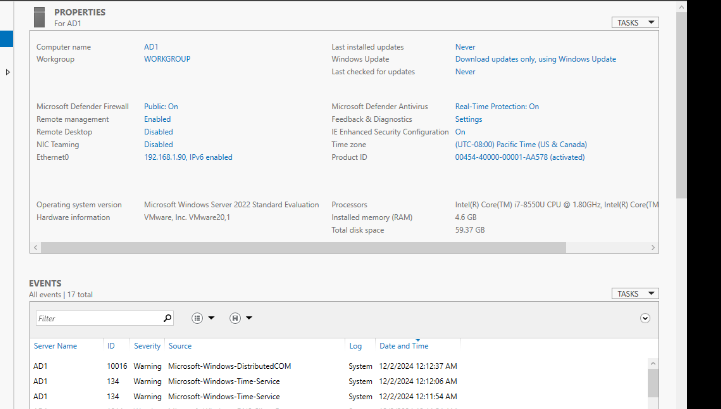
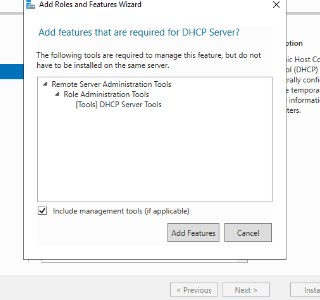
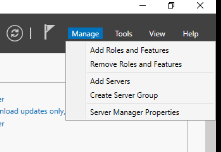
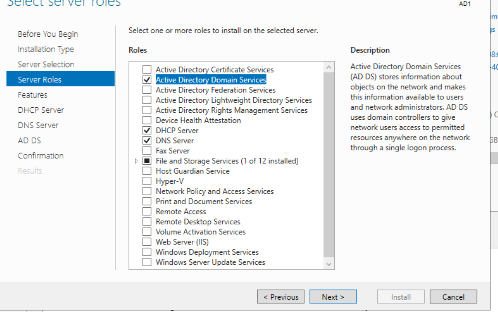
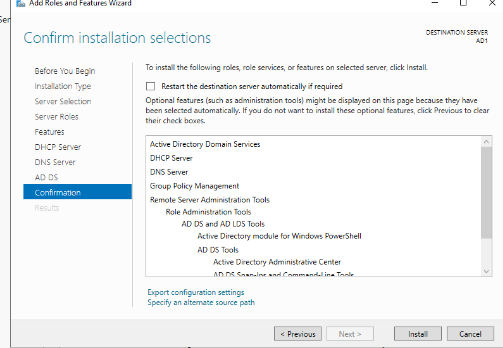
TP2- Ismail Moussaoui

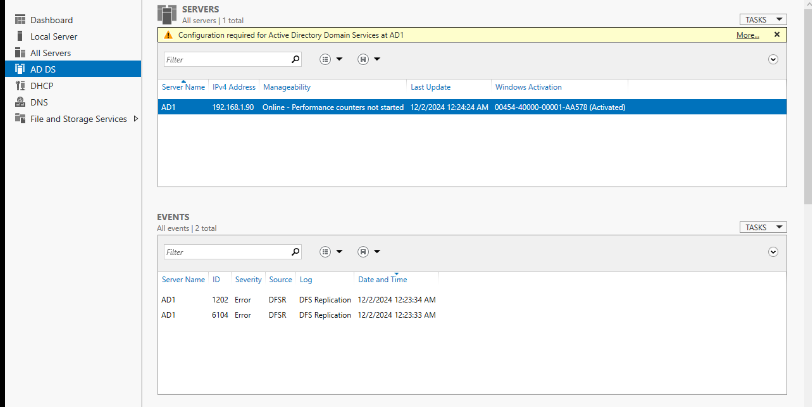
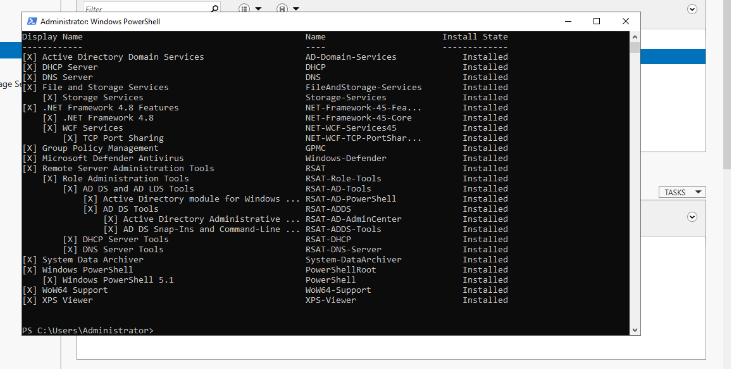
Étape 1. Installation des rôles et fonctionnalités

Activités :



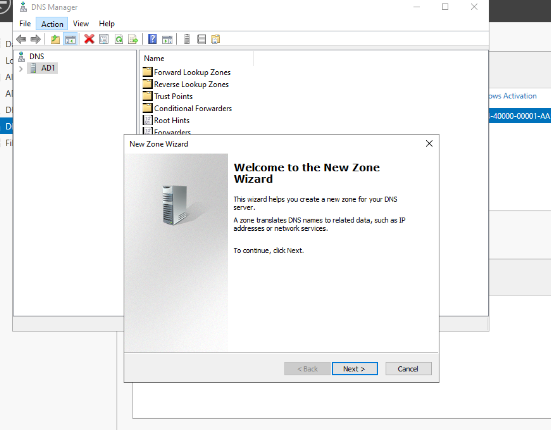
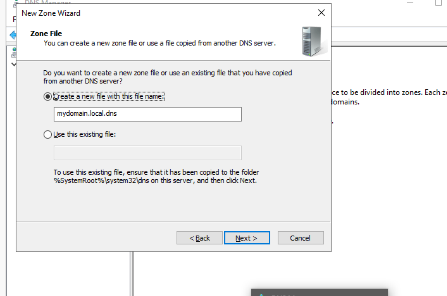


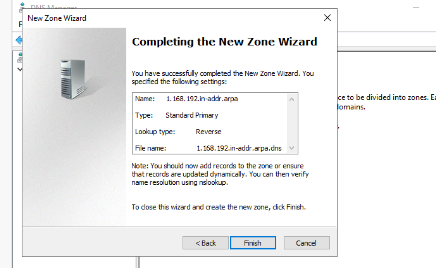
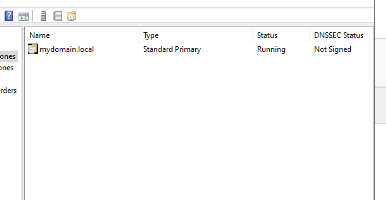
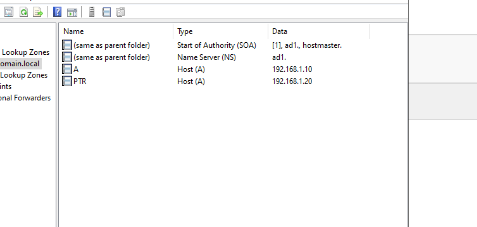
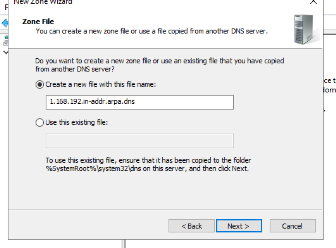




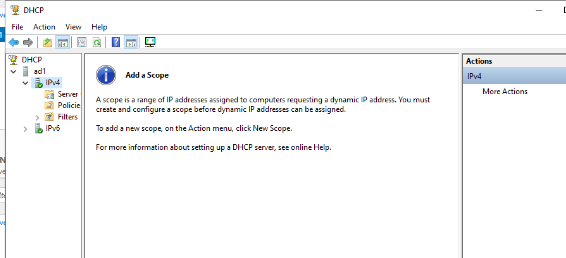
Étape 2. Configuration de base des rôles

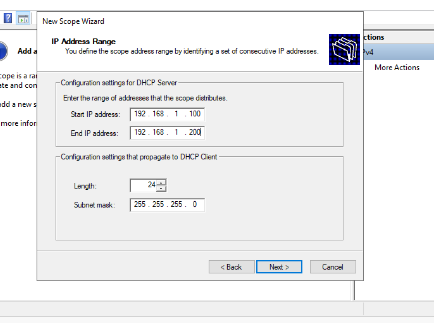
* **DNS Server :**

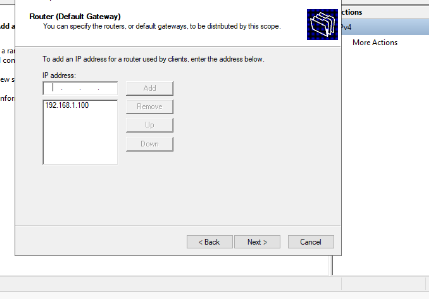
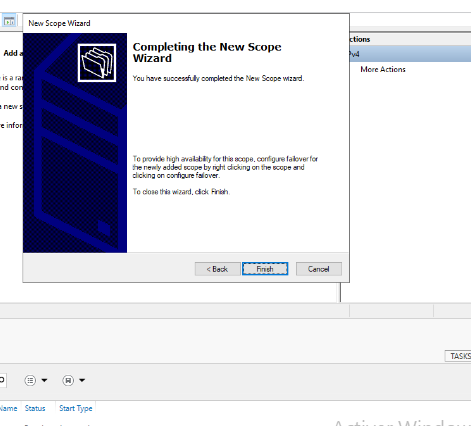


* ****

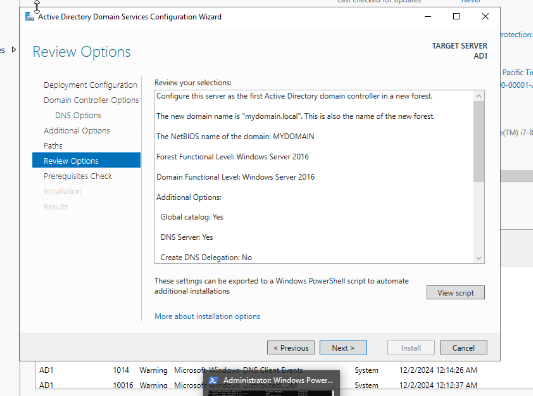
* **DHCP Server :**

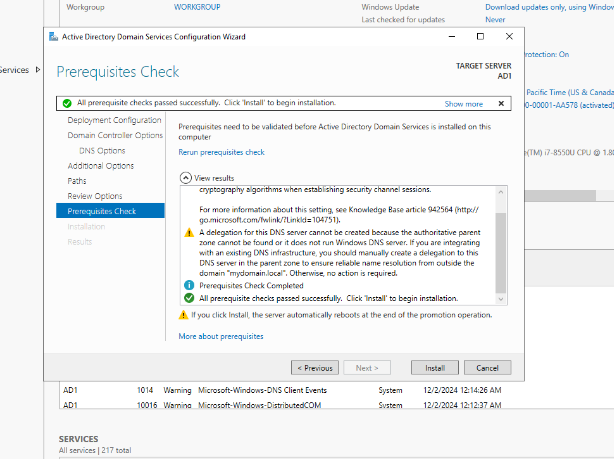
****

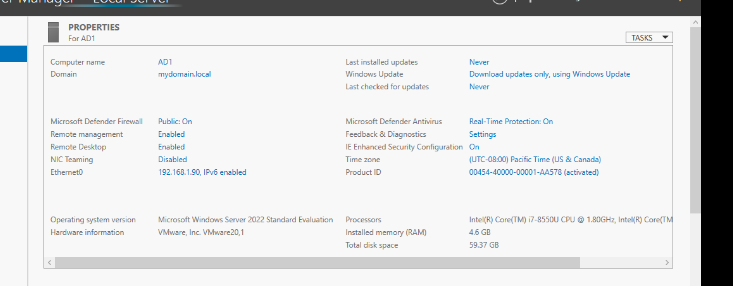
****

****

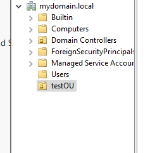
* **AD DS :**

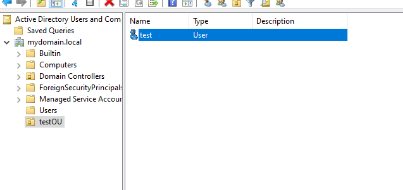
****

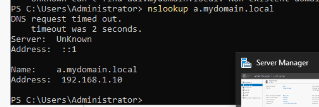
****

****

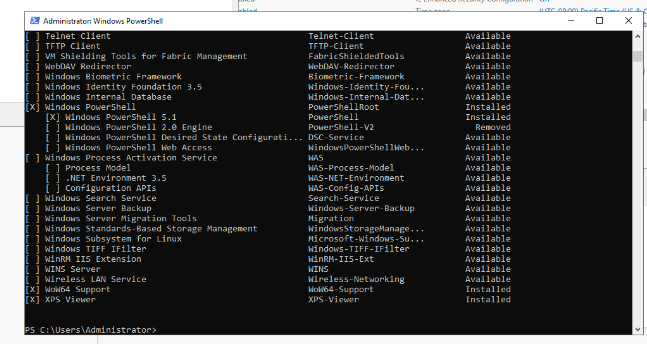
**Créer des unités organisationnelles (OUs) et des utilisateurs**

**de test.**

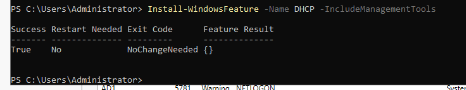
****

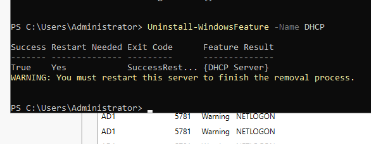
** Powershell:**

**Étape 3. Gestion via PowerShell**

** Get-WindowsFeature Install-WindowsFeature -Name DHCP -IncludeManagementTools**

**Uninstall-WindowsFeature -Name DHCP**

****

****

**** ****

**Étape 4. Exploration des options avancées**

**Questions de réflexion**

**1. Avantages de gérer les rôles via PowerShell par rapport à Server Manager :**

* **Automatisation** : PowerShell permet de créer des scripts pour automatiser les tâches répétitives et complexes.
* **Efficacité** : Les commandes PowerShell sont souvent plus rapides à exécuter qu'une interaction manuelle dans Server Manager.
* **Contrôle à distance** : PowerShell peut gérer des serveurs à distance sans nécessiter une interface graphique.

**2. Étapes de dépannage en cas d’erreur dans le rôle DNS :**

* **Vérification des services** : S’assurer que le service DNS est en cours d’exécution (Get-Service -Name DNS).
* **Analyse des logs** : Examiner les journaux d'événements liés au DNS pour détecter les erreurs spécifiques (Event Viewer).
* **Test de résolution de noms** : Utiliser nslookup pour vérifier la résolution des noms DNS.

**3. Comment sécuriser un serveur DHCP contre les utilisateurs non autorisés :**

* **Activer le filtrage MAC** :
  + Configurer une liste blanche pour n'autoriser que des adresses MAC spécifiques.
* **Segmenter le réseau** :
  + Utiliser des VLANs pour isoler les zones réseau sensibles.
* **Superviser les baux DHCP** :
  + Auditer les adresses IP attribuées et identifier les connexions suspectes.