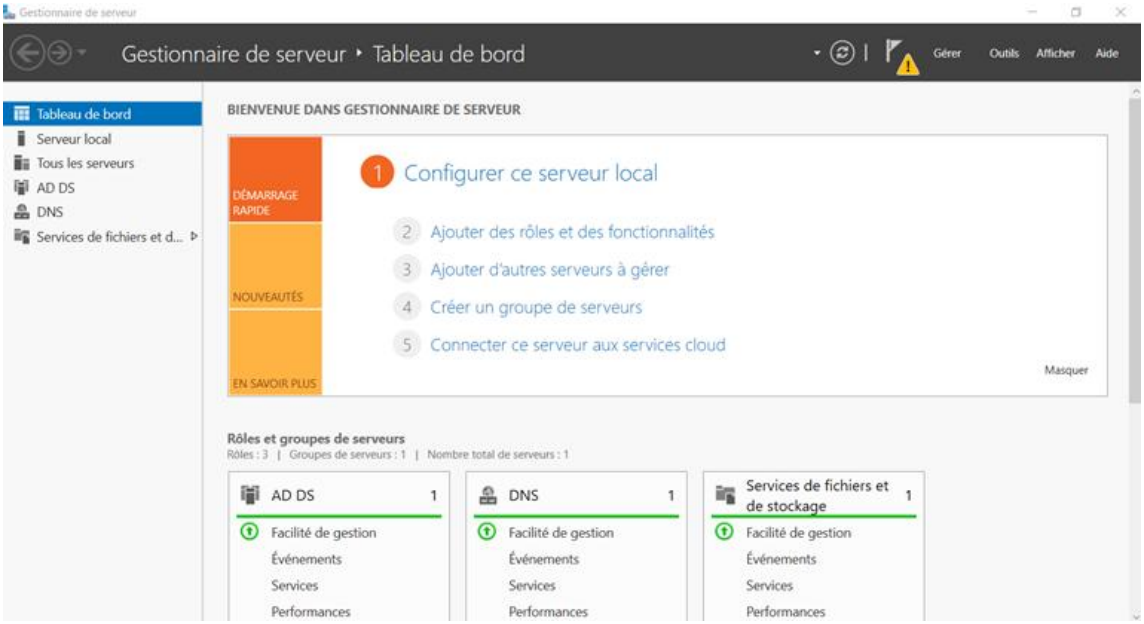


Une fois l'installation terminer, le rôle à bien étais ajouter, on peut donc fermer cette page.

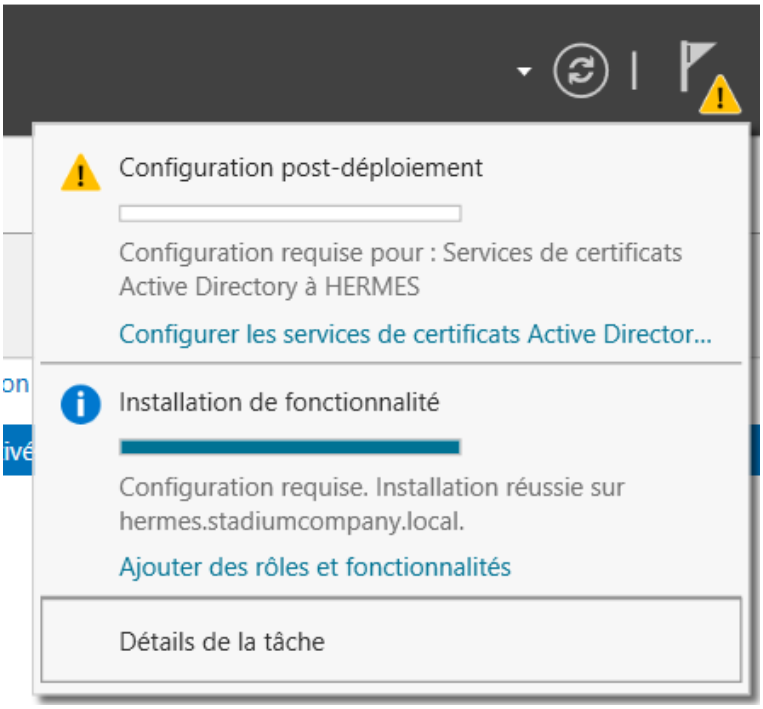


Configuration du service de certificat Active Directory

De retour sur le tableau de bord, un panneau d'alerte est désormais présent en haut à droite, ce qui signifie qu'une configuration est requise.

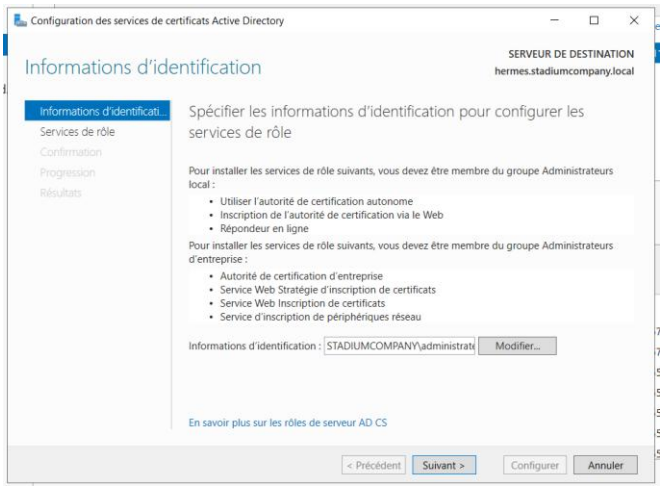


On va donc cliquer sur configurer les services de certificats Active Directory.

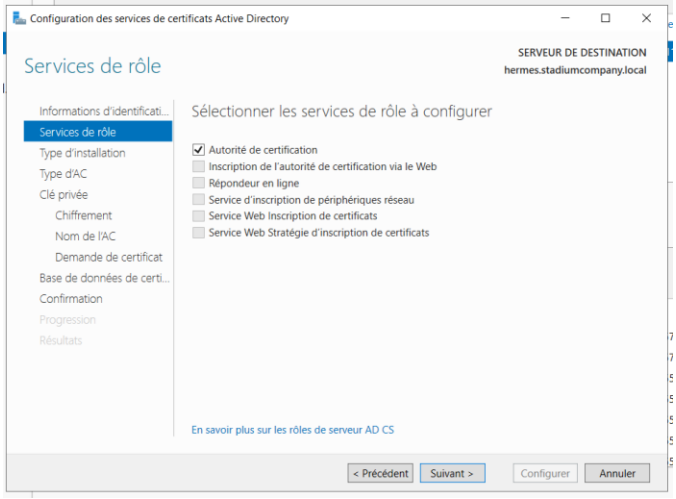


Kevin Roussel
Chloe Houivet
Ajay Muthu Kumar
Ecole IRIS

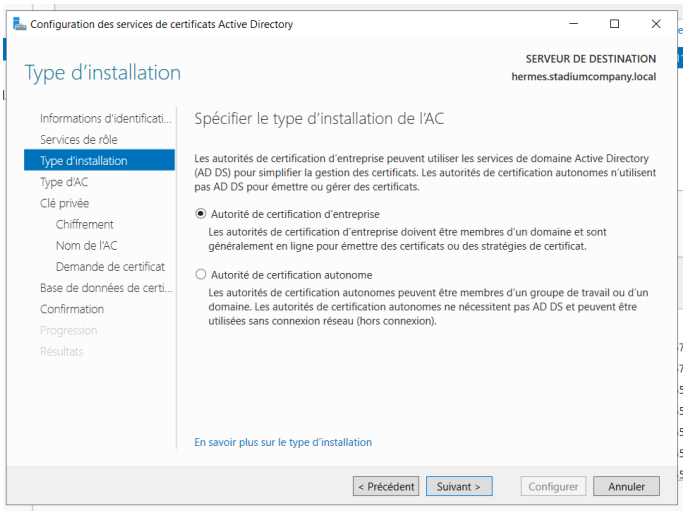
On renseigne les informations d'identification du compte administrateur qui gérera le rôle sur le réseau.



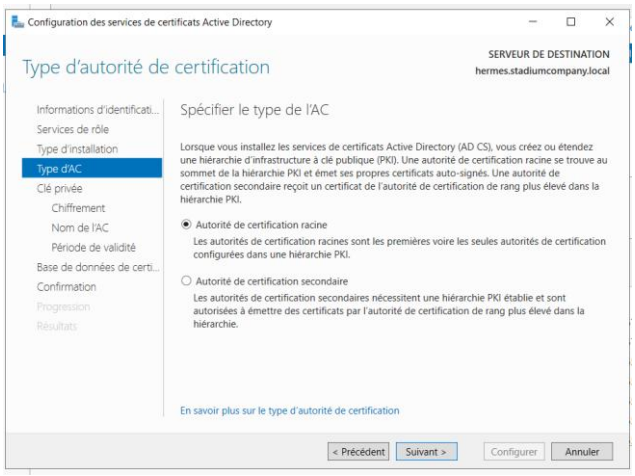
On sélectionne le service à configurer « Autorité de certification ».



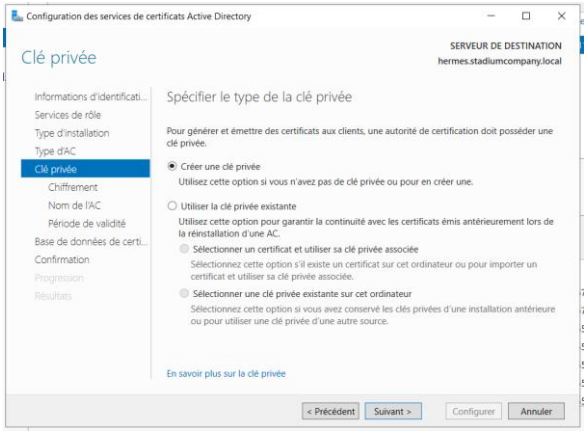
On sélection « L'autorité de certification d'entreprise ».



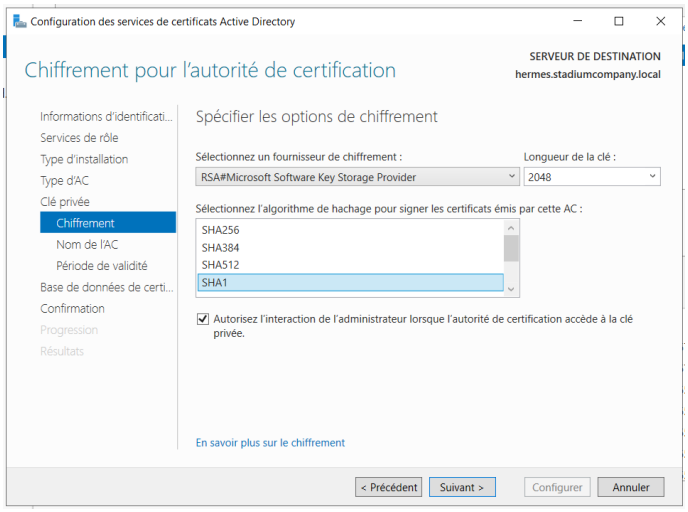
On veut que le certificat soit à la racine, donc « Autorité de certification racine ».



Actuellement, on aura besoin de créée notre première clé privé, « Crée une clé privé » puis « Suivant ».

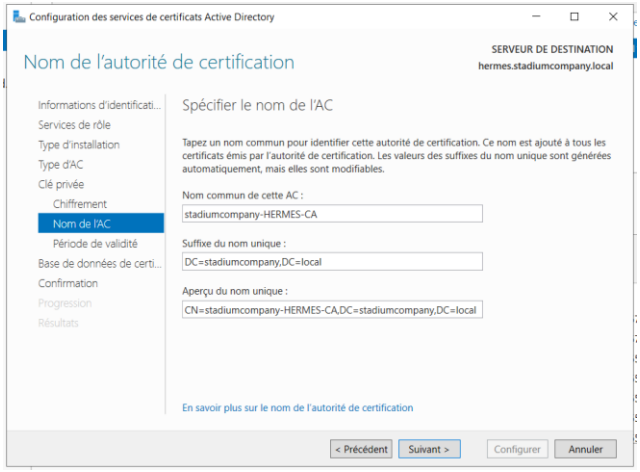


On prend l'algorithme de hash SHA1 et « Suivant ».
(SHA1 est obsolète, on l'utilise uniquement pour la mise en place pédagogique, en situation réel, un encryptage plus fort est préconisé).

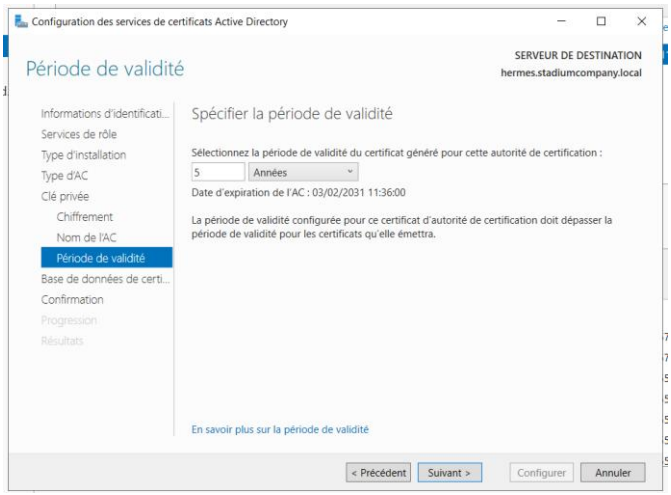


Kevin Roussel
Chloe Houivet
Ajay Muthu Kumar
Ecole IRIS

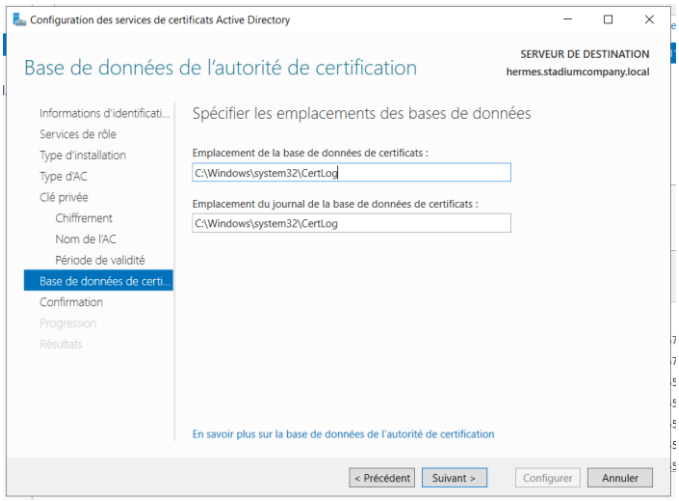
Ici, tout sera remplis par défaut par rapport à notre configuration, « Suivant ».



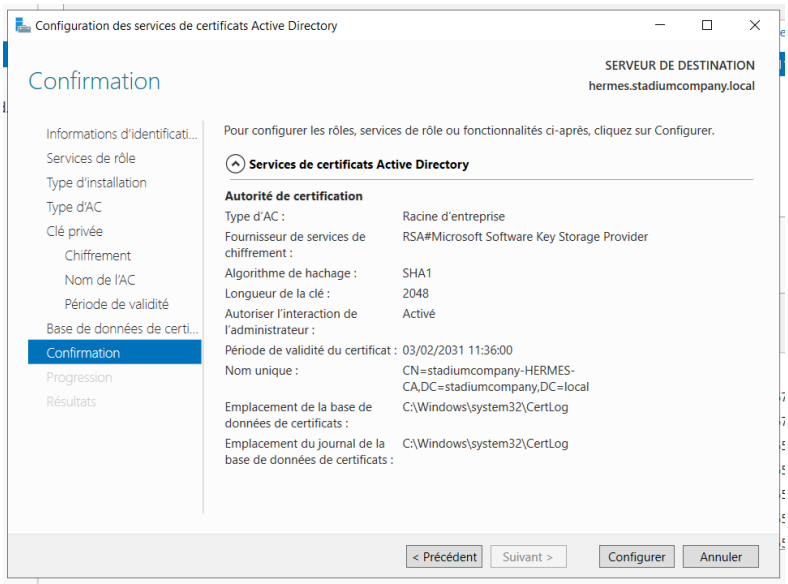
Période de validité par défaut « 5 ans » à modulé en fonction du besoin.



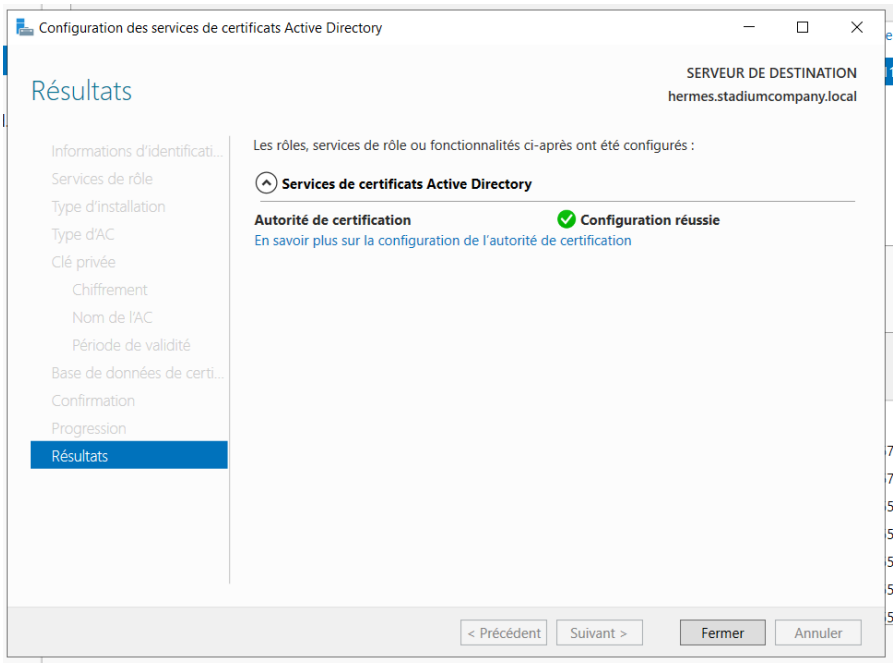
On laisse par défaut, indique l'emplacement des informations de certificats émis/révoqués et des logs.



Récapitulatif de la configuration, on vérifie puis on valide en cliquant sur « Configurer ».



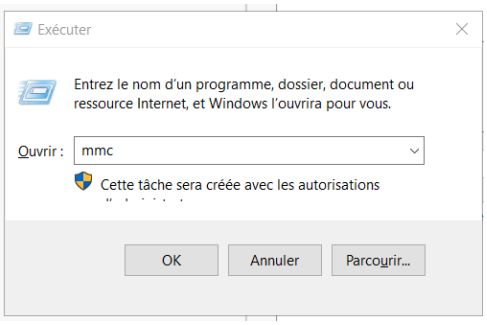
Une fois terminer, on a le message « Configuration réussie ».



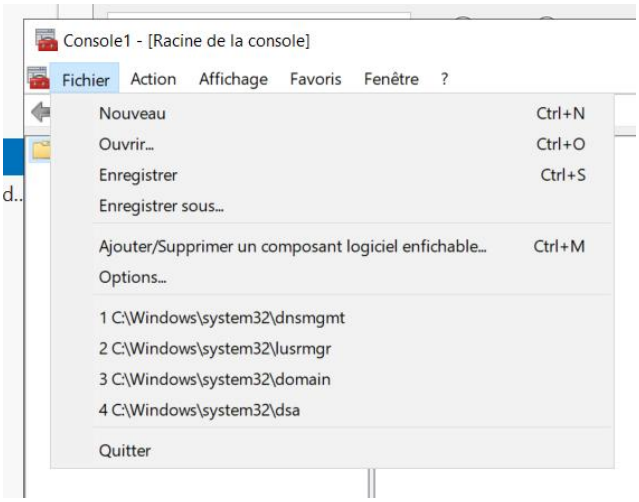
Kevin Roussel
Chloe Houivet
Ajay Muthu Kumar
Ecole IRIS

Ajout d'un certificat

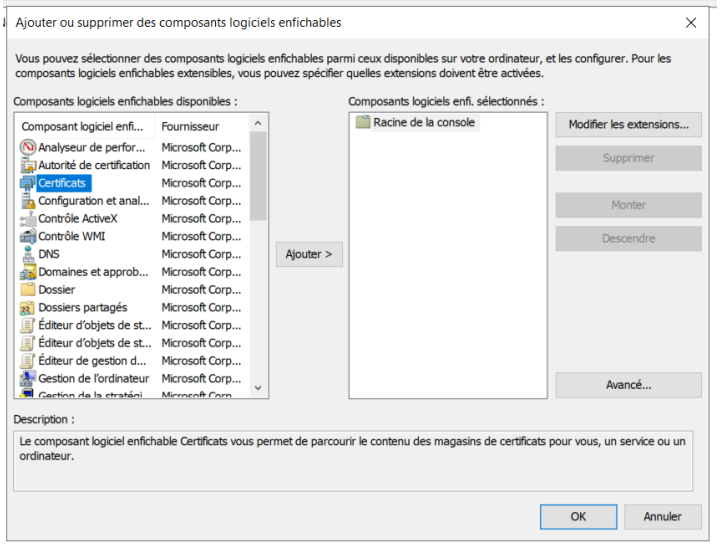
Avec la commande Windows + r, on accède au menu Exécuter, on tape la commande mmc gérer nos certificats.



On fait, « ajouter un composant logiciel enfichable ».

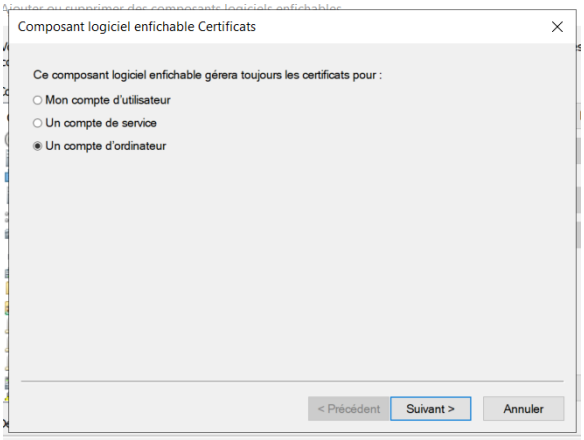


Pour ajouter notre certificat, on sélectionne « certificats » puis on fait « Ajouter ».

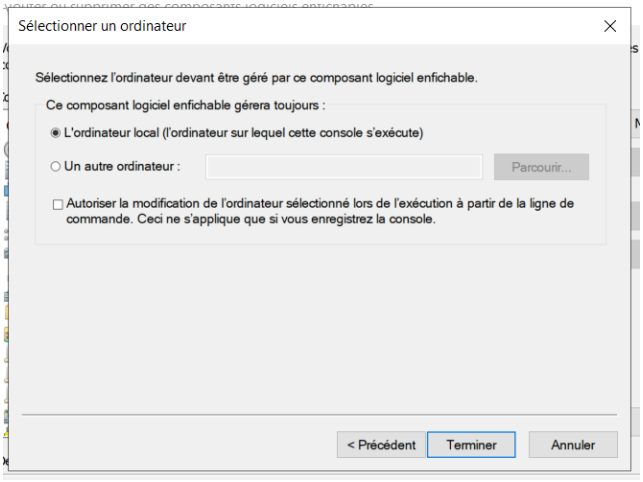


Kevin Roussel
Chloe Houivet
Ajay Muthu Kumar
Ecole IRIS

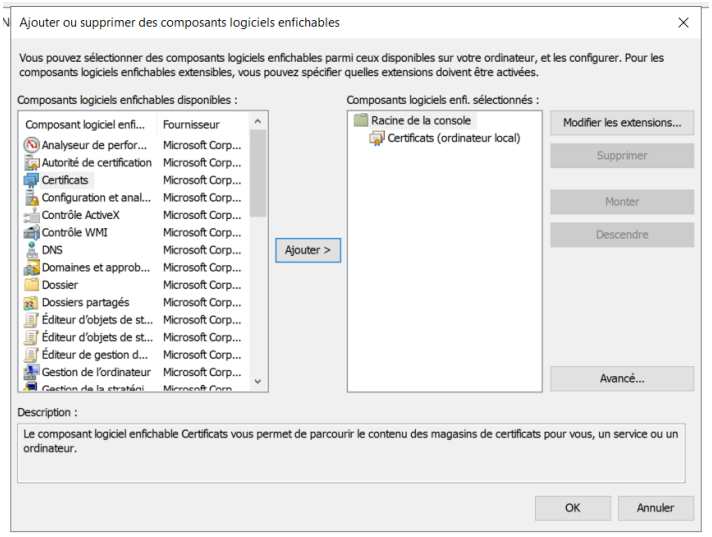
On souhaite que le composant logiciel génère les certificats pour « un compte d'ordinateur ».



On choisit « L'ordinateur local » pour les ordinateurs connecter en local.

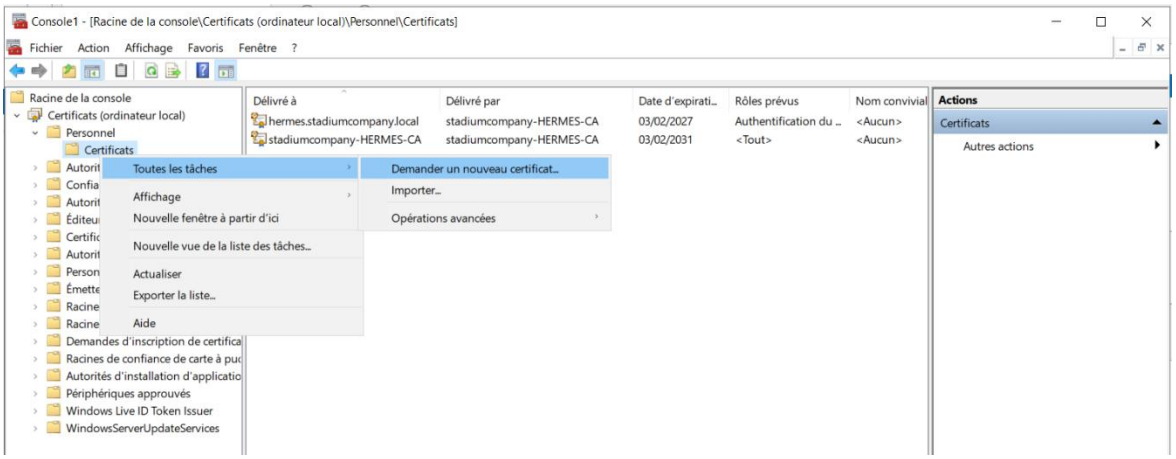


Maintenant, notre certificat est créé et à étais ajouter dans les composants logiciels.

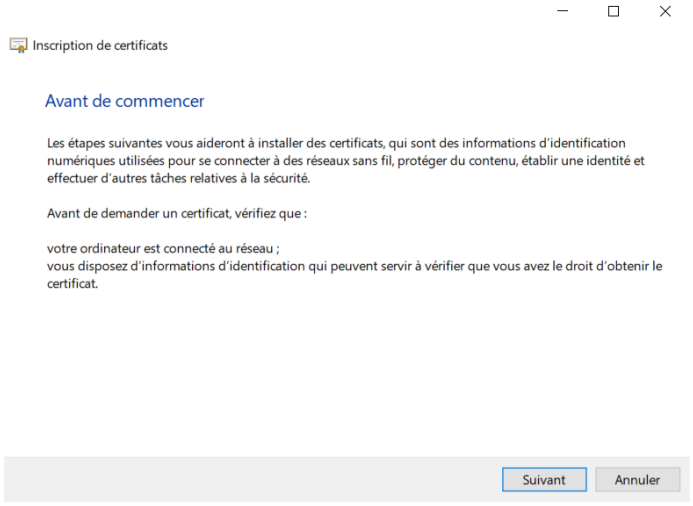


Kevin Roussel
Chloe Houivet
Ajay Muthu Kumar
Ecole IRIS

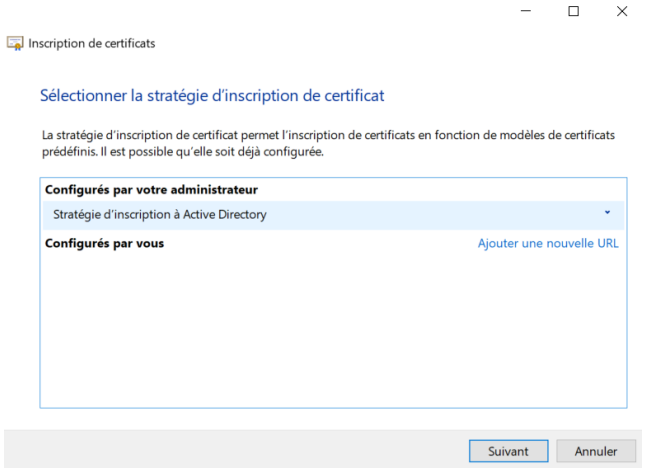
Désormais, on va demander un nouveau certificat
Dans Certificats (ordinateur local) -> personnel, on fait clique droit sur Certificats.
Puis demander un nouveau certificat.



On aura en amonts des informations concernant la demande du nouveau certificat.

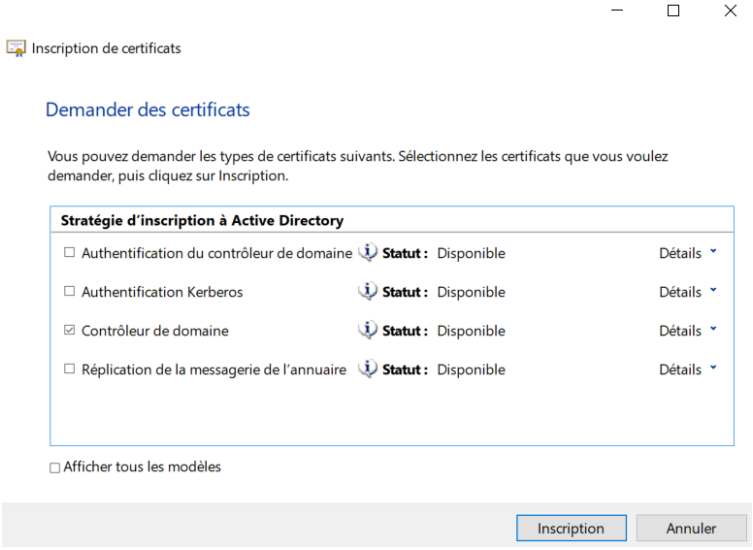


On sélectionne la stratégie d'inscription choisi par défaut.

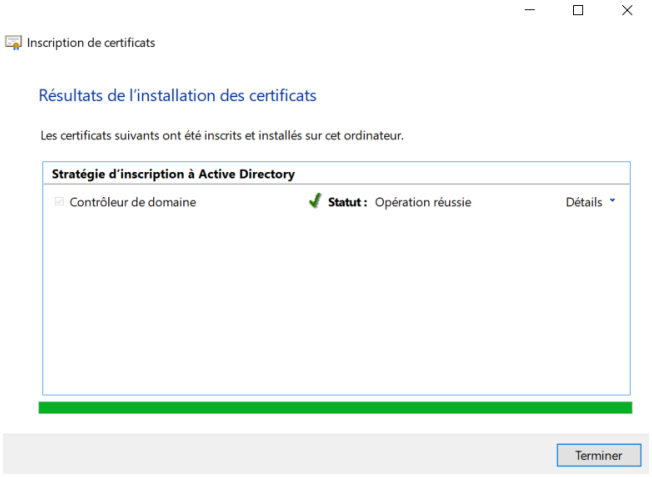


Kevin Roussel
Chloe Houivet
Ajay Muthu Kumar
Ecole IRIS

On choisit « Contrôleur de domaine » puis inscription.



Une validation pour nous dire que l'opération est réussie.

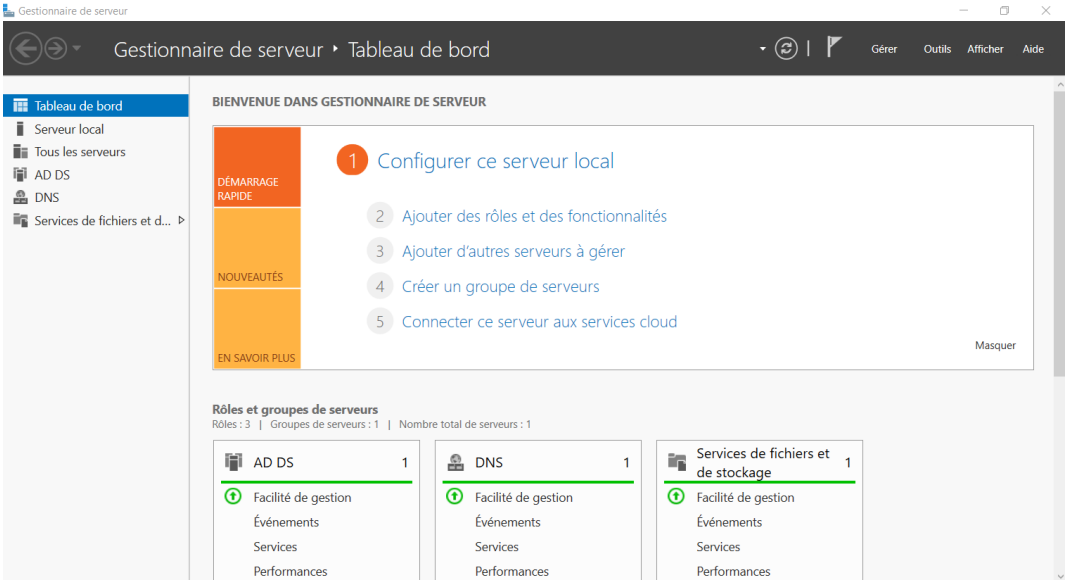


On le voit désormais dans le dossier de certifications.

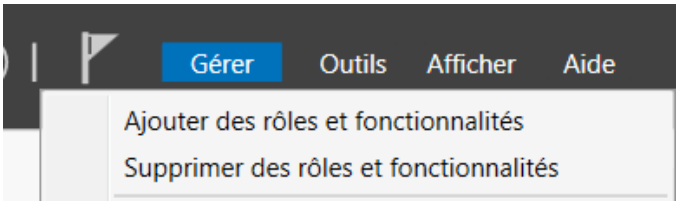
Délivré à	Délivré par	Date d'expirati...	Rôles prévus	Nom convivia
hermes.stadiumcompany.local	stadiumcompany-HERMES-CA	03/02/2027	Authentification du ...	<Aucun>
hermes.stadiumcompany.local	stadiumcompany-HERMES-CA	03/02/2027	Authentification du ...	<Aucun>
stadiumcompany-HERMES-CA	stadiumcompany-HERMES-CA	03/02/2031	<Tout>	<Aucun>

Installation du service de stratégie et d'accès réseau

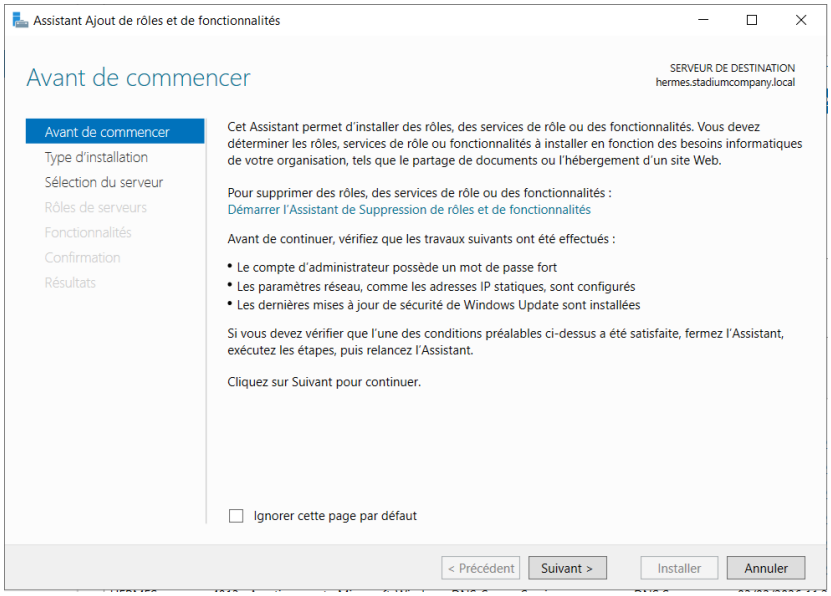
Sur le tableau de bord du gestionnaire de serveur Windows.



On ajoute un nouveau rôle, « gérer » puis ajouter des rôles et fonctionnalités.

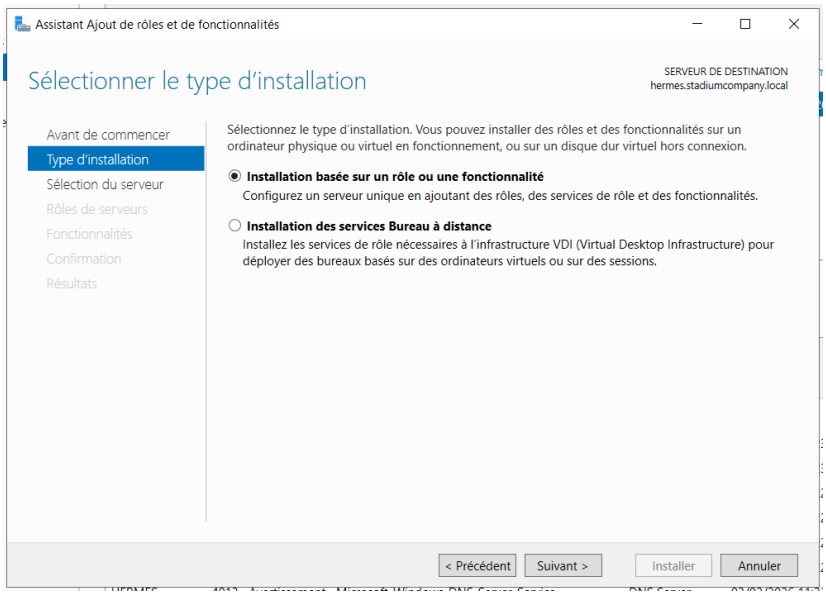


Suivant jusqu'à avoir le choix du rôle de serveurs qu'on souhaite mettre en place.

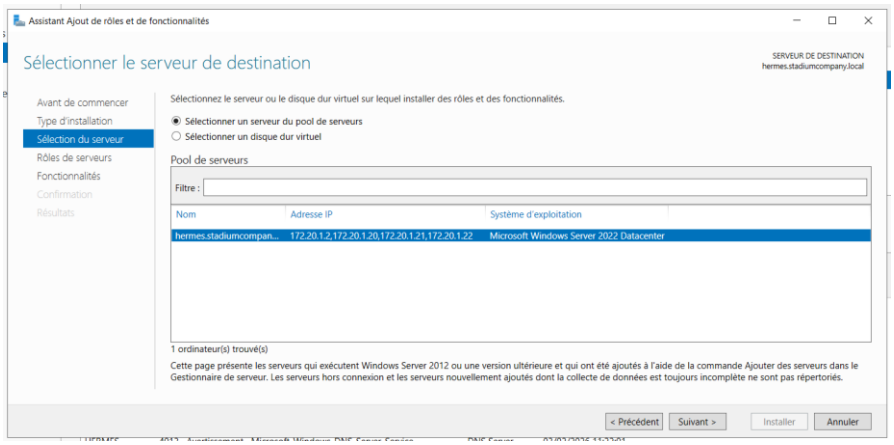


Kevin Roussel
Chloe Houivet
Ajay Muthu Kumar
Ecole IRIS

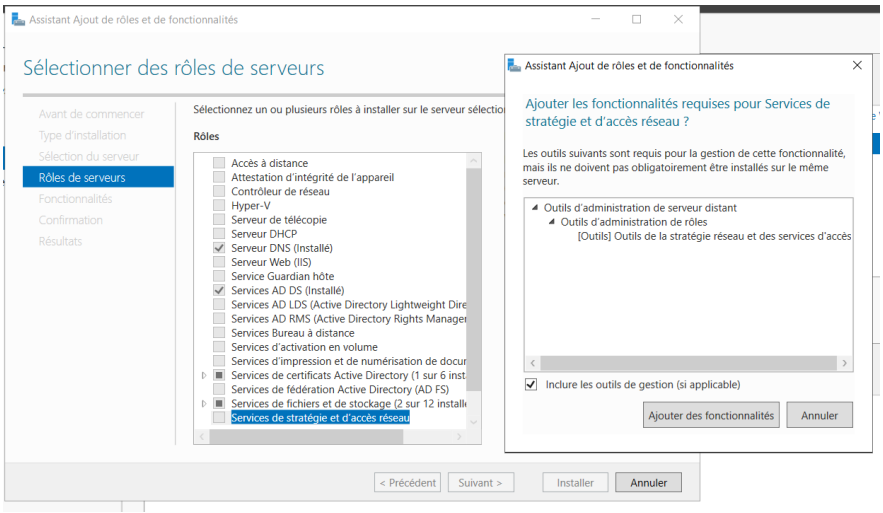
Un effectue l'installation d'une fonctionnalité, et non d'un services Bureau à distance « Suivant ».



Ici, on valide que le service sera installé sur le serveur de notre choix, « Suivant ».

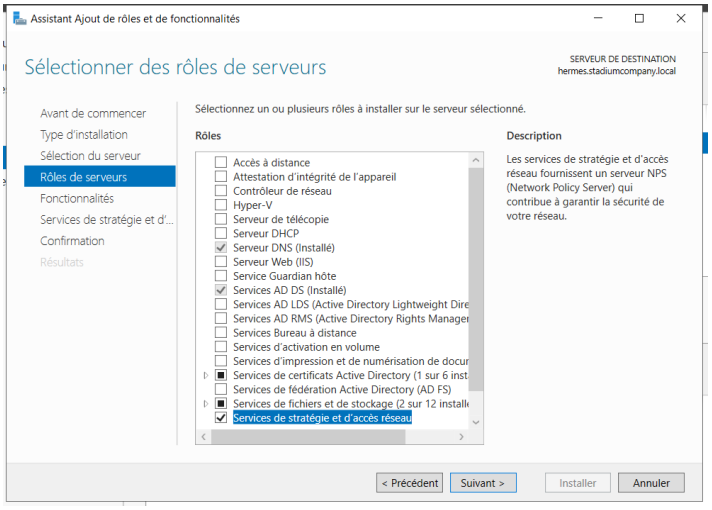


On sélectionne le « service de stratégie et d'accès réseau » et on ajoute la fonctionnalité.

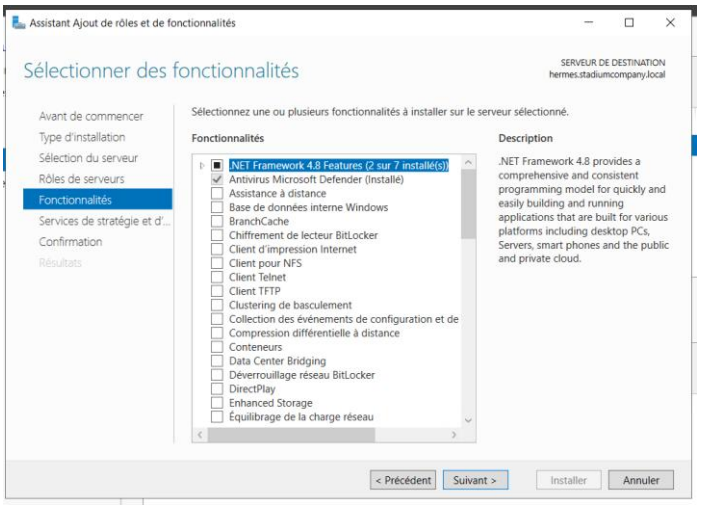


Kevin Roussel
Chloe Houivet
Ajay Muthu Kumar
Ecole IRIS

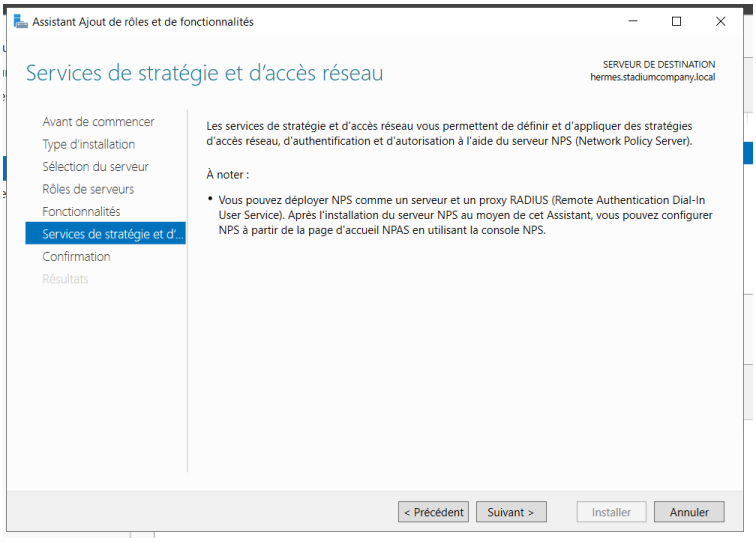
Une fois validé, la case est cochée, ce qui nous permet de faire suivant pour valider.



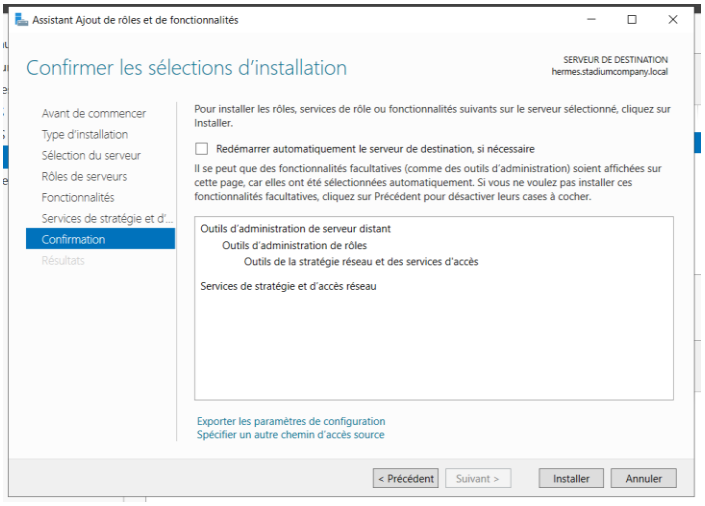
Ici, on laisse par défaut puis « Suivant ».



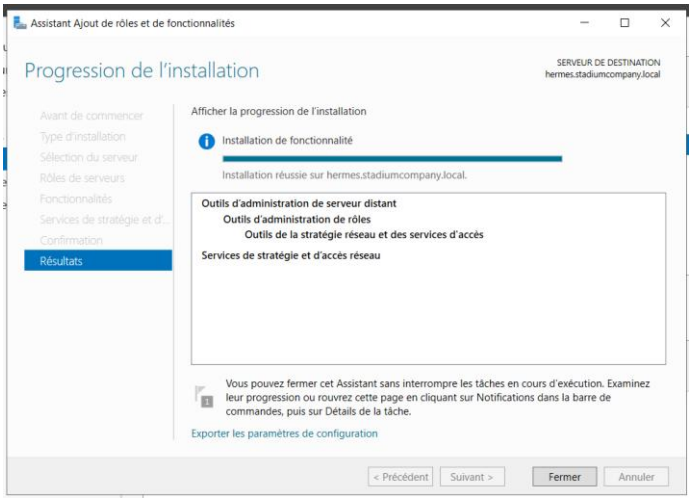
Information par rapport au service de stratégie et d'accès réseau, « Suivant ».



Et on lance l'installation avec « Installer ».

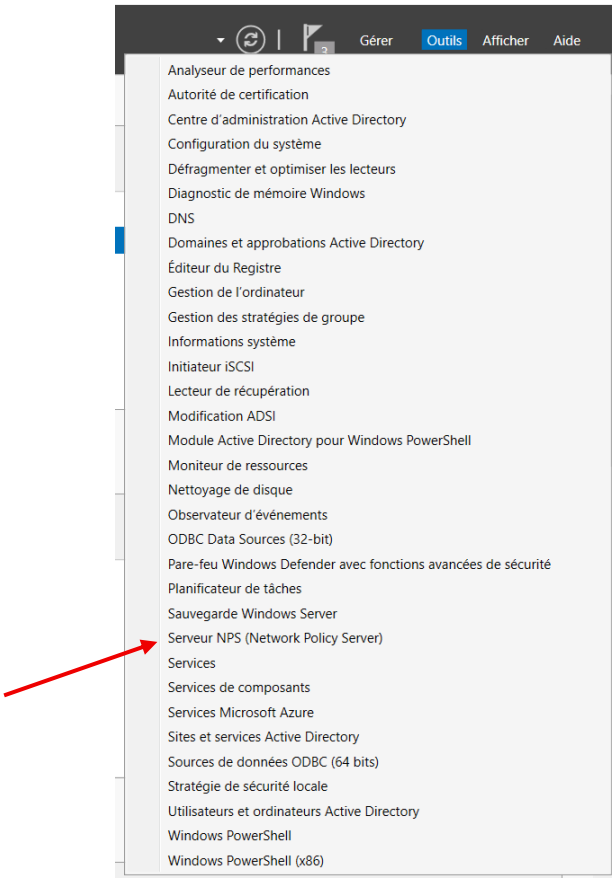


Une fois l'installation terminer, le rôle à bien étais ajouter, on peut donc fermer cette page.

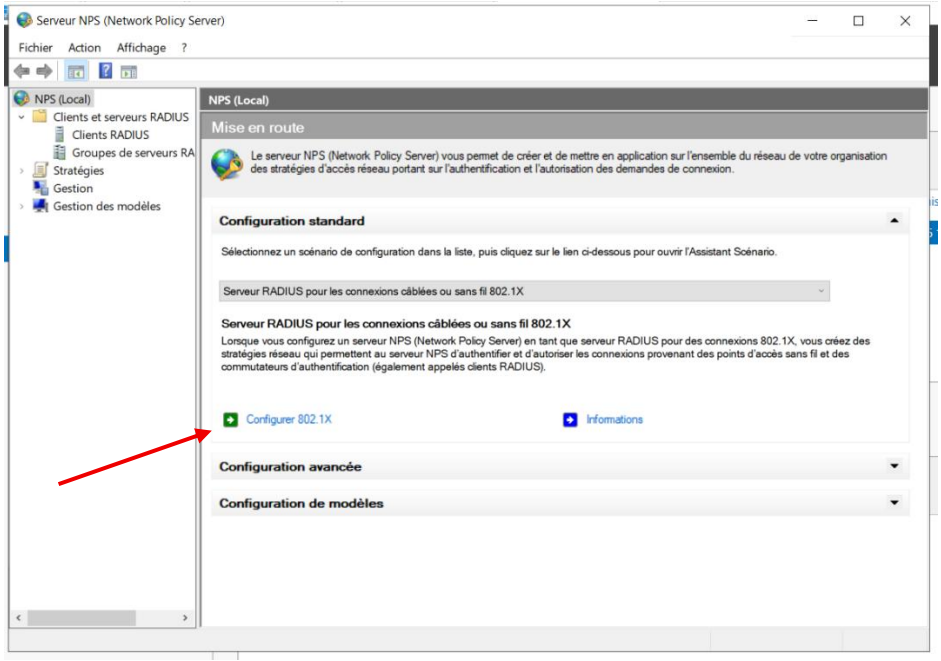


Configuration NPS en « RADIUS pour Wifi »

Dans outils, on va configurer le service NPS via l'onglet, Serveur NPS.

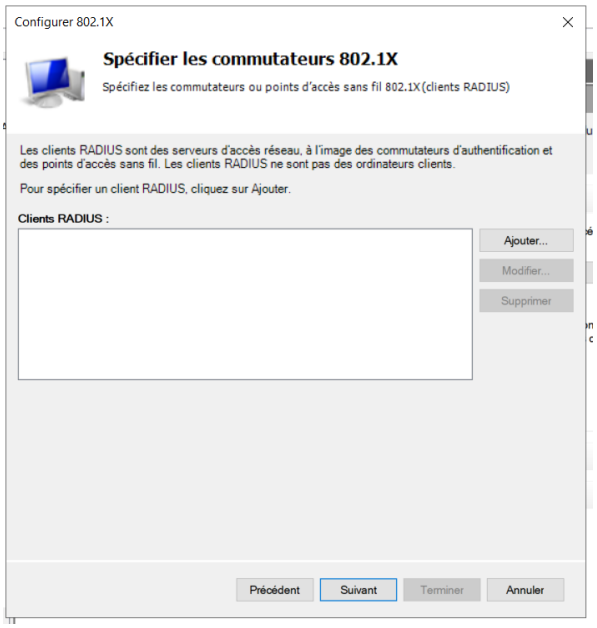


On sélectionne la configuration « Serveur RADIUS pour les connexions câblées ou sans fil »
Puis on clique sur « Configurer 802.1X ».



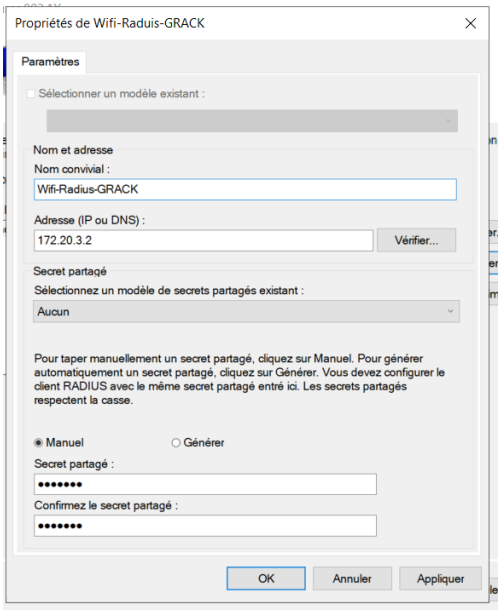
On a le choix entre une connexion filaire ou sans fil. Dans notre cas, nous voulons une connections sans fil sécurisées.

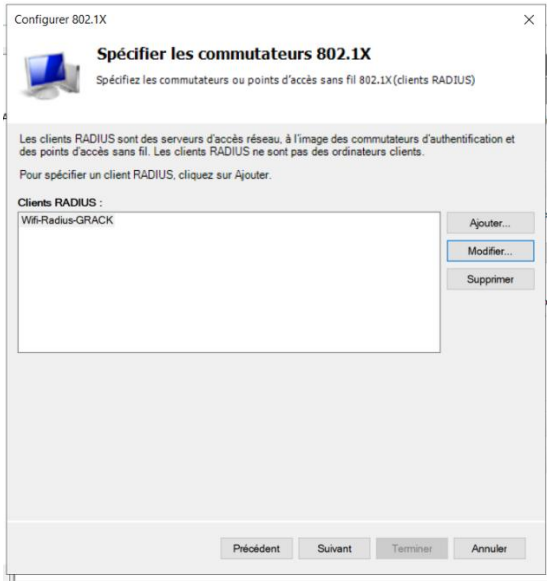
On fait ajouter pour crée notre wifi, puis « Suivant ».



Le nom du wifi sera le ssid partager, l'adresse IP, celui de la borne wifi, et le Secret partagé sera le mot de passe du réseau wifi.

Une fois validé, notre réseau sera sélectionnable.



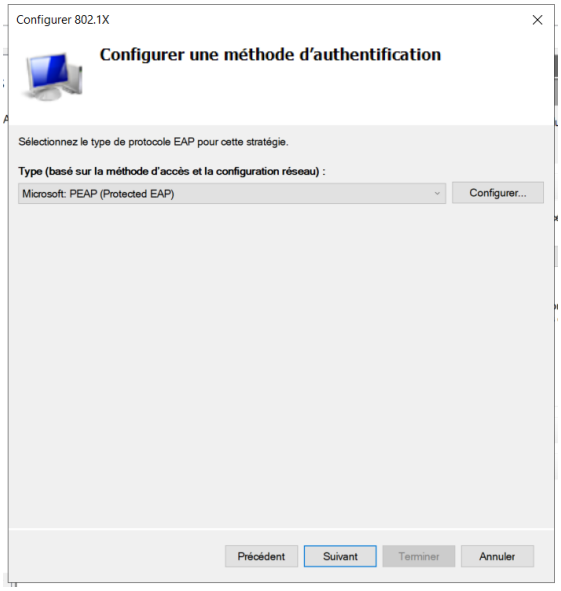


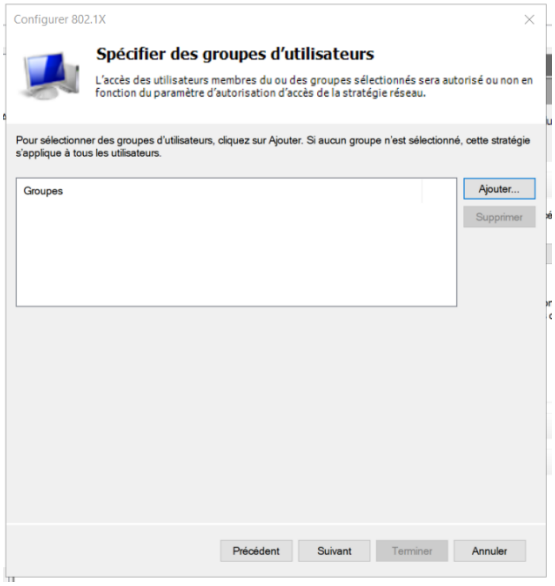
On sélectionne le type Microsoft PEAP.

On ajoute un groupe.

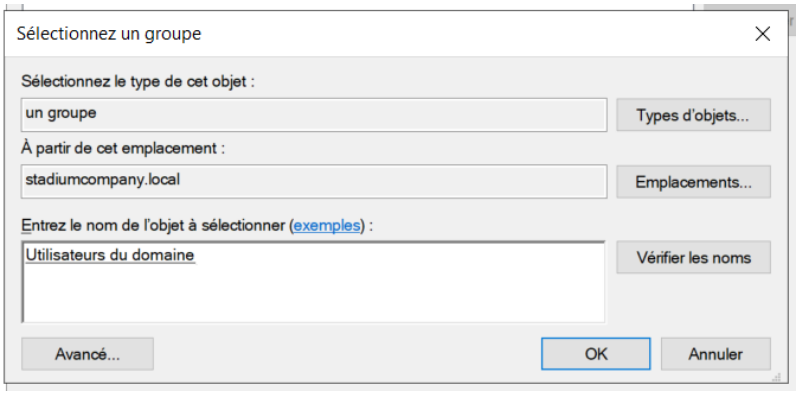
Kevin Roussel
Chloe Houivet
Ajay Muthu Kumar

Ecole IRIS

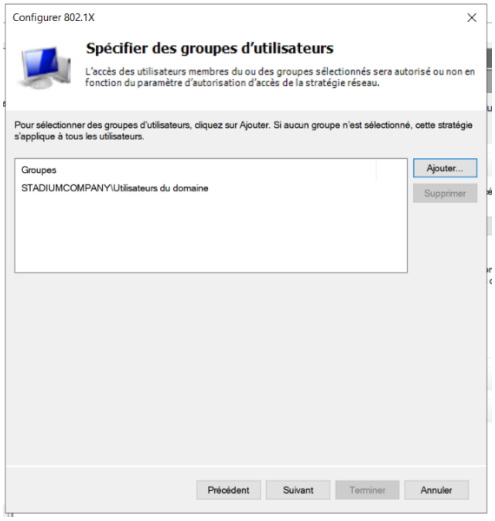




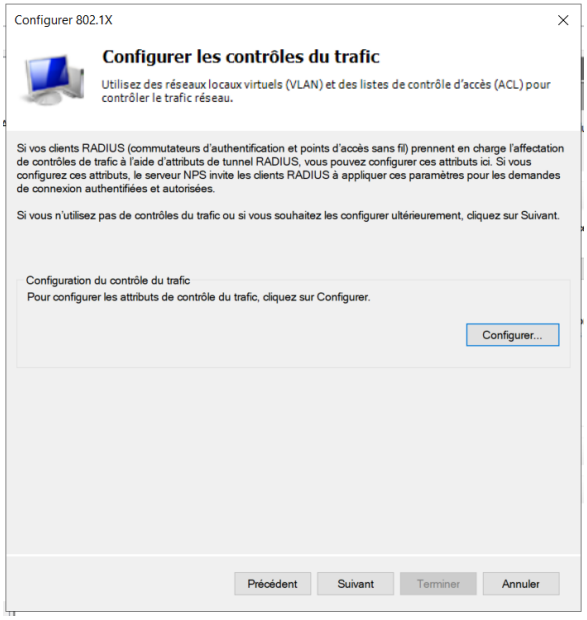
Laisser les informations par défaut, appuyer sur « OK ».



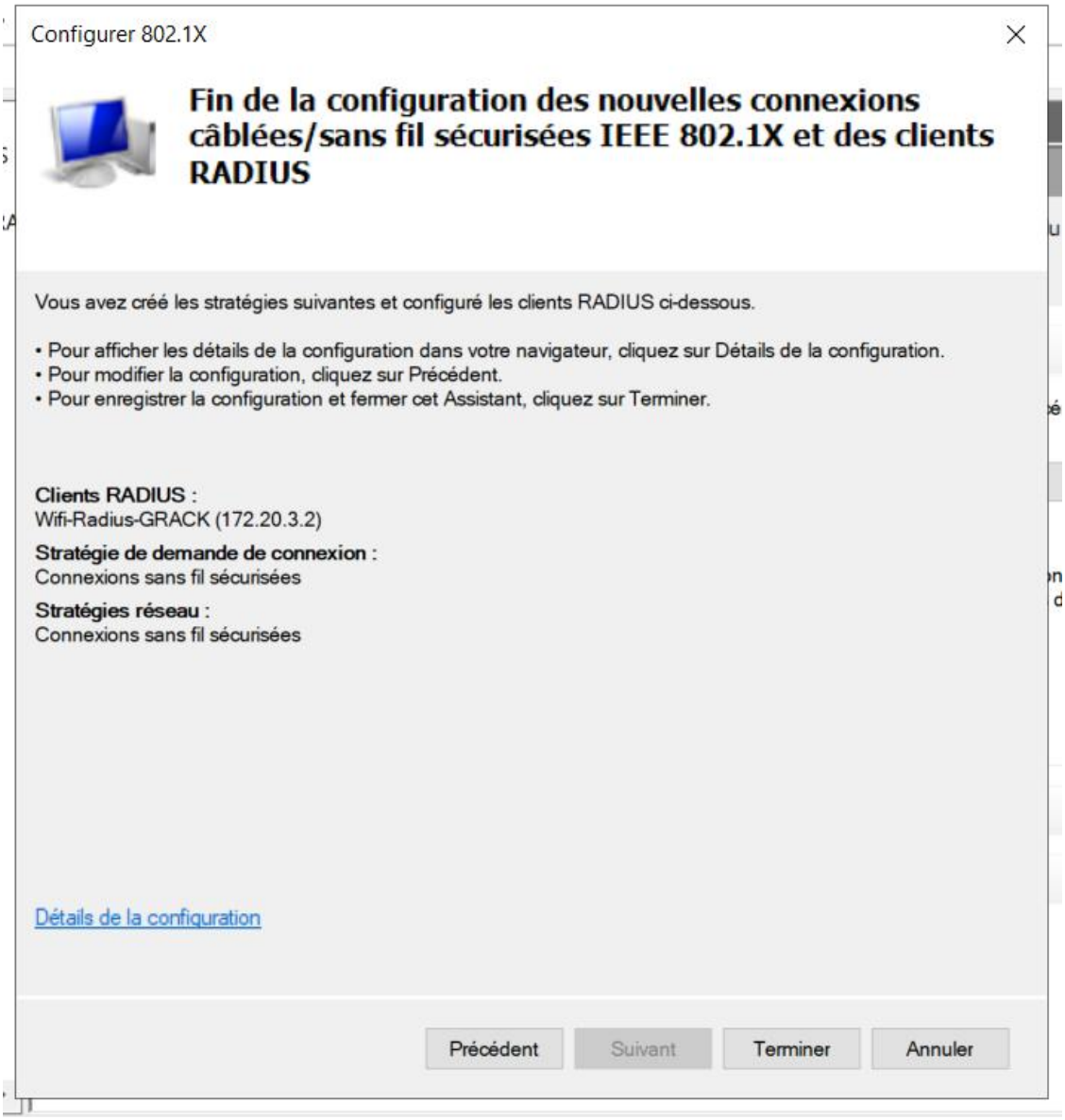
On sélectionne le groupe crée, puis « Suivant ».



On laisse la configuration du contrôle de trafic par défaut, « Suivant ».



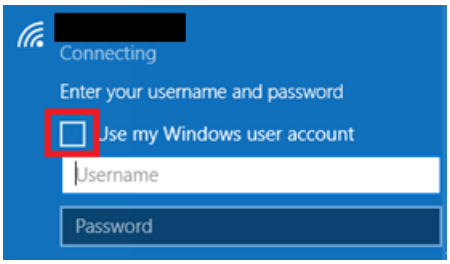
Et c'est fini, la configuration est opérationnelle.



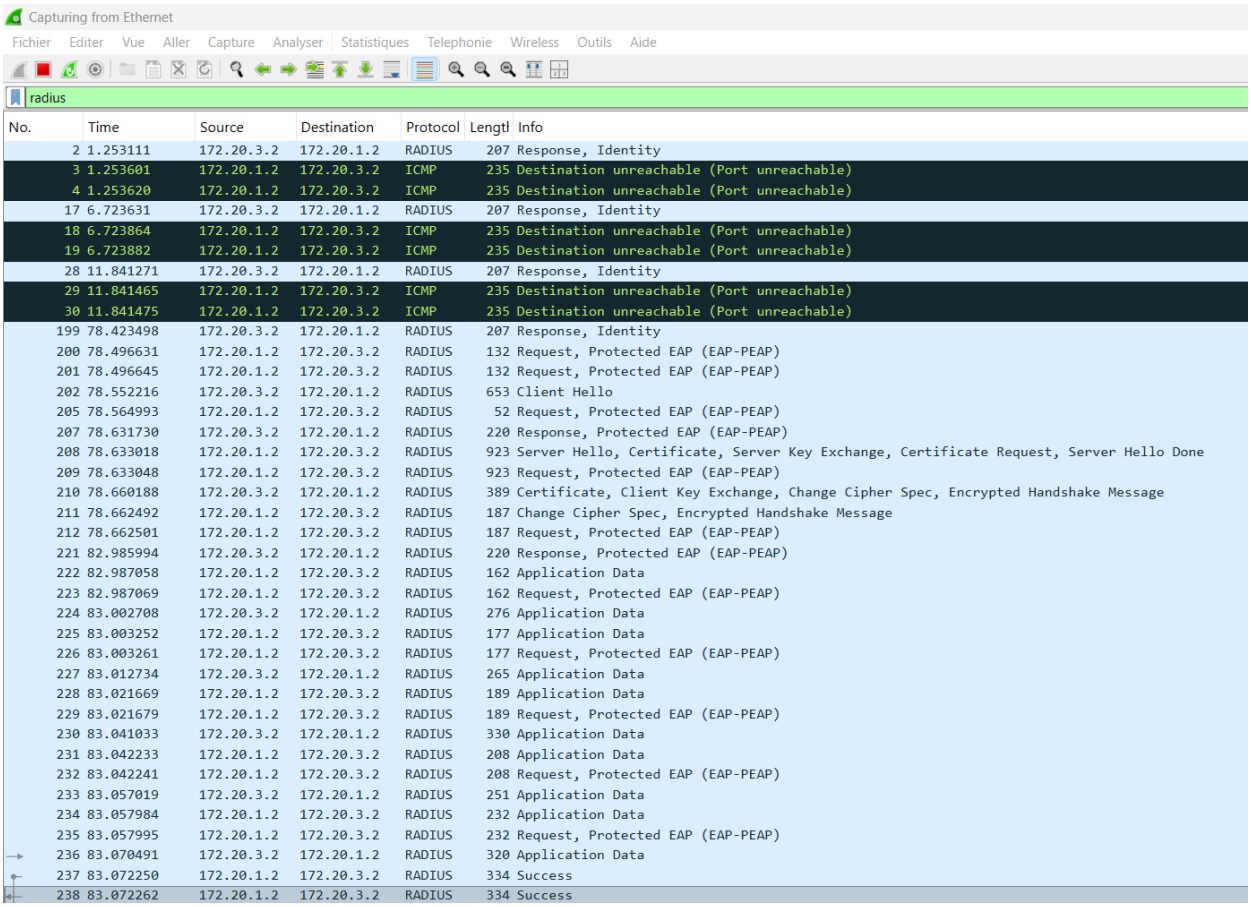
Kevin Roussel
Chloe Houivet
Ajay Muthu Kumar
Ecole IRIS

7. Test

A la fin, se connecter sur Wireshark pour vérifier la connectivité du Wifi.
Désormais, pour se connecter à notre réseau par wifi, le nom d'utilisateur et le mot de passe d'un utilisateur AD sera demander



De plus, on peut constater que des paquets de radius son bien présent sur le réseau via ce screen qui détail la connexion d'un utilisateur sur le réseau



No.	Time	Source	Destination	Protocol	Lengtl	Info
2	1.253111	172.20.3.2	172.20.1.2	RADIUS	207	Response, Identity
3	1.253601	172.20.1.2	172.20.3.2	ICMP	235	Destination unreachable (Port unreachable)
4	1.253620	172.20.1.2	172.20.3.2	ICMP	235	Destination unreachable (Port unreachable)
17	6.723631	172.20.3.2	172.20.1.2	RADIUS	207	Response, Identity
18	6.723864	172.20.1.2	172.20.3.2	ICMP	235	Destination unreachable (Port unreachable)
19	6.723882	172.20.1.2	172.20.3.2	ICMP	235	Destination unreachable (Port unreachable)
28	11.841271	172.20.3.2	172.20.1.2	RADIUS	207	Response, Identity
29	11.841465	172.20.1.2	172.20.3.2	ICMP	235	Destination unreachable (Port unreachable)
30	11.841475	172.20.1.2	172.20.3.2	ICMP	235	Destination unreachable (Port unreachable)
199	78.423498	172.20.3.2	172.20.1.2	RADIUS	207	Response, Identity
200	78.496631	172.20.1.2	172.20.3.2	RADIUS	132	Request, Protected EAP (EAP-PEAP)
201	78.496645	172.20.1.2	172.20.3.2	RADIUS	132	Request, Protected EAP (EAP-PEAP)
202	78.552216	172.20.3.2	172.20.1.2	RADIUS	653	Client Hello
205	78.564993	172.20.1.2	172.20.3.2	RADIUS	52	Request, Protected EAP (EAP-PEAP)
207	78.631730	172.20.3.2	172.20.1.2	RADIUS	220	Response, Protected EAP (EAP-PEAP)
208	78.633018	172.20.1.2	172.20.3.2	RADIUS	923	Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
209	78.633048	172.20.1.2	172.20.3.2	RADIUS	923	Request, Protected EAP (EAP-PEAP)
210	78.660188	172.20.3.2	172.20.1.2	RADIUS	389	Certificate, Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
211	78.662492	172.20.1.2	172.20.3.2	RADIUS	187	Change Cipher Spec, Encrypted Handshake Message
212	78.662501	172.20.1.2	172.20.3.2	RADIUS	187	Request, Protected EAP (EAP-PEAP)
221	82.985994	172.20.3.2	172.20.1.2	RADIUS	220	Response, Protected EAP (EAP-PEAP)
222	82.987058	172.20.1.2	172.20.3.2	RADIUS	162	Application Data
223	82.987069	172.20.1.2	172.20.3.2	RADIUS	162	Request, Protected EAP (EAP-PEAP)
224	83.002708	172.20.3.2	172.20.1.2	RADIUS	276	Application Data
225	83.003252	172.20.1.2	172.20.3.2	RADIUS	177	Application Data
226	83.003261	172.20.1.2	172.20.3.2	RADIUS	177	Request, Protected EAP (EAP-PEAP)
227	83.012734	172.20.3.2	172.20.1.2	RADIUS	265	Application Data
228	83.021669	172.20.1.2	172.20.3.2	RADIUS	189	Application Data
229	83.021679	172.20.1.2	172.20.3.2	RADIUS	189	Request, Protected EAP (EAP-PEAP)
230	83.041033	172.20.3.2	172.20.1.2	RADIUS	330	Application Data
231	83.042233	172.20.1.2	172.20.3.2	RADIUS	208	Application Data
232	83.042241	172.20.1.2	172.20.3.2	RADIUS	208	Request, Protected EAP (EAP-PEAP)
233	83.057019	172.20.3.2	172.20.1.2	RADIUS	251	Application Data
234	83.057984	172.20.1.2	172.20.3.2	RADIUS	232	Application Data
235	83.057995	172.20.1.2	172.20.3.2	RADIUS	232	Request, Protected EAP (EAP-PEAP)
236	83.070491	172.20.3.2	172.20.1.2	RADIUS	320	Application Data
237	83.072250	172.20.1.2	172.20.3.2	RADIUS	334	Success
238	83.072262	172.20.1.2	172.20.3.2	RADIUS	334	Success

ANNEXE

Dossier annexe de configuration wifi cisco

WiFi cours et TP

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



AP(config)#interface dot11Radio 0
AP(config-if)#ssid WiFi-Stade_GRXXXXX
ap(config-if-ssid)#exit
AP(config-if)#encryption mode ciphers aes-ccm tkip
AP(config-if)#no shutdown

AP(config-if)#exit

AP(config)#dot11 ssid WiFi-Stade_GRXXXXX
ap(config-ssid)#authentication open
ap(config-ssid)#guest-mode
ap(config-ssid)#authentication key-management wpa version 2
ap(config-ssid)#wpa-psk ascii Bts2026$
ap(config-ssid)#exit
```