Rapport de configuration d’un contrôleur de domaine Active Directory et connexion d’un client Windows

Réalisé par : Chater Ahmed et Daouda David Coulibaly
Date : 30/12/2024

Introduction

Ce rapport détaille les étapes suivies pour :

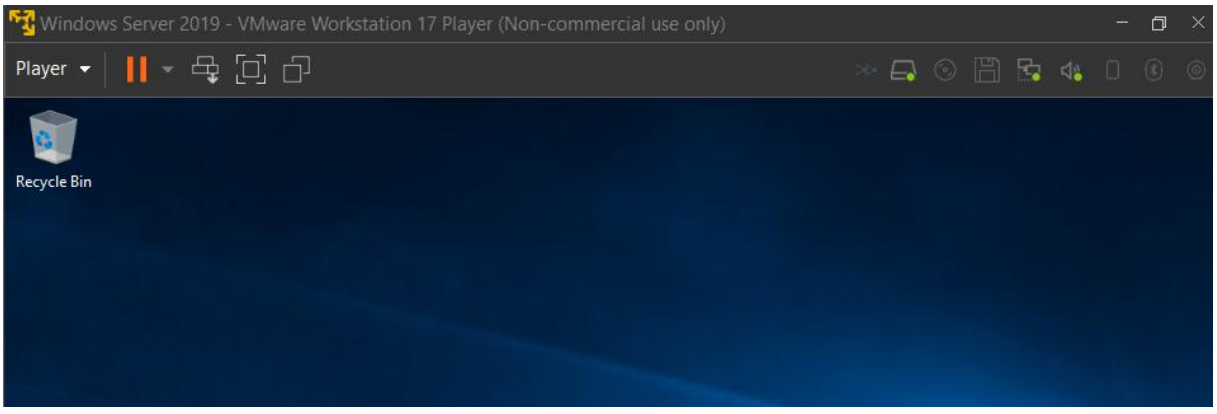
- Configurer un contrôleur de domaine Active Directory (AD) sur Windows Server 2019.
- Connecter une machine cliente Windows à ce domaine.
- Installer et configurer un client Linux pour l’authentification via Kerberos.

Des captures d’écran sont prévues pour chaque étape afin d’illustrer le processus.

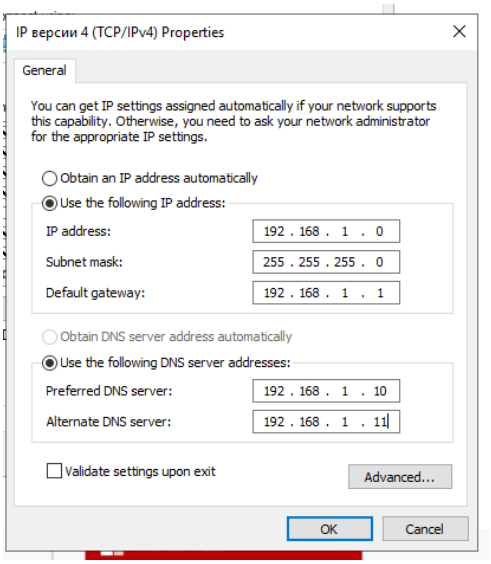
Étape 1 : Installation de Windows Server 2019

1. **Installation du système :**
    - Installer Windows Server 2019 sur une machine virtuelle ou physique.
    - Configuration réseau en NAT pour assurer la communication avec les clients.

    (Capture d’écran : Installation de Windows Server 2019)

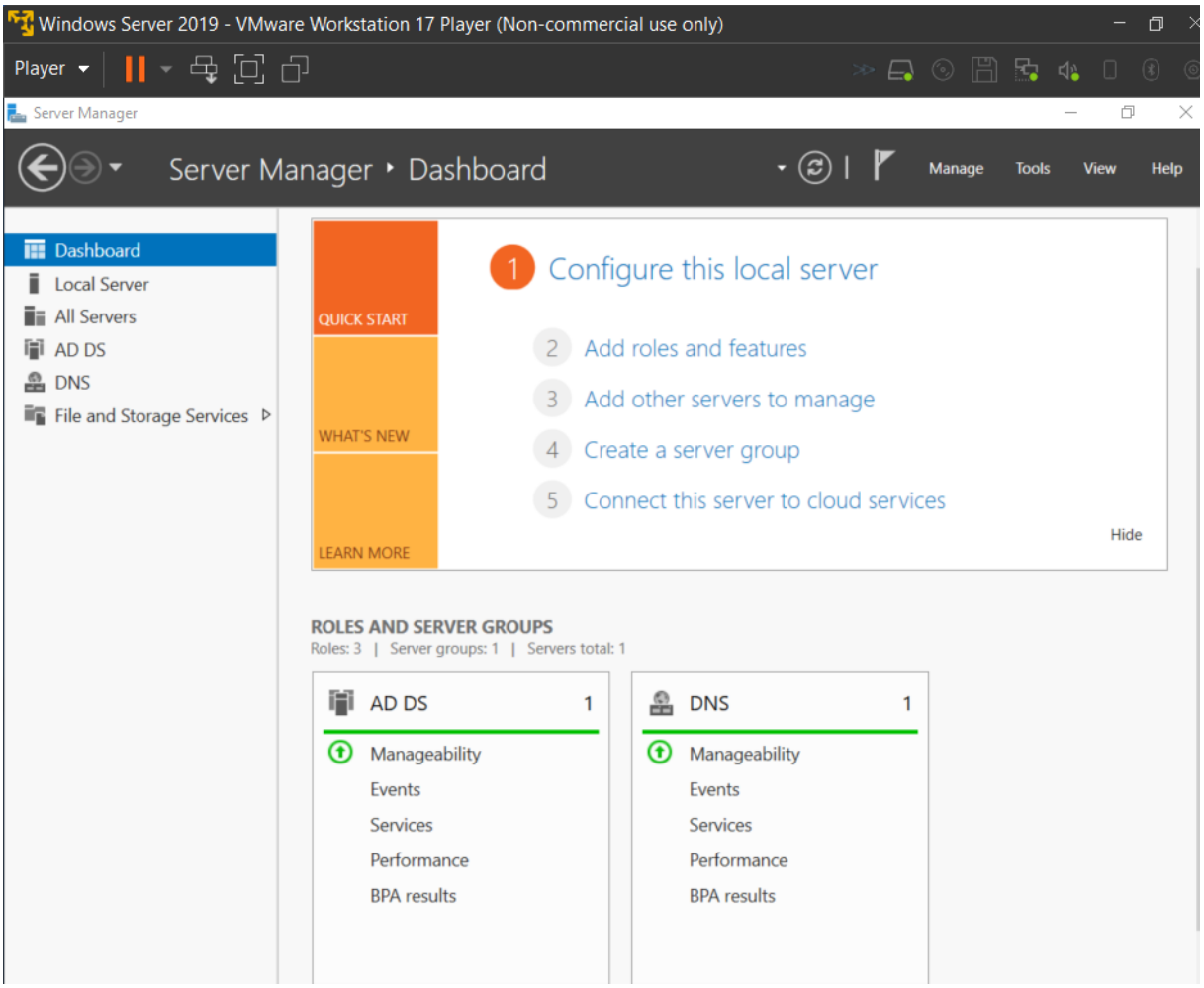


2. **Configuration de l’adresse IP statique :**
    - Configurer une adresse IP statique, par exemple : `192.168.1.10`.

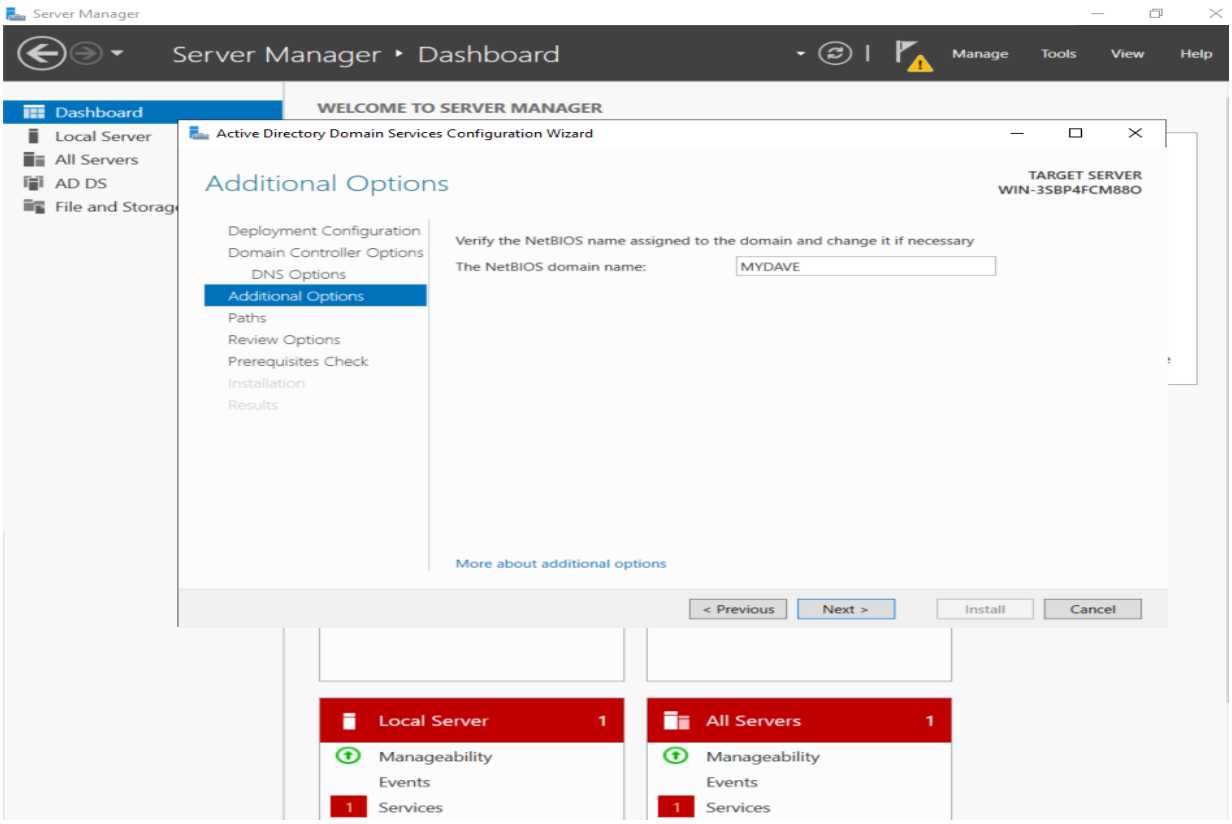


Étape 2 : Promotion en contrôleur de domaine

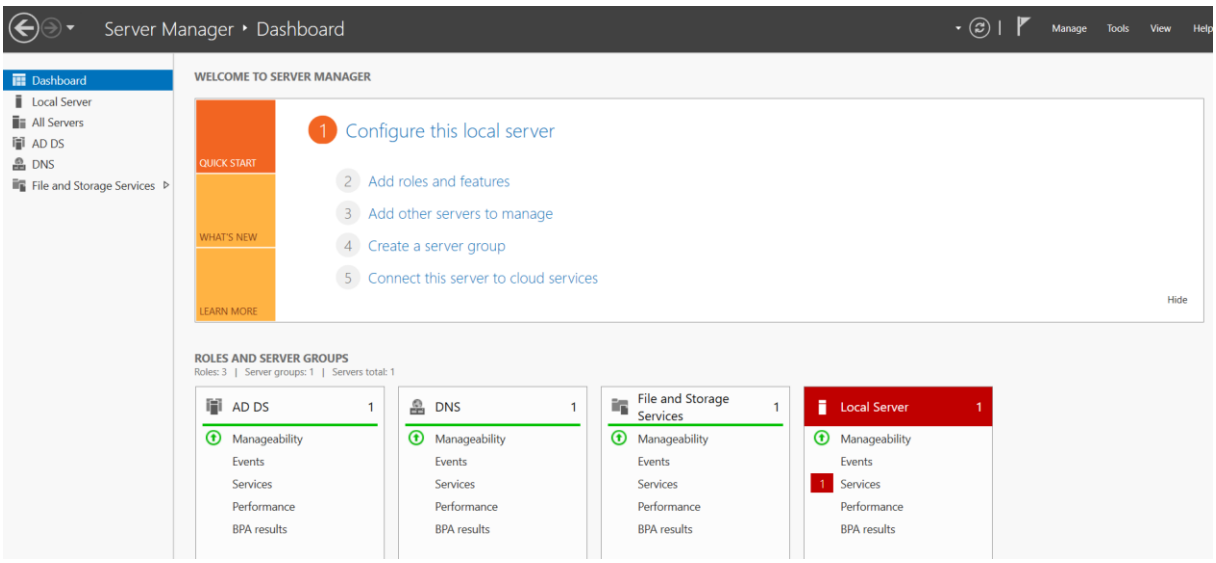
1. **Ajout du rôle Active Directory Domain Services (AD DS) :**
    - Ouvrir le Gestionnaire de serveur et ajouter le rôle AD DS.



2. **Promotion en contrôleur de domaine :**
    - Créer un nouveau domaine (exemple : `mondomaine.local`).
    - Configurer les niveaux fonctionnels et définir un mot de passe DSRM.



3. **Redémarrage du serveur :**
    - Redémarrer le serveur pour appliquer les modifications.



Étape 3 : Configuration du DNS

1. **Vérification du rôle DNS :**
   - S’assurer que le rôle DNS est actif dans le Gestionnaire de serveur.

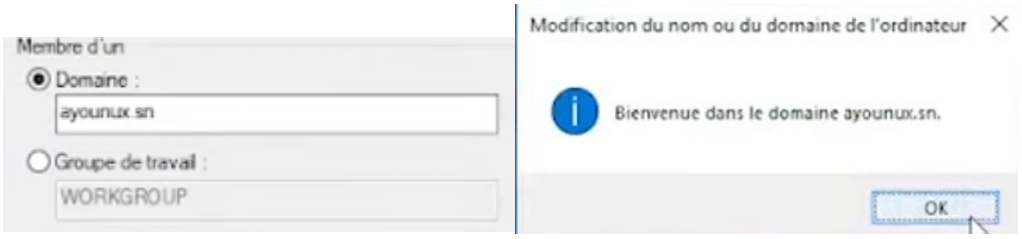
```
PS C:\Windows\system32> nslookup mydave.local
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  ::1

Name:    mydave.local
Address:  192.168.1.10
```

2. **Configuration des clients pour utiliser le DNS du serveur :**
   - Modifier les paramètres réseau des clients pour utiliser `192.168.1.10` comme serveur DNS.

Étape 4 : Connexion d’un client Windows au domaine

1. **Configurer l’adresse IP :**
   - Configurer une adresse IP statique pour le client ou utiliser DHCP.

2. **Rejoindre le domaine :**
    - Aller dans `Panneau de configuration > Système > Modifier les paramètres`.
    - Spécifier le domaine (exemple : `ayounux.sn`).



Étape 5 : Réponses aux Questions

1. Pourquoi est-il nécessaire de générer un fichier keytab pour le serveur et le client ?

Le fichier keytab est comme un "remplaçant" du mot de passe. Sur le serveur, il sert à prouver son identité automatiquement sans demander de mot de passe à chaque fois. Pour le client, c'est pareil : il utilise ce fichier pour s'authentifier aux services sans intervention manuelle. Ça simplifie tout et évite de taper des mots de passe.

---

2. Analysez le rôle du fichier `kadm5.acl` et son impact sur les permissions dans Kerberos.

Ce fichier sert à définir qui a le droit de faire quoi dans Kerberos, comme créer des utilisateurs ou changer des mots de passe. Par exemple, si on ne configure pas bien ce fichier, n'importe qui pourrait modifier des choses importantes, ce qui est dangereux. Par contre, si on limite trop, on bloque des administrateurs qui doivent gérer Kerberos.

---

3. Que signifie GSSAPI dans le contexte d'authentification SSH ? Quels sont ses avantages ?

GSSAPI, c'est un système qui permet à SSH d'utiliser Kerberos pour l'authentification. Avec ça, on n'a pas besoin de mots de passe ni de clés SSH : c'est Kerberos qui gère tout. C'est super pratique parce que tout est centralisé et sécurisé.

---

4. Quelles sont les étapes spécifiques permettant de tester si Kerberos fonctionne correctement sur le client ?

- **1ère étape** : Taper `kinit utilisateur@REALM.COM` pour voir si le client obtient un ticket.
- **2ème étape** : Vérifier avec `klist` si le ticket est bien là.
- **3ème étape** : Essayer de se connecter à un service comme SSH pour voir si ça marche.
- **4ème étape** : Regarder les fichiers de logs si quelque chose ne fonctionne pas.

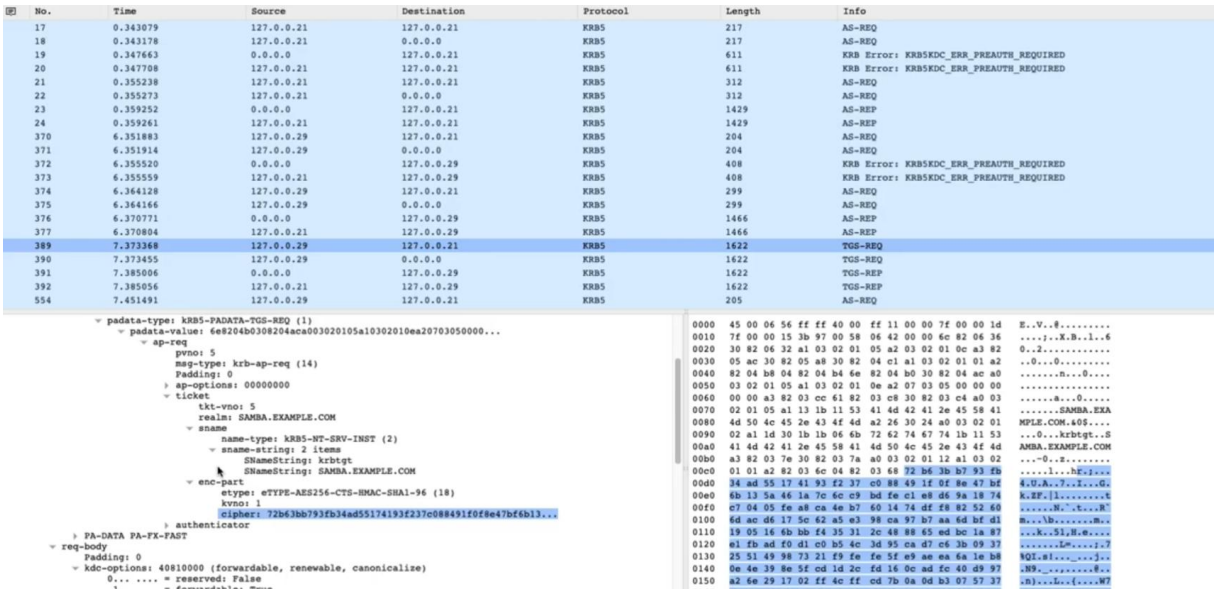
---

5. Identifiez les sources d'erreurs possibles lors de la configuration des principaux et proposez des solutions pour les éviter.

- Si le nom du principal est mal écrit (exemple : erreur dans le REALM), ça ne marchera pas. **Solution** : Bien vérifier.
- Si l'horloge du client et du KDC ne sont pas synchronisées, Kerberos refuse de fonctionner. **Solution** : Activer NTP.
- Si le fichier keytab n'a pas les bonnes permissions, ça peut causer des problèmes. **Solution** : Utiliser `chmod 600`.

---

6. Utiliser Wireshark pour tracer Authentication Service Exchange et Ticket-Granting Service Exchange



Conclusion

Ce rapport démontre la mise en place d’un environnement Active Directory fonctionnel, incluant la connexion de clients Windows .Les captures d’écran associées documentent les étapes pour faciliter la reproduction du processus.