

ASSUR-MER

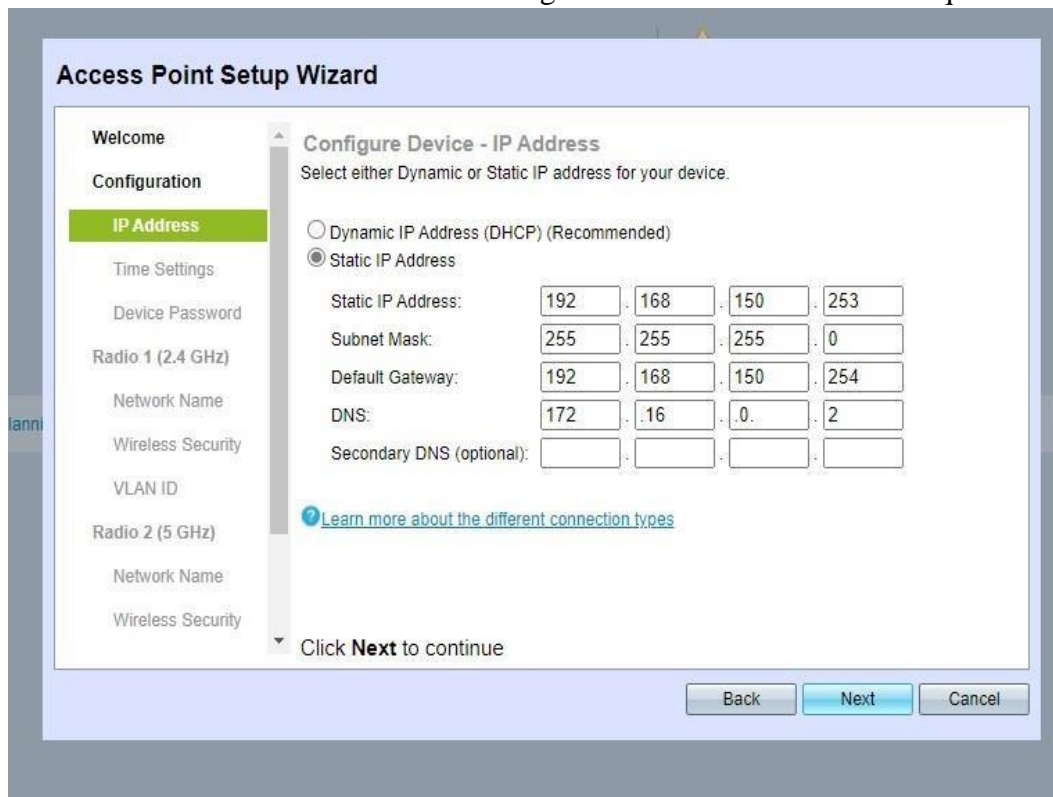
PROCEDURE DE CONFIGURATION DE LA BORNE WIFI ET DU SERVICE RADIUS

Auteur : Ben Hassine Aladin

Date de création : 20/04/2022
Version : 1.2

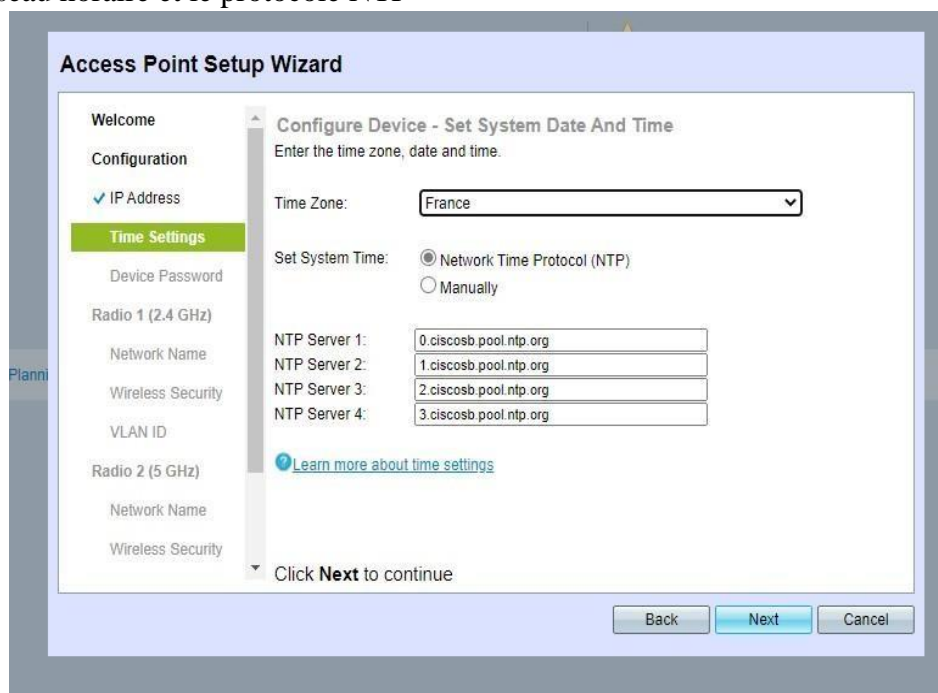
Configuration de la borne Wifi

Un fois sur l'interface Web de la borne il faut configurer la borne avec une IP statique.



The screenshot shows the 'Access Point Setup Wizard' interface. On the left, a sidebar lists configuration steps: Welcome, Configuration, IP Address (highlighted), Time Settings, Device Password, Radio 1 (2.4 GHz), Network Name, Wireless Security, VLAN ID, Radio 2 (5 GHz), Network Name, and Wireless Security. The main panel is titled 'Configure Device - IP Address' and instructs the user to 'Select either Dynamic or Static IP address for your device.' Two radio buttons are present: 'Dynamic IP Address (DHCP) (Recommended)' and 'Static IP Address' (which is selected). Below the radio buttons, there are input fields for 'Static IP Address' (192, 168, 150, 253), 'Subnet Mask' (255, 255, 255, 0), 'Default Gateway' (192, 168, 150, 254), 'DNS' (172, 16, 0, 2), and 'Secondary DNS (optional)'. A link 'Learn more about the different connection types' is visible. At the bottom, there are 'Back', 'Next', and 'Cancel' buttons.

Choisir le fuseau horaire et le protocole NTP



The screenshot shows the 'Access Point Setup Wizard' interface at the 'Set System Date And Time' step. The sidebar is identical to the previous screen, but 'Time Settings' is now highlighted. The main panel is titled 'Configure Device - Set System Date And Time' and instructs the user to 'Enter the time zone, date and time.' There is a 'Time Zone' dropdown menu set to 'France'. Below it, 'Set System Time' has two radio buttons: 'Network Time Protocol (NTP)' (selected) and 'Manually'. Under 'NTP', there are four input fields for 'NTP Server 1' through 'NTP Server 4', all containing the address '0.ciscosb.pool.ntp.org'. A link 'Learn more about time settings' is visible. At the bottom, there are 'Back', 'Next', and 'Cancel' buttons.

Mettre le mot de passe administrateur de la borne.

Access Point Setup Wizard

Welcome

Configuration

- ✓ IP Address
- ✓ Time Settings
- Device Password**

Radio 1 (2.4 GHz)

- Network Name
- Wireless Security
- VLAN ID

Radio 2 (5 GHz)

- Network Name
- Wireless Security

Configure Device - Set Password


The administrative password protects your access point from unauthorized access. For security reasons, you should change the access point password from its default settings. Please write this password down for future reference.

Enter a new device password:

New password needs at least 8 characters composed of lower and upper case letters as well as numbers/symbols by default.

New Password:

Confirm Password:

Password Strength Meter:  Weak

Password Complexity: ☒ Enable

[Learn more about passwords](#)

Click **Next** to continue

Back Next Cancel

Mettre le SSID Administrateur avec sa clé de sécurité

Access Point Setup Wizard

Welcome

Configuration

- ✓ IP Address
- ✓ Time Settings
- ✓ Device Password

Radio 1 (2.4 GHz)

- Network Name**
- Wireless Security
- VLAN ID

Radio 2 (5 GHz)

- Network Name
- Wireless Security

Configure Radio 1 - Name Your Wireless Network

The name of your wireless network, known as an SSID, identifies your network so that wireless devices can find it.

Enter a name for your wireless network:

Network Name (SSID):

For example: MyNetwork

[Learn more about network names](#)

Click **Next** to continue

Back Next Cancel

Access Point Setup Wizard

Welcome

Configuration

- ✓ IP Address
- ✓ Time Settings
- ✓ Device Password
- ✓ Network Name
- Wireless Security**

Radio 1 (2.4 GHz)

- VLAN ID

Radio 2 (5 GHz)

- Network Name
- Wireless Security

Configure Radio 1 - Secure Your Wireless Network

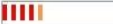
Select your network security strength.

☒ Best Security (WPA2 Personal - AES)
Recommended for new wireless computers and devices that support this option. Older wireless devices might not support this option.

☐ Better Security (WPA/WPA2 Personal - TKIP/AES)
Recommended for older wireless computers and devices that might not support WPA2.

☐ No Security (Not recommended)

Enter a security key with 8-63 characters.

 Weak

☒ Show Key as Clear Text

[Learn more about your network security options](#)

Click **Next** to continue

Back Next Cancel

Entrer le numéro du VLAN administrateur de votre Wifi dans votre réseau

Access Point Setup Wizard

Welcome

Configuration

- ✓ IP Address
- ✓ Time Settings
- ✓ Device Password
- Radio 1 (2.4 GHz)**
- ✓ Network Name
- ✓ Wireless Security
- VLAN ID**
- Radio 2 (5 GHz)
- Network Name
- Wireless Security

Configure Radio 1 - Assign The VLAN ID For Your Wireless Network

By default, the VLAN ID assigned to the management interface for your access point is 1, which is also the default untagged VLAN ID. If the management VLAN ID is the same as the VLAN ID assigned to your wireless network, then the wireless clients associated with this specific wireless network can administer this device. If needed, an access control list (ACL) can be created to disable administration from wireless clients.

Enter a VLAN ID for your wireless network:

VLAN ID: (Range: 1 - 4094)

[Learn more about vlan ids](#)

Click **Next** to continue

Refaire la même chose pour la Radio en 5 GHz.

Il faut ensuite créer les différents SSID que vous voulez.

Non sécurisé | http://192.168.150.252/admin.cgi?action=main

WAP131 Wireless-N Dual Radio Access Point with PoE

- Getting Started
- Run Setup Wizard
- Status and Statistics
- Administration
- LAN
- Wireless**
 - Radio
 - Network
 - Scheduler
 - Scheduler Association
 - Bandwidth Utilization
 - MAC Filtering
 - WDS Bridge
 - WorkGroup Bridge
 - Quality of Service
- System Security
- Quality of Service
- ACL
- SNMP

Select the radio interface first, and then enter the configuration parameters.

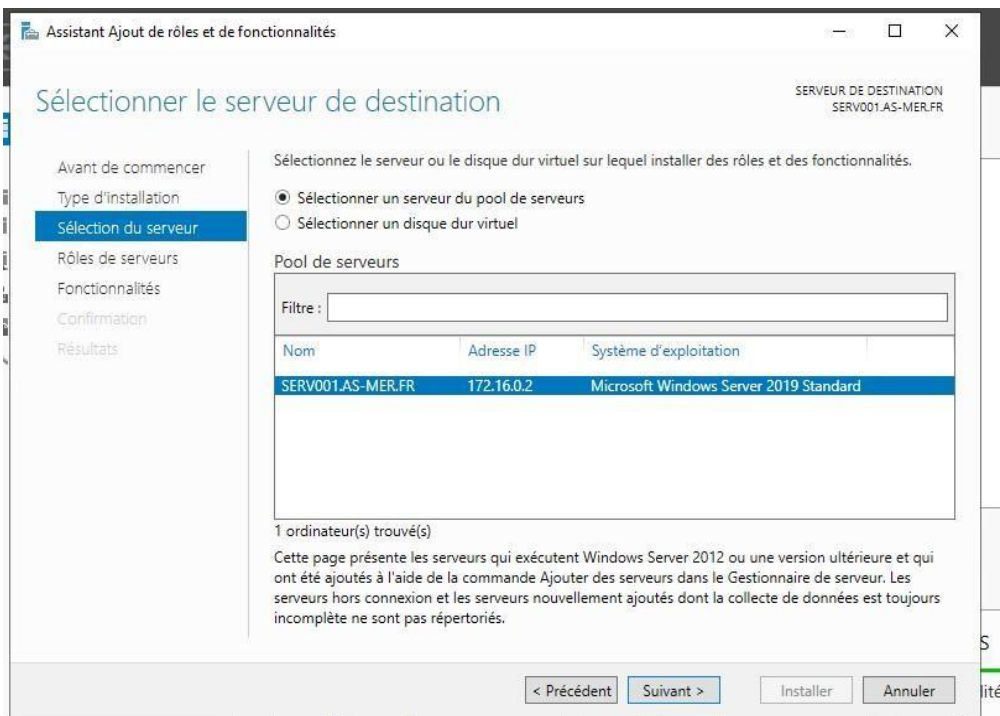
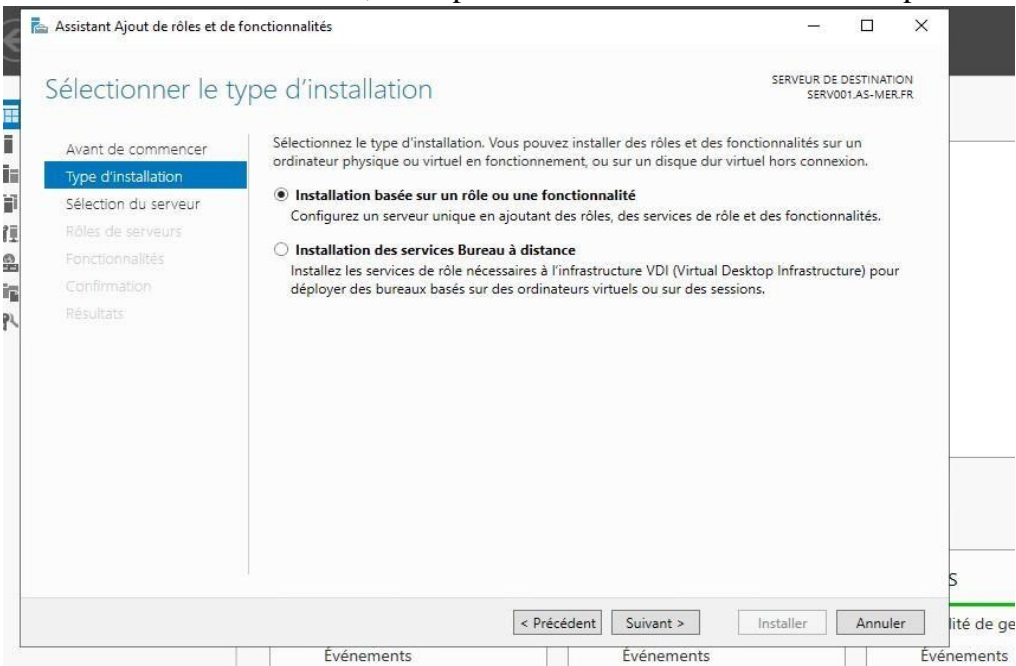
Radio: ☒ Radio 1 (2.4 GHz) ☐ Radio 2 (5 GHz)

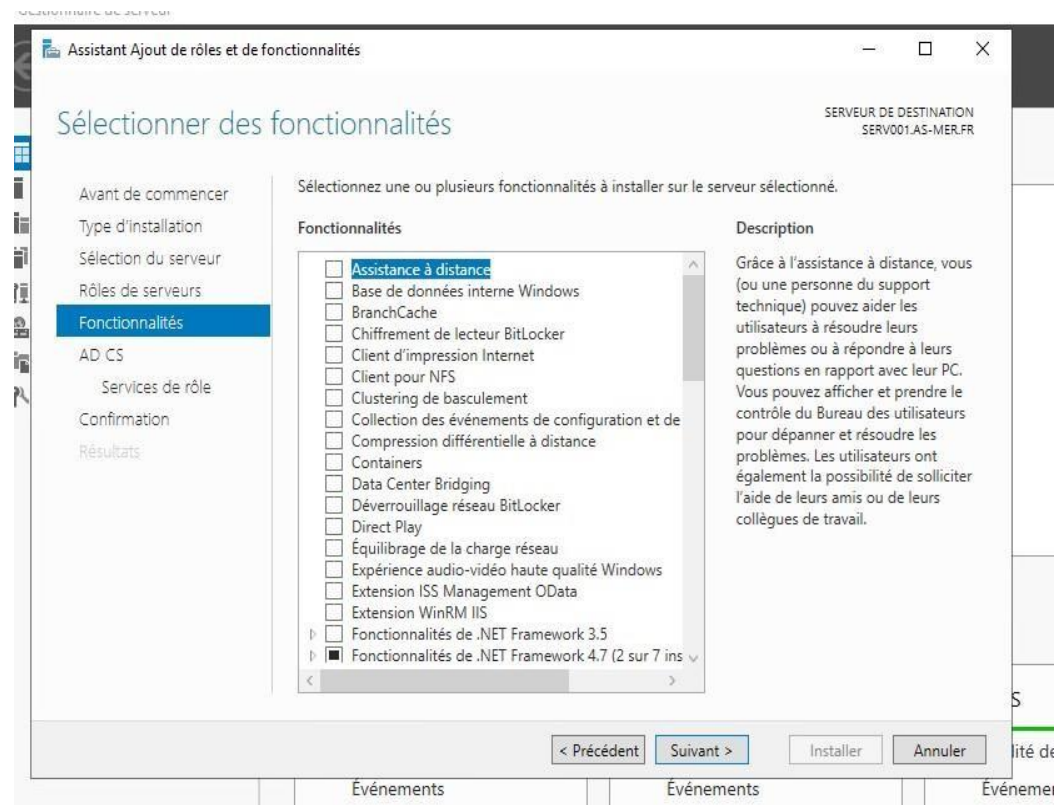
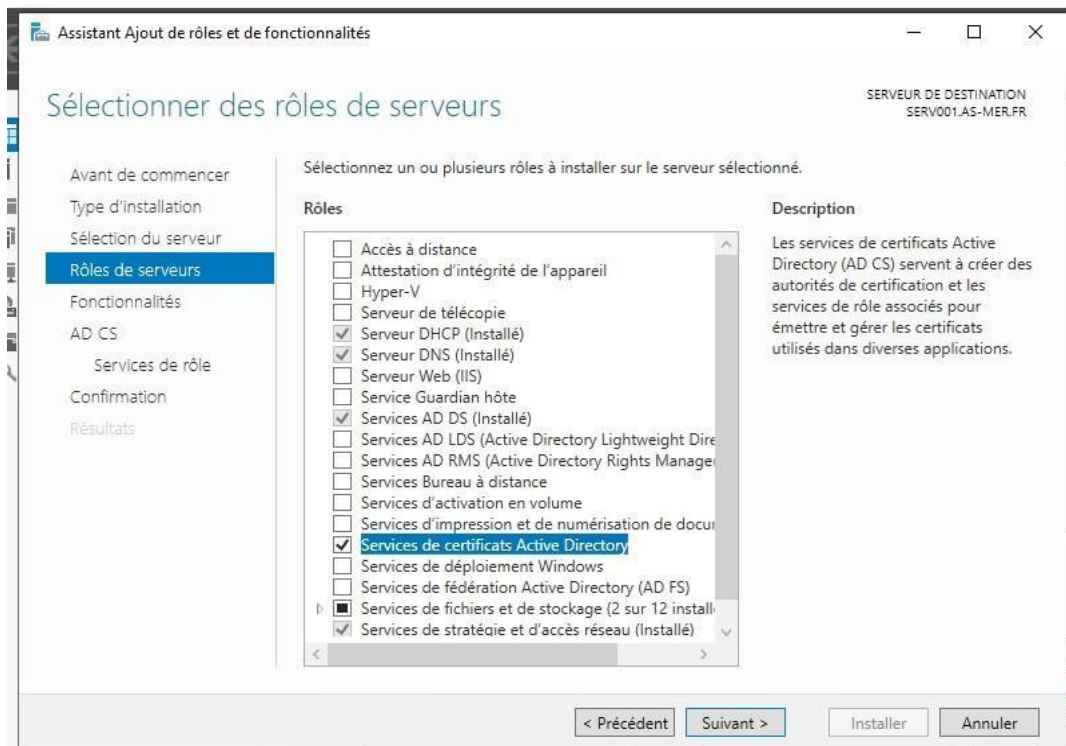
VAP No	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation
<input type="checkbox"/> 0	<input checked="" type="checkbox"/>	150	AdministratAS-MER	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>
<input type="checkbox"/> 1	<input checked="" type="checkbox"/>	19	AdministratAS-MER	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>
<input type="checkbox"/> 2	<input checked="" type="checkbox"/>	29	ComptAS-MER	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>

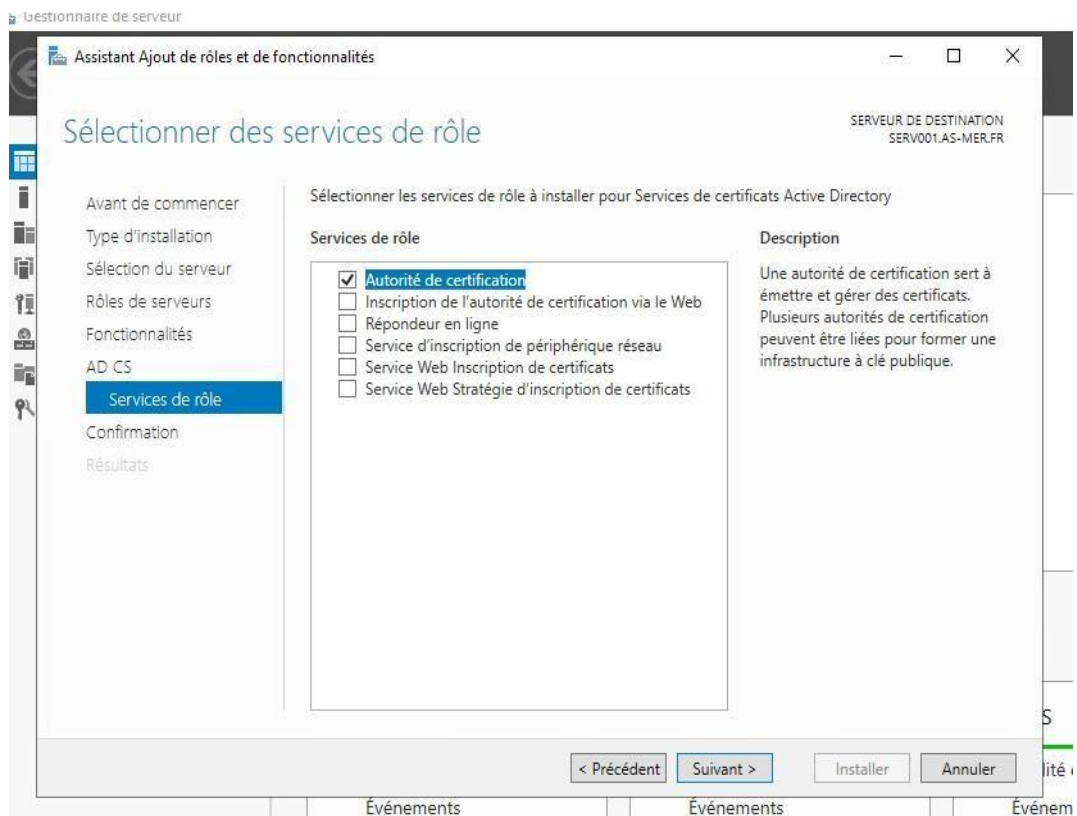
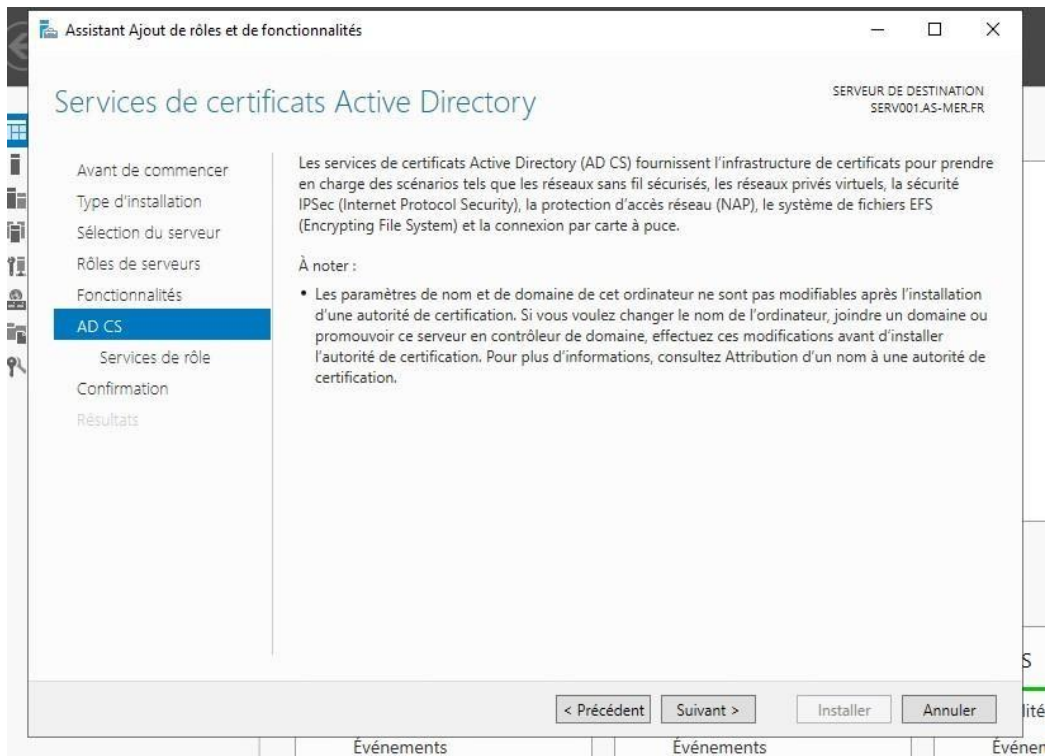
Si vous n'avez pas de service Radius, il faut mettre la sécurité WPA Personnel et rentrer la clé de sécurité de chaque SSID.

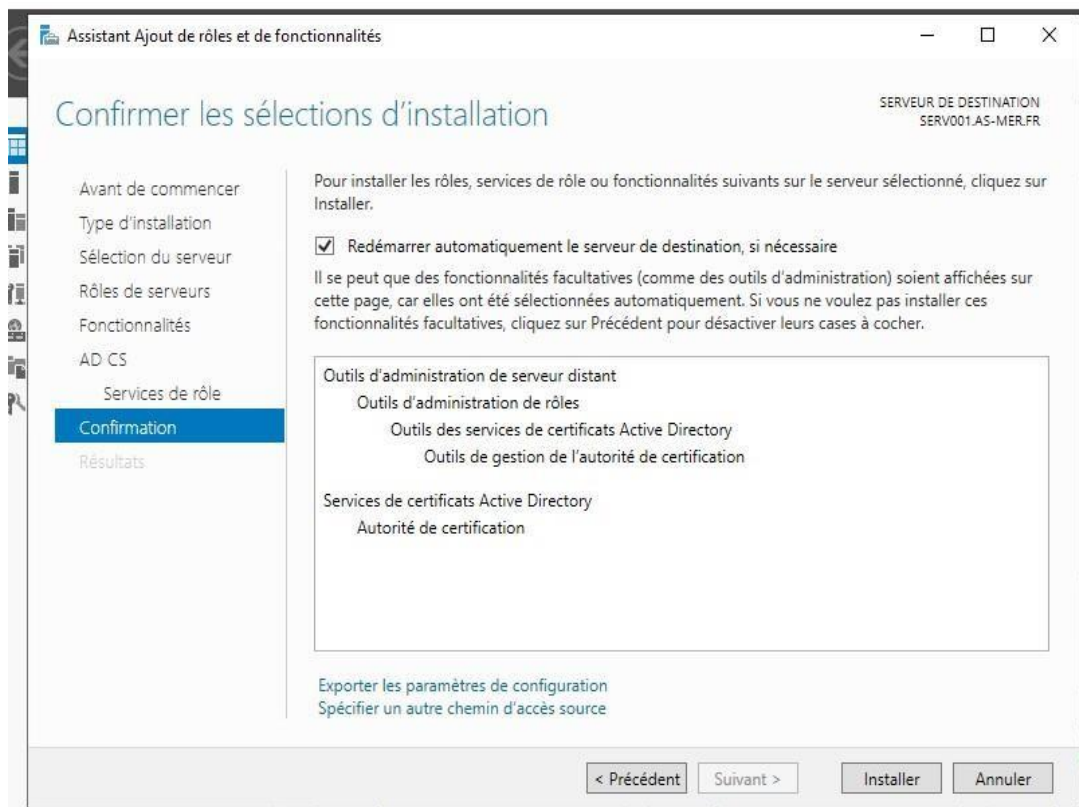
Configuration du Service Radius

Il faut installer le service sur le serveur, les captures d'écrans vous montrerons le processus.

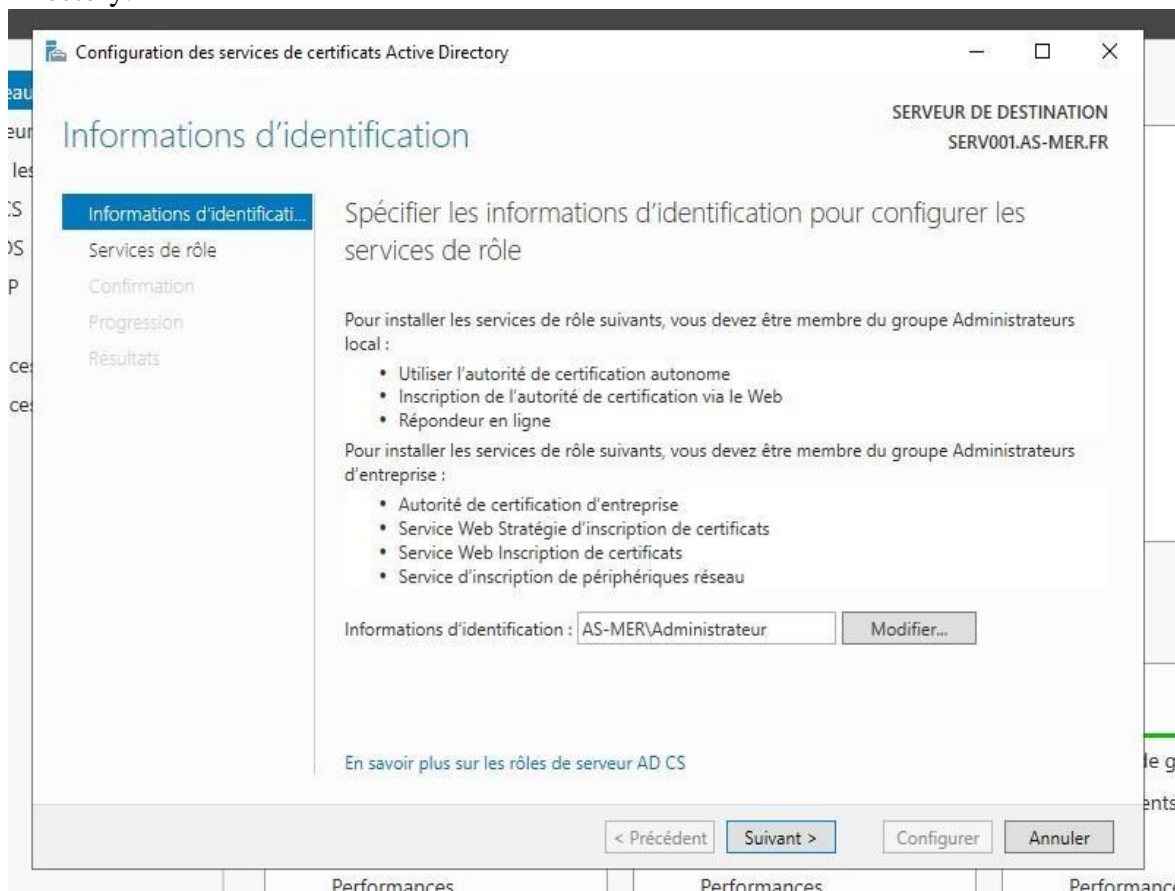


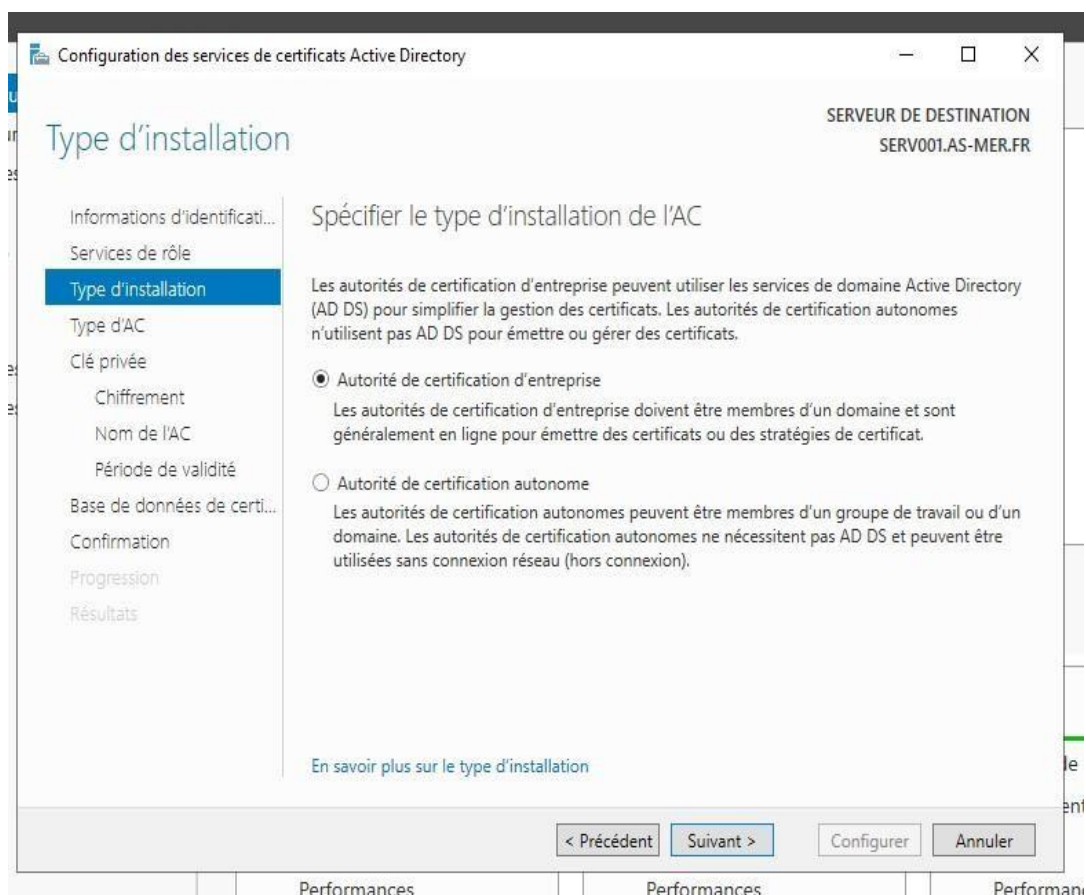
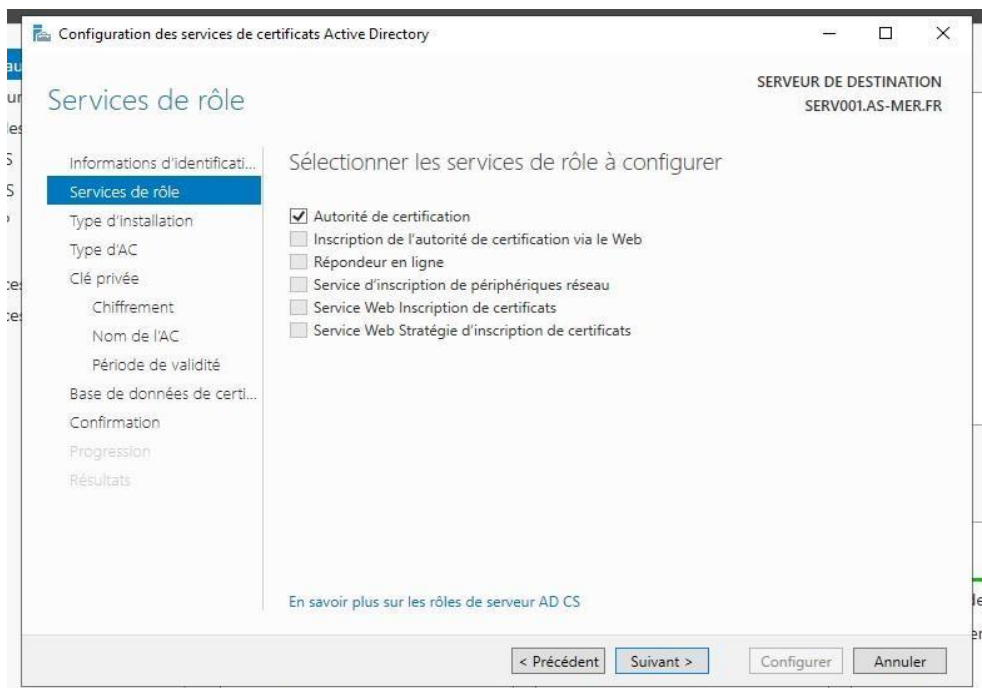






Après installation et redémarrage du service, il faut configurer les service de certificats Active Directory.





Configuration des services de certificats Active Directory

TYPE D'AUTORITÉ DE CERTIFICATION

SERVEUR DE DESTINATION
SERV001.AS-MER.FR

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

Spécifier le type de l'AC

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

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

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

[En savoir plus sur le type d'autorité de certification](#)

< Précédent Suivant > Configurer Annuler

Configuration des services de certificats Active Directory

CLÉ PRIVÉE

SERVEUR DE DESTINATION
SERV001.AS-MER.FR

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

Spécifier le type de la clé privée

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

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

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

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

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

[En savoir plus sur la clé privée](#)

< Précédent Suivant > Configurer Annuler

Configuration des services de certificats Active Directory

SERVEUR DE DESTINATION
SERV001.AS-MER.FR

Chiffrement pour 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 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

Configuration des services de certificats Active Directory

SERVEUR DE DESTINATION
SERV001.AS-MER.FR

Nom 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 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 :
AS-MER-SERV001-CA-1

Suffixe du nom unique :
DC=AS-MER,DC=FR

Aperçu du nom unique :
CN=AS-MER-SERV001-CA-1,DC=AS-MER,DC=FR

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

< Précédent Suivant > Configurer Annuler

Configuration des services de certificats Active Directory

PERIODE DE VALIDITE

SERVER DE DESTINATION
SERV001.AS-MER.FR

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

Spécifier la période de validité

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

5 Années

Date d'expiration de l'AC : 10/05/2027 12:44:00

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

Configuration des services de certificats Active Directory

BASE DE DONNEES DE L'AUTORITE DE CERTIFICATION

SERVER DE DESTINATION
SERV001.AS-MER.FR

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

Spécifier les emplacements des bases de données

Emplacement de la base de données de certificats :

C:\Windows\system32\CertLog

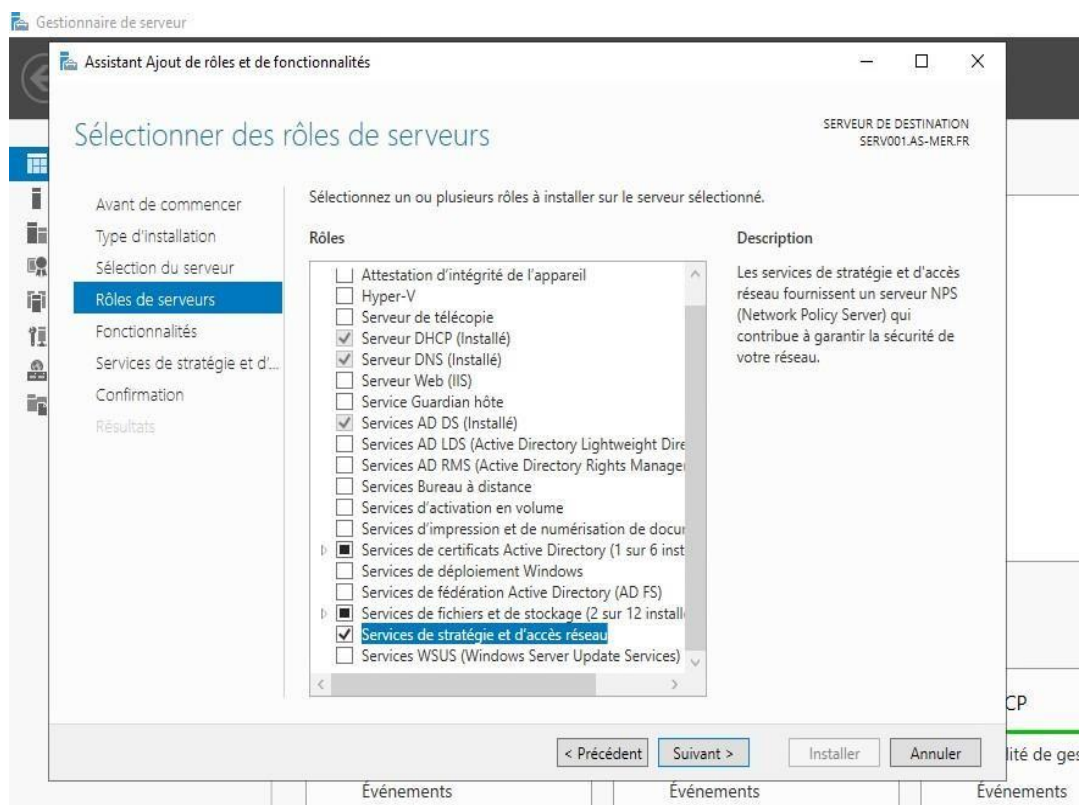
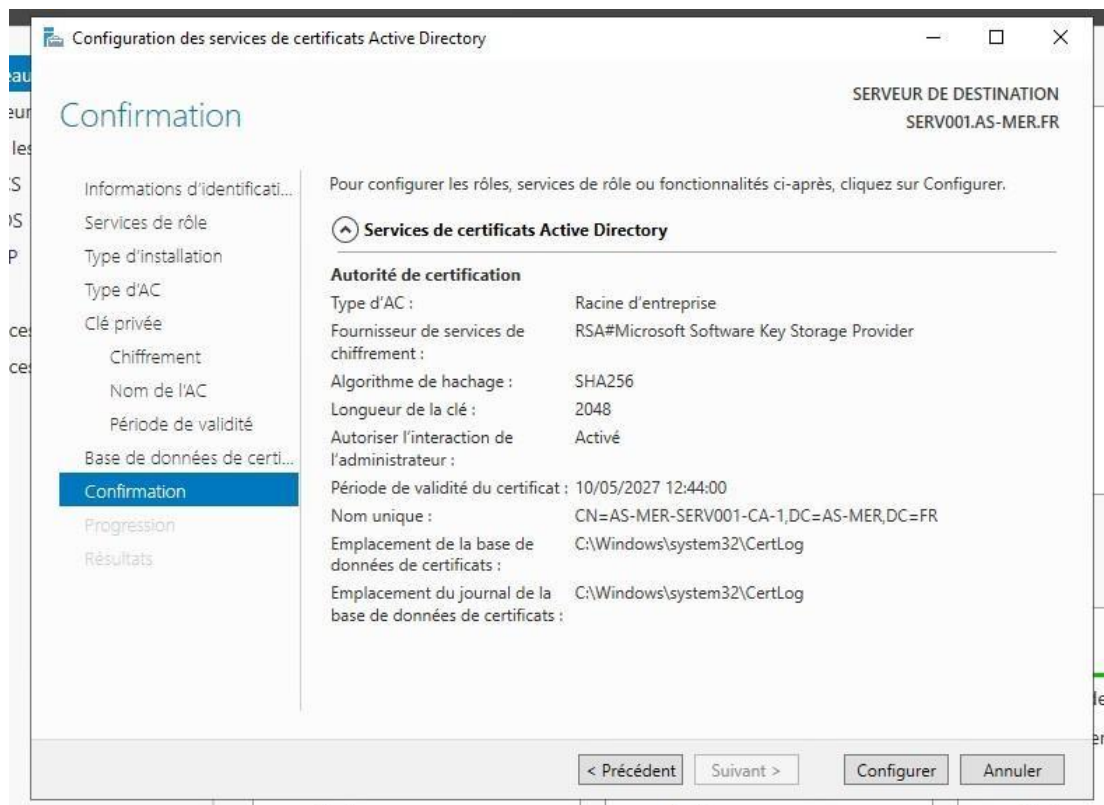
Emplacement du journal de la base de données de certificats :

C:\Windows\system32\CertLog

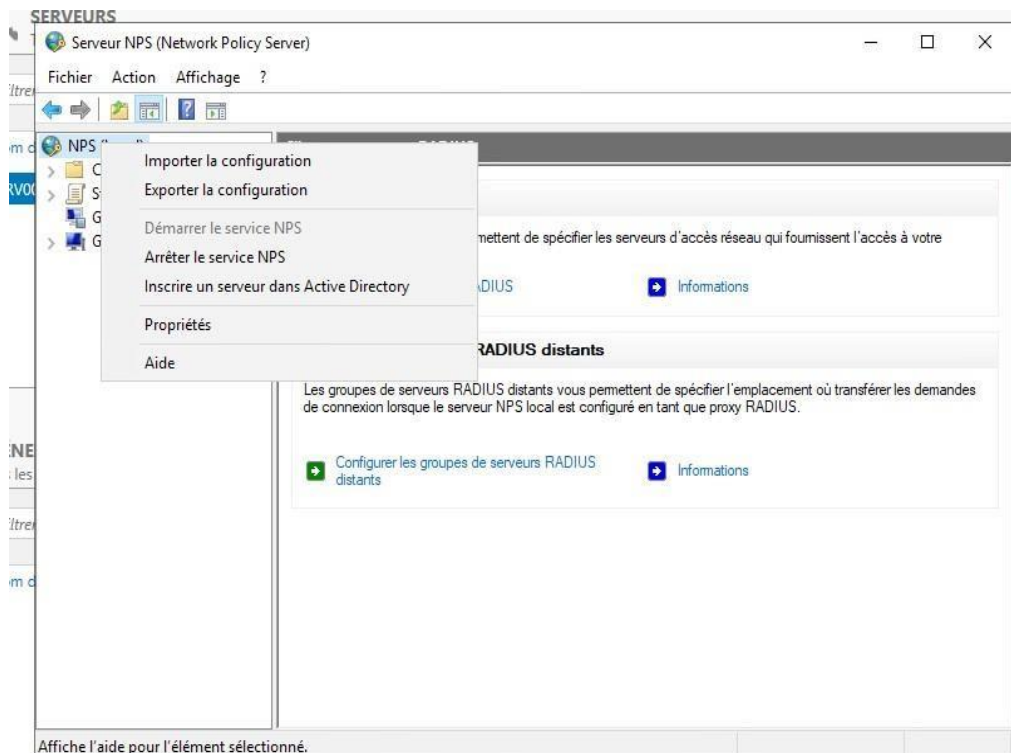
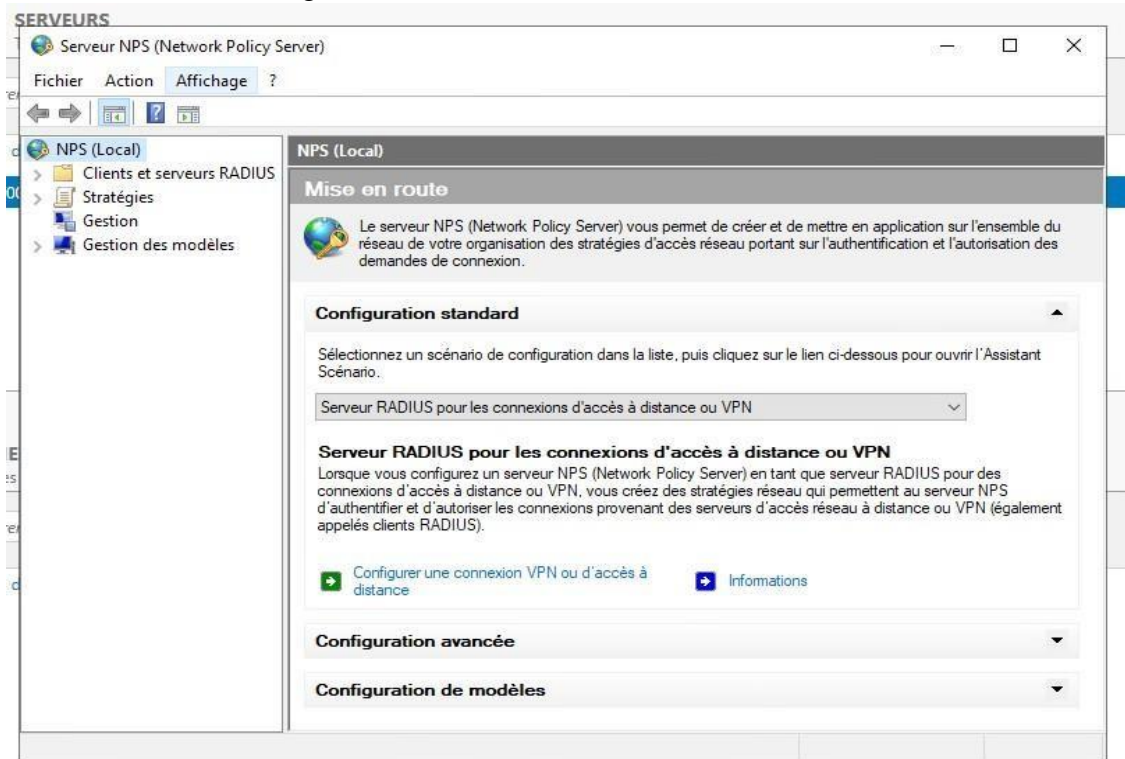
[En savoir plus sur la base de données de l'autorité de certification](#)

< Précédent Suivant > Configurer Annuler

Performances



Passons maintenant à la configuration du service NPS



Nouveau client RADIUS

Paramètres Avancé

☒ Activer ce client RADIUS

☐ Sélectionner un modèle existant :

BorneWifi

Nom et adresse

Nom convivial :

Adresse (IP ou DNS) :

Vérifier...

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 :

OK Annuler

SERVEURS

Serveur NPS (Network Policy Server)

Fichier Action Affichage ?

NPS (Local)

- Clients et serveurs RADIUS
 - Clients RADIUS
 - Groupes de serveurs RA
- Stratégies
 - Stratégies de demande
 - Stratégies réseau
- Gestion
 - Gestion des modèles
 - Secrets partagés
 - Clients RADIUS
 - Serveurs RADIUS distan
 - Filtres IP

Stratégies réseau

Les stratégies réseau vous permettent d'autoriser les connexions au réseau de manière sélective, et d'indiquer les circonstances dans lesquelles ces connexions peuvent s'effectuer ou non.

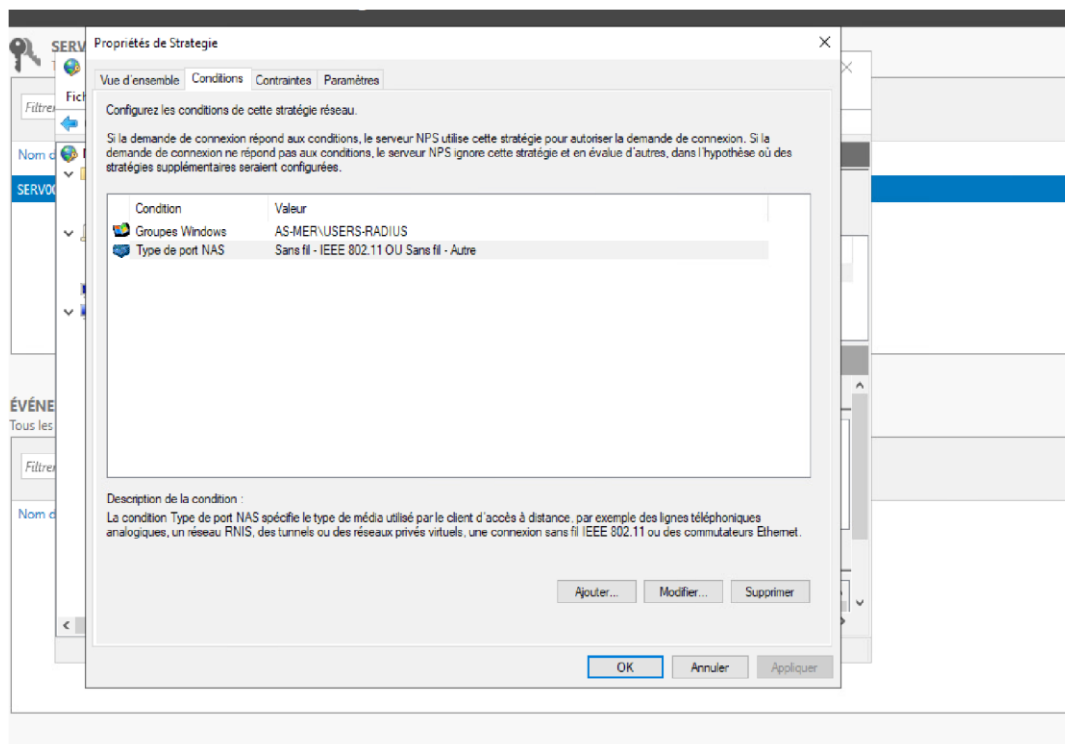
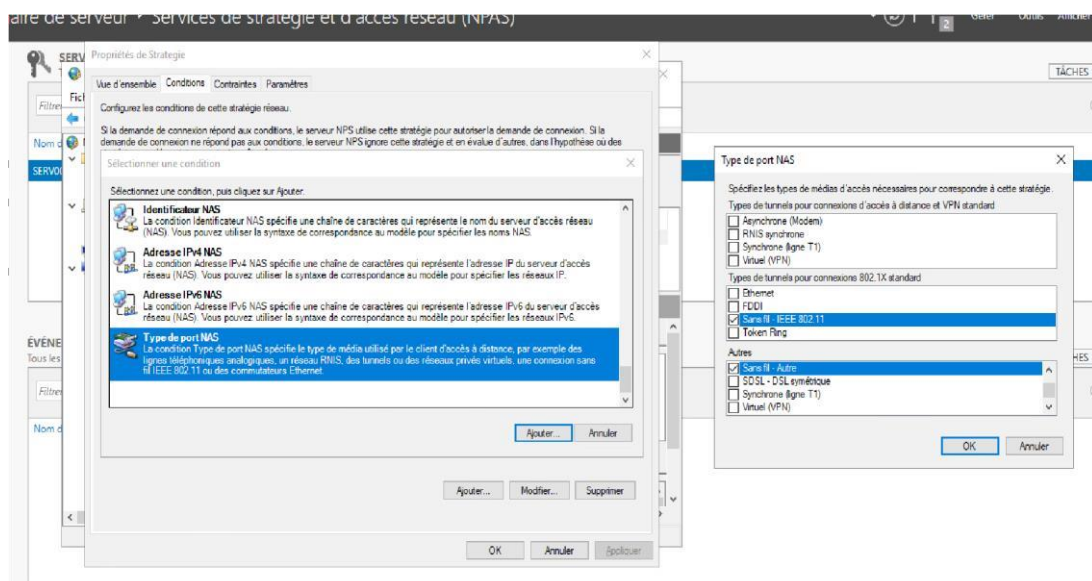
Nom de la stratégie	État	Ordre de traitement	Type d'accès	Source
Strategie	Activé	1	Accorder l'accès	Non spécifié

Conditions - Si les conditions suivantes sont réunies :

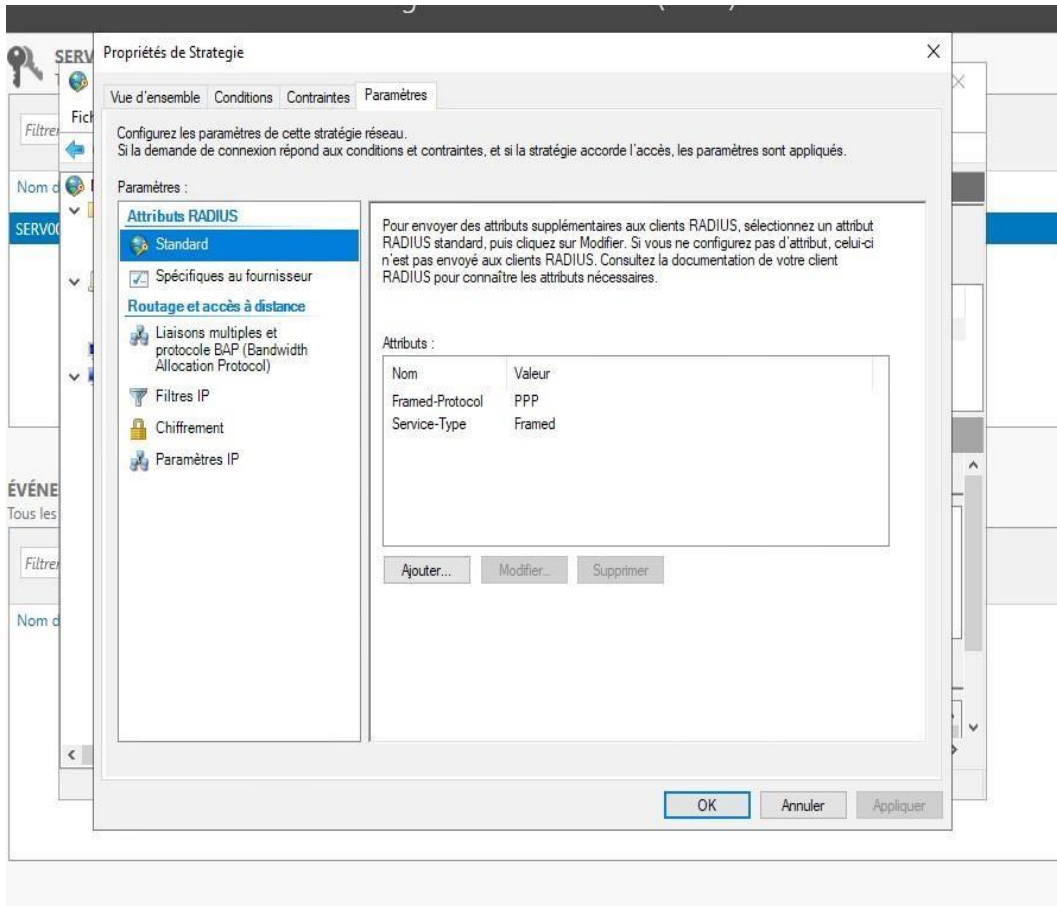
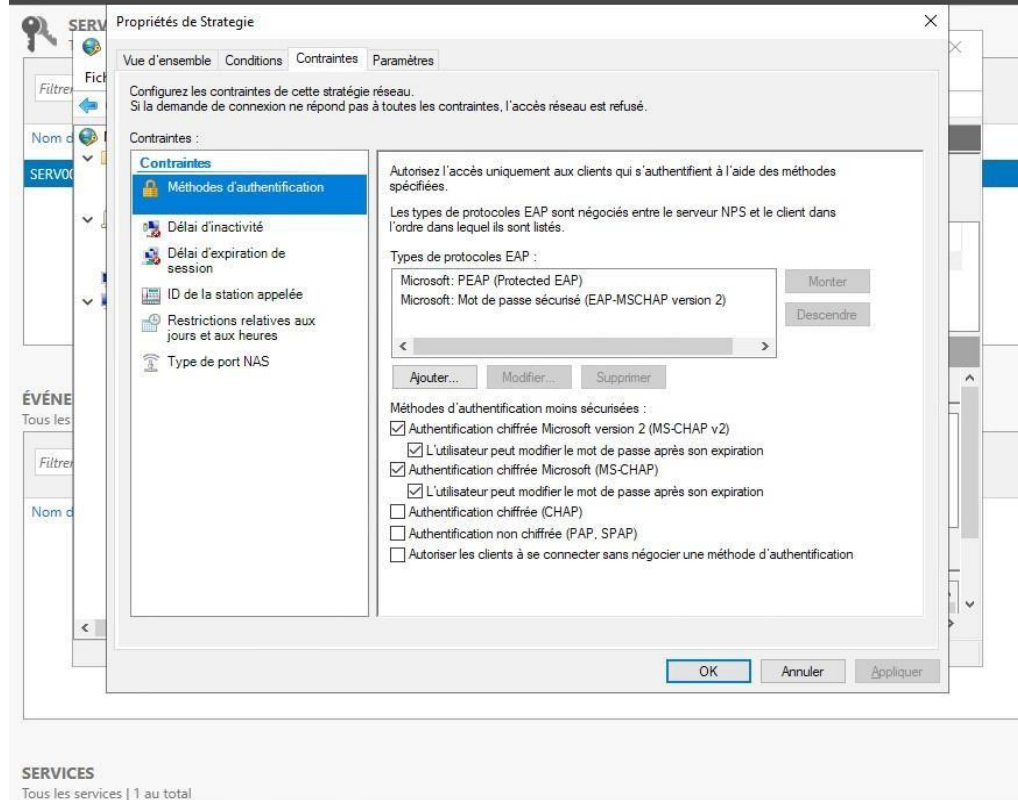
Condition	Valeur

Paramètres - Les paramètres suivants sont appliqués :

Paramètre	Valeur



Centre de serveur ▸ Services de stratégie et d'accès réseau (NPAS)



Un fois la configuration du service Radius terminée, il faut modifier la sécurité sur les SSID.

1 10 Administrat@AS-MER WPA Enterprise Disabled

Hide Details

WPA Versions: ☒ WPA-TKIP ☒ WPA2-AES
☒ Enable pre-authentication
☐ Use global RADIUS server settings

Server IP Address Type: ☒ IPv4 ☐ IPv6

Server IP Address-1: 172.16.0.2 (xxx.xxx.xxx.xxx)
Server IP Address-2: (xxx.xxx.xxx.xxx)
Server IP Address-3: (xxx.xxx.xxx.xxx)
Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)
Key-2: (Range: 1-64 Characters)
Key-3: (Range: 1-64 Characters)
Key-4: (Range: 1-64 Characters)

☒ Enable RADIUS Accounting
Active Server: Server IP Address-1
Broadcast Key Refresh Rate: 300 Sec (Range: 0-86400, 0 = Disable, Default: 300)
Session Key Refresh Rate: 0 Sec (Range: 30-86400, 0 = Disable, Default: 0)

Virtual Access Points (SSIDs)								
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	
<input type="checkbox"/> 0	<input checked="" type="checkbox"/>	150	Administrat@AS-MER	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>	
Show Details								
<input type="checkbox"/> 1	<input checked="" type="checkbox"/>	10	Administrat@AS-MER	<input checked="" type="checkbox"/>	WPA Enterprise	Disabled	<input type="checkbox"/>	
Show Details								
<input type="checkbox"/> 2	<input checked="" type="checkbox"/>	20	Compla@AS-MER	<input checked="" type="checkbox"/>	WPA Enterprise	Disabled	<input type="checkbox"/>	
Show Details								

RADIUS Server

Server IP Address Type: ☒ IPv4 ☐ IPv6

No.	Server IP Address (xxx.xxx.xxx.xxx)	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)
1	172.16.0.2	*****	1812
2			1812
3			1812
4			1812

☒ Enable RADIUS Accounting