# 

# 

# 

# 

# 

# **Compte rendu : Configuration du serveur Windows Server 2016/2019**

**Tables des matières :**

[**Compte rendu : Configuration du serveur Windows Server 2016/2019 1**](#_j9dl7whrnj94)

[1. Configuration de l’adresse IP statique 4](#_vaq926c7t7fz)

[Étapes détaillées : 4](#_b5bk2kac7yc4)

[2. Installation des rôles DHCP et DNS 5](#_t5jg5j4m9mxw)

[3. Configuration du service DHCP 6](#_dayl3neo4zzl)

[3. Configuration du service DNS 7](#_gxd8m8bspjzb)

[1. Ouvrir DNS Manager 7](#_wccvm271zu9m)

[2. Création d'une zone principale 7](#_vyno0i5sg7zz)

[3. Ajouter des enregistrements DNS 7](#_ru85ya85hljp)

[a. Ajouter un enregistrement A pour le mail : 7](#_hd418j9f422m)

[b. Ajouter un enregistrement A pour le proxy : 8](#_g6yvn5jkus8j)

[c. Ajouter un enregistrement MX : 8](#_hvjildh8kggb)

[4. Tester la configuration DNS 8](#_9pmmjvot6ncf)

[a. Tester l’enregistrement A du mail : 8](#_n6bgyns9rq1t)

[b. Tester l’enregistrement A du proxy : 9](#_go8kbcg3eds7)

[c. Tester l’enregistrement MX : 9](#_nt8rcb8r6z4x)

[6. Configurer le DNS Forwarding 9](#_lvkudhz9c5i6)

[Résumé de la configuration 10](#_bacxut94ztum)

[4.Configuration d’un serveur proxy 10](#_5yjsl7jr0c89)

[1. Installation de Squid 10](#_cjko4yy76fzr)

[2. Configuration de Squid 11](#_3dpvq37bdbao)

[3. Configuration du service Squid 12](#_d1hi4n4y912o)

[4. Configuration des clients pour utiliser le proxy 12](#_8rfr4dk0ss1s)

[5. Ajout des DNS et ajustement des plages IP 13](#_kg0unuo8454g)

[6. Résolution des problèmes fréquents 13](#_8lxxbp3t9o6t)

[7. Logs et maintenance 14](#_qongr14e39qy)

[8. Redémarrage et tests 14](#_hs46bumsbstx)

[Résumé des points clés 15](#_gh28ru2b96rh)

[5. Configuration du service Mail avec MailEnable 15](#_7l21152iffte)

[Étape 1 : Téléchargement et installation de MailEnable 15](#_viqir6w3dts4)

[Étape 2 : Création des boîtes aux lettres 16](#_h775woljw3xe)

[Étape 3 : Configuration du Webmail dans IIS 17](#_dgvj389yl5y5)

[Étape 4 : Tester le Webmail 18](#_dnyw6cmrxy5p)

[Étape 5 : Configurer un client de messagerie 18](#_psh2t6or6k)

[6. Configuration du serveur RADIUS avec spécification des IP/DNS 19](#_uchyt8a8jdch)

[Étape 1 : Ajouter le rôle NPS (Network Policy Server) 19](#_ylich71lyet4)

[Étape 2 : Configurer le serveur NPS comme un serveur RADIUS 20](#_8fjwts5xcidd)

[Étape 3 : Ajouter des clients RADIUS (par exemple, des points d’accès Wi-Fi) 20](#_fmy0jbkx496a)

[Étape 4 : Configurer les stratégies réseau (Network Policies) 21](#_y8c0clabntaa)

[Étape 5 : Configurer les clients (par exemple, les points d’accès Wi-Fi) 22](#_66twxwal1h7j)

[Étape 6 : Vérifications et tests 22](#_z2q4rd2v6g33)

[7. Active Directory interconnectés : 23](#_c70fzzfigy87)

[1. Configuration du premier serveur AD (172.31.10.10) 23](#_srhf7jtvrcsb)

[Étape 1 : Installer Active Directory Domain Services (AD DS) 23](#_pb51khxzxvgl)

[Étape 2 : Promouvoir le serveur en tant que contrôleur de domaine principal (PDC) 23](#_pb45v8rdrogv)

[2. Configuration du second serveur AD (172.31.10.20) 24](#_duj8gfmd84k0)

[Étape 1 : Préparer le serveur 24](#_wveei4l8g8sp)

[Étape 2 : Installer Active Directory Domain Services (AD DS) 25](#_ywxbfrji4pmb)

[Étape 3 : Promouvoir le serveur en contrôleur de domaine secondaire (ADC) 25](#_3zzpqtn85roa)

[3. Vérifications et tests 26](#_57kfbbrxpm6)

Ce guide explique la configuration d’un serveur Windows Server 2016 pour fournir des services essentiels : DHCP, DNS, Mail (via MailEnable) et Proxy (via IIS et Application Request Routing - ARR). Il est conçu pour que même une personne débutante puisse suivre les étapes sans difficulté.

## 1. Configuration de l’adresse IP statique

### Étapes détaillées :

1. Ouvrir les paramètres réseau :
   * Cliquez sur Démarrer (icône Windows en bas à gauche).
   * Sélectionnez Panneau de configuration.
   * Dans le Panneau de configuration, cliquez sur Réseau et Internet.
   * Cliquez sur Centre Réseau et partage.
   * Dans le menu de gauche, cliquez sur Modifier les paramètres de la carte.
2. Configurer l’IP statique :
   * Identifiez votre adaptateur réseau actif (Ethernet, par exemple).
   * Faites un clic droit sur l’adaptateur réseau actif, puis cliquez sur Propriétés.
   * Dans la liste des éléments, double-cliquez sur Protocole Internet version 4 (TCP/IPv4).
   * Dans la fenêtre Propriétés de Protocole Internet version 4 (TCP/IPv4) :
     + Cochez Utiliser l’adresse IP suivante.
     + Entrez les informations suivantes :
       - Adresse IP : 172.31.10.10
       - Masque de sous-réseau : 255.255.255.0
       - Passerelle par défaut : 172.31.10.1
     + Cochez Utiliser les serveurs DNS suivants et entrez :
       - Serveur DNS préféré : 127.0.0.1 (cela pointe vers votre serveur DNS local).
3. Ajouter des adresses IP secondaires :
   * Toujours dans la fenêtre Propriétés TCP/IPv4, cliquez sur Avancé....
   * Sous l’onglet Paramètres IP, dans la section Adresses IP, cliquez sur Ajouter.
     + Entrez :
       - Adresse IP : 172.31.10.11
       - Masque de sous-réseau : 255.255.255.0
     + Cliquez sur Ajouter.
   * Répétez l’opération pour ajouter :
     + Adresse IP : 172.31.10.12
     + Masque de sous-réseau : 255.255.255.0.

Répétez l’opération pour ajouter :

* + - Adresse IP : 172.31.10.13
    - Masque de sous-réseau : 255.255.255.0.
  + Cliquez sur OK dans toutes les fenêtres pour valider.

## 2. Installation des rôles DHCP et DNS

1. Ouvrir le Gestionnaire de serveur :
   * Cliquez sur Démarrer > Gestionnaire de serveur.
2. Ajouter les rôles :
   * Cliquez sur Gérer > Ajouter des rôles et fonctionnalités.
   * Sélectionnez Installation basée sur un rôle ou une fonctionnalité et cliquez sur Suivant.
   * Cochez les rôles suivants :
     + Serveur DHCP
     + Serveur DNS
   * Cliquez sur Suivant, puis sur Installer.
3. Redémarrer le serveur si demandé :
   * Si l’installation vous demande de redémarrer le serveur, cliquez sur Oui et attendez qu’il redémarre.

### 3. Configuration du service DHCP

1. Ouvrir l’outil DHCP :
   * Dans le Gestionnaire de serveur, cliquez sur Outils > DHCP.
   * La console Gestion DHCP s’ouvre.
2. Créer une étendue pour chaque VLAN :
   * Faites un clic droit sur IPv4 > Nouvelle étendue....
   * L’assistant Nouvelle étendue s’ouvre.
   * Suivez les étapes pour configurer chaque VLAN. Voici un exemple pour le VLAN Admin (VLAN 10) :
     + Nom de l’étendue : VLAN 10 - Admin.
     + Plage d’adresses IP :
       - Début : 172.31.10.100
       - Fin : 172.31.10.200
     + Masque de sous-réseau : 255.255.255.0.
     + Passerelle : 172.31.10.1.
     + Domaine parent : societe7.pepiniere.rt
     + Serveur DNS préféré : 172.31.10.10.
3. Répéter l’opération pour les autres VLANs :
   * VLAN 20 - Personnel :
     + Début : 172.31.20.100, Fin : 172.31.20.200, Passerelle : 172.31.20.1.
   * VLAN 30 - Vidéo :
     + Début : 172.31.30.100, Fin : 172.31.30.200, Passerelle : 172.31.30.1.
   * Continuez pour les VLANs 40, 50, 60, et 70.
4. Activer l’étendue :
   * Assurez-vous que chaque étendue est activée après configuration.
5. Tester le DHCP :
   * Connectez un client à chaque VLAN.

Sur le client, ouvrez une invite de commande et exécutez :  
  
  
ipconfig /release

ipconfig /renew

* + Vérifiez que l’adresse IP est attribuée correctement.

## 3. Configuration du service DNS

### **1. Ouvrir DNS Manager**

1. Connectez-vous à votre serveur Windows.
2. Accédez au **Gestionnaire de serveur**.
3. Cliquez sur **Outils** dans le coin supérieur droit.
4. Sélectionnez **DNS** dans la liste pour ouvrir la console de gestion DNS.

### **2. Création d'une zone principale**

1. Dans le panneau de gauche de la console DNS, cliquez avec le bouton droit sur **Zones de recherche directe**.
2. Sélectionnez **Nouvelle zone…** pour lancer l'assistant de création de zones.
3. Configurez la zone :
   * **Type de zone** : Sélectionnez **Zone principale**.
   * **Répliquer vers** : Laissez la configuration par défaut.
   * **Nom de la zone** : Entrez societeX.pepiniere.rt comme nom de la zone.
   * **Chemin du fichier** : Laissez le chemin proposé automatiquement.
   * Terminez l’assistant en cliquant sur **Terminer**.

### **3. Ajouter des enregistrements DNS**

#### **a. Ajouter un enregistrement A pour le mail :**

1. Faites un clic droit sur la zone societeX.pepiniere.rt dans la liste des zones.
2. Sélectionnez **Nouvel hôte (A ou AAAA)…**.
3. Dans la fenêtre qui s’ouvre :
   * **Nom** : Tapez mail.
   * **Adresse IP** : Entrez 172.31.10.11.
4. Cliquez sur **Ajouter un hôte** pour sauvegarder.

#### **b. Ajouter un enregistrement A pour le proxy :**

1. Répétez les étapes ci-dessus.
2. Cette fois :
   * **Nom** : Tapez proxy.
   * **Adresse IP** : Entrez 172.31.10.12.
3. Cliquez sur **Ajouter un hôte**.

#### **c. Ajouter un enregistrement MX :**

1. Faites un clic droit sur la zone societeX.pepiniere.rt.
2. Sélectionnez **Nouvel enregistrement de ressource…**.
3. Dans la liste, choisissez **Enregistrement de messagerie (MX)**, puis cliquez sur **Créer…**.
4. Configurez les champs :
   * **Priorité** : Entrez 10.
   * **Nom du serveur de messagerie** : Entrez mail.societeX.pepiniere.rt.
5. Cliquez sur **OK** pour valider.

### **4. Tester la configuration DNS**

Pour vérifier que votre DNS est correctement configuré, effectuez les commandes suivantes dans une invite de commande :

#### **a. Tester l’enregistrement A du mail :**

nslookup mail.societeX.pepiniere.rt

Vous devriez voir l’adresse IP 172.31.10.11 associée au nom mail.societeX.pepiniere.rt.

#### **b. Tester l’enregistrement A du proxy :**

nslookup proxy.societeX.pepiniere.rt

Vous devriez voir l’adresse IP 172.31.10.12 associée au nom proxy.societeX.pepiniere.rt.

#### **c. Tester l’enregistrement MX :**

nslookup -type=MX societeX.pepiniere.rt

Vous devriez voir l’enregistrement MX pointant vers mail.societeX.pepiniere.rt avec la priorité 10.

### 6. Configurer le DNS Forwarding

1. **Ouvrir les propriétés du serveur DNS :**
   * Dans la console DNS, faites un clic droit sur le nom de votre serveur DNS (exemple : WINDOWS-SRV-2016) dans le panneau gauche.
   * Sélectionnez **Propriétés**.
2. **Configurer les redirecteurs :**
   * Allez dans l’onglet **Redirecteurs**.
   * Cliquez sur le bouton **Modifier** pour ajouter des serveurs DNS externes à utiliser en cas de requête non résolue localement.
3. **Ajouter les adresses IP des serveurs DNS de l’IUT :**
   * Par exemple, ajoutez 10.0.0.1 en tant que serveur DNS distant.
   * Cliquez sur **OK** pour valider.
4. **Tester le forwarding DNS :**

Dans une invite de commande, tapez :  
  
  
nslookup www.google.com

* + Si la résolution fonctionne, cela signifie que les requêtes externes sont correctement transmises au serveur DNS de l’IUT (10.0.0.1).

### **Résumé de la configuration**

* **Zone créée** : societeX.pepiniere.rt.
* **Enregistrements créés** :
  + Enregistrement A pour le mail : mail.societeX.pepiniere.rt → 172.31.10.11.
  + Enregistrement A pour le proxy : proxy.societeX.pepiniere.rt → 172.31.10.12.
  + Enregistrement MX pour la messagerie : mail.societeX.pepiniere.rt avec priorité 10.
* **Forwarding configuré** : Les requêtes non résolues sont transmises au DNS externe (10.0.0.1).

## 4.Configuration d’un serveur proxy

### **1. Installation de Squid**

1. **Téléchargez Squid pour Windows :**
   * Rendez-vous sur le site officiel de Squid pour Windows ou un dépôt fiable.
   * Téléchargez le package adapté à votre version de Windows.
2. **Installez Squid :**
   * Lancez le programme d'installation.
   * Choisissez un répertoire d'installation (par défaut : C:\Squid).

### **2. Configuration de Squid**

**Accédez au fichier de configuration :**

* + Le fichier principal de configuration se trouve dans le répertoire d’installation : C:\Squid\etc\squid.conf.

**Modifiez le fichier squid.conf selon vos besoins :** Exemple d’une configuration fonctionnelle pour un réseau incluant des plages IP de 172.32.0.0/15 :  
  
# Configuration de base

http\_port 172.33.10.12:3128

dns\_nameservers 172.33.10.10 10.0.0.1

# Définition des réseaux locaux autorisés

acl localnet src 172.32.0.0/15

acl Safe\_ports port 80

acl Safe\_ports port 443

acl CONNECT method CONNECT

# Règles d'accès

http\_access allow localnet

http\_access allow localhost

http\_access deny all

# Autres paramètres

coredump\_dir /var/cache/squid

refresh\_pattern ^ftp: 1440 20% 10080

refresh\_pattern ^gopher: 1440 0% 1440

refresh\_pattern -i (/cgi-bin/|\?) 0 0% 0

refresh\_pattern . 0 20% 4320

max\_filedescriptors 3200

cache\_peer cache-etu.univ-artois.fr parent 3128 0 no-query default

icp\_port 0

never\_direct allow all

**Sauvegardez les modifications :**

* + Enregistrez le fichier après vos modifications.

### **3. Configuration du service Squid**

1. **Ajoutez Squid comme service Windows :**
   * Ouvrez une console en administrateur.

Exécutez la commande suivante dans le répertoire d’installation de Squid :  
  
squid -i

* + Cela configure Squid en tant que service Windows.

1. **Démarrez le service Squid :**

Lancez la commande suivante :  
  
net start squid

### **4. Configuration des clients pour utiliser le proxy**

1. **Configurez manuellement un navigateur web :**
   * Allez dans les paramètres réseau du navigateur.
   * Dans la configuration proxy, ajoutez les informations suivantes :
     + **Proxy HTTP** : 172.33.10.12
     + **Port** : 3128
     + **Proxy HTTPS** : Même configuration.
2. **Testez la connectivité :**
   * Essayez d'accéder à des sites web pour vérifier le bon fonctionnement.

### **5. Ajout des DNS et ajustement des plages IP**

1. **DNS Nameservers :**

Si vous utilisez un serveur DNS local (par ex. 172.33.10.10 qui fait un forward vers un DNS externe comme 10.0.0.1), ajoutez ces serveurs dans la directive dns\_nameservers de squid.conf.  
  
dns\_nameservers 172.33.10.10 10.0.0.1

1. **Extension des plages IP :**

Si votre réseau inclut plusieurs plages, comme 172.32.0.0/15, modifiez ou ajoutez une directive acl localnet pour les inclure :  
plaintext  
  
acl localnet src 172.32.0.0/15

htt

### **6. Résolution des problèmes fréquents**

1. **Service Squid ne démarre pas :**
   * Assurez-vous que le fichier squid.conf ne contient pas d'erreurs de syntaxe.
   * Consultez les logs à C:\Squid\var\logs pour identifier les erreurs.
2. **Les clients n’accèdent pas au web via le proxy :**

Vérifiez que le service Squid est démarré :  
  
  
net start squid

* + Vérifiez que les machines clientes sont dans la plage IP autorisée (localnet).
  + Testez la connectivité avec la commande ping vers le proxy.

### **7. Logs et maintenance**

1. **Logs d’accès :**
   * Consultez les logs à l'emplacement suivant : C:\Squid\var\logs\access.log.
   * Ces logs vous permettent de vérifier quelles requêtes passent ou sont bloquées.
2. **Maintenance des caches :**

Si nécessaire, videz le cache pour libérer de l’espace ou résoudre des erreurs :  
  
  
squid -z

### **8. Redémarrage et tests**

1. **Redémarrage de Squid après modification :**

Pour appliquer les modifications de configuration, redémarrez le service :  
  
  
net stop squid

net start squid

1. **Tests finaux :**
   * Vérifiez que les clients accèdent correctement à Internet via le proxy.
   * Consultez les logs pour confirmer que les requêtes passent par Squid.

### **Résumé des points clés**

* **Adresse IP du proxy** : 172.33.10.12.
* **Port du proxy** : 3128.
* **Plages IP autorisées** : 172.32.0.0/15.
* **DNS configurés** : 172.33.10.10 (local) et 10.0.0.1 (externe).

## 5. Configuration du service Mail avec MailEnable

Le service MailEnable sera configuré pour fournir un service de messagerie, y compris un accès Webmail. Cette section détaille chaque étape de l’installation, la configuration et la vérification du Webmail.

### Étape 1 : Téléchargement et installation de MailEnable

1. Télécharger MailEnable :
   * Sur le serveur Windows, ouvrez un navigateur web.
   * Rendez-vous sur le site officiel : [www.mailenable.com](https://www.mailenable.com).
   * Téléchargez la version Standard Edition (gratuite).
2. Installer MailEnable :
   * Exécutez le fichier d'installation téléchargé.
   * Pendant l’installation, suivez les étapes ci-dessous :
     + Acceptez le contrat de licence.
     + Laissez le chemin d'installation par défaut (généralement C:\Program Files\Mail Enable).
   * Lorsqu’il vous est demandé de saisir le Nom de domaine, entrez :  
       
     societeX.pepiniere.rt
   * Pour le DNS Host(s), entrez :  
       
     127.0.0.1
     + Terminez l'installation avec les paramètres par défaut.

### Étape 2 : Création des boîtes aux lettres

1. Ouvrir la console MailEnable Management :
   * Cliquez sur Démarrer > Tous les programmes > MailEnable > MailEnable Management.
2. Créer un Post Office :
   * Dans le panneau de gauche, déroulez Messaging Manager.
   * Faites un clic droit sur Post Offices, puis sélectionnez New > Post Office....
   * Renseignez les champs suivants :
     + Post Office Name : societeX
     + Domain Name : societeX.pepiniere.rt
     + Postmaster Password : définissez un mot de passe sécurisé pour l’administrateur.
   * Cliquez sur OK.
3. Créer des utilisateurs et boîtes aux lettres :
   * Sous Post Offices > societeX > Mailboxes, faites un clic droit > New > Mailbox....
   * Renseignez les informations :
     + Mailbox Name : admin (par exemple).
     + Password : définissez un mot de passe sécurisé.
   * Cliquez sur OK.
   * Répétez cette opération pour d'autres utilisateurs si nécessaire (par exemple, user1).

### Étape 3 : Configuration du Webmail dans IIS

1. Installer le rôle IIS (si non installé) :
   * Ouvrez le Gestionnaire de serveur.
   * Cliquez sur Gérer > Ajouter des rôles et fonctionnalités.
   * Cochez Serveur Web (IIS) et assurez-vous que les services suivants sont activés :
     + Console de gestion IIS
     + Contenu statique
     + Document par défaut
     + Redirection HTTP (optionnel mais recommandé).
   * Terminez l'installation et redémarrez le serveur si demandé.
2. Configurer les liaisons dans IIS :
   * Ouvrez Gestionnaire des services Internet (IIS) :
     + Cliquez sur Démarrer > Outils d’administration > Gestionnaire des services Internet (IIS).
   * Dans le panneau de gauche, déroulez le serveur (exemple : WIN-SERVER).
   * Cliquez sur Sites, puis sur Default Web Site.
   * Faites un clic droit sur Default Web Site, puis sélectionnez Modifier les liaisons....
   * Dans la fenêtre Liaisons de site :
     + Cliquez sur Ajouter....
     + Configurez comme suit :
       - Type : http
       - Adresse IP : 172.31.10.11
       - Port : 80
       - Nom d’hôte : mail.societeX.pepiniere.rt
     + Cliquez sur OK, puis fermez la fenêtre.
3. Configurer le Webmail dans MailEnable :
   * Dans MailEnable Management, déroulez Servers > localhost > Services and Connectors.
   * Cliquez sur Web Mail.
   * Dans le panneau de droite, cliquez sur Configure Sites....
   * Vérifiez que le site Default Web Site est listé et associé à votre nom d’hôte mail.societeX.pepiniere.rt.
   * Si ce n'est pas le cas :
     + Cliquez sur New Host Header... et entrez :
       - Nom du site : mail.societeX.pepiniere.rt
       - Port : 80
       - Adresse IP : 172.31.10.11.
   * Cliquez sur OK.
4. Redémarrer le site Webmail :
   * Dans IIS Manager, sélectionnez Default Web Site.
   * Dans le panneau de droite, cliquez sur Redémarrer pour appliquer les modifications.

### Étape 4 : Tester le Webmail

1. Accéder au Webmail :
   * Ouvrez un navigateur web sur une machine cliente ou le serveur.
   * Accédez à l’URL suivante :  
       
       
     http://mail.societeX.pepiniere.rt/mewebmail
2. Connexion :
   * Une page de connexion MailEnable s’affiche.
   * Entrez les informations d’un utilisateur créé précédemment (par exemple : admin et son mot de passe).
3. Tester l’envoi et la réception d’emails :
   * Depuis le Webmail, envoyez un email à une autre boîte aux lettres locale (par exemple, de admin à user1).
   * Vérifiez que l’email est bien reçu.

### Étape 5 : Configurer un client de messagerie

Pour vérifier le bon fonctionnement du service Mail, configurez un client comme Outlook ou Thunderbird avec les paramètres suivants :

* Serveur entrant (IMAP) :
  + Adresse : 172.31.10.11
  + Port : 143
* Serveur sortant (SMTP) :
  + Adresse : 172.31.10.11
  + Port : 25
* Nom d’utilisateur : admin@societeX.pepiniere.rt
* Mot de passe : celui défini lors de la création de la boîte aux lettres.

1. Configurer un client de messagerie pour tester :
   * IMAP : 172.31.10.11, port 143.
   * SMTP : 172.31.10.11, port 25

## 

## 6. Configuration du serveur RADIUS avec spécification des IP/DNS

### **Étape 1 : Ajouter le rôle NPS (Network Policy Server)**

1. **Ouvrir le Gestionnaire de serveur :**
   * Cliquez sur **Démarrer** et sélectionnez **Gestionnaire de serveur**.
2. **Ajouter des rôles et fonctionnalités :**
   * Dans le **Gestionnaire de serveur**, cliquez sur **Gérer > Ajouter des rôles et fonctionnalités**.
   * Sélectionnez **Installation basée sur un rôle ou une fonctionnalité**, puis cliquez sur **Suivant**.
3. **Sélectionner le rôle NPS :**
   * Dans la liste des rôles de serveur, cochez **Network Policy and Access Services** (Services de stratégie et d'accès réseau).
   * Une fenêtre contextuelle peut apparaître pour ajouter les fonctionnalités nécessaires. Cliquez sur **Ajouter des fonctionnalités**.
   * Cliquez sur **Suivant**.
4. **Installer le rôle :**
   * Continuez avec l’assistant jusqu’à l’écran de confirmation.
   * Cliquez sur **Installer** et attendez que l’installation se termine.
   * Si un redémarrage est requis, redémarrez le serveur.

### **Étape 2 : Configurer le serveur NPS comme un serveur RADIUS**

1. **Ouvrir la console NPS :**
   * Une fois le rôle installé, cliquez sur **Démarrer > Outils d’administration > Network Policy Server**.
2. **Enregistrer le serveur dans Active Directory :**
   * Dans la console NPS, faites un clic droit sur **NPS (Local)** dans le panneau de gauche.
   * Sélectionnez **Register server in Active Directory**.
   * Une fenêtre de confirmation s’affiche. Cliquez sur **OK**, puis sur **OK** à nouveau.
3. **Configurer NPS comme serveur RADIUS :**
   * Dans le panneau de gauche, faites un clic droit sur **RADIUS Clients and Servers**, puis sélectionnez **Configure RADIUS Server for 802.1X**.
   * Suivez les étapes de l’assistant :
     + **Type de configuration** : Sélectionnez **Secure Wireless Connections** si vous configurez un réseau Wi-Fi, ou **Secure Wired Connections** pour un réseau filaire.
     + **Nom du réseau** : Donnez un nom à votre configuration (exemple : Wi-Fi RADIUS).

### **Étape 3 : Ajouter des clients RADIUS (par exemple, des points d’accès Wi-Fi)**

1. **Accéder à la section des clients RADIUS :**
   * Dans la console NPS, développez **RADIUS Clients and Servers**, puis cliquez sur **RADIUS Clients**.
2. **Ajouter un nouveau client RADIUS :**
   * Faites un clic droit sur **RADIUS Clients** et sélectionnez **New RADIUS Client**.
   * Remplissez les champs comme suit :
     + **Friendly Name** : Donnez un nom descriptif (exemple : AP-WiFi1).
     + **Address (IP or DNS)** : Entrez l’adresse IP ou le DNS de l’équipement (par exemple, l’adresse IP de votre point d’accès Wi-Fi, 172.31.10.13).
     + **Shared Secret** : Saisissez un mot de passe partagé (par exemple : progtr00) que le client RADIUS et le serveur RADIUS utiliseront pour sécuriser les communications. **Notez ce mot de passe**, car il devra être configuré sur le client RADIUS.
3. **Enregistrer la configuration :**
   * Cliquez sur **OK** pour ajouter le client.

### **Étape 4 : Configurer les stratégies réseau (Network Policies)**

1. **Accéder aux stratégies réseau :**
   * Dans la console NPS, cliquez sur **Policies**, puis sur **Network Policies**.
2. **Créer une nouvelle stratégie :**
   * Faites un clic droit sur **Network Policies** et sélectionnez **New**.
   * Remplissez les champs comme suit :
     + **Policy Name** : Donnez un nom à la stratégie (exemple : Wi-Fi Auth Policy).
     + **Type of network access server** : Sélectionnez **Unspecified**.
3. **Configurer les conditions de la stratégie :**
   * Cliquez sur **Add** pour ajouter des conditions. Par exemple :
     + **User Groups** : Sélectionnez les groupes Active Directory qui seront autorisés à se connecter.
     + **Client IPv4 Address** : Entrez l’adresse IP des clients RADIUS (par exemple, 172.31.10.13).
4. **Configurer les autorisations :**
   * Sous l’onglet **Permissions**, sélectionnez **Grant Access** (Autoriser l'accès).
5. **Configurer les méthodes d’authentification :**
   * Dans l’onglet **Authentication Methods**, sélectionnez **Microsoft: Protected EAP (PEAP)**.
   * Cliquez sur **Configure** à côté de PEAP, puis :
     + Choisissez un certificat de serveur valide (généré ou importé).
     + Configurez l’authentification utilisateur si nécessaire.
6. **Configurer les contraintes :**
   * Configurez les contraintes comme le temps de session, les ports spécifiques, etc., si nécessaire.
7. **Enregistrer la stratégie :**
   * Cliquez sur **OK** pour sauvegarder la stratégie.

### **Étape 5 : Configurer les clients (par exemple, les points d’accès Wi-Fi)**

1. **Accéder à la configuration RADIUS sur le client :**
   * Connectez-vous à l’interface de gestion de votre point d’accès Wi-Fi (ou autre appareil).
   * Accédez à la section **RADIUS Server Settings** (ou similaire).
2. **Entrer les informations du serveur RADIUS :**
   * **IP Address** : L’adresse IP du serveur Windows où NPS est configuré (par exemple, 172.31.10.13).
   * **Shared Secret** : Entrez le mot de passe partagé configuré précédemment (MotDePasseRadius).
3. **Configurer l’authentification :**
   * Sélectionnez **WPA2-Enterprise** comme méthode de sécurité.
   * Configurez l’authentification avec **PEAP** si elle est disponible.
4. **Tester la connexion :**
   * Essayez de connecter un appareil utilisateur (comme un PC ou un smartphone) au réseau Wi-Fi.
   * Si tout est configuré correctement, l’appareil demandera les informations d’identification de l’utilisateur (nom d’utilisateur et mot de passe).

### **Étape 6 : Vérifications et tests**

1. **Tester la connectivité :**
   * Connectez un appareil client au réseau (Wi-Fi ou VPN selon la configuration).
   * Utilisez des informations d'identification valides pour vous connecter.
2. **Vérifier les journaux NPS :**
   * Dans la console NPS, cliquez sur **Accounting** pour vérifier les tentatives d’authentification réussies et échouées.
   * Consultez les événements NPS dans **Observateur d'événements** :
     + Allez dans **Journaux Windows > Sécurité** pour voir les tentatives d'accès.

## t7. Active Directory interconnectés :

### 1. Configuration du premier serveur AD (172.31.10.10)

### **Étape 1 : Installer Active Directory Domain Services (AD DS)**

1. **Ouvrir le Gestionnaire de serveur :**
   * Cliquez sur **Démarrer > Gestionnaire de serveur**.
2. **Ajouter le rôle AD DS :**
   * Cliquez sur **Gérer > Ajouter des rôles et fonctionnalités**.
   * Sélectionnez **Installation basée sur un rôle ou une fonctionnalité**, puis cliquez sur **Suivant**.
   * Cochez **Active Directory Domain Services (AD DS)**.
   * Une fenêtre contextuelle s’affiche pour ajouter les fonctionnalités nécessaires. Cliquez sur **Ajouter des fonctionnalités**, puis cliquez sur **Suivant**.
   * Cliquez sur **Installer** et attendez la fin de l’installation.

### **Étape 2 : Promouvoir le serveur en tant que contrôleur de domaine principal (PDC)**

1. **Démarrer l’assistant de promotion :**
   * Une fois l’installation terminée, dans le **Gestionnaire de serveur**, cliquez sur l’icône d’alerte (triangle jaune) en haut à droite.
   * Cliquez sur **Promouvoir ce serveur en contrôleur de domaine**.
2. **Créer une nouvelle forêt :**
   * Dans l’assistant de configuration, sélectionnez **Ajouter une nouvelle forêt**.
   * Entrez le **Nom de domaine racine** (par exemple : societeX.pepiniere.rt).
   * Cliquez sur **Suivant**.
3. **Configurer les options de domaine :**
   * Choisissez le **niveau fonctionnel du domaine et de la forêt** (par exemple : **Windows Server 2016**).
   * Assurez-vous que l’option **Serveur DNS** est activée.
   * Définissez un mot de passe pour le **mode de restauration des services d'annuaire (DSRM)**.
4. **Vérification et installation :**
   * Suivez les étapes de l’assistant. Une vérification des prérequis sera effectuée.
   * Si tout est correct, cliquez sur **Installer**. Le serveur redémarrera automatiquement après la promotion.
5. **Vérifier la configuration AD DS :**
   * Une fois redémarré, ouvrez **Outils > Utilisateurs et ordinateurs Active Directory** dans le Gestionnaire de serveur.
   * Vérifiez que le domaine societeX.pepiniere.rt est bien créé.

### 2. Configuration du second serveur AD (172.31.10.20)

### **Étape 1 : Préparer le serveur**

1. **Configurer une adresse IP statique :**
   * Répétez les étapes mentionnées dans la section précédente, mais utilisez les paramètres suivants :
     + **Adresse IP** : 172.31.10.20
     + **Masque de sous-réseau** : 255.255.255.0
     + **Passerelle par défaut** : 172.31.10.1
     + **Serveur DNS préféré** : 172.31.10.10 (adresse du PDC).
2. **Renommer le serveur :**
   * Donnez-lui un nom descriptif, par exemple ADC-Server.
   * Redémarrez le serveur.
3. **Vérifier la connectivité avec le PDC :**
   * Ouvrez une invite de commandes (**Windows + R**, tapez cmd).
   * Testez la connectivité avec le PDC en tapant :  
       
     ping 172.31.10.10
   * Assurez-vous que le serveur principal répond.

### **Étape 2 : Installer Active Directory Domain Services (AD DS)**

1. **Ouvrir le Gestionnaire de serveur :**
   * Cliquez sur **Démarrer > Gestionnaire de serveur**.
2. **Ajouter le rôle AD DS :**
   * Cliquez sur **Gérer > Ajouter des rôles et fonctionnalités**.
   * Sélectionnez **Installation basée sur un rôle ou une fonctionnalité**, puis cliquez sur **Suivant**.
   * Cochez **Active Directory Domain Services (AD DS)**.
   * Cliquez sur **Ajouter des fonctionnalités**, puis sur **Suivant**.
   * Cliquez sur **Installer**.

### **Étape 3 : Promouvoir le serveur en contrôleur de domaine secondaire (ADC)**

1. **Démarrer l’assistant de promotion :**
   * Une fois le rôle AD DS installé, cliquez sur l’icône d’alerte (triangle jaune) dans le Gestionnaire de serveur.
   * Cliquez sur **Promouvoir ce serveur en contrôleur de domaine**.
2. **Joindre le domaine existant :**
   * Sélectionnez **Ajouter un contrôleur de domaine à un domaine existant**.
   * Cliquez sur **Sélectionner** et entrez le nom de domaine (par exemple : societeX.pepiniere.rt).
   * Entrez les informations d’identification d’un administrateur du domaine principal.
3. **Configurer les options de domaine :**
   * Activez les rôles suivants :
     + **Serveur DNS** : Cela permet au serveur secondaire de servir de DNS secondaire pour la résilience.
     + **Catalogue global (Global Catalog)** : Cela permet au serveur secondaire de gérer les requêtes des utilisateurs et des applications.
   * Entrez un mot de passe pour le **mode de restauration des services d'annuaire (DSRM)**.
4. **Vérification et installation :**
   * L’assistant vérifiera les prérequis. Si tout est correct, cliquez sur **Installer**.
   * Le serveur redémarrera automatiquement une fois la configuration terminée.
5. **Vérifier la réplication :**
   * Connectez-vous au serveur secondaire.
   * Ouvrez **Outils > Utilisateurs et ordinateurs Active Directory**.
   * Vérifiez que les unités d’organisation, les utilisateurs et les groupes sont synchronisés avec le PDC.

## 3. Vérifications et tests

1. **Tester la réplication :**
   * Sur le PDC, créez un utilisateur ou un groupe dans Active Directory.
   * Connectez-vous au serveur secondaire (ADC) et vérifiez que les modifications sont répliquées.
2. **Joindre un poste client au domaine :**
   * Configurez l’adresse IP du client pour utiliser le DNS principal (172.31.10.10) ou le secondaire (172.31.10.20).
   * Ajoutez le client au domaine via **Propriétés système > Nom de l’ordinateur > Modifier > Domaine**.
   * Entrez le nom du domaine (societeX.pepiniere.rt) et les informations d’un administrateur du domaine.
3. **Vérifier les rôles FSMO (Flexible Single Master Operations) :**
   * Sur le PDC, ouvrez une invite de commande et tapez :  
     bash  
       
     netdom query fsmo
   * Vérifiez que les rôles FSMO sont correctement attribués au PDC.
4. **Vérifier la résolution DNS :**
   * Testez la résolution DNS depuis le client ou les serveurs avec les commandes suivantes :  
     bash  
       
     nslookup societeX.local
   * nslookup -type=SRV \_ldap.\_tcp.societeX.local