

# \_\_ Cours Active Directory

---

Ecrit par Youenn DUVAL

Mail: [youenn@barbed.fr](mailto:youenn@barbed.fr)

Linkedin: [Youenn DUVAL](#)

Dernière mise à jour : **02/12/2025**

---

## Table des matières

1. [Active directory et LDAP](#)
2. [C'est quoi un LDAP ?!](#)
3. [OpenLDAP](#)
  1. [Exercice 1](#)
  2. [Faire une recherche avec ldapsearch](#)
  3. [Créer un utilisateur](#)
  4. [Créer des OU](#)
  5. [Créer des Utilisateurs](#)
  6. [Créer un groupe](#)
  7. [Se connecter avec une GUI](#)
4. [Active Directory](#)
  1. [Définition](#)
  2. [Objectifs pour la suite:](#)
  3. [Schéma visé](#)
  4. [Qu'est ce qu'une forêt AD?](#)
  5. [Les machines nécessaires](#)
  6. [Installer un Active Directory \(AD\)](#)
  7. [Vérifier que tout est fonctionnel](#)
  8. [Les interfaces et consoles](#)
  9. [Créer une organisation](#)
  10. [Connecter un deuxième AD](#)
  11. [Connecter un client Windows 11](#)
5. [AD et Powershell](#)
  1. [Exercice 2:](#)
6. [Serveur de fichier](#)
  1. [Exercice 3](#)
  2. [Exercice 4](#)
  3. [Attribution des droits, méthode « AGDLP »](#)
  4. [Exercice 5](#)
7. [Group Policy Object \(GPO\)](#)
  1. [Mise à jour des Policies](#)
  2. [Sauvegarde, copie et importation de GPO](#)
  3. [Gestion et blocage de l'héritage](#)
  4. [Exercice 6](#)

8. [Les profils itinérants](#)
  1. [Exercice 7](#)
9. [Les quotas](#)
10. [Les politiques de sécurité](#)
11. [Les modèles utilisateurs](#)
12. [Les backups](#)
  1. [Utiliser l'outil Windows Server Backup](#)
  2. [Sauvegarde via PowerShell](#)
  3. [Sauvegarde avec les Snapshots \(VM\)](#)
  4. [Configurer une Sauvegarde avec un Logiciel Tiers](#)
    1. [Points clés pour les backups d'AD](#)
5. [La sécurité](#)
  1. [Exercice 8](#)

## Active directory et LDAP

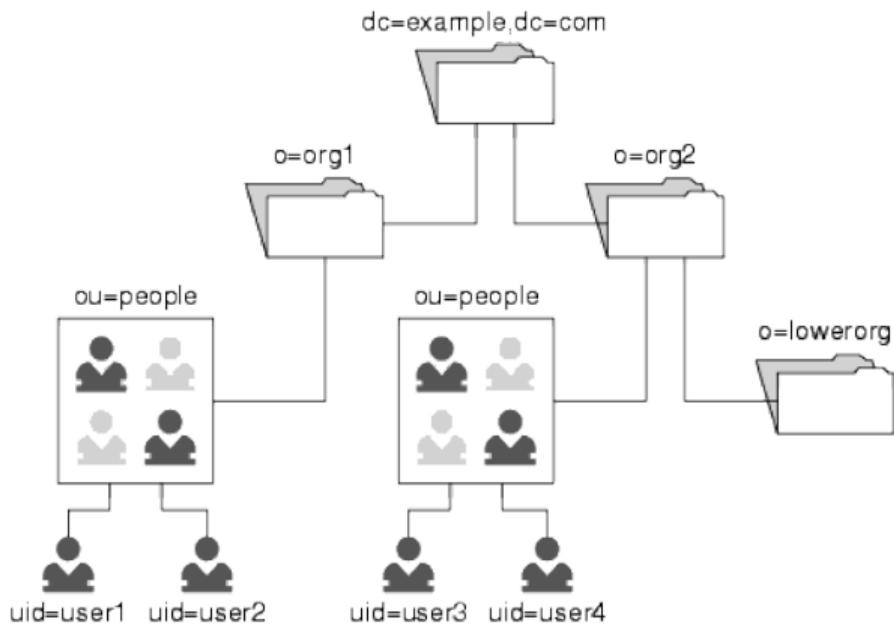
### C'est quoi un LDAP ?!

LDAP (**L**ightweight **D**irectory **A**ccess **P**rotocol) est un protocole permettant d'interroger et de modifier des services d'annuaires distants. Utilisé principalement pour gérer les informations des utilisateurs et des ressources dans les réseaux informatiques, LDAP est couramment employé dans :

- L'authentification des utilisateurs (ex. : connexion à un réseau ou une application)
- La gestion des accès (ex. : autorisations et rôles)
- La centralisation des données d'annuaire (ex. : noms, emails, numéros de téléphone)
- Modèle client-serveur
- Utilisation de Standard / Interopérabilité

Quelques exemples d'utilisation de LDAP :

- **Authentification centralisée** : Utilisé pour authentifier les utilisateurs sur plusieurs applications et services (ex. : connexion unique - SSO).
- **Gestion des accès et des permissions** : Contrôle d'accès aux ressources réseau (ex. : dossiers partagés, imprimantes) en fonction des rôles ou groupes définis dans LDAP.
- **Annuaire d'entreprise** : Répertoire des employés contenant informations de contact, postes, et départements, accessible via des outils internes.
- **Configuration des postes clients** : Chargement automatique des paramètres (ex. : serveur de messagerie, configuration réseau) pour les utilisateurs lors de la connexion.
- **Gestion des accès aux applications web** : Utilisé dans des applications comme Jira, GitLab ou Confluence pour l'authentification des utilisateurs.
- **Annuaire pour messagerie électronique** : Annuaire centralisé des adresses email pour une organisation, permettant un accès rapide aux contacts.



### Avantages :

- Très rapide en lecture
- Facilite la gestion
- Arborescence en annuaire intuitive
- Protocole ancien et robuste
- Scalabilité et réPLICATION
- Un standard de l'industrie

### Inconvénients :

- Lent en écriture
- Gestion difficile à maintenir
- Uniquement de l'annuaire
- Protocole manquant de modernité
- Scalabilité complexe
- De plus en plus délaissé par les applis modernes

### Fonctionnement Général

- **Modèle Client-Serveur** : Le serveur LDAP détient l'annuaire, une base de données hiérarchique ou organisée en arbre contenant des informations, souvent des informations sur les utilisateurs, groupes, et autres ressources informatiques.
- **Sessions** : Les interactions commencent par l'établissement d'une session entre le client et le serveur LDAP. Le client envoie des requêtes, et le serveur répond.
- **Communication** : La communication entre le client et le serveur LDAP utilise généralement le protocole TCP/IP. Le port standard pour LDAP est le port 389, et le port 636 pour LDAP sur SSL (LDAPS).

### Structure de Données et Requêtes

- **Entrées** : Les données dans LDAP sont organisées sous forme d'entrées. Chaque entrée a un identifiant unique, appelé Distinguished Name (DN), et contient un ensemble d'attributs.
- **Attributs** : Chaque entrée contient des attributs, qui sont des paires clé-valeur décrivant quelque chose sur l'entrée, comme un nom d'utilisateur, un mot de passe, une adresse e-mail, etc.
- **Schéma** : Le schéma LDAP définit les types d'objets et d'attributs pouvant être utilisés dans l'annuaire. Il assure la cohérence des données.

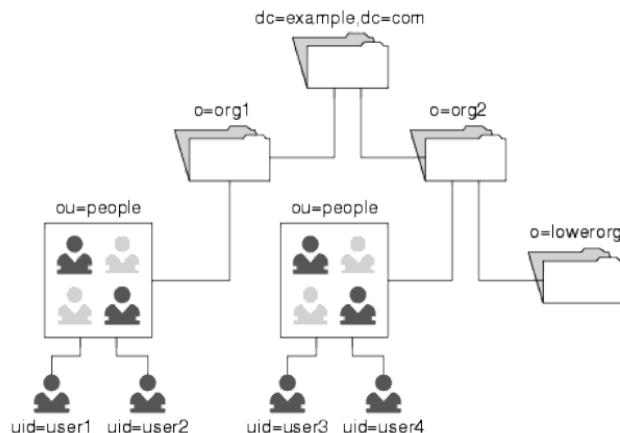
### Types d'Opérations

- **Recherche** : Rechercher des entrées dans l'annuaire en utilisant divers critères de filtrage.
- **Ajout, Suppression, et Modification** : Ajouter, supprimer ou modifier des entrées dans l'annuaire.

- **Comparaison** : Comparer la valeur d'un attribut spécifié dans une entrée.
- **Modification du Mot de Passe** : Opération spécifique pour changer les mots de passe des utilisateurs.

## Sécurité et Authentification

- **Authentification** : Authentification simple (envoi de DN et mot de passe en clair) et authentification SASL (Simple Authentication and Security Layer).
- **Chiffrement** : LDAPS (LDAP over SSL) et StartTLS.
- **Contrôle d'Accès** : Les serveurs LDAP peuvent avoir des mécanismes de contrôle d'accès pour restreindre les opérations que les clients peuvent effectuer.



## Organisation

- **Root domain** : Composant de domaine
- **OU** : Unité d'organisation ou dossier
- **Entrée** : Ici un utilisateur
- **Attributs** : informations générales
- **Attributs Spécifique** : Mot de passe
- **Groupes** : Groupe d'utilisateurs ou de groupes
- **URL** : uid=user4;ou=people;o=org2;dc=example;dc=com

## OpenLDAP

OpenLDAP est une implémentation open-source du protocole LDAP (Lightweight Directory Access Protocol).

### Exercice 1

- Installer OpenLDAP
- Configurer OpenLDAP
- Créer un admin
- Créer des OU
- Créer des utilisateurs
- Créer un groupe
- Se connecter au LDAP

Aide sur une debian 12 :

- sudo apt update
- sudo apt install -y slapd ldap-utils
- sudo dpkg-reconfigure slapd
- Omit ? NO
- Choisir un nom de domaine, ex : test.fr
- Retapez le nom de votre domaine, ex : test
- Tapez votre mot de passe admin

- Remove database ? no
- Move Old Database ? Yes
- Vérifier avec : sudo ldapsearch -Q -L -Y EXTERNAL -H ldapi:/// -b dc=test,dc=fr

Ou, un Vagrantfile

```
Vagrant.configure("2") do |config|
  # Configuration de la VM
  config.vm.box = "debian/bullseye64"
  config.vm.provider "virtualbox" do |vb|
    vb.name = "Debian-OpenLDAP"
    vb.memory = 512
    vb.cpus = 1
  end

  # Réseau : accès depuis l'hôte via une adresse IP privée
  config.vm.network "private_network", ip: "192.168.56.10"

  # Nom d'hôte de la VM
  config.vm.hostname = "debian-ldap"

  # Provisionnement pour installer OpenLDAP sans interaction
  config.vm.provision "shell", inline: <<-SHELL
    # Mise à jour des paquets et installation de vim
    export DEBIAN_FRONTEND=noninteractive
    apt-get update
    apt-get upgrade -y
    apt-get install -y vim slapd ldap-utils

    # Configuration automatique d'OpenLDAP sans invite interactive
    echo "slapd slapd/no_configuration boolean false" | debconf-set-selections
    echo "slapd slapd/internal/adminpw password admin" | debconf-set-selections
    echo "slapd slapd/internal/generated_adminpw password admin" | debconf-set-selections
    echo "slapd slapd/password2 password admin" | debconf-set-selections
    echo "slapd slapd/password1 password admin" | debconf-set-selections
    echo "slapd slapd/domain string example.com" | debconf-set-selections
    echo "slapd shared/organization string ExampleOrg" | debconf-set-selections

    # Reconfiguration silencieuse de slapd
    dpkg-reconfigure -f noninteractive slapd

    # Activer et démarrer le service OpenLDAP
    systemctl enable slapd
    systemctl start slapd

    # Vérification du service LDAP
    ldapsearch -x -H ldap://localhost -b dc=example,dc=com
  SHELL
end
```

## Faire une recherche avec ldapsearch

ldapsearch -Q -L -Y EXTERNAL -H ldapi:/// -b dc=example,dc=com  
Permet d'effectuer un recherche  
-Q : Mode silencieux pour le log  
-L : Reponse au format ldif  
-Y EXTERNAL : permet de se log avec le compte de la machine (uid)  
-H : type d'URI  
-b : nœud pour la recherche

## Créer un utilisateur

- Il faut créer un fichier ldif avec les différents paramètres
- Insérer ce fichier dans le serveur openldap  
Fichier admin.ldif

```
dn: cn=admin,dc=example,dc=com
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword: motdepasse
```

- Insérer avec : sudo ldapadd -x -D "cn=admin,dc=example,dc=com" -W -f admin.ldif
- Tester la connexion avec : ldapwhoami -x -D "cn=admin,dc=example,dc=com" -W

## Créer des OU

- Il faut créer un fichier ldif avec les différents paramètres
- Insérer ce fichier dans le serveur openldap  
Fichier : structure.ldif

```
#Ajouter l'OU 'utilisateurs'
dn: ou=utilisateurs,dc=example,dc=com
objectClass: organizationalUnit
ou: utilisateurs
description: Unité organisationnelle pour les utilisateurs

#Ajouter l'OU 'ordinateurs'
dn: ou=ordinateurs,dc=example,dc=com
objectClass: organizationalUnit
ou: ordinateurs
description: Unité organisationnelle pour les ordinateurs
```

Insérer avec : sudo ldapadd -x -D "cn=admin,dc=example,dc=com" -W -f structure.ldif

## Créer des Utilisateurs

- Il faut créer un fichier ldif avec les différents paramètres
- Insérer ce fichier dans le serveur openldap  
Fichier : utilisateurs.ldif

```
#Alice Durand
dn: cn=Alice Durand,ou=utilisateurs,dc=example,dc=com
objectClass: inetOrgPerson
cn: Alice Durand
sn: Durand
userPassword: motdepasseAlice
mail: alice@test.fr
telephoneNumber: +33000000001
```

```
#Bob Dupont
dn: cn=Bob Dupont,ou=utilisateurs,dc=example,dc=com
objectClass: inetOrgPerson
cn: Bob Dupont
sn: Dupont
userPassword: motdepasseBob
```

```
mail: bob@test.fr  
telephoneNumber: +33000000002
```

Inserer avec : sudo ldapadd -x -D "cn=admin,dc=example,dc=com" -W -f utilisateurs.ldif

## Créer un groupe

- Il faut créer un fichier ldif avec les différents paramètres
- Insérer ce fichier dans le serveur openldap

Fichier : groupe.ldif

```
dn: cn=comptabilite,ou=utilisateurs,dc=example,dc=com  
objectClass: groupOfNames  
cn: comptabilite  
description: Groupe pour l'équipe de comptabilité  
member: cn=Alice Durand,ou=utilisateurs,dc=example,dc=com  
member: cn=Bob Dupont,ou=utilisateurs,dc=example,dc=com
```

Inserer avec : sudo ldapadd -x -D "cn=admin,dc=example,dc=com" -W -f groupe.ldif

## Se connecter avec une GUI

Exemple :

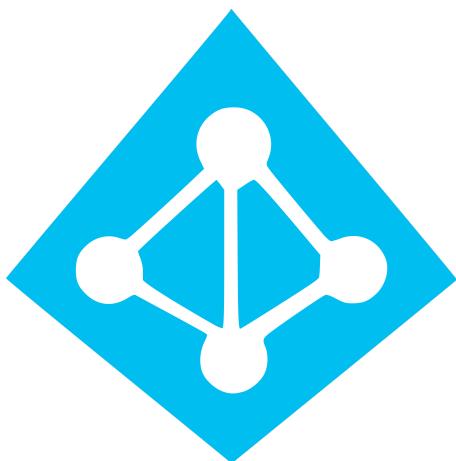
- « LDAP Admin » pour windows
- « JXplorer » pour linux

En ligne de commande :

- sudo ldapsearch -Q -L -Y EXTERNAL -H ldapi:/// -b dc=example,dc=com

	Attribute	Value	Type	Size
	objectClass	inetOrgPerson	Text	13
	cn	Alice Durand	Text	12
	sn	Durand	Text	6
	mail	alice@test.fr	Text	13
	telephoneNumber	+3300000001	Text	11

## Active Directory



## Définition

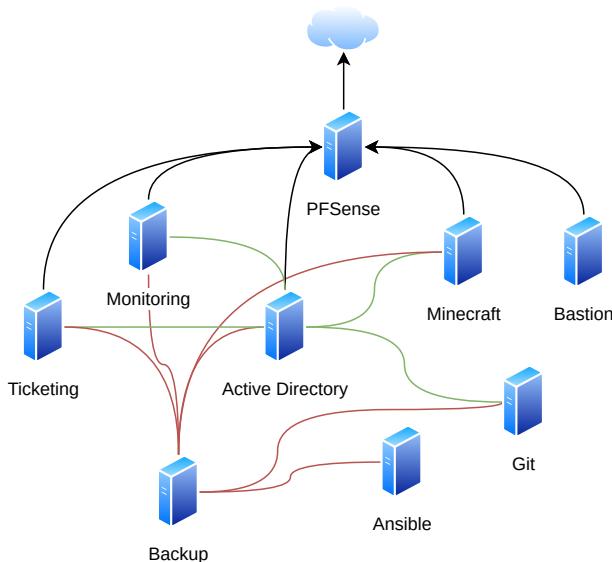
- Service d'annuaire de Microsoft
- Compatible avec le protocole LDAP
- Gestion des utilisateurs, ordinateurs, groupes etc.
- Systèmes de réplication et haute disponibilité
- Organisation et schéma LDAP Spécifique à l'écosystème Windows

- Politiques de groupes (Group Policy)
- Gestion authentification spécifique (kerberos)

## Objectifs pour la suite:

- Mettre en place une forêt AD
- Créer un groupe et utilisateur
- Connecter et manager des machines clients W10/11
- Gestion des fichiers et partages
- Powershell et scripting
- GPO
- Sécurité et bonnes pratiques

## Schéma visé



## Qu'est ce qu'une forêt AD?

Structure de sécurité de plus haut niveau dans l'architecture d'Active Directory de Microsoft. Elle représente la somme de plusieurs domaines AD qui partagent un schéma commun (structure de base de données), une configuration globale, et une relation de confiance entre eux. Une forêt agit comme un conteneur sécurisé pour l'ensemble des domaines, permettant une gestion centralisée des utilisateurs, des groupes, des politiques, et des ressources sur tous les domaines inclus. Chaque forêt est une instance complètement isolée d'Active Directory, fournissant un niveau élevé de sécurité et d'isolation par rapport à d'autres forêts.

## Les machines nécessaires

Pour le TP complet il vous faut 3 machines:

- 2 serveurs Win2022
- 1 machine Win11 Pro

Vous pouvez les installer en manuel mais vous pouvez aussi utiliser le Vagrantfile suivant:

```
Vagrant.configure("2") do |config|
  config.vm.define "ad1" do |ad1|
    ad1.vm.box = "gusztavvargadr/windows-server-2022-standard"
    ad1.vm.box_version = "2102.0.2409"
    ad1.vm.provider :virtualbox do |v|
      v.customize ["modifyvm", :id, "--memory", 2048]
      v.customize ["modifyvm", :id, "--cpus", 2]
      v.customize ["modifyvm", :id, "--name", "Windows-ad1"]
    end
  end
end
```

```

ad1.vm.network "private_network", ip: "192.168.51.2"
ad1.vm.provision "shell", inline: <<-SHELL
  powershell Set-WinUILanguageOverride -Language "fr-FR"
  powershell Set-WinSystemLocale -SystemLocale "fr-FR"
  powershell Set-WinUserLanguageList -LanguageList "fr-FR" -Force
  powershell -command "New-NetIPAddress -InterfaceAlias 'Ethernet 2' -IPAddress
'192.168.51.2'"
SHELL
end

config.vm.define "ad2" do |ad2|
  ad2.vm.box = "gusztavvargadr/windows-server-2022-standard"
  ad2.vm.box_version = "2102.0.2409"
  ad2.vm.hostname = "RW-AD2"
  ad2.vm.provider :virtualbox do |v|
    v.customize ["modifyvm", :id, "--memory", 2048]
    v.customize ["modifyvm", :id, "--cpus", 2]
    v.customize ["modifyvm", :id, "--name", "Windows-ad2"]
  end
  ad2.vm.network "private_network", ip: "192.168.51.3"
  ad2.vm.provision "shell", inline: <<-SHELL
    powershell Set-WinUILanguageOverride -Language "fr-FR"
    powershell Set-WinSystemLocale -SystemLocale "fr-FR"
    powershell Set-WinUserLanguageList -LanguageList "fr-FR" -Force
    powershell -command "New-NetIPAddress -InterfaceAlias 'Ethernet 2' -IPAddress
'192.168.51.3'"
SHELL
end

config.vm.define "w11" do |w11|
  w11.vm.box = "gusztavvargadr/windows-11-22h2-enterprise"
  w11.vm.box_version = "2202.0.2409"
  w11.vm.provider :virtualbox do |v|
    v.customize ["modifyvm", :id, "--memory", 2048]
    v.customize ["modifyvm", :id, "--cpus", 2]
    v.customize ["modifyvm", :id, "--name", "Windows-w11"]
  end
end

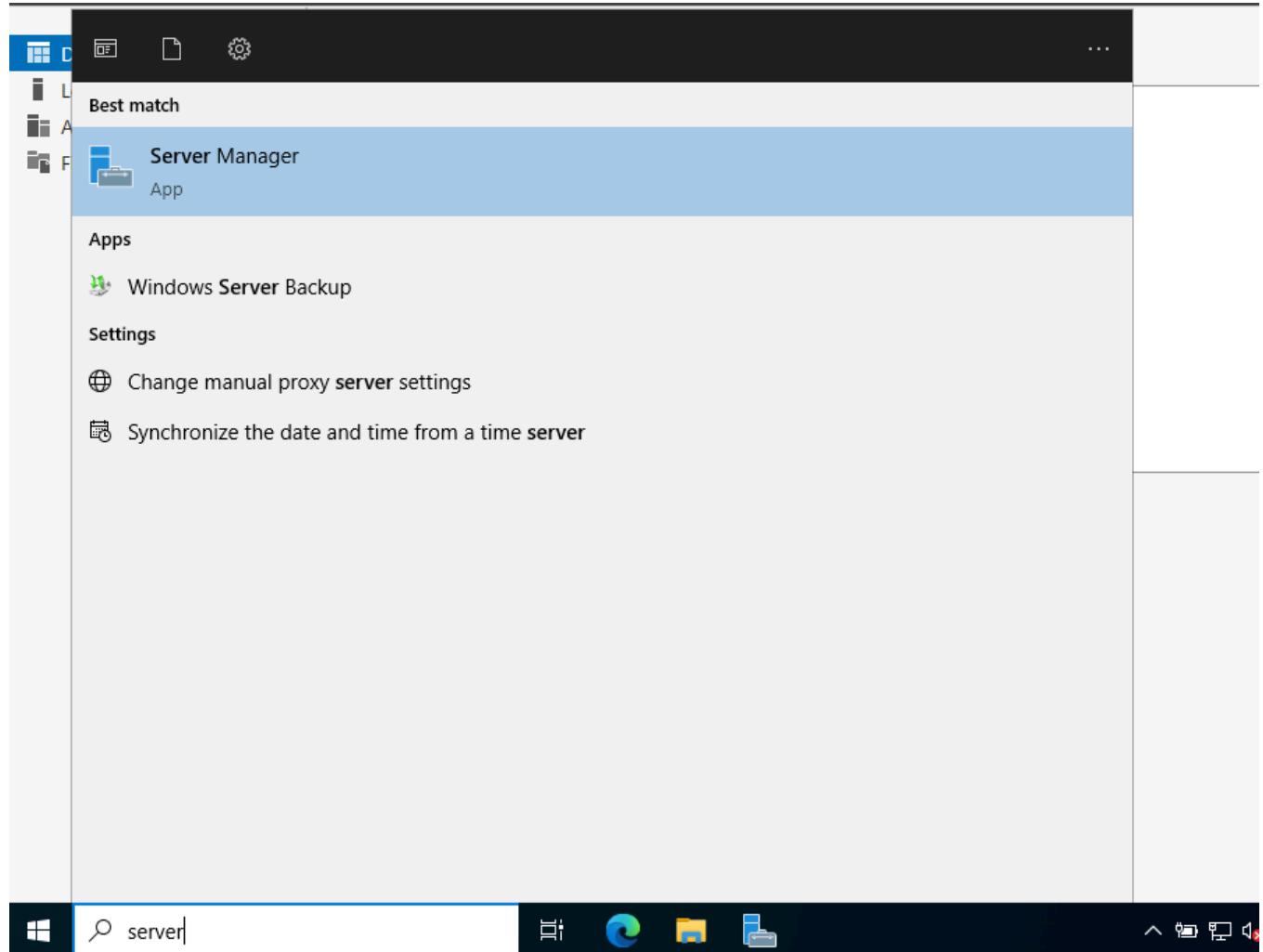
```

## Installer un Active Directory (AD)

### Les prérequis :

- IP FIXE : Il a le rôle de serveur DNS donc il doit être accessible à une adresse fixe
- Préparer un nom de domaine : Il doit être unique, pleinement qualifié (FQDN), ne doit pas être un domaine public, il doit être non routable.

## Lancer le Serveur Manager

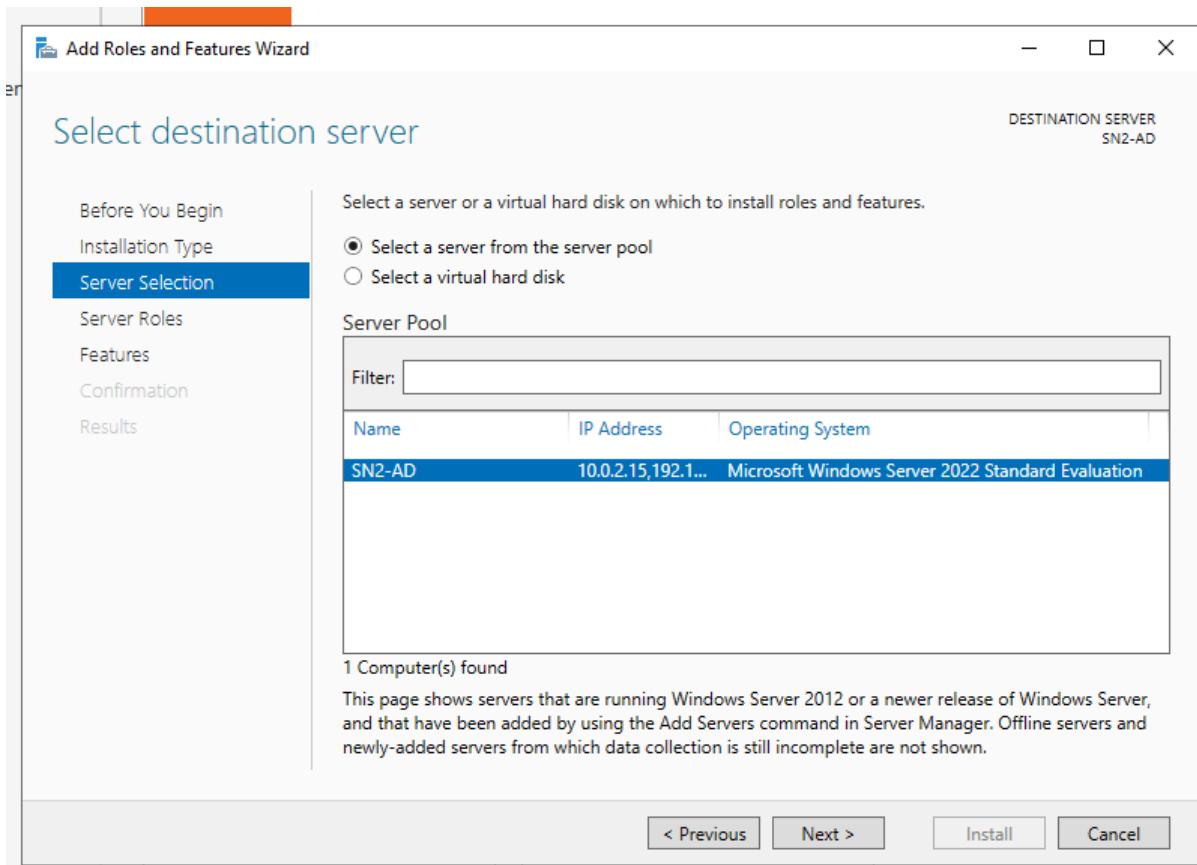


Ajouter un Rôle:

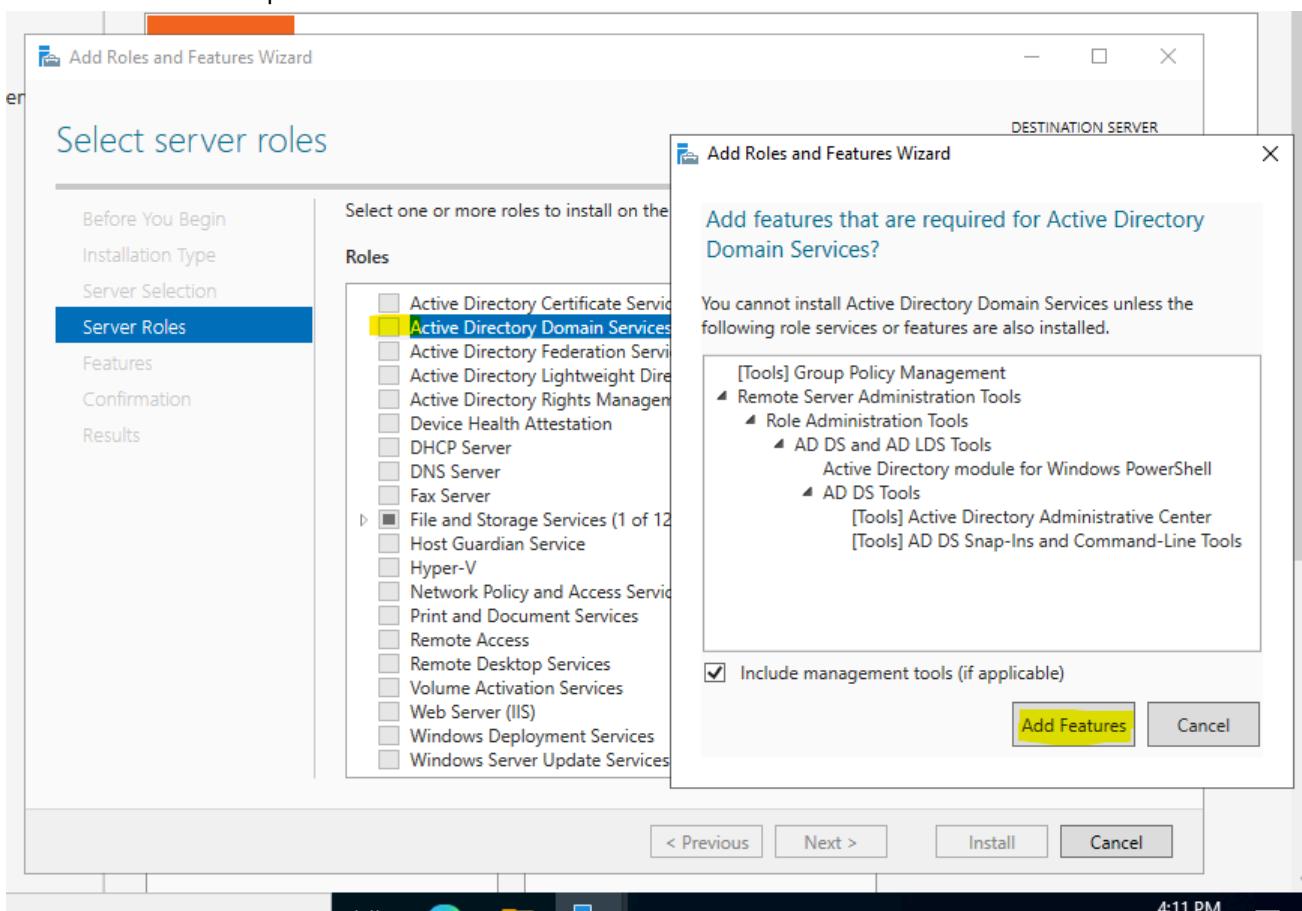
The screenshot shows the "Server Manager" dashboard. The left sidebar has "Dashboard" selected, along with "Local Server", "All Servers", and "File and Storage Services". The main area is titled "WELCOME TO SERVER MANAGER" and features a "QUICK START" section with five numbered steps: 1. Configure this local server, 2. Add roles and features, 3. Add other servers to manage, 4. Create a server group, and 5. Connect this server to cloud services. A "WHAT'S NEW" section and a "LEARN MORE" button are also present. On the right, a "Manage" dropdown menu is open, showing options like "Add Roles and Features" (which is highlighted), "Remove Roles and Features", "Add Servers", "Create Server Group", and "Server Manager Properties". At the bottom, there's a "ROLES AND SERVER GROUPS" section showing one role and one server group, each with their respective details.

File and Storage Services	1
Manageability	
Events	
Performance	

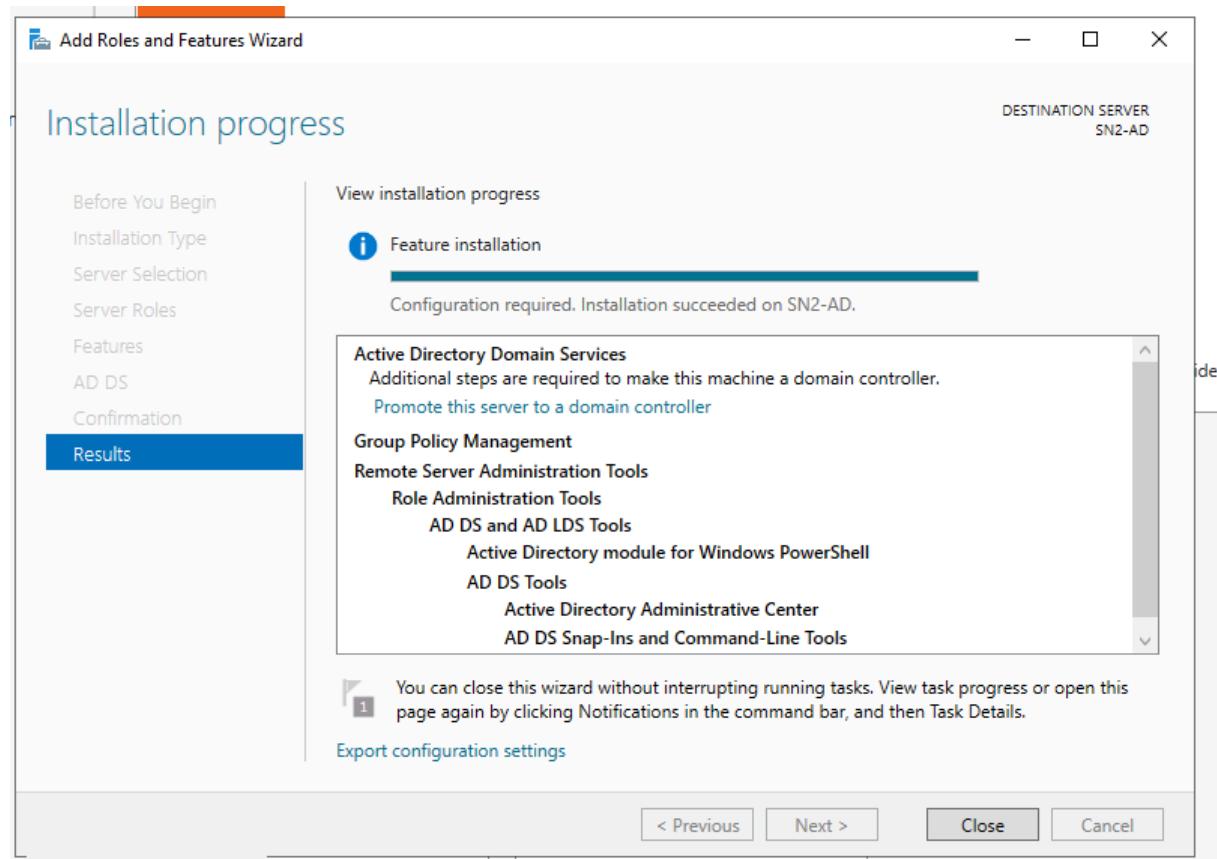
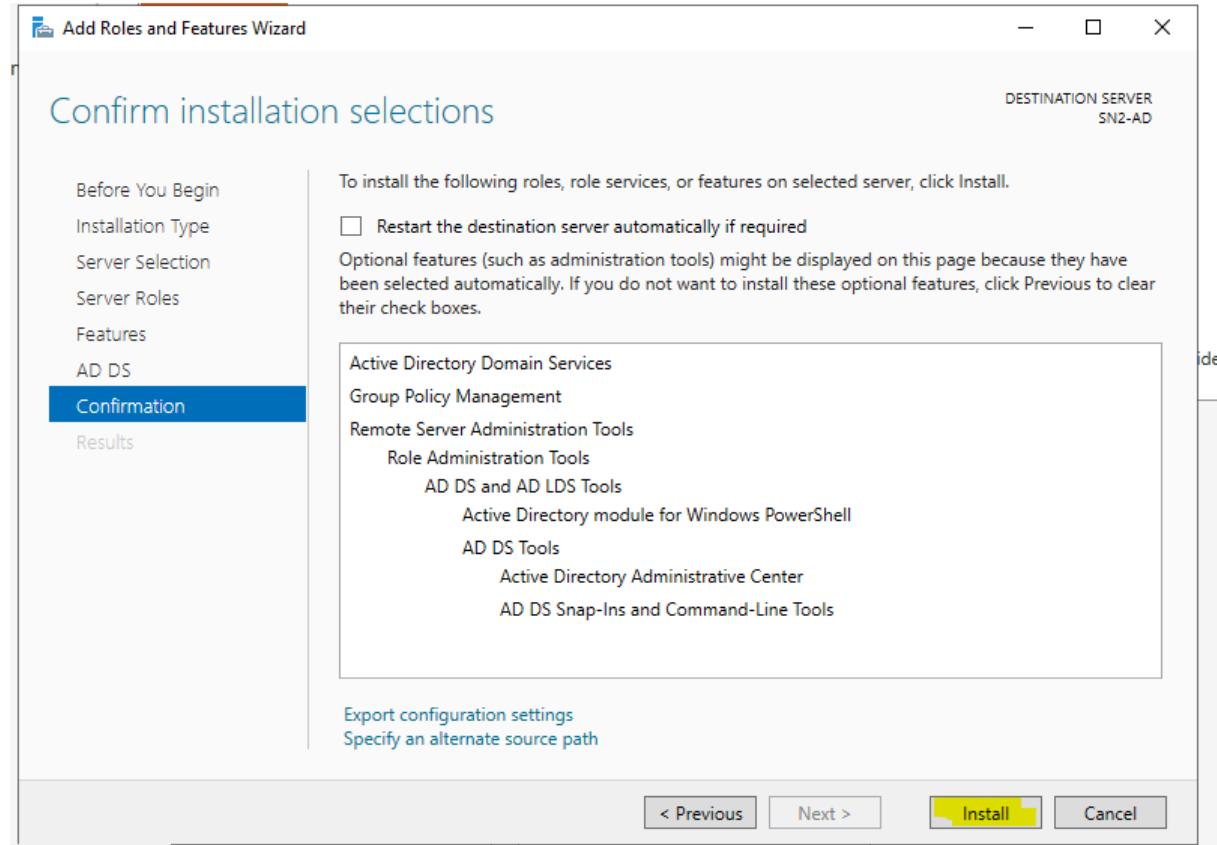
Local Server	1
Manageability	
Events	
Services	



Valider le Rôle et ses options:



## Installation en cours



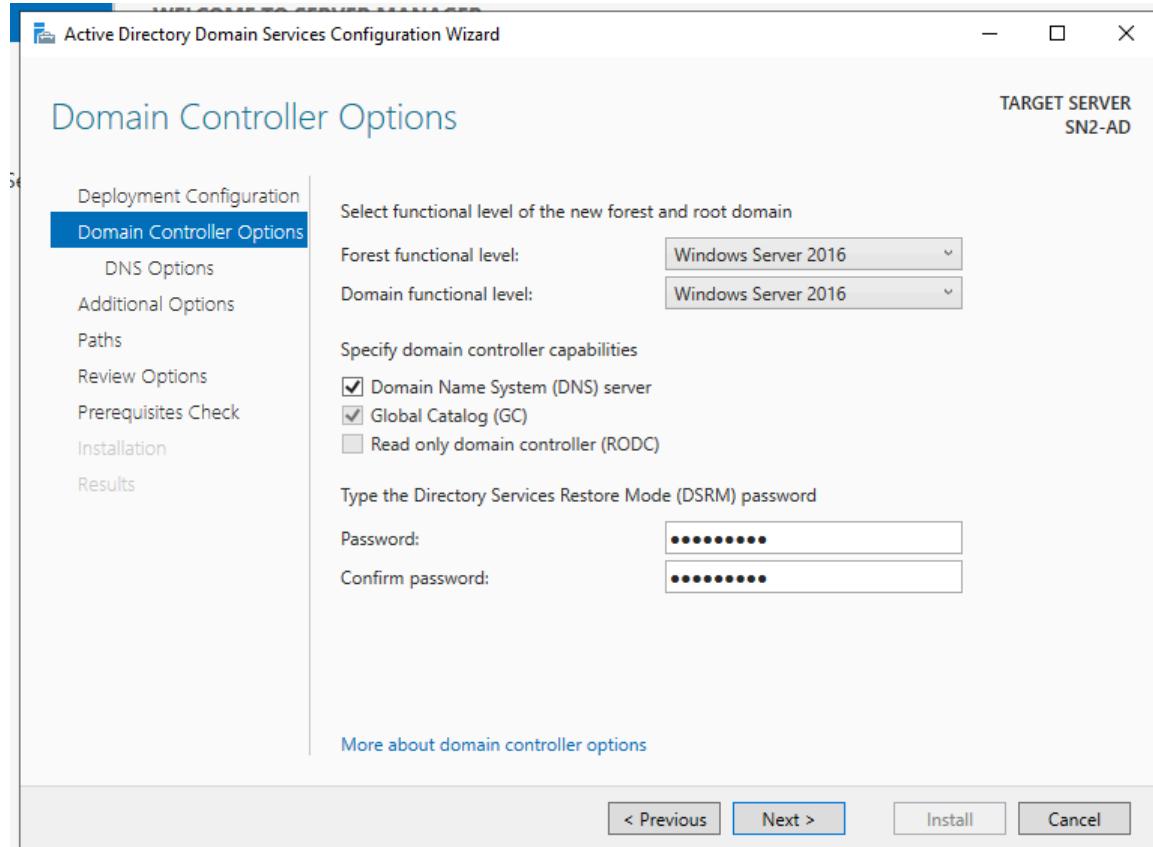
Promouvoir Contrôleur de domaine principale:

The screenshot shows the Windows Server Manager Dashboard. A prominent yellow warning icon with an exclamation mark is circled in red at the top right. A callout bubble points to the message "Post-deployment Configuration" which says "Promote this server to a domain controller". Below it, another message indicates "Feature installation" was successful. The dashboard also features sections for "QUICK START", "WHAT'S NEW", and "LEARN MORE".

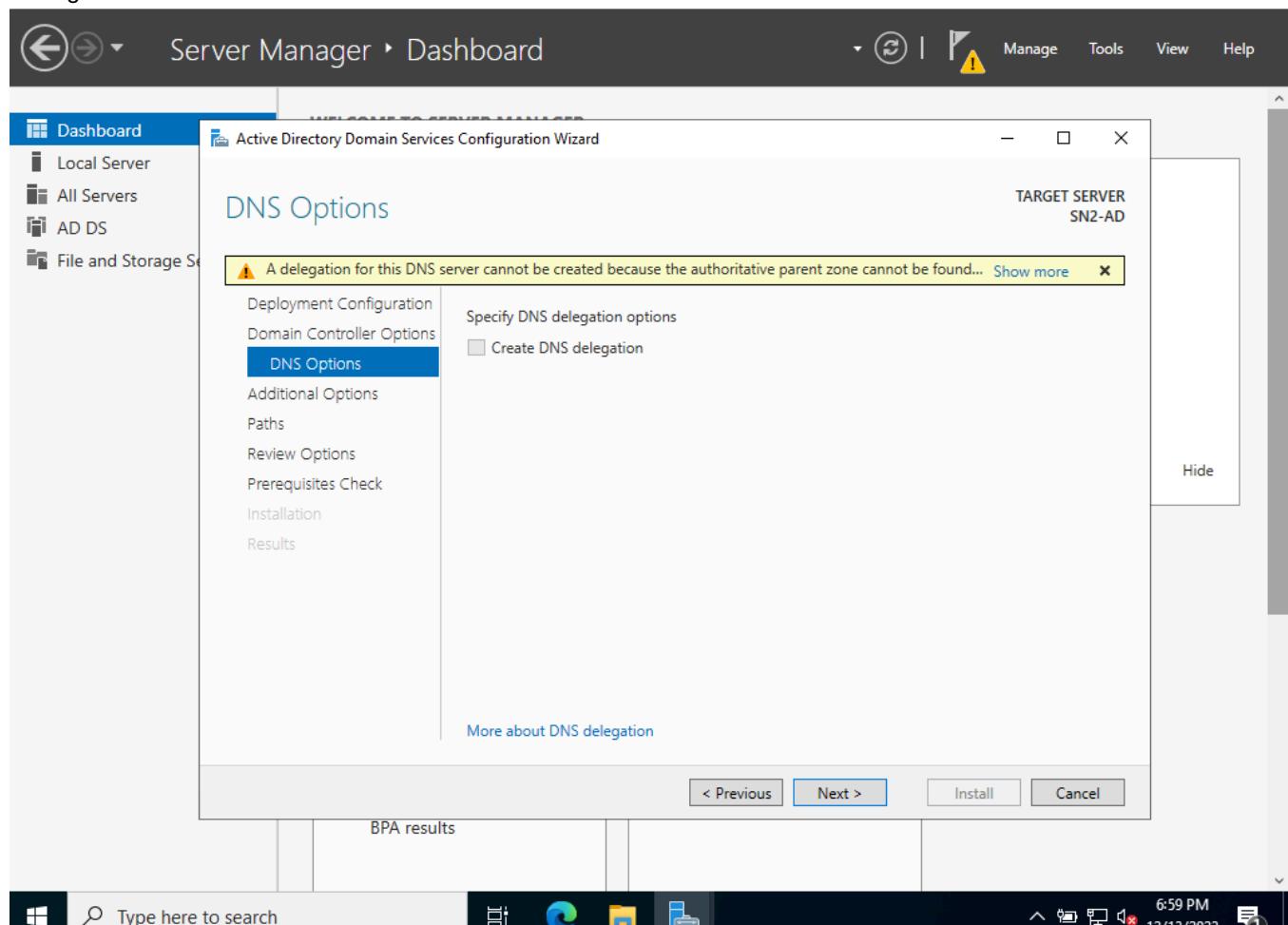
Configuration du Domaine Racine:

The screenshot shows the "Active Directory Domain Services Configuration Wizard" window. The title bar reads "Deployment Configuration". On the left, a navigation pane lists steps: Deployment Configuration, Domain Controller Options, Additional Options, Paths, Review Options, Prerequisites Check, Installation, and Results. The main area shows the "TARGET SERVER SN2-AD". It asks to "Select the deployment operation" with three options: "Add a domain controller to an existing domain", "Add a new domain to an existing forest", and "Add a new forest". The third option is selected. It then asks to "Specify the domain information for this operation" with a "Root domain name" field containing "remoteworks.local". At the bottom, there are buttons for "< Previous", "Next >", "Install", and "Cancel".

## Choix du niveau fonctionnel et du mot de passe de restauration



## Configuration du serveur DNS

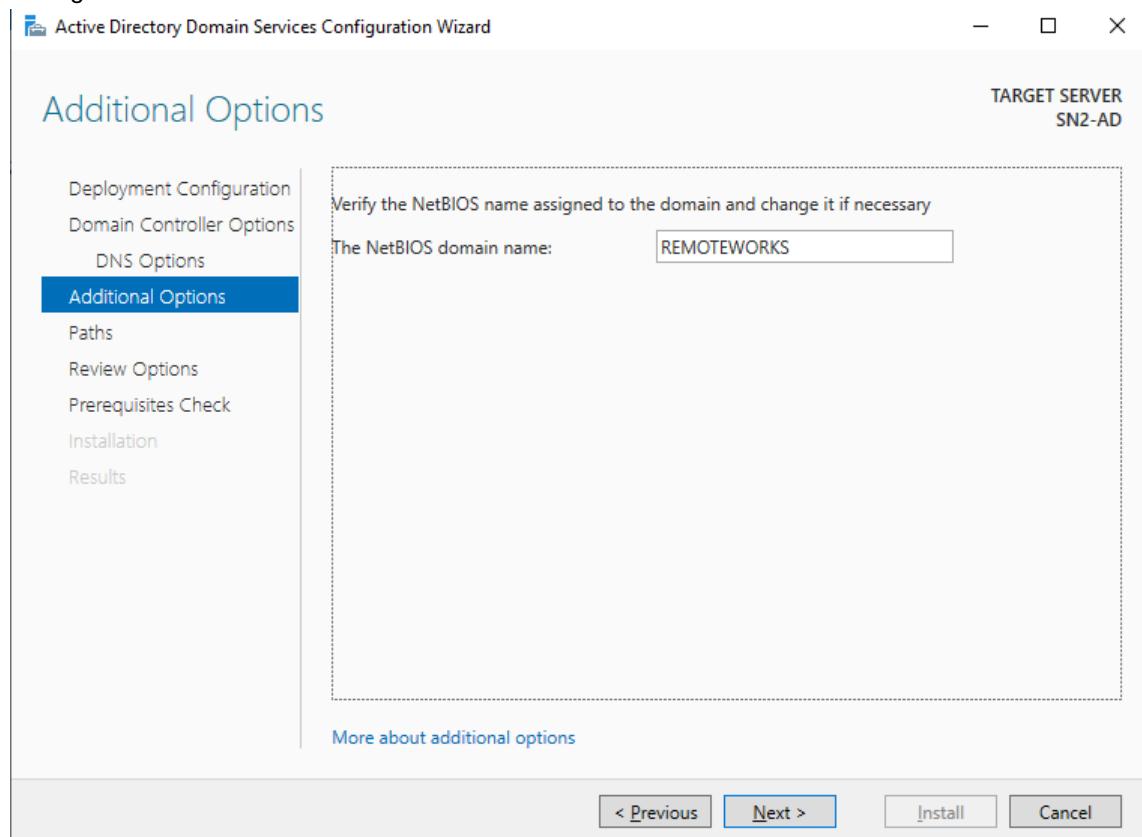


### Note

Un domaine a toujours son serveur DNS!

- Il fait la relation de tous les noms de domaines enfant du root avec les IP des machines et services.
- Il doit être joignable par toutes les machines du domaine.

## Configuration du nom NETBIOS

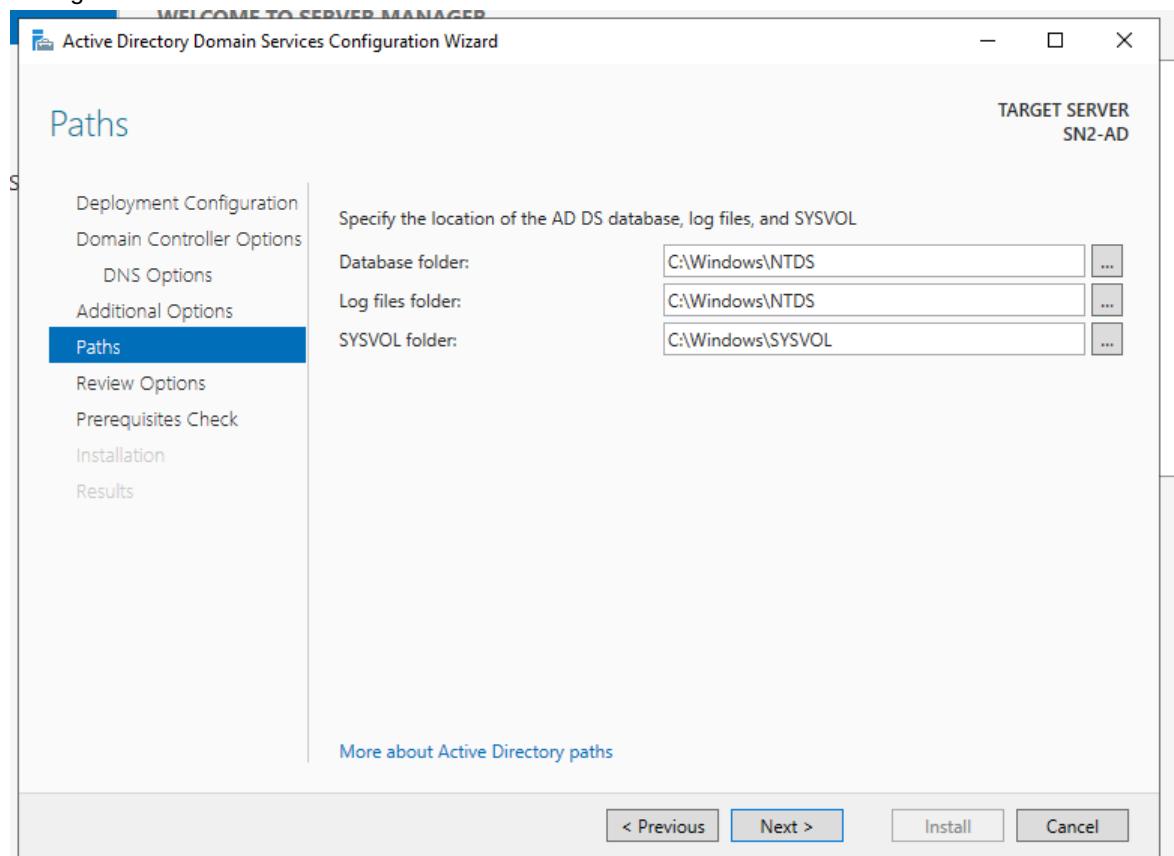


### Note

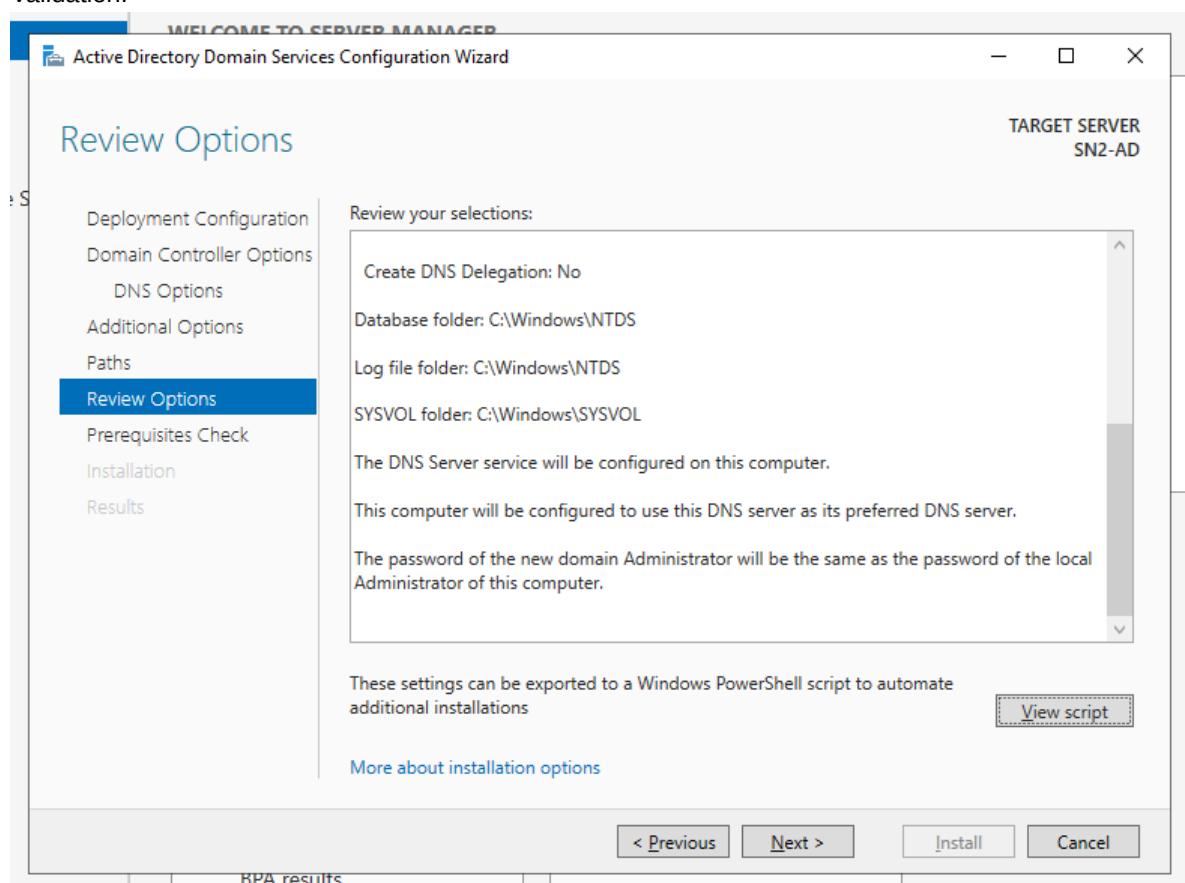
Netbios est un protocol ancien (années 80)

- Il est utilisé pour faciliter les échanges entre machines sur un même LAN
- Il est présent de façon historique

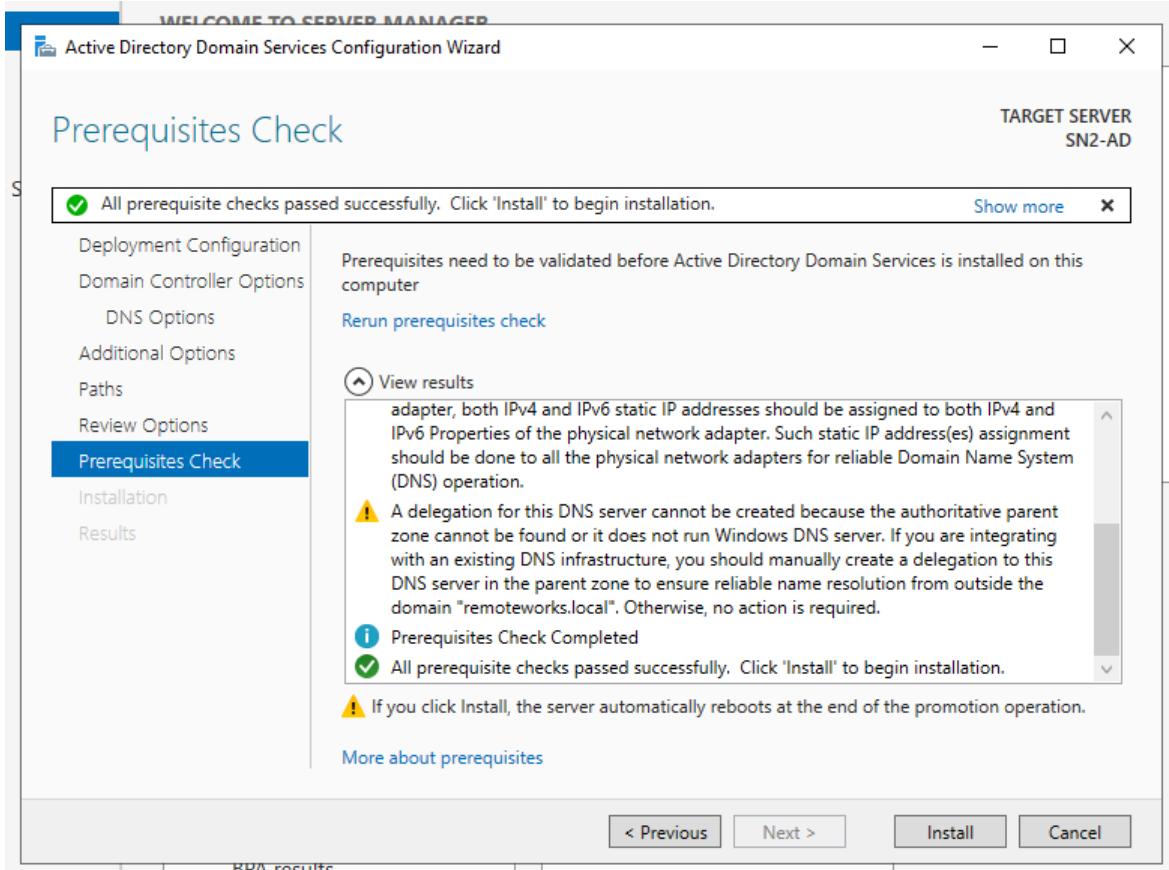
## Configuration des PATHS



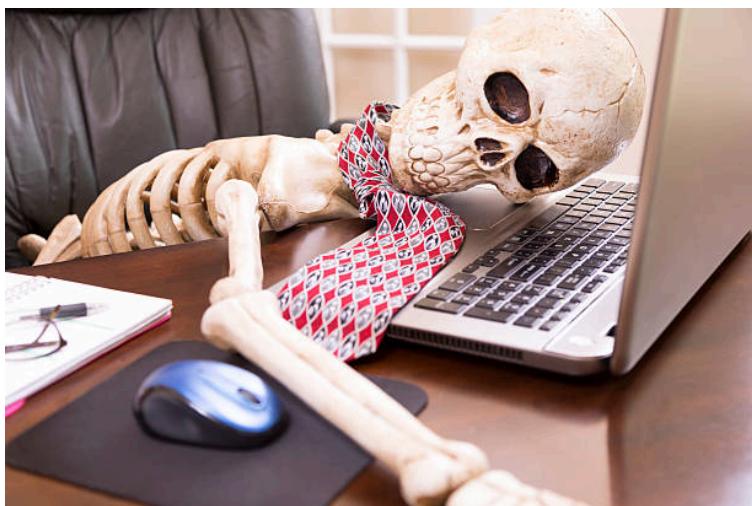
## Validation:



Vérification des prérequis:



On reboot:



## Vérifier que tout est fonctionnel

Verifier que tous les services sont installés

- Get-Service adws,kdc,netlogon,dns  
Récuperer les détails du contrôleur de domaine
- Get-ADDomainController  
Récuperer les détail du domaine
- Get-ADDomain remoteworks.local

## Les interfaces et consoles

Les outils:

The screenshot shows the Windows Server Manager Dashboard. On the left, a navigation bar includes links for Dashboard, Local Server, All Servers, AD DS, DNS, and File and Storage Services. The main area features a "WELCOME TO SERVER MANAGER" section with a "QUICK START" panel containing five numbered steps: 1. Configure this local server, 2. Add roles and features, 3. Add other servers to manage, 4. Create a server group, and 5. Connect this server to cloud. Below this is a "ROLES AND SERVER GROUPS" section showing 3 roles and 1 server group. A large list of management tools is on the right, including Active Directory Administrative Center, Active Directory Domains and Trusts, Active Directory Module for Windows PowerShell, Active Directory Sites and Services, Active Directory Users and Computers, ADSI Edit, Component Services, Computer Management, Defragment and Optimize Drives, Disk Cleanup, DNS, Event Viewer, Group Policy Management, iSCSI Initiator, Local Security Policy, Microsoft Azure Services, ODBC Data Sources (32-bit), ODBC Data Sources (64-bit), Performance Monitor, Recovery Drive, Registry Editor, Resource Monitor, Services, System Configuration, System Information, Task Scheduler, Windows Defender Firewall with Advanced Security, Windows Memory Diagnostic, and Windows PowerShell.

## Active directory Users and Computers

The screenshot shows the Active Directory Users and Computers console. The left pane displays a tree view of the Active Directory structure under "remoteworks.local". The right pane lists users and groups with columns for Name, Type, and Description. The list includes:

Name	Type	Description
Administrator	User	Built-in account for ad...
Allowed RODC Password Replicatio...	Security Group...	Members in this group c...
Cert Publishers	Security Group...	Members of this group ...
Cloneable Domain Controllers	Security Group...	Members of this group t...
Denied RODC Password Replication...	Security Group...	Members in this group c...
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateProxy	Security Group...	DNS clients who are per...
Domain Admins	Security Group...	Designated administrato...
Domain Computers	Security Group...	All workstations and ser...
Domain Controllers	Security Group...	All domain controllers i...
Domain Guests	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise Admins	Security Group...	Designated administrato...
Enterprise Key Admins	Security Group...	Members of this group ...
Enterprise Read-only Domain Contr...	Security Group...	Members of this group ...
Group Policy Creator Owners	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...
Key Admins	Security Group...	Members of this group ...
Protected Users	Security Group...	Members of this group ...
RAS and IAS Servers	Security Group...	Servers in this group can...
Read-only Domain Controllers	Security Group...	Members of this group ...
Schema Admins	Security Group...	Designated administrato...
vagrant	User	Vagrant

## DNS

Fichier Machine Écran Entrée Périphériques Aide

DNS Manager

File Action View Help

Back Forward Home Refresh Stop Find Copy Paste

Name	Type	Data	Timestamp
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[26], sn2-ad.remoteworks....	static
(same as parent folder)	Name Server (NS)	sn2-ad.remoteworks.local.	static
(same as parent folder)	Host (A)	10.0.2.15	12/13/2023 7:00:00 PM
(same as parent folder)	Host (A)	192.168.51.2	12/13/2023 7:00:00 PM
sn2-ad	Host (A)	192.168.51.2	static
sn2-ad	Host (A)	10.0.2.15	static

## Group Policy Management

Group Policy Management

File Action View Window Help

Back Forward Home Refresh Stop Find Copy Paste

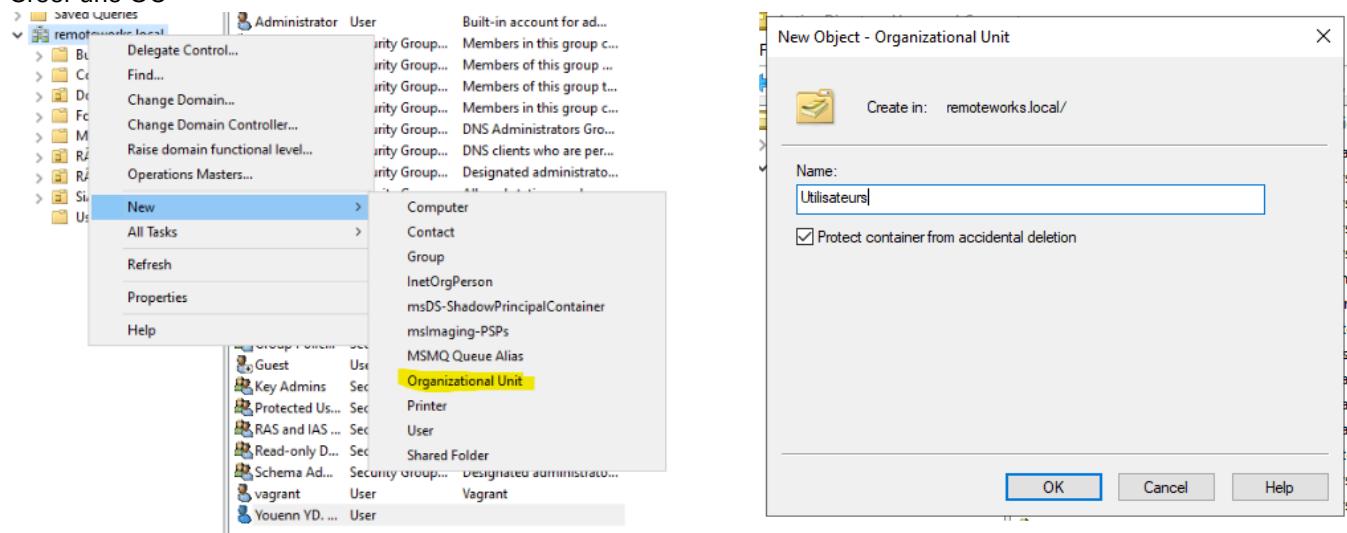
Name
Forest: remoteworks.local

# Créer une organisation

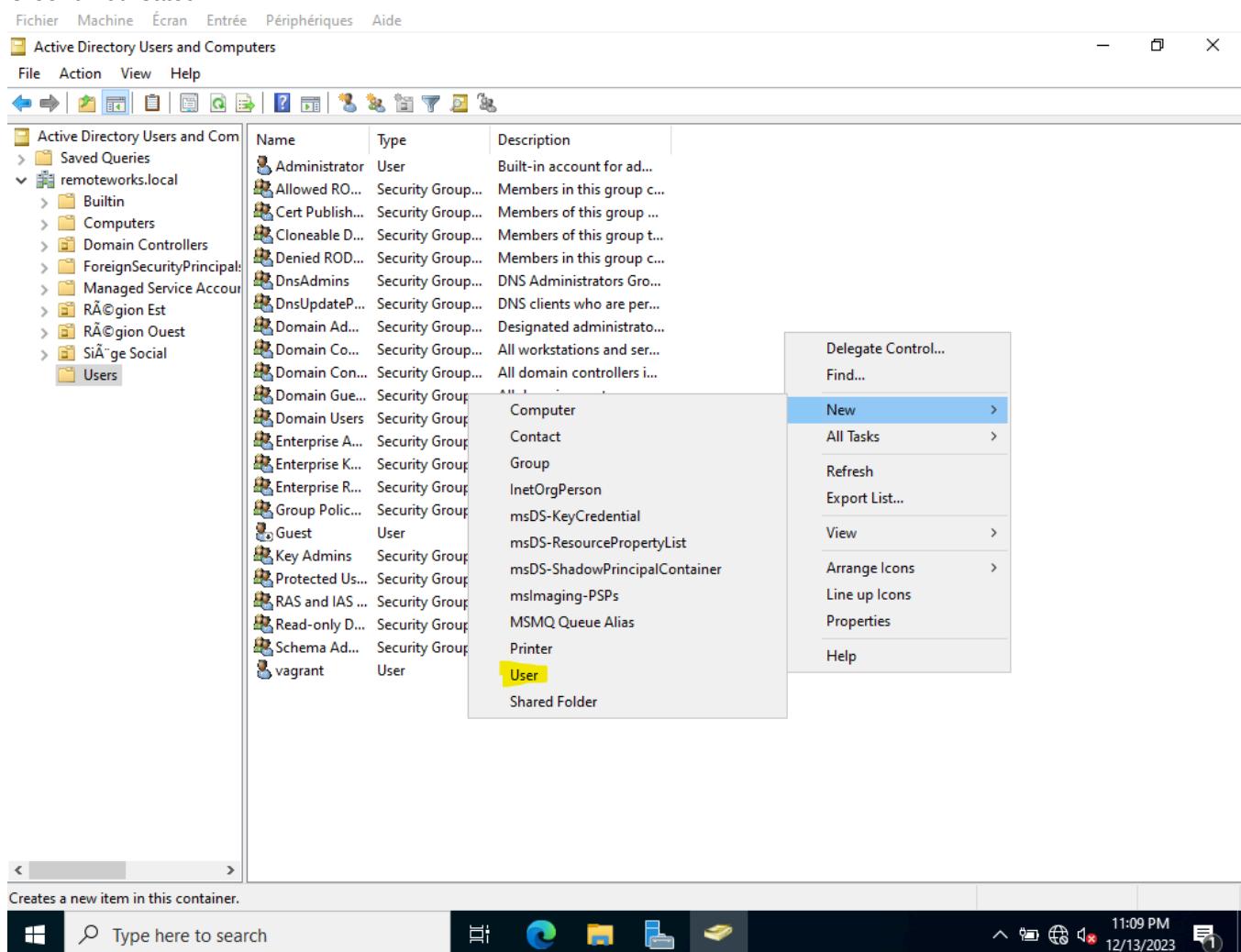
Résumé:

- Créer une OU : Utilisateurs
- Créer un utilisateur : Youenn DUVAL
- Changer le mot de passe de l'utilisateur
- Ajouter l'utilisateur au groupe d'administrateur du domaine
- Verrouillage
- Recherche dans AD

## Créer une OU



## Créer un utilisateur



New Object - User

Create in: remoteworks.local/Users

First name: Youenn Initials: YD

Last name: Duvql

Full name: Youenn YD. Duvql

User logon name:  
youenn @remoteworks.local

User logon name (pre-Windows 2000):  
REMOTEWORKS\ youenn

< Back Next > Cancel

New Object - User

Create in: remoteworks.local/Users

Password:  Confirm password:

User must change password at next logon  
 User cannot change password  
 Password never expires  
 Account is disabled

< Back Next > Cancel

New Object - User

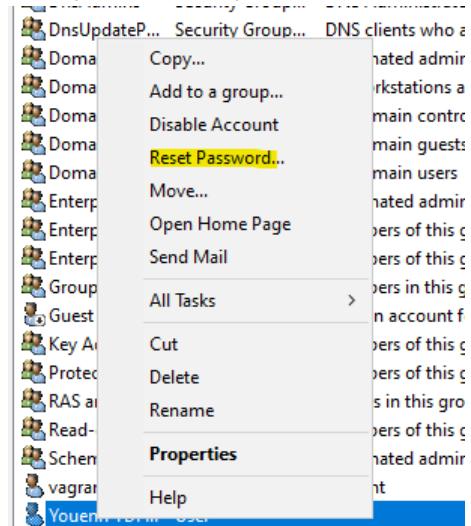
Create in: remoteworks.local/Users

When you click Finish, the following object will be created:

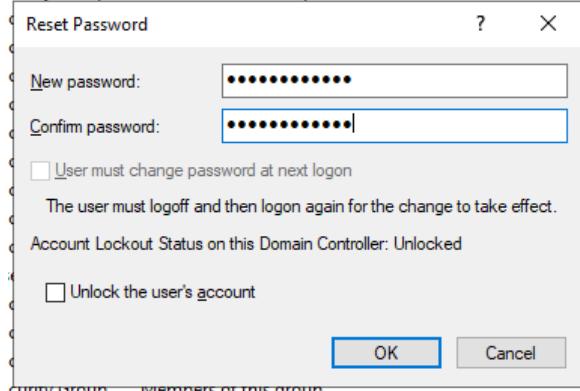
Full name: Youenn YD. Duvql  
User logon name: youenn@remoteworks.local  
The password never expires.

< Back Finish Cancel

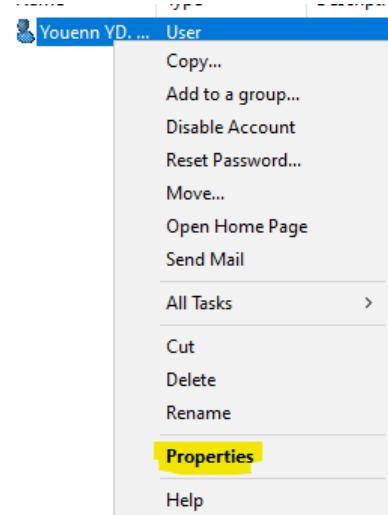
## Changer un mot de passe Utilisateur

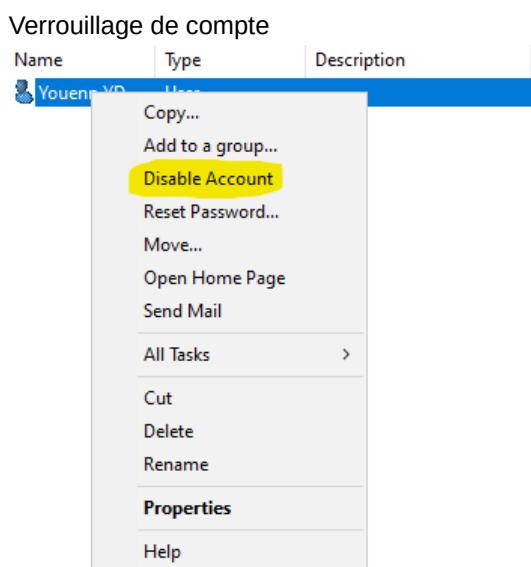
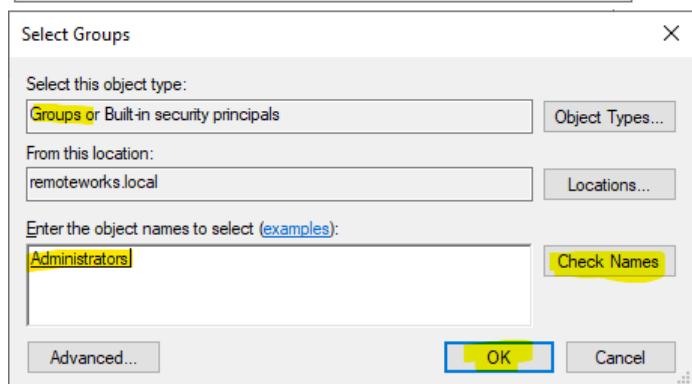
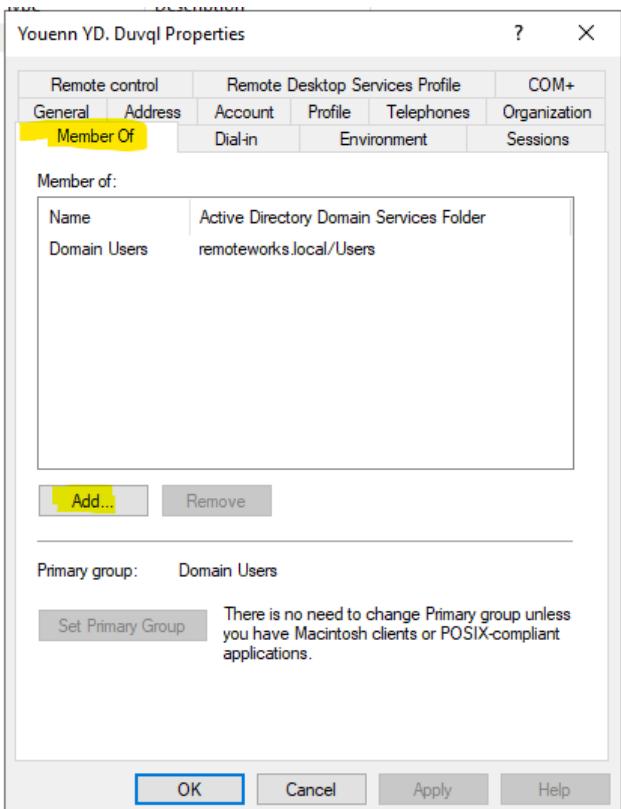


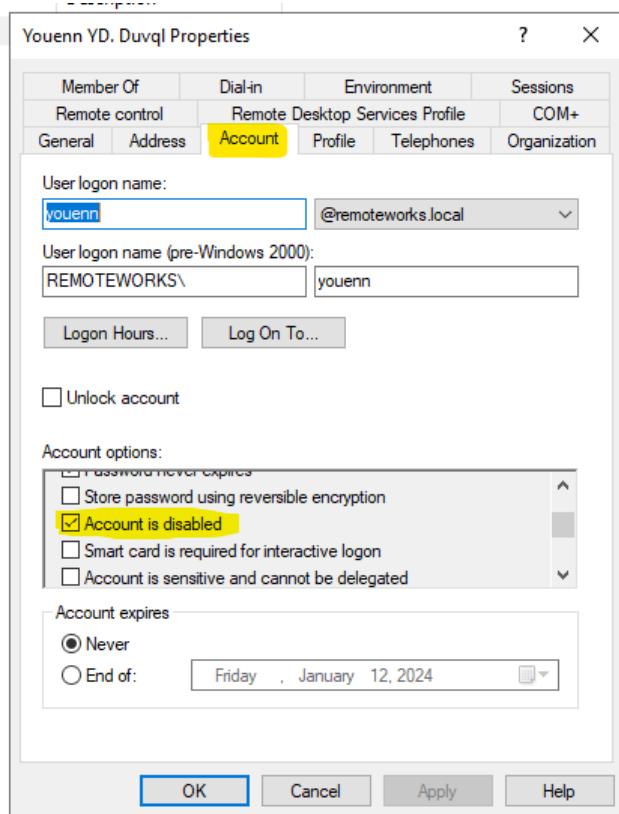
curry group... DNS clients who are per...



## Ajouter l'utilisateur au groupe d'administrateur du domaine







## Rechercher dans l'AD

The screenshot shows the Active Directory Users and Computers interface. On the left, the navigation pane shows the tree structure of the domain: Active Directory Users and Com, Saved Queries, remoteworks.local (with subfolders like BuiltIn, Computers, Domain Controllers, ForeignSecurityPrincipal, Managed Service Account, Région Est, Région Ouest, Siège Social, Users, Utilisateurs), and a local folder. On the right, there is a search results window titled 'Find Users, Contacts, and Groups'. The search term 'Admin' is entered in the 'Find:' field, and the results are displayed in a table:

Name	Type	Description
Administrators	Group	Administrators have complete and
Administrator	User	Built-in account for administering t

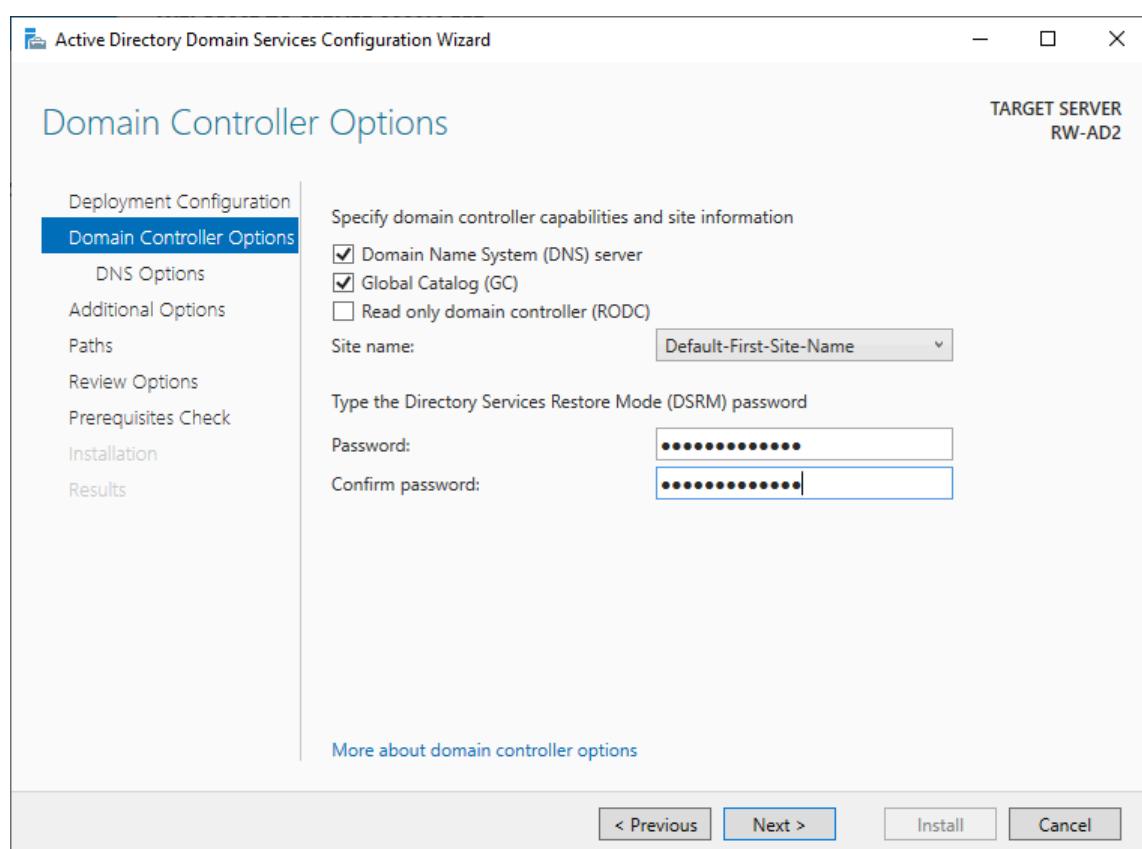
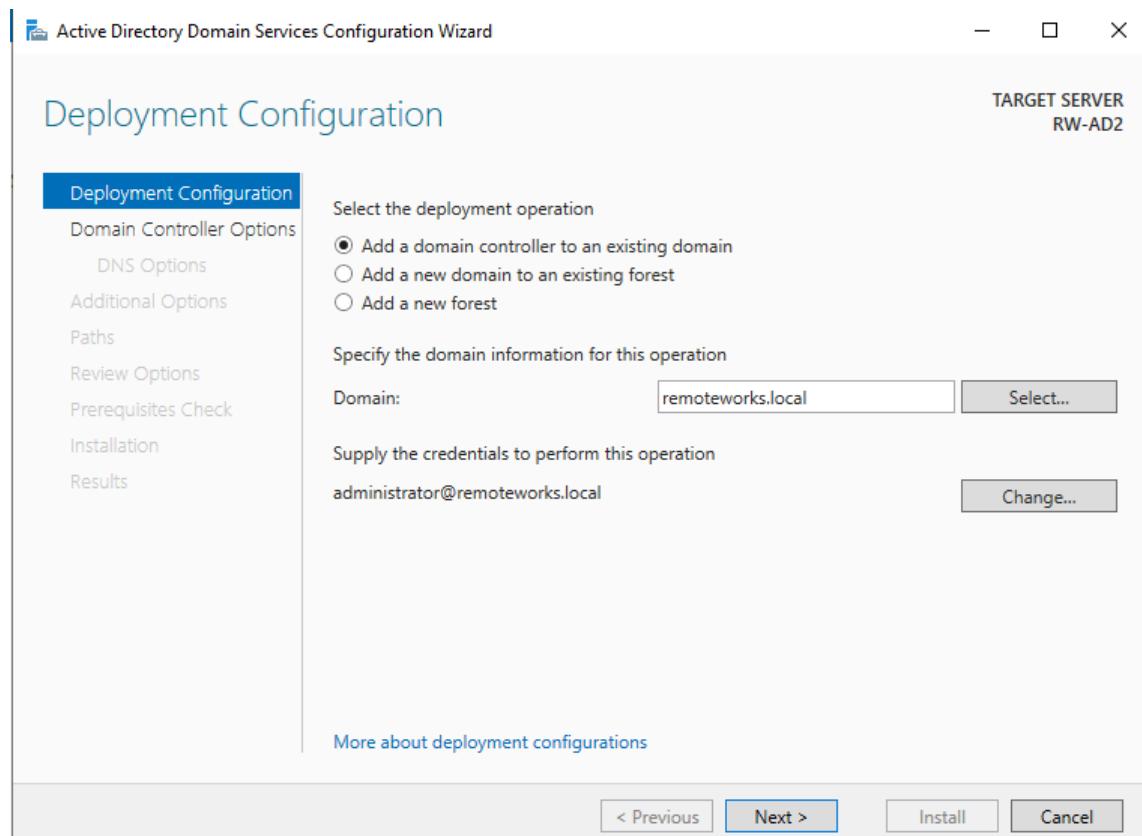
At the bottom of the search results window, it says '2 item(s) found'.

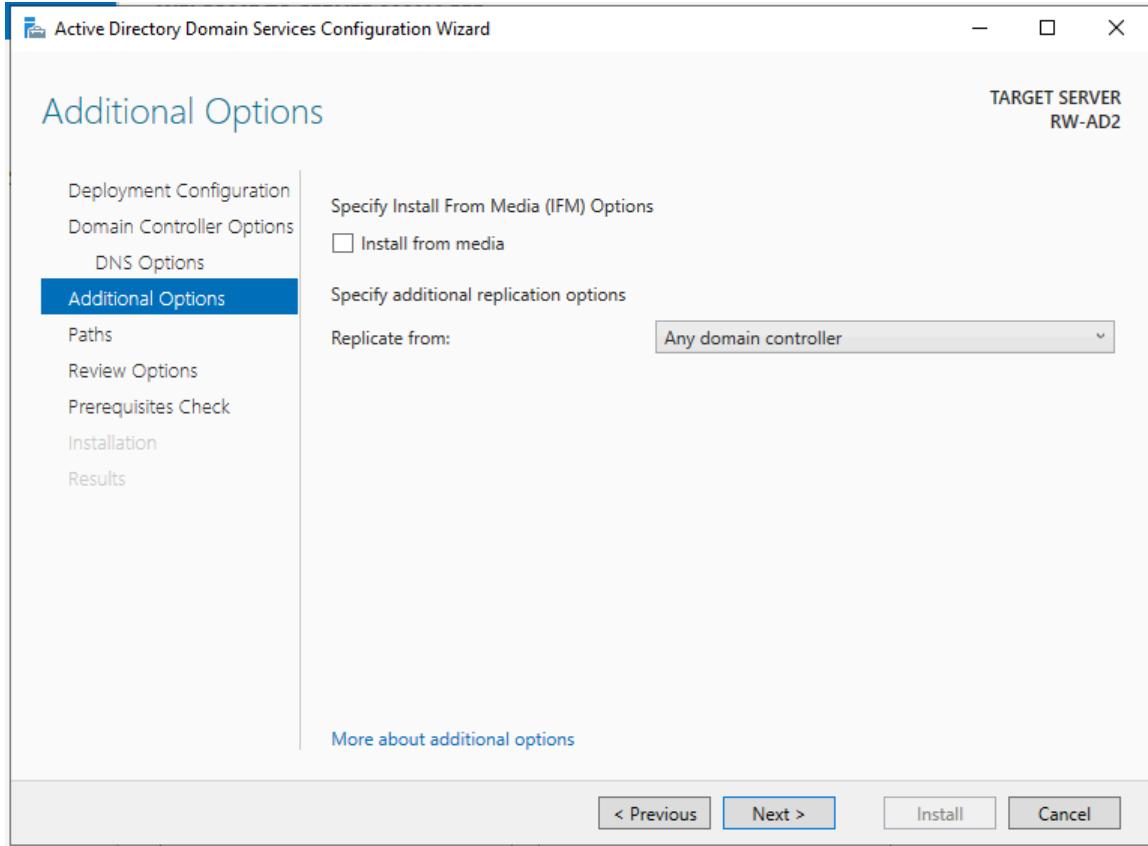
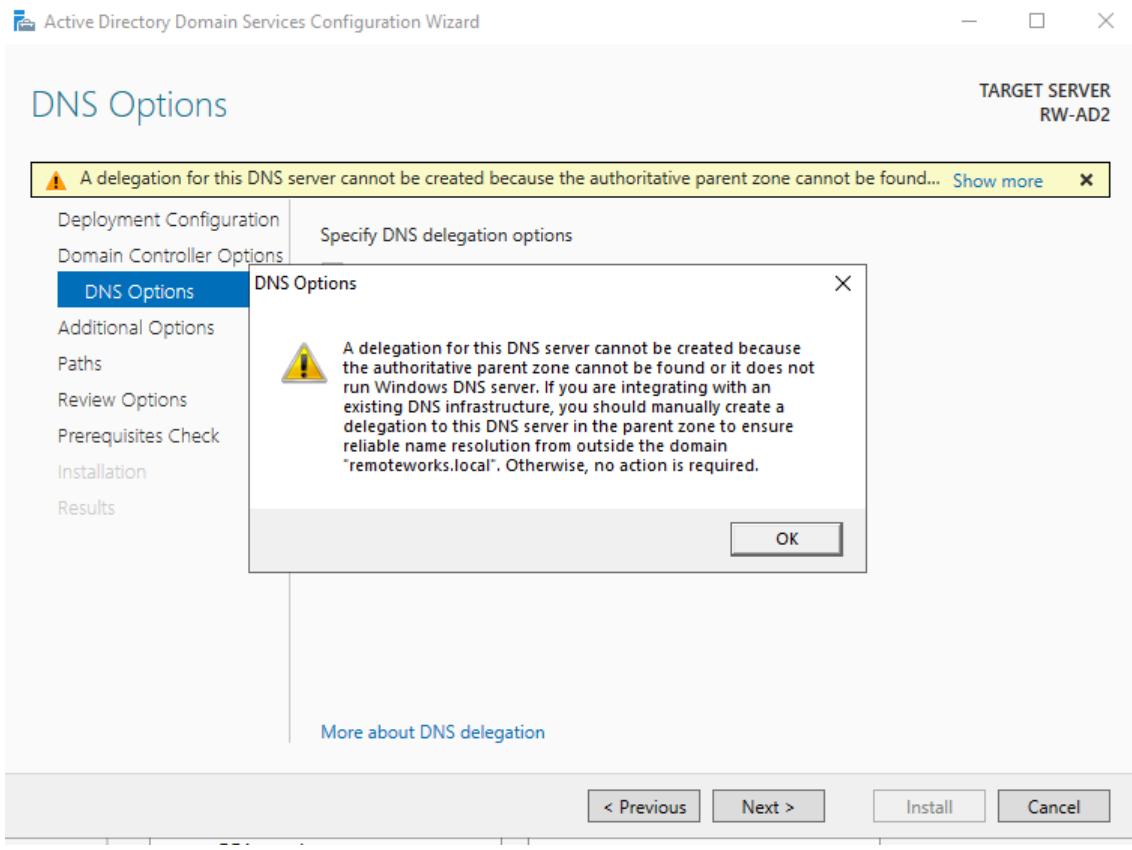
## Connecter un deuxième AD

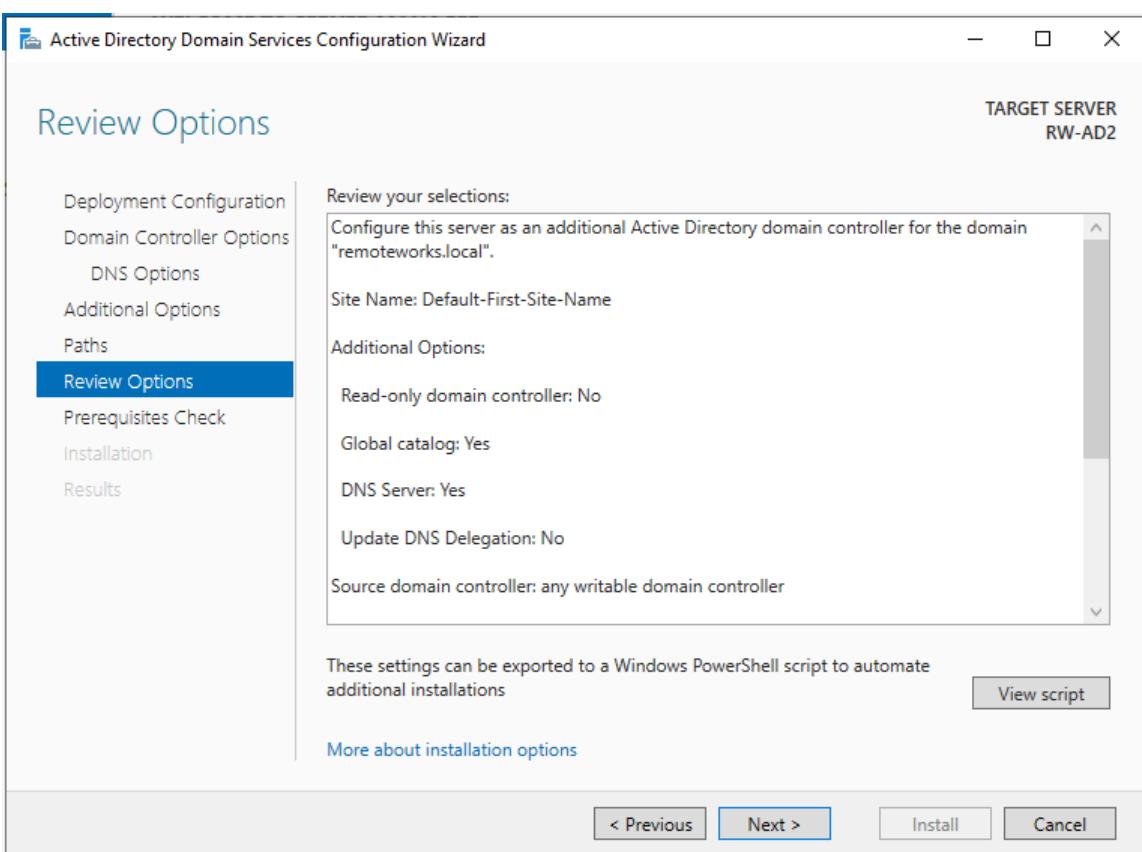
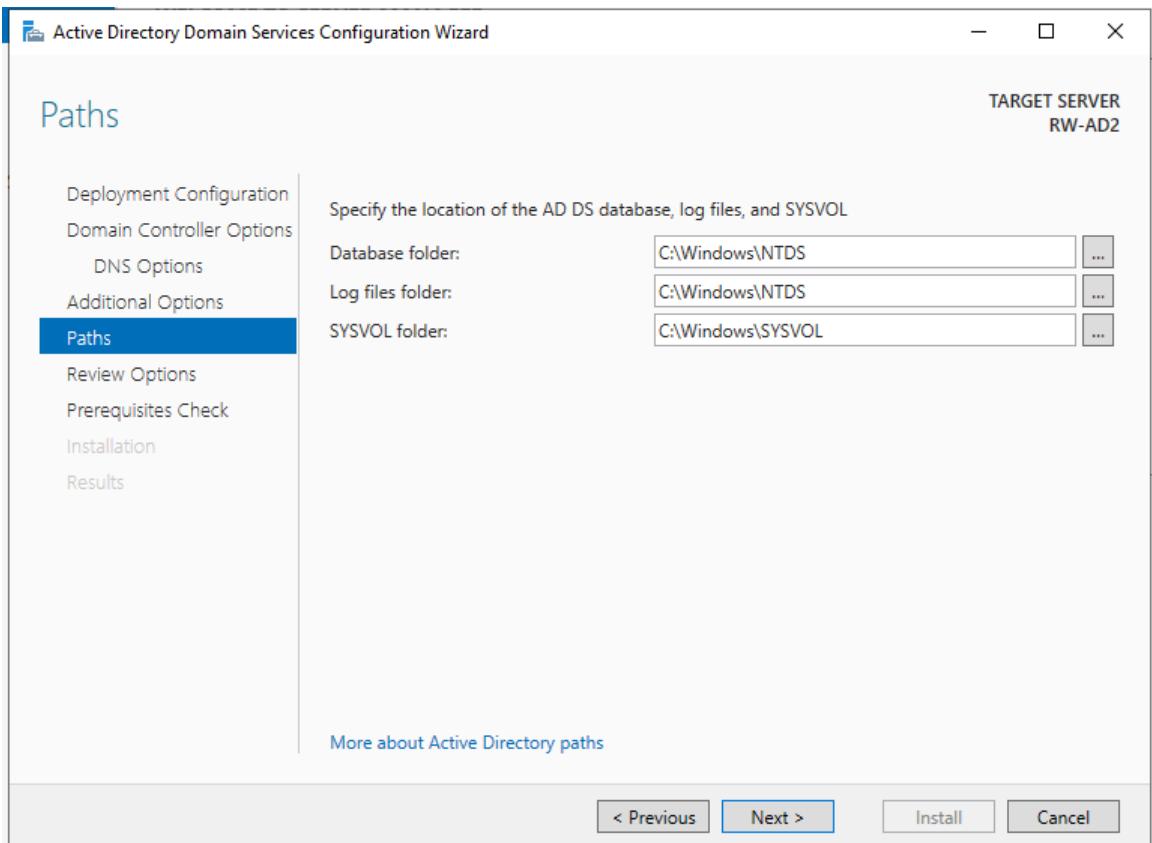
- Bonne pratique
- Redondance pour une meilleure disponibilité

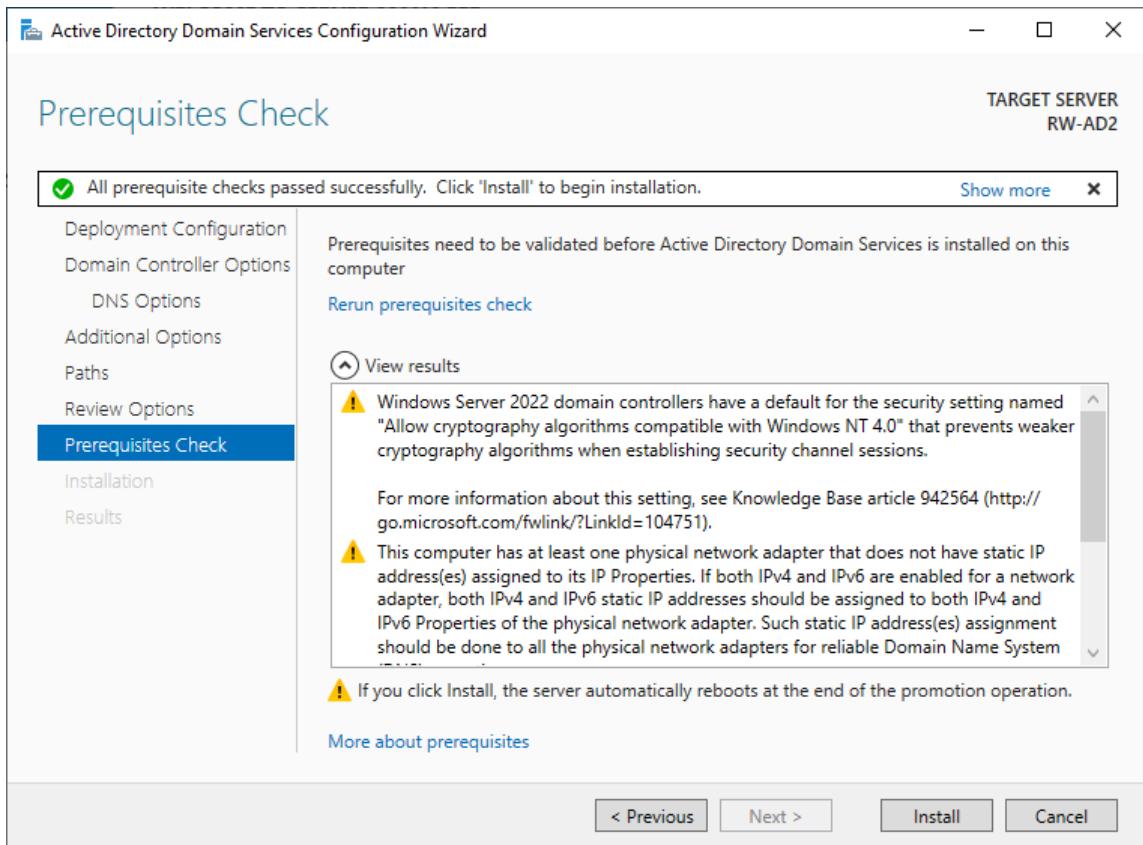
- Équilibrage de charge
- Concept « Contrôleur Principale et Secondaire »
  - Un principale
  - Des secondaires
  - Possibilité de promouvoir un secondaire en principale

Pour cela on va démarrer le deuxième serveur Windows puis on va lui rajouter le même rôle avec certaines nuances.





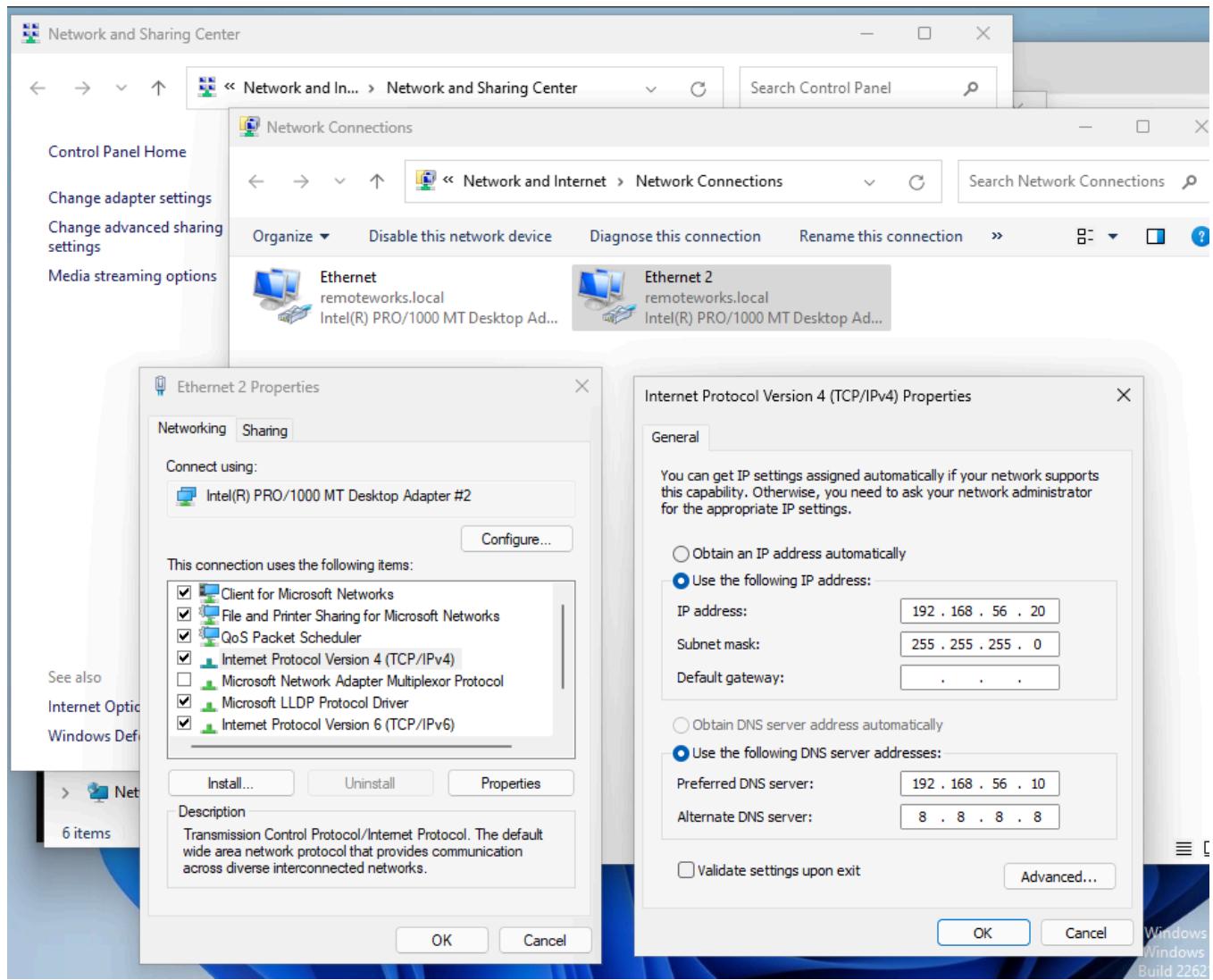


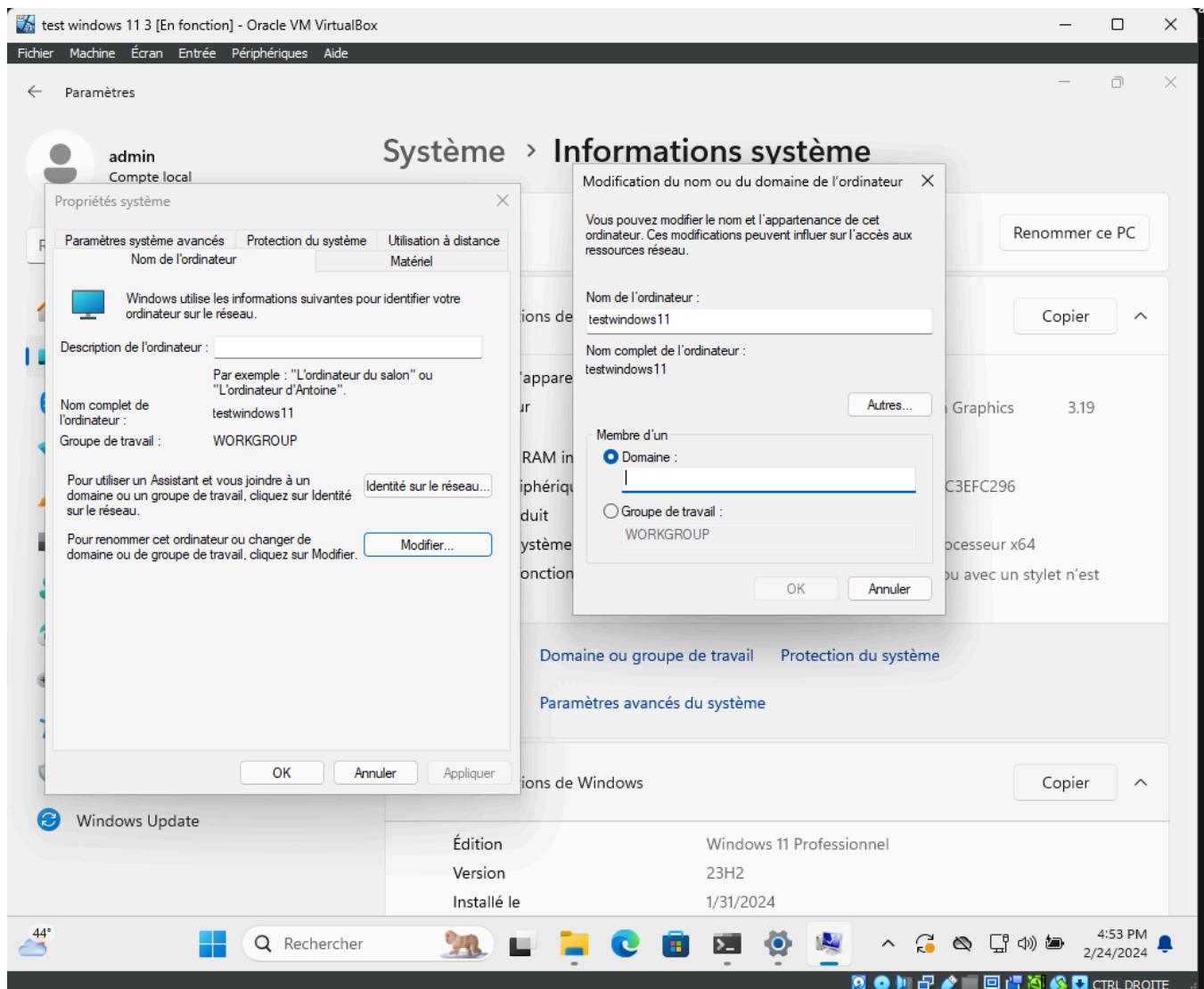


Un reboot plus tard et notre 2eme AD est connecté!

## Connecter un client Windows 11

- En-roller un windows 10/11 à l'AD
- Ce windows doit avoir le serveur AD en tant que serveur DNS !





## AD et Powershell

### Exercice 2:

Recreer tout ce qu'on vient de voir entièrement en powershell !

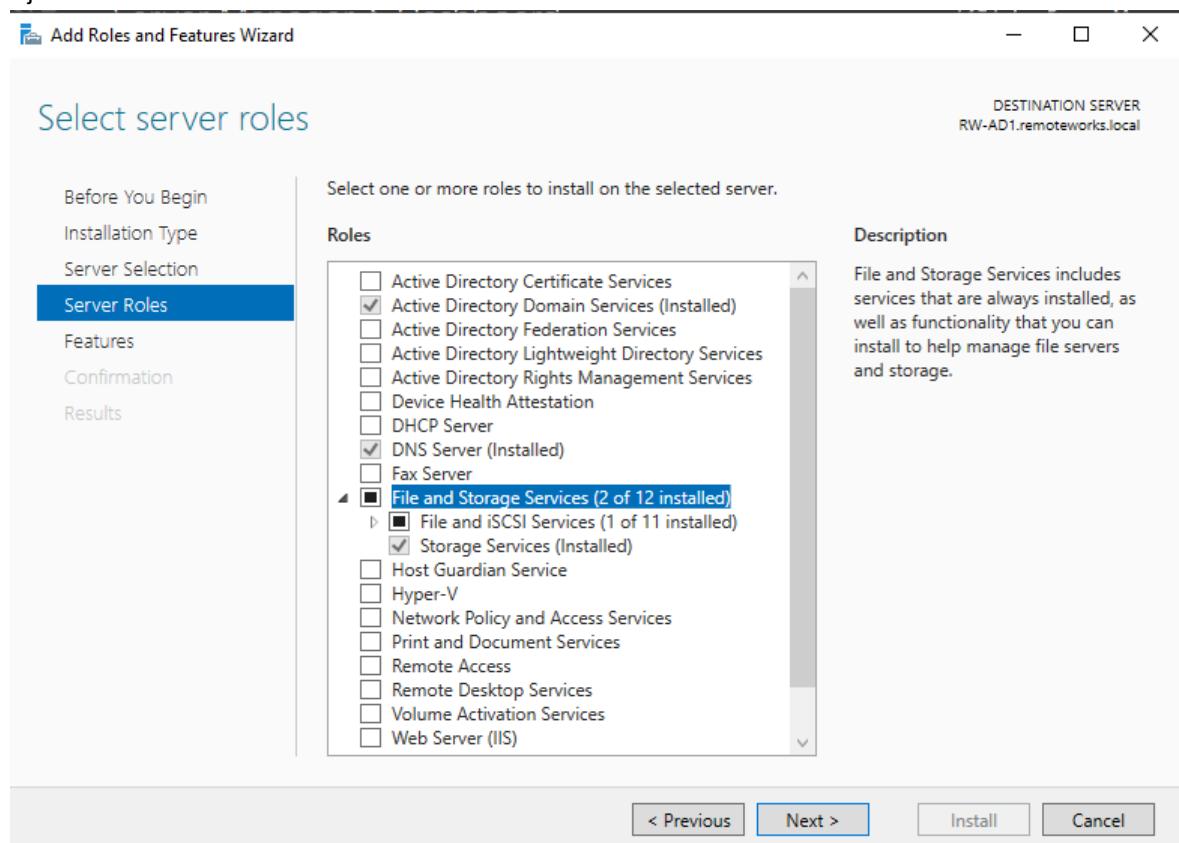
Je veux un script capable de configurer un contrôleur de domaine principale, un autre script pour le second et un troisième script pour enrôler une machine client.

## Serveur de fichier

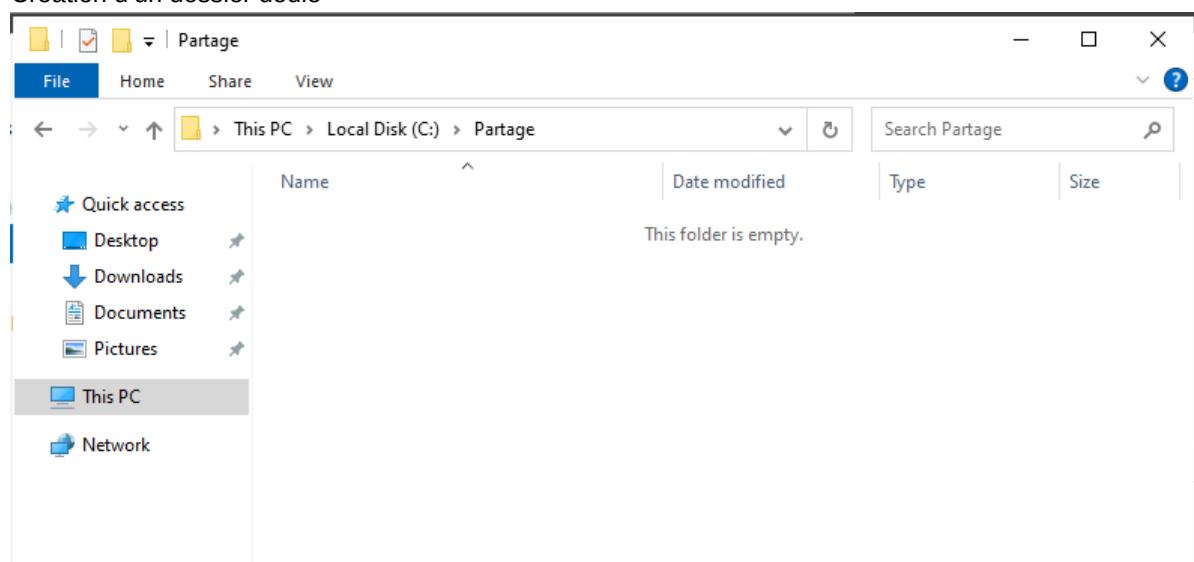
### Objectifs

- Installer le rôle serveur de fichier
- Partager un dossier
- Donner les droits
- Accès à des dossier réseau
- Montage automatique de disque réseau
- Gestion des droits NTFS
- Fichier Hors Connexion

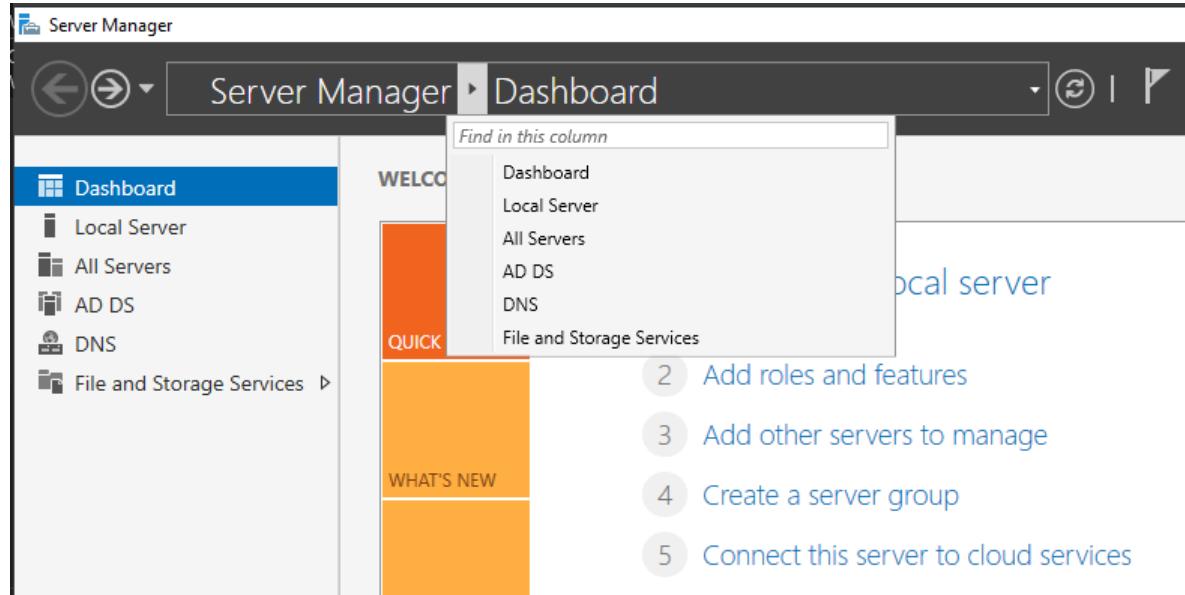
## Ajout d'un nouveau rôle:



## Création d'un dossier dédié



## Console Partage de fichier



This screenshot shows the 'Servers' blade under 'File and Storage Services'. The left sidebar has links for 'Volumes', 'Disks', 'Storage Pools', 'Shares', 'iSCSI', and 'Work Folders'. The main area displays a table of servers:

Server Name	IPv4 Address	Manageability	Last Update	Windows Activation
RW-AD1	10.0.2.15,192.168.56.10	Online - Performance counters not started	3/6/2024 2:36:55 PM	00454-40000-00001-AA627 (Ac)

Below this is an 'EVENTS' section showing log entries:

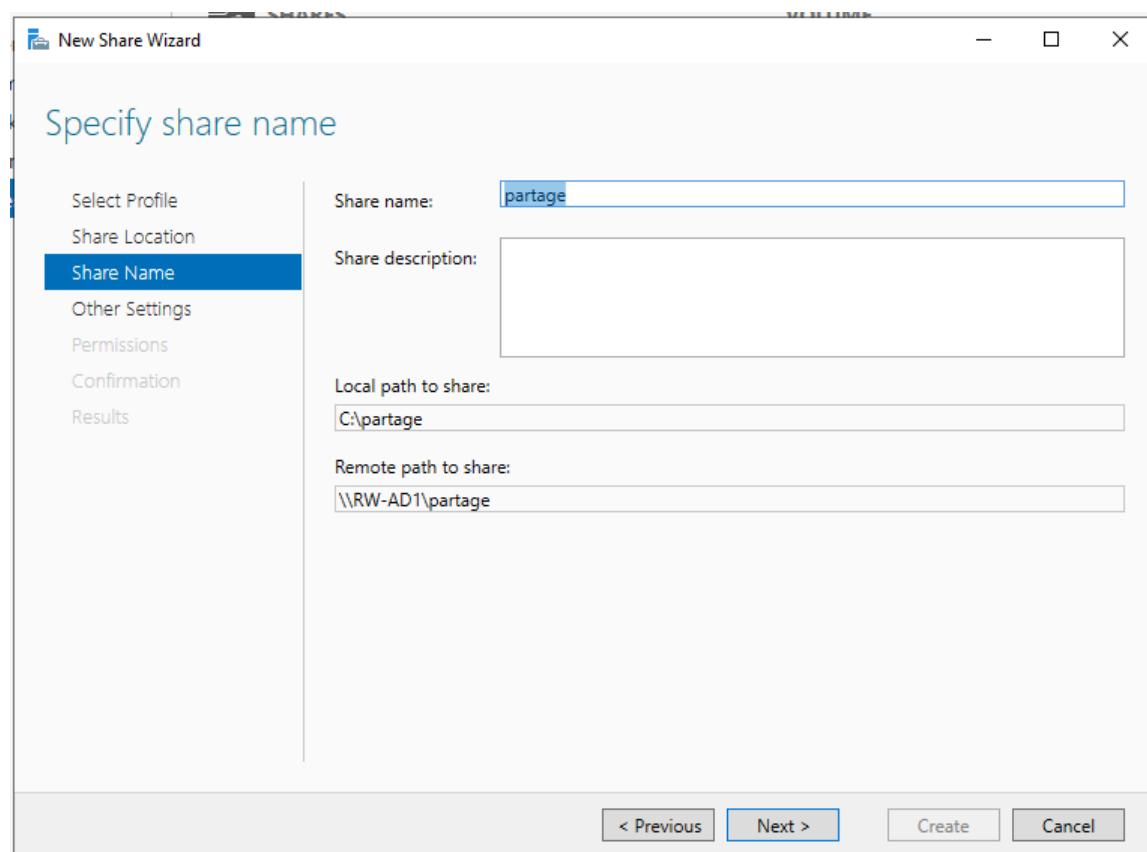
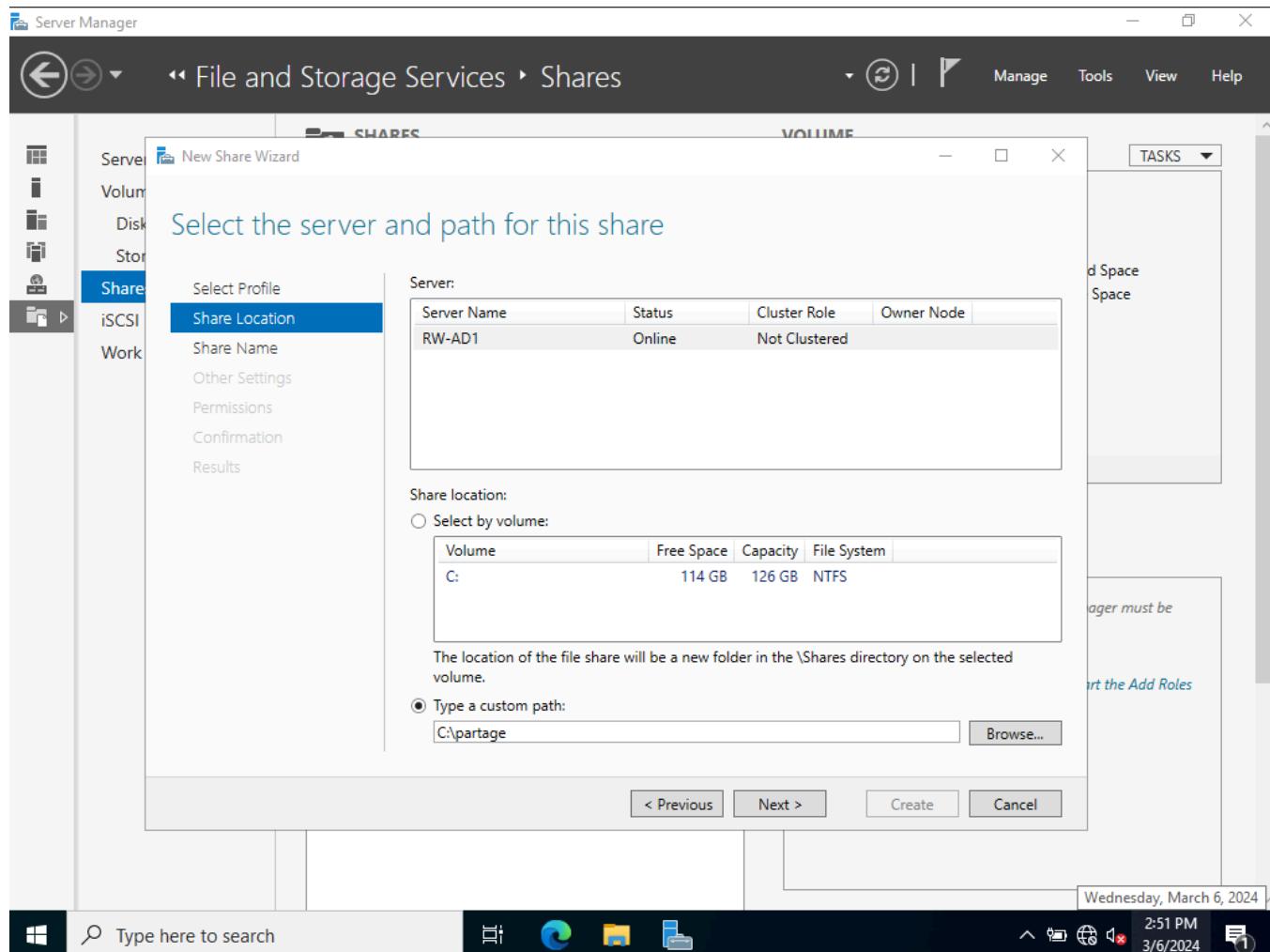
Server Name	ID	Severity	Source	Log	Date and Time
RW-AD1	6016	Warning	DFSR	DFS Replication	3/6/2024 1:52:42 PM
RW-AD1	1202	Error	DFSR	DFS Replication	3/6/2024 1:48:03 PM
RW-AD1	2505	Error	Server	System	3/6/2024 1:47:41 PM
RW-AD1	1202	Error	DFSR	DFS Replication	3/6/2024 1:45:09 PM
RW-AD1	2505	Error	Server	System	3/6/2024 1:02:55 PM
RW-AD1	2505	Error	Server	System	3/6/2024 1:01:39 PM

The bottom of the screen shows the Windows taskbar with the Start button, a search bar, pinned icons for File Explorer, Task View, and Printers, and system status icons.

## Nouveau Partage

The screenshot shows the Windows Server 2012 File and Storage Services interface. On the left, a navigation pane lists 'Servers', 'Volumes', 'Disks', 'Storage Pools', **Shares**, 'iSCSI', and 'Work Folders'. The 'Shares' option is selected. The main area displays the 'SHARES' section with a table showing two shares: 'NETLOGON' (Local Path: C:\Windows\SYSVOL\sysvol\remo...) and 'SYSVOL' (Local Path: C:\Windows\SYSVOL\sysvol). A 'TASKS' dropdown menu at the top right has 'New Share...' highlighted. To the right of the share table is a 'VOLUME' section for 'NETLOGON on RW-AD1', showing a capacity of 126 GB with 10% used (12.7 GB Used Space, 114 GB Free Space). Below the volume info is a link 'Go to Volumes Overview >'. At the bottom right of the main area is a 'QUOTA' section for 'NETLOGON on RW-AD1' with a note: 'To use quotas, File Server Resource Manager must be installed.' and instructions to 'To install File Server Resource Manager, start the Add Roles and Features Wizard.'

The screenshot shows the 'New Share Wizard' window. The title bar says 'New Share Wizard'. The left sidebar shows steps: 'Select Profile', 'Share Location', 'Share Name', 'Other Settings', 'Permissions', 'Confirmation', and 'Results'. The current step is 'Select Profile'. The main area has three sections: 'File share profile:' (with 'SMB Share - Quick' selected), 'Description:' (which states: 'This basic profile represents the fastest way to create an SMB file share, typically used to share files with Windows-based computers.' and lists: '• Suitable for general file sharing' and '• Advanced options can be configured later by using the Properties dialog'), and buttons at the bottom: '< Previous', 'Next >', 'Create', and 'Cancel'. The 'Next >' button is highlighted.



## Configure share settings

Select Profile

Share Location

Share Name

**Other Settings**

Permissions

Confirmation

Results

Enable access-based enumeration

Access-based enumeration displays only the files and folders that a user has permissions to access. If a user does not have Read (or equivalent) permissions for a folder, Windows hides the folder from the user's view.

Allow caching of share

Caching makes the contents of the share available to offline users. If the BranchCache for Network Files role service is installed, you can enable BranchCache on the share.

Enable BranchCache on the file share

BranchCache enables computers in a branch office to cache files downloaded from this share, and then allows the files to be securely available to other computers in the branch.

Encrypt data access

When enabled, remote file access to this share will be encrypted. This secures the data against unauthorized access while the data is transferred to and from the share. If this box is checked and grayed out, an administrator has turned on encryption for the entire server.

&lt; Previous

Next &gt;

Create

Cancel

## Specify permissions to control access

Select Profile

Share Location

Share Name

Other Settings

**Permissions**

Confirmation

Results

Permissions to access the files on a share are set using a combination of folder permissions, share permissions, and, optionally, a central access policy.

Share permissions: Everyone Full Control

Folder permissions:

Type	Principal	Access	Applies To
Allow	CREATOR OWNER	Full Control	Subfolders and files only
Allow	BUILTIN\Users	Special	This folder and subfolders
Allow	BUILTIN\Users	Read & execu...	This folder, subfolders, and files
Allow	BUILTIN\Administrators	Full Control	This folder, subfolders, and files
Allow	NT AUTHORITY\SYSTEM	Full Control	This folder, subfolders, and files

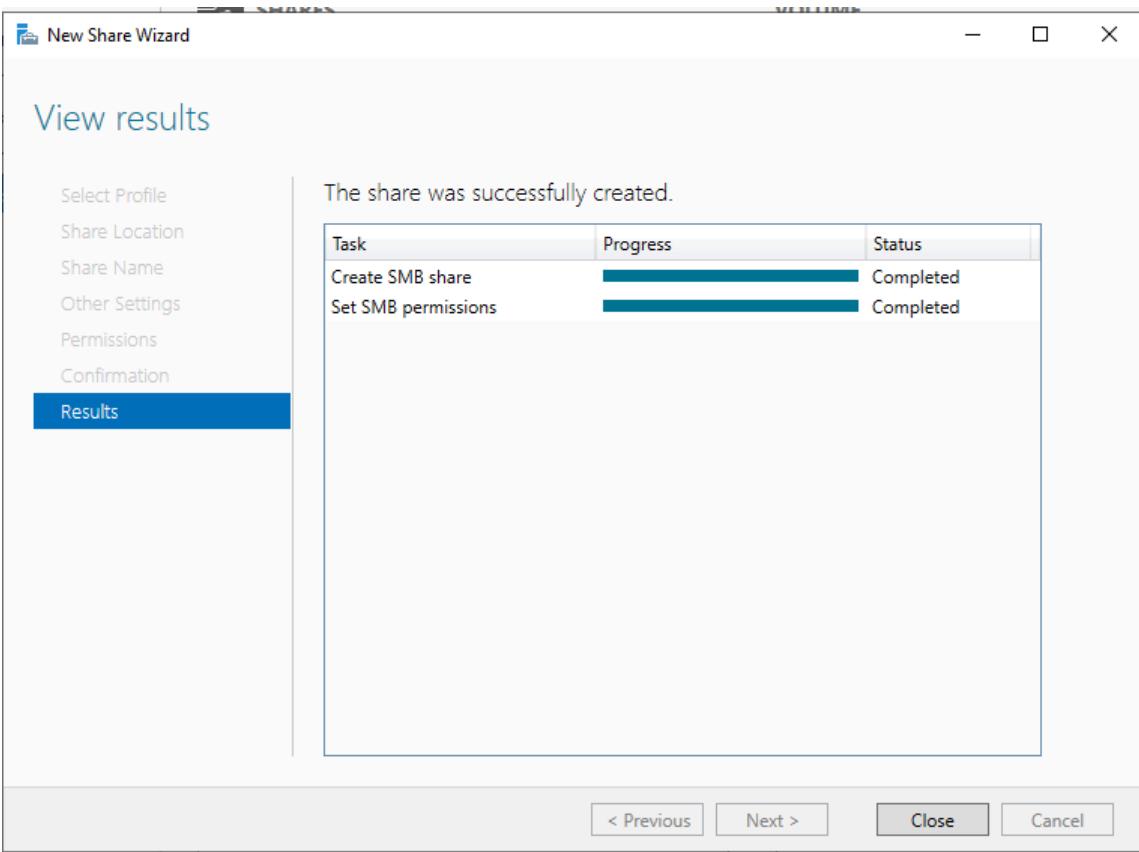
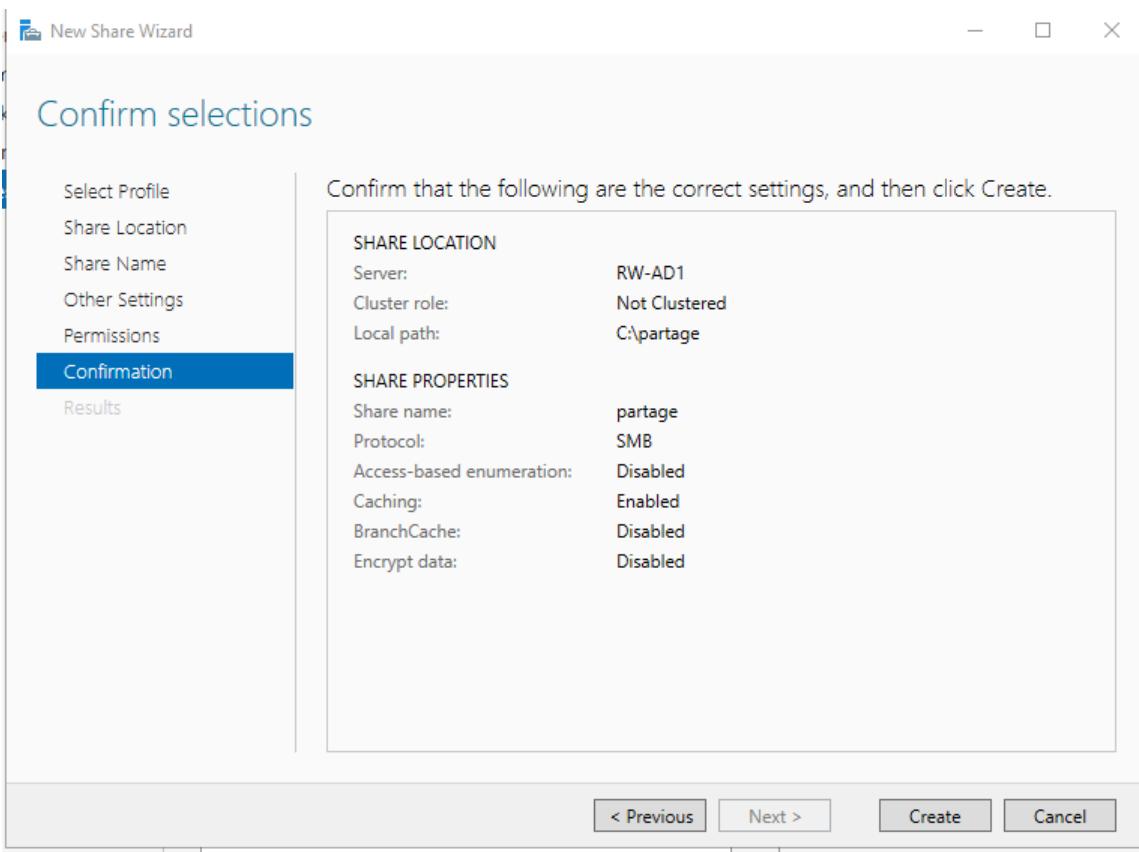
[Customize permissions...](#)

&lt; Previous

Next &gt;

Create

Cancel



The screenshot shows the Windows Server 2016 File and Storage Services interface. On the left, a navigation pane lists 'Servers', 'Volumes', 'Disks', 'Storage Pools', 'Shares' (which is selected), 'iSCSI', and 'Work Folders'. The main area has two tabs: 'SHARES' and 'VOLUME'. The 'SHARES' tab shows 'All shares | 3 total' with a table for 'Share' and 'Local Path'. The 'VOLUME' tab shows 'partage on RW-AD1' with details like '(C:)', Capacity: 126 GB, 10% Used (12.7 GB Used Space, 114 GB Free Space), and a link to 'Go to Volumes Overview >'. Below these tabs is a 'QUOTA' section with a note: 'To use quotas, File Server Resource Manager must be installed.'

This screenshot shows the 'Advanced Security Settings for partage' dialog. It displays the share's name (C:\partage) and owner (Administrators). It includes tabs for 'Permissions', 'Share', 'Auditing', and 'Effective Access'. The 'Permissions' tab is active, showing a list of security entries:

Type	Principal	Access	Inherited from	Applies to
Allow	SYSTEM	Full control	C:\	This folder, subfolders and files
Allow	Administrators (REMO...	Full control	C:\	This folder, subfolders and files
Allow	Users (REMO...	Read & execute	C:\	This folder, subfolders and files
Allow	Users (REMO...	Special	C:\	This folder and subfolders
Allow	CREATOR OWNER	Full control	C:\	Subfolders and files only

Buttons at the bottom include 'Add', 'Remove', 'View', 'Disable inheritance', and checkboxes for 'Replace all child object permission entries with inheritable permission entries from this object' and 'Replace all child object audit entries with inheritable audit entries from this object'. The 'OK', 'Cancel', and 'Apply' buttons are also present.

## Exercice 3

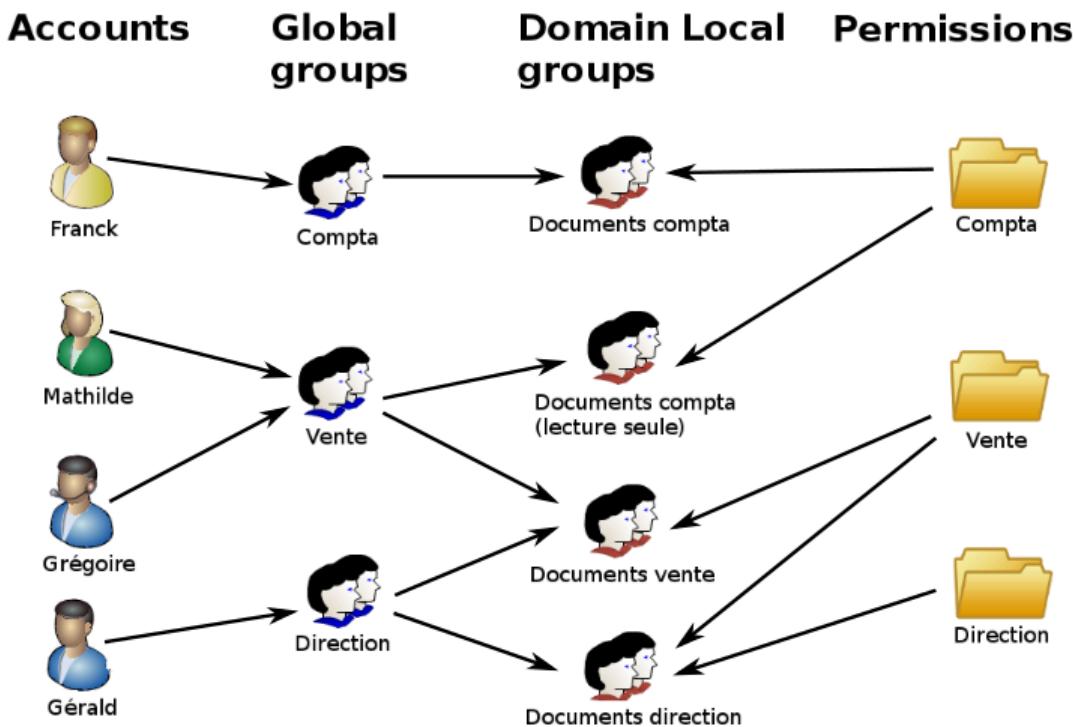
Créer un script pour la création de dossier et son partage

## Exercice 4

Créer une OU, un groupe, un utilisateur et mettre ce dernier dans le groupe créé. Via Script

## Attribution des droits, méthode « AGDLP »

Account, Global, Domain Local, Permission



- **Comptes utilisateurs** : Les identités individuelles des utilisateurs dans le système.
- **Groupes globaux** : Groupes utilisés pour rassembler des utilisateurs en fonction de leurs rôles ou fonctions similaires au sein de l'organisation.
- **Groupes locaux de domaine** : Groupes utilisés pour attribuer des permissions à des ressources dans un domaine spécifique. Ces groupes peuvent contenir des groupes globaux.
- **Permissions** : Droits d'accès attribués aux groupes locaux de domaine pour contrôler l'accès aux ressources.
- **Héritage de permissions** : Mécanisme par lequel les permissions sont transmises des groupes aux utilisateurs.
- **Principe de moindre privilège** : Attribuer aux utilisateurs uniquement les permissions strictement nécessaires pour leurs tâches.
- **Séparation des tâches** : Séparer les responsabilités parmi différents utilisateurs ou groupes pour augmenter la sécurité.
- **Gestion centralisée** : Centraliser la gestion des permissions et des accès pour simplifier l'administration et améliorer la sécurité.

## Avantages

- **Simplification de la gestion** : Facilite l'administration des droits d'accès en regroupant les utilisateurs dans des groupes globaux.
- **Scalabilité** : Permet d'ajuster facilement les permissions pour de nombreux utilisateurs en modifiant les appartences aux groupes, sans avoir à gérer les permissions individuellement.
- **Sécurité renforcée** : Minimise les risques de permissions inappropriées en limitant l'accès direct aux ressources.
- **Déploiement efficace** : Facilite le déploiement de nouvelles politiques de sécurité et l'intégration de nouveaux utilisateurs ou ressources.
- **Flexibilité** : Offre une structure flexible qui peut s'adapter à divers besoins organisationnels et changements structurels.

## Problématiques

- **Complexité initiale** : Peut être complexe à mettre en place initialement, surtout dans des environnements avec de nombreux utilisateurs et groupes.
- **Maintenance** : Nécessite une maintenance régulière pour s'assurer que les groupes reflètent correctement les besoins actuels en termes d'accès.
- **Risque de sur-assignation** : Risque d'assigner trop de permissions si les groupes ne sont pas correctement gérés ou si les politiques ne sont pas régulièrement revues.

- **Formation nécessaire** : Les administrateurs doivent être bien formés pour gérer efficacement la structure AGDLP, ce qui peut représenter un coût additionnel.
- **Délais de propagation** : Les changements d'appartenance à des groupes peuvent prendre du temps à se propager dans un grand réseau, causant des délais dans l'application des permissions.

## Exercice 5

Créer un script d'ajout de droit

## Group Policy Object (GPO)

Ou Objet de stratégie de groupe.

Les GPO sont utilisées pour gérer les paramètres de configuration des ordinateurs et des utilisateurs au sein d'un domaine Active Directory. Les GPO permettent aux administrateurs de définir des politiques de sécurité, des configurations système et des paramètres de logiciel qui sont appliqués de manière cohérente à tous les utilisateurs et ordinateurs dans un domaine Windows.

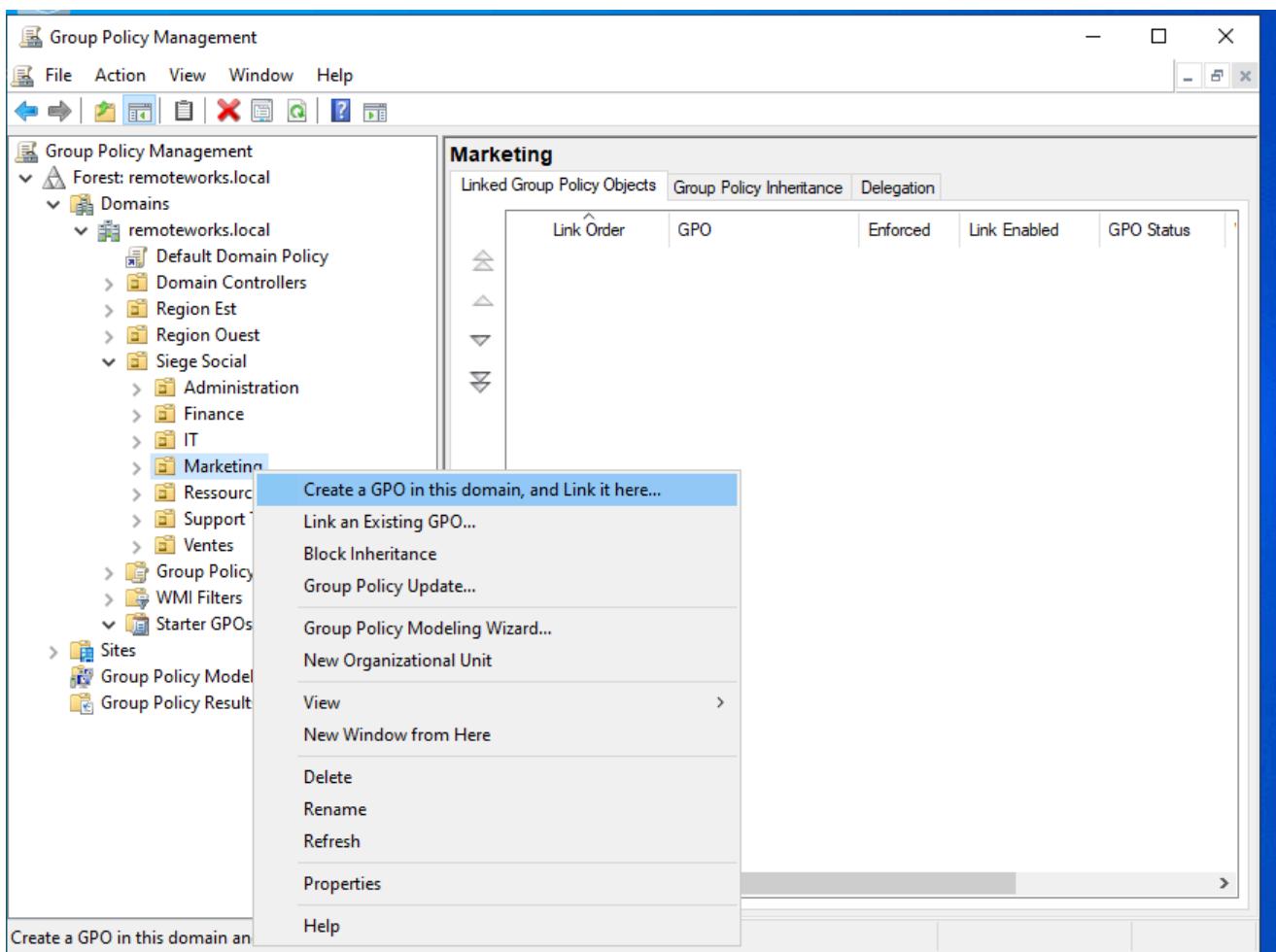
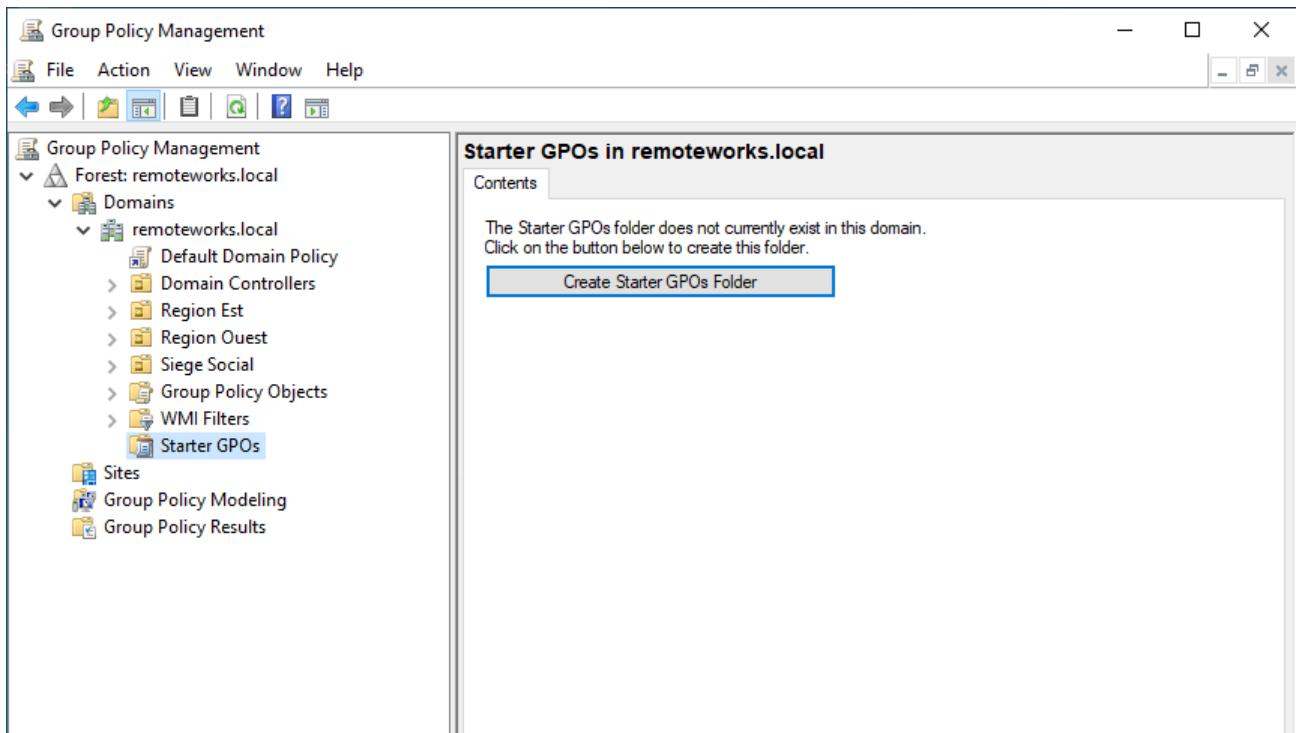
Les GPO sont créées, configurées et gérées à l'aide de l'éditeur de stratégie de groupe (Group Policy Management Console, GPMC) sur un contrôleur de domaine ou un autre ordinateur Windows Server au sein du domaine. Une fois déployées, les GPO sont distribuées aux ordinateurs clients du domaine, où elles sont ensuite appliquées en fonction de la hiérarchie et de la priorité des GPO.

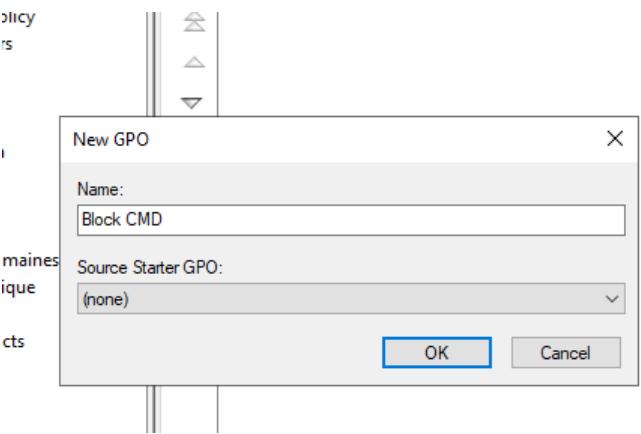
Objectif

- Interface de gestion des GPO
- Créer une GPO
- Sauvegarde, copie et importation de GPO
- Gestion et blocage de l'héritage
- Modélisation d'un objet GPO
- TP Création de GPO

Interface de gestion des GPO:

- Console : Group Policy Management
  - gpmc.msc
- Configuration Locale :
  - gpedit.msc





Forest: remoteworks.local

- Domains
  - remoteworks.local
    - Default Domain Policy
    - Domain Controllers
    - Region Est
    - Region Ouest
    - Siege Social
      - Administration
      - Finance
      - IT
      - Marketing
        - Block CMD
        - Ressources
        - Support T
        - Ventes
      - Group Policy
      - WMI Filters
    - Starter GPOs
  - Sites
  - Group Policy Modeli
  - Group Policy Results

Link Order | GPO | Enforced | Link Enabled | GPO Status

Link Order	GPO	Enforced	Link Enabled	GPO Status
1	Block CMD	No	Yes	Enabled

Block... Enforced Link Enabled Save Report... New Window from Here Delete Rename Refresh Help

Group Policy Management Editor

File Action View Help

Block CMD [RW-AD1.REMOTWORKS.LOCAL]

Computer Configuration

- Policies
- Preferences

User Configuration

- Policies
  - Software Settings
  - Windows Settings
  - Administrative Templates: Policy
    - Control Panel
    - Desktop
    - Network
    - Shared Folders
    - Start Menu and Taskbar
    - System**
      - Ctrl+Alt+Del Options
      - Display
      - Driver Installation
      - Folder Redirection
      - Group Policy
      - Internet Communication Management
      - Locale Services
      - Logon
      - Mitigation Options
      - Power Management
      - Removable Storage Access
      - Scripts
      - User Profiles
    - Custom User Interface
    - Prevent access to the command prompt
    - Prevent access to registry editing tools
    - Don't run specified Windows applications
    - Run only specified Windows applications
    - Windows Automatic Updates
- Internet Communication Management
- Locale Services
- Logon
- Mitigation Options
- Power Management
- Removable Storage Access
- Scripts
- User Profiles

Prevent access to the command prompt

Edit policy setting

Requirements: At least Windows 2000

Description: This policy setting prevents users from running the interactive command prompt, Cmd.exe. This policy setting also determines whether batch files (.cmd and .bat) can run on the computer.

If you enable this policy setting and the user tries to open a command window, the system displays a message explaining that a setting prevents the action.

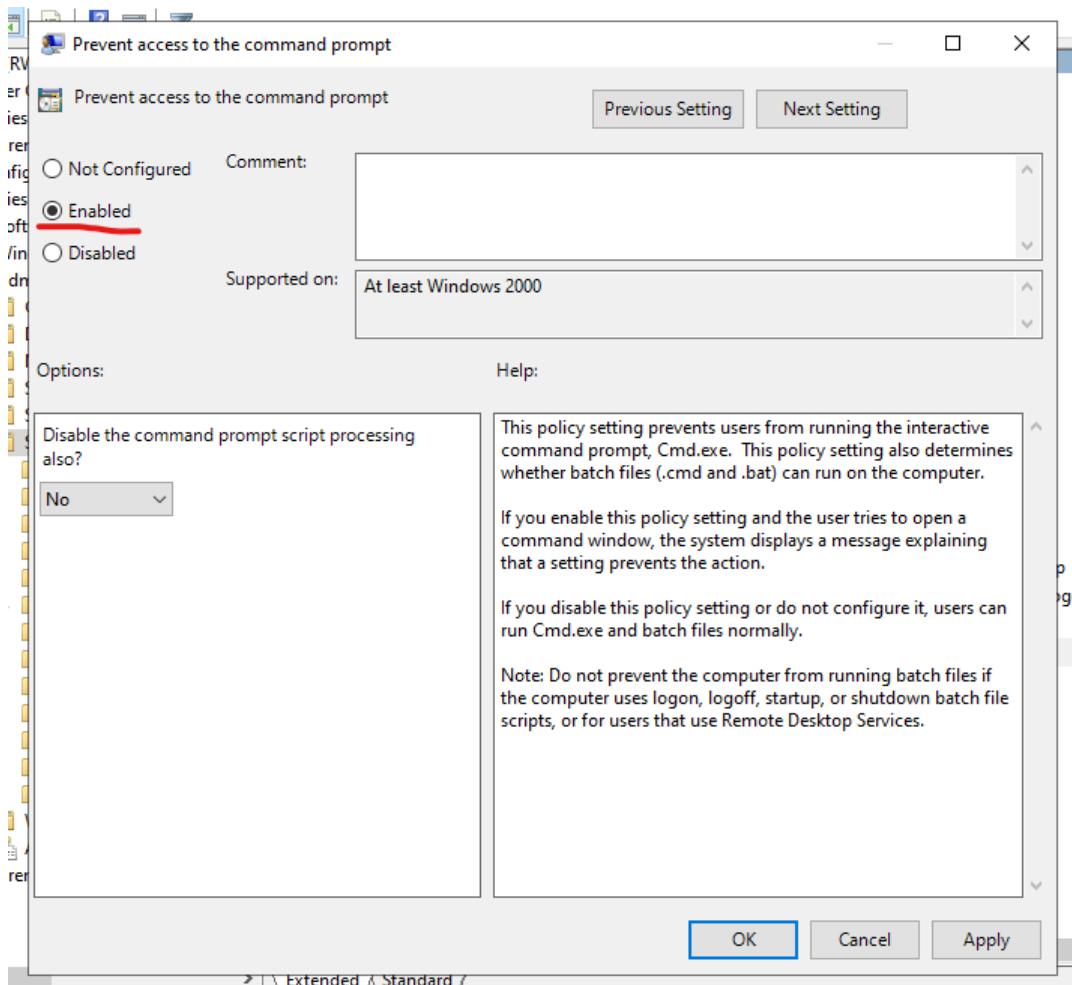
If you disable this policy setting or do not configure it, users can run Cmd.exe and batch files normally.

Note: Do not prevent the computer from running batch files if the computer uses logon, logoff, startup, or shutdown batch file scripts, or for users that use Remote Desktop Services.

Setting State

Ctrl+Alt+Del Options	Not configured
Display	Not configured
Driver Installation	Not configured
Folder Redirection	Not configured
Group Policy	Not configured
Internet Communication Management	Not configured
Locale Services	Not configured
Logon	Not configured
Mitigation Options	Not configured
Power Management	Not configured
Removable Storage Access	Not configured
Scripts	Not configured
User Profiles	Not configured
Download missing COM components	Not configured
Century interpretation for Year 2000	Not configured
Restrict these programs from being launched from Help	Not configured
Do not display the Getting Started welcome screen at logon	Not configured
Custom User Interface	Not configured
<b>Prevent access to the command prompt</b>	<b>Enabled</b>
Prevent access to registry editing tools	Not configured
Don't run specified Windows applications	Not configured
Run only specified Windows applications	Not configured
Windows Automatic Updates	Not configured

Edit Filter On Filter Options... Re-Apply Filter All Tasks > Help



Policy setting or option	Description	Status
Restrict these programs from being launched from Help		Not configured
Do not display the Getting Started welcome screen at logon		Not configured
Custom User Interface		Not configured
<b>Prevent access to the command prompt</b>	<b>Enabled</b>	
Prevent access to registry editing tools		Not configured
Don't run specified Windows applications		Not configured
Run only specified Windows applications		Not configured

### Note

Le dossier Group Policy Objects contient toutes vos GPO, mais pour qu'elles soient appliquées vous devez les lier à une OU. C'est possible simplement en faisant un glisser-déposer de cette dernière. Cela ne va pas la déplacer ou la copier mais en faire un "raccourci" comme sur le screenshot ci-dessous

Group Policy Management

File Action View Window Help

Group Policy Management

Forest: remoteworks.local

Domains

remoteworks.local

Default Domain Policy

Domain Controllers

Region Est

Region Ouest

Siege Social

Administration

Finance

IT

Marketing

Block CMD

Ressources Humaines

Support Technique

Ventes

Group Policy Objects

Block CMD

Default Domain Controllers Policy

Default Domain Policy

test

WMI Filters

Starter GPOs

Sites

Group Policy Modeling

Group Policy Results

Block CMD

Scope Details Settings Delegation Status

Details

Links

Security Filtering

Delegation

Computer Configuration (Enabled)

No settings defined.

User Configuration (Enabled)

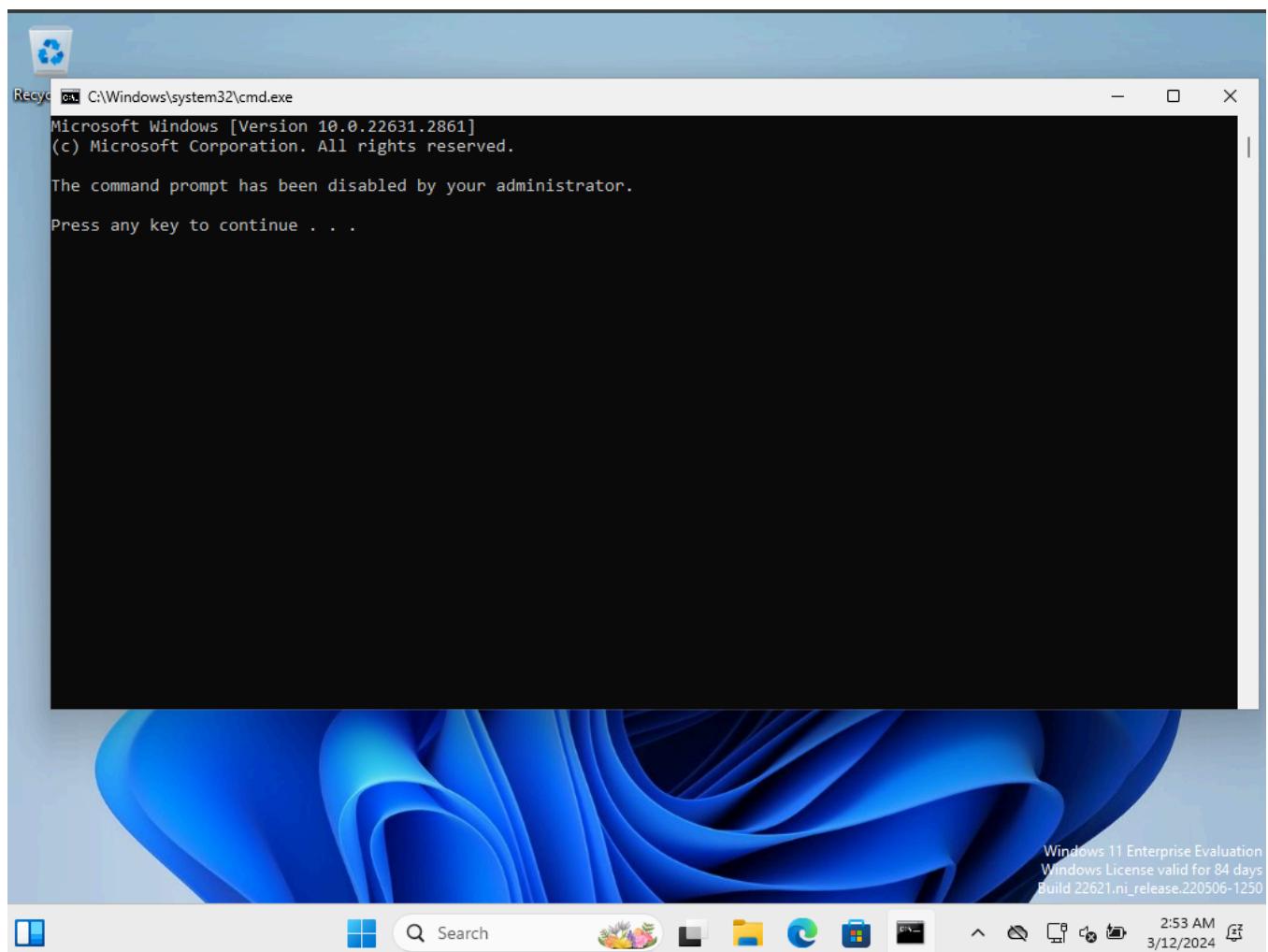
Policies

Administrative Templates

Policy definitions (ADMX files) retrieved from the local computer.

System

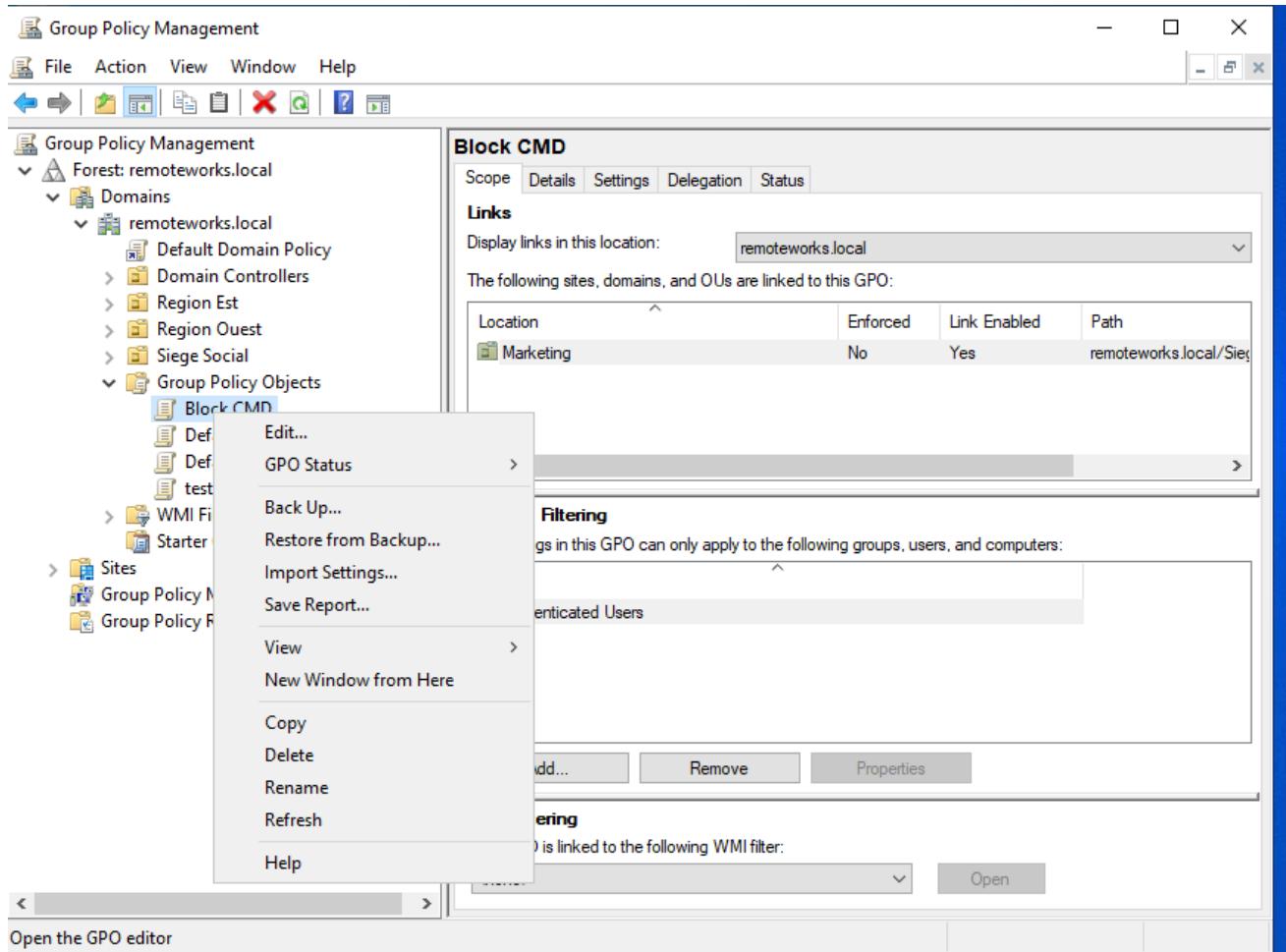
Policy	Setting	Comment
Prevent access to the command prompt	Enabled	Disable the command prompt script processing also? No



## Mise à jour des Policies

- gpupdate : Permet de forcer la mise à jour des stratégies de groupe sur un ordinateur. Utilisée après avoir apporté des modifications à une GPO pour s'assurer que les changements sont appliqués immédiatement.
- gprestart : Génère un rapport sur les stratégies de groupe appliquées à un utilisateur ou à un ordinateur spécifique. Elle est utile pour vérifier quelles politiques sont en vigueur sur un système.
- Get-GPO : Commande PowerShell permet de lister toutes les GPO configurées dans le domaine.
- New-GPO / Remove-GPO : Ajouter/Supprimer des GPO

## Sauvegarde, copie et importation de GPO



Group Policy Management

File Action View Window Help

Group Policy Management

Forest: remoteworks.local

Domains

remoteworks.local

- Default Domain Policy
- Domain Controllers
- Region Est
- Region Ouest
- Siege Social

Group Policy Objects

- New
- Back Up All...
- Manage Backups...
- Open Migration Table Editor
- View
- New Window from Here
- Refresh
- Help

Group Policy Objects in remoteworks.local

Name	GPO Status	WMI Filter	Modified	Owner
Block CMD	Enabled	None	3/11/2024 3:35...	Vagrant
Default Domain Controller...	Enabled	None	3/6/2024 1:46:3...	Domai
Default Domain Policy	Enabled	None	3/6/2024 1:46:3...	Domai
test	Enabled	None	3/11/2024 3:30:...	Vagr

Manage backed up GPOs for this domain

Group Policy Management

File Action View Window Help

Group Policy Management

Forest: remoteworks.local

Domains

remoteworks.local

- Default Domain Policy
- Domain Controllers
- Region Est
- Region Ouest
- Siege Social

Group Policy Objects

- Block CMD
- Default Domain Controller...
- Default Domain Policy
- test

Manage Backups

Backup location:

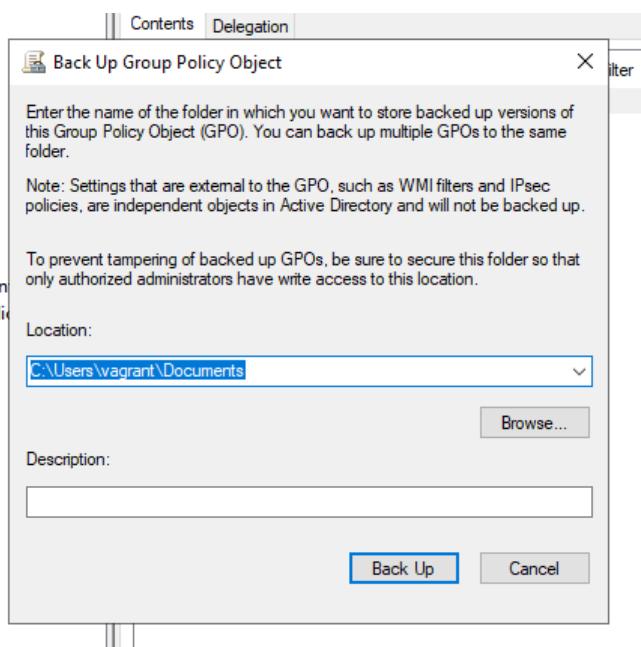
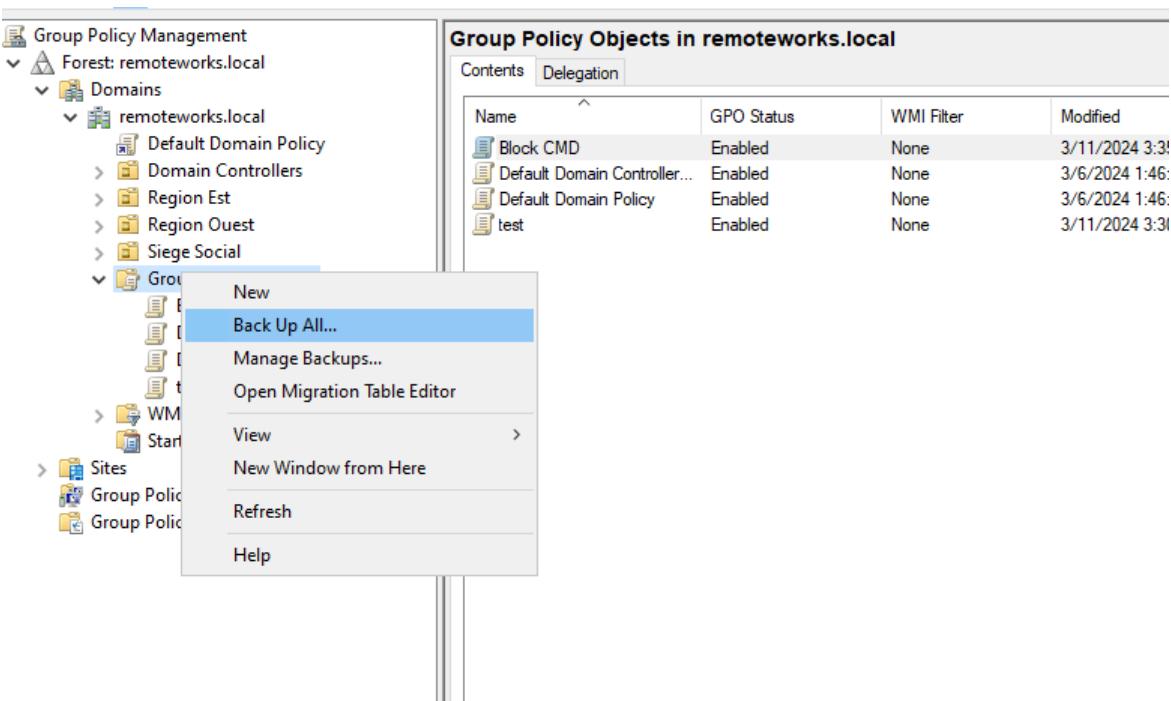
C:\Users\vagrant\Documents

Backed up GPOs:

Domain	Name	Time Stamp	Description	GPO ID
remoteworks.local	Block CMD	3/12/2024 10:06:07 AM		{DEA26E24-9B...
remoteworks.local	Default Dom...	3/12/2024 10:06:12 AM		{6AC1786C-01...
remoteworks.local	Default Dom...	3/12/2024 10:06:13 AM		{31B2F340-016...
remoteworks.local	test	3/12/2024 10:06:13 AM		{54526A4A-58...

Show only the latest version of each GPO

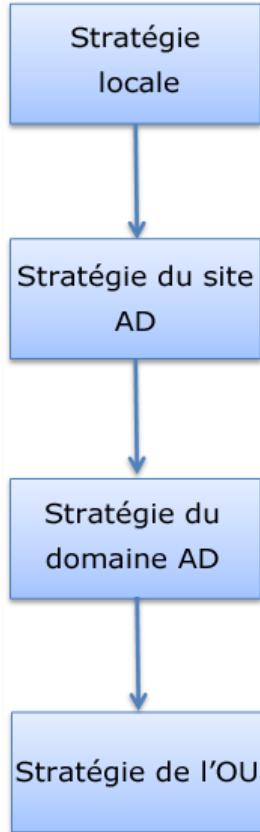
Restore Delete View Settings... Close



## Gestion et blocage de l'héritage

L'héritage désigne le processus par lequel les politiques appliquées à un niveau supérieur de l'Active Directory (comme un domaine ou une unité d'organisation parente) sont automatiquement transmises aux niveaux inférieurs (comme les unités d'organisation enfant ou les objets individuels). Cela permet une gestion centralisée et cohérente.

des paramètres de configuration pour les utilisateurs et les ordinateurs au sein du réseau.



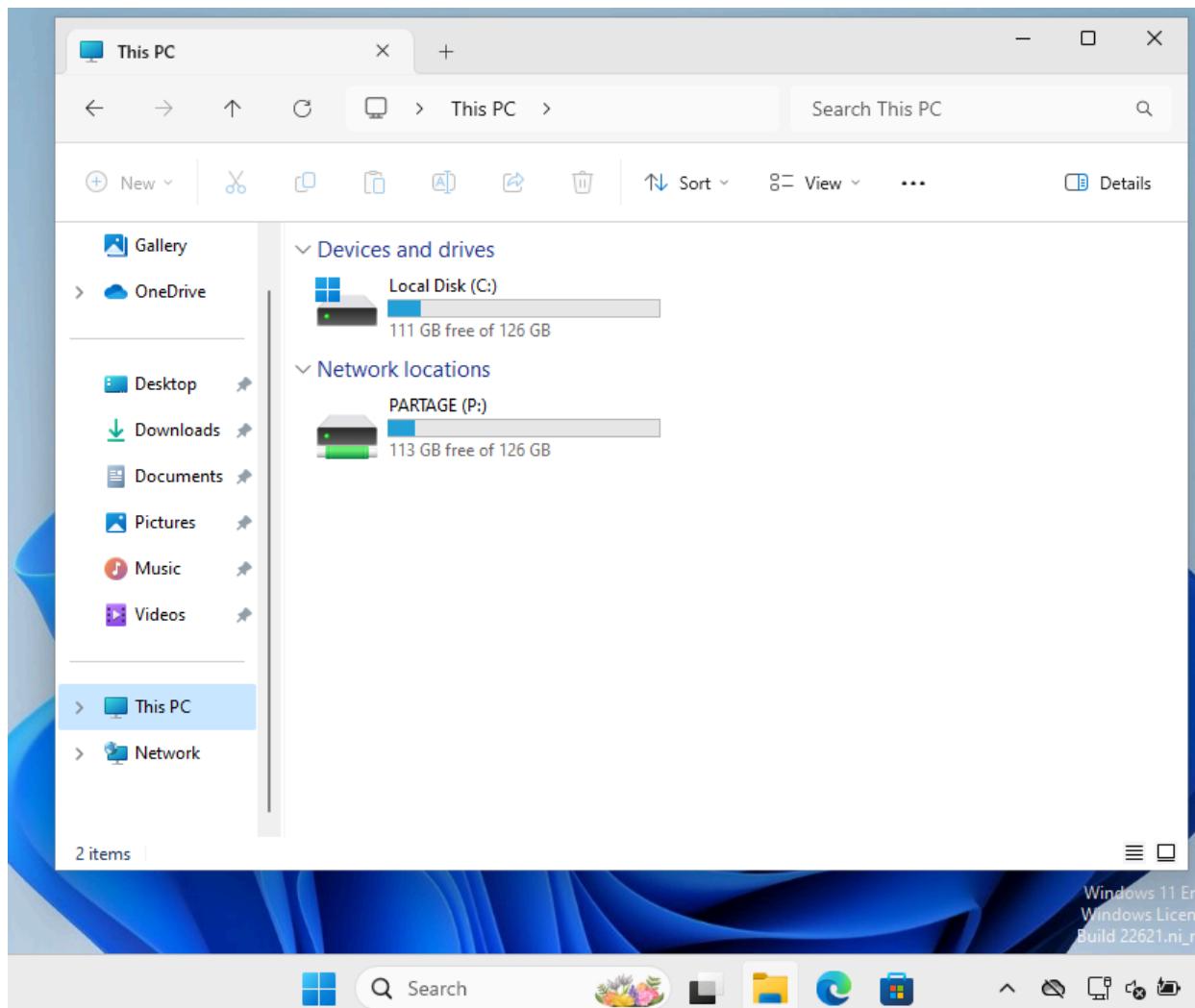
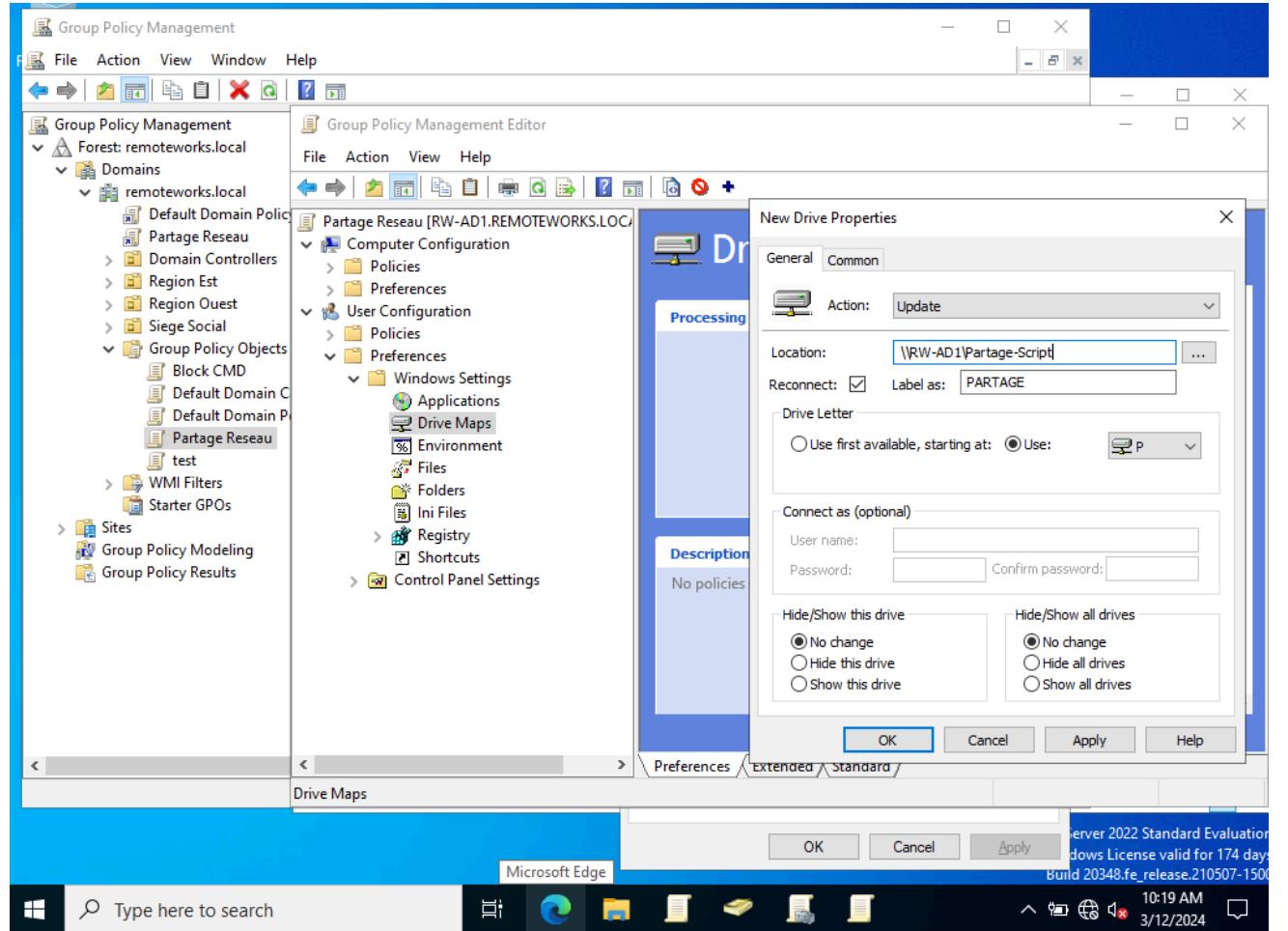
The screenshot shows the Group Policy Management console interface. On the left, the navigation pane displays the forest structure: Forest: remoteworks.local > Domains > remoteworks.local > Siege Social > Marketing. The Marketing OU is selected. On the right, the main pane shows the 'Marketing' GPO list with one entry: 'Block CMD'. Below this list is a context menu for the Marketing OU, with 'Block Inheritance' highlighted. Other options in the menu include: Create a GPO in this domain, and Link it here..., Link an Existing GPO..., Block Inheritance, Group Policy Update..., Group Policy Modeling Wizard..., New Organizational Unit, View, New Window from Here, Delete, Rename, Refresh, Properties, and Help.

Precedence	GPO	Location	GPO Status	WMI Filter
1	Block CMD	Marketing	Enabled	None
2	Default Domain Policy	remoteworks.local	Enabled	None

## Exercice 6

- Créer une GPO pour toute l'organisation
- Elle doit permettre de mapper un lecteur réseau sous la lettre « P: »

- Le partage est un des dossier créé plus tôt

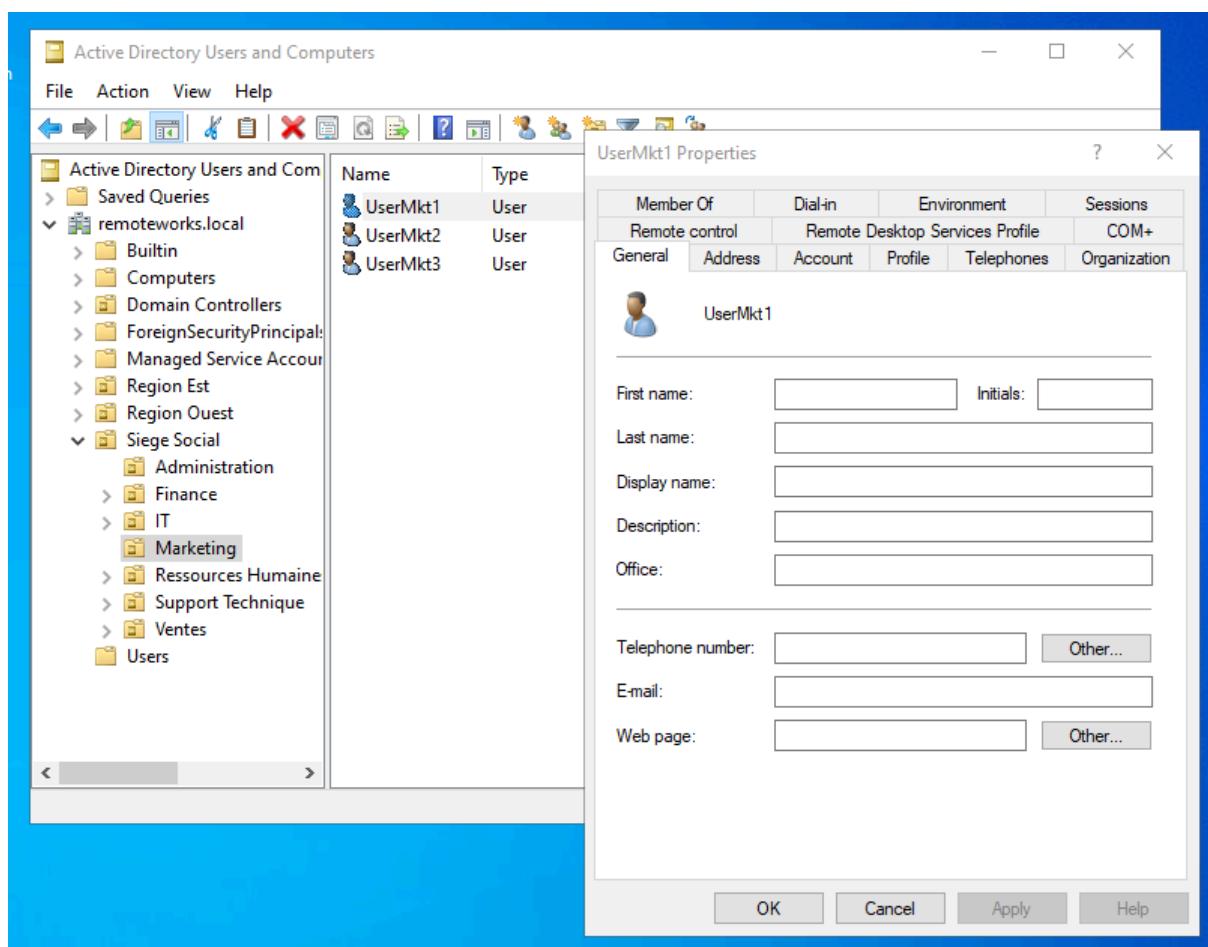
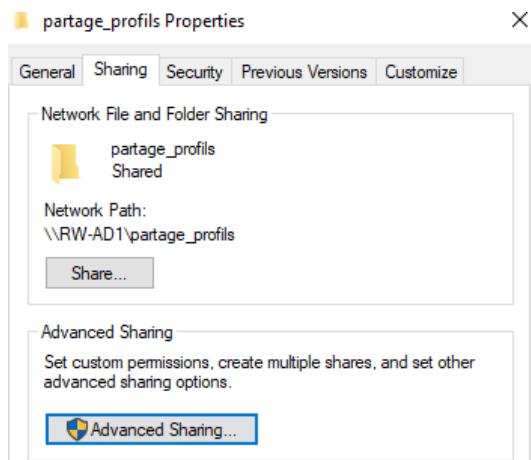


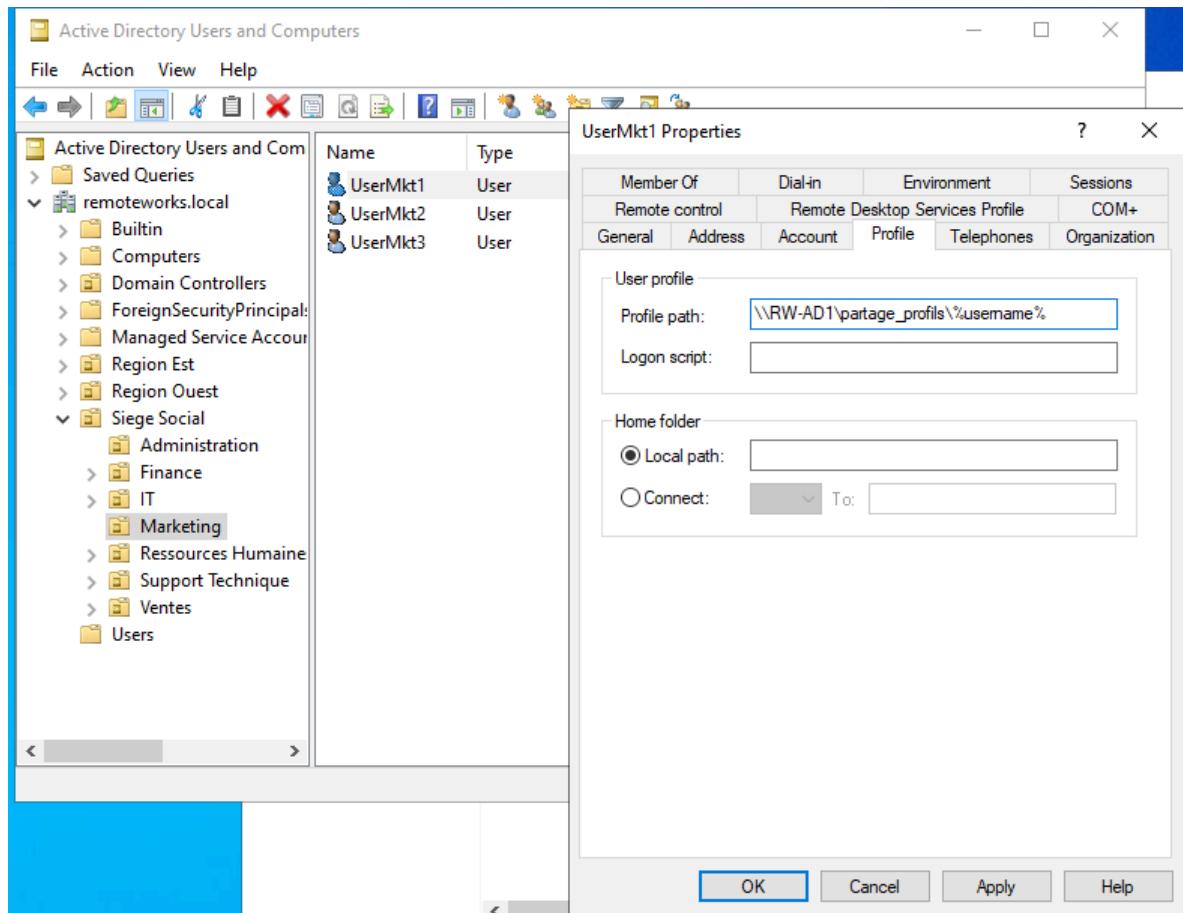
# Les profils itinérants

Un profil itinérant est un concept dans les environnements réseau Windows qui permet de stocker les paramètres et configurations utilisateur sur un serveur central. Ceci permet aux utilisateurs de retrouver leur environnement personnalisé sur n'importe quel ordinateur du réseau en se connectant avec leur identifiant.

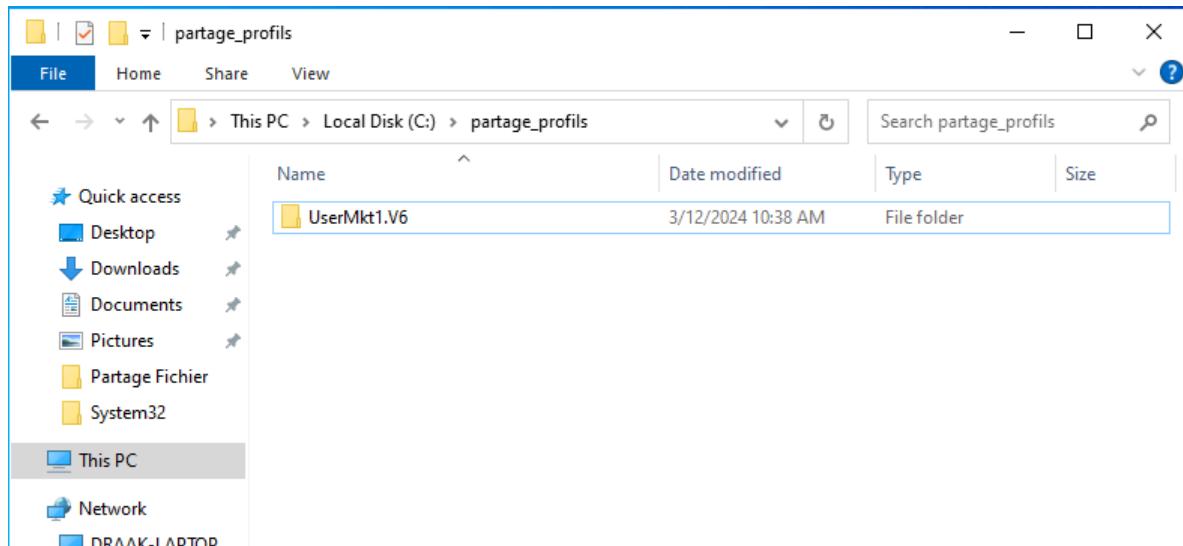
## Création d'un partage

- C:\partage\_profiles
- \RW-AD1\partage\_profiles
- \RW-AD1\partage\_profiles%username%





On redémarre le client impacté



#### Note

- Possibilité de gérer les PI via des GPO
- Possible de gérer des Quotas

## Exercice 7

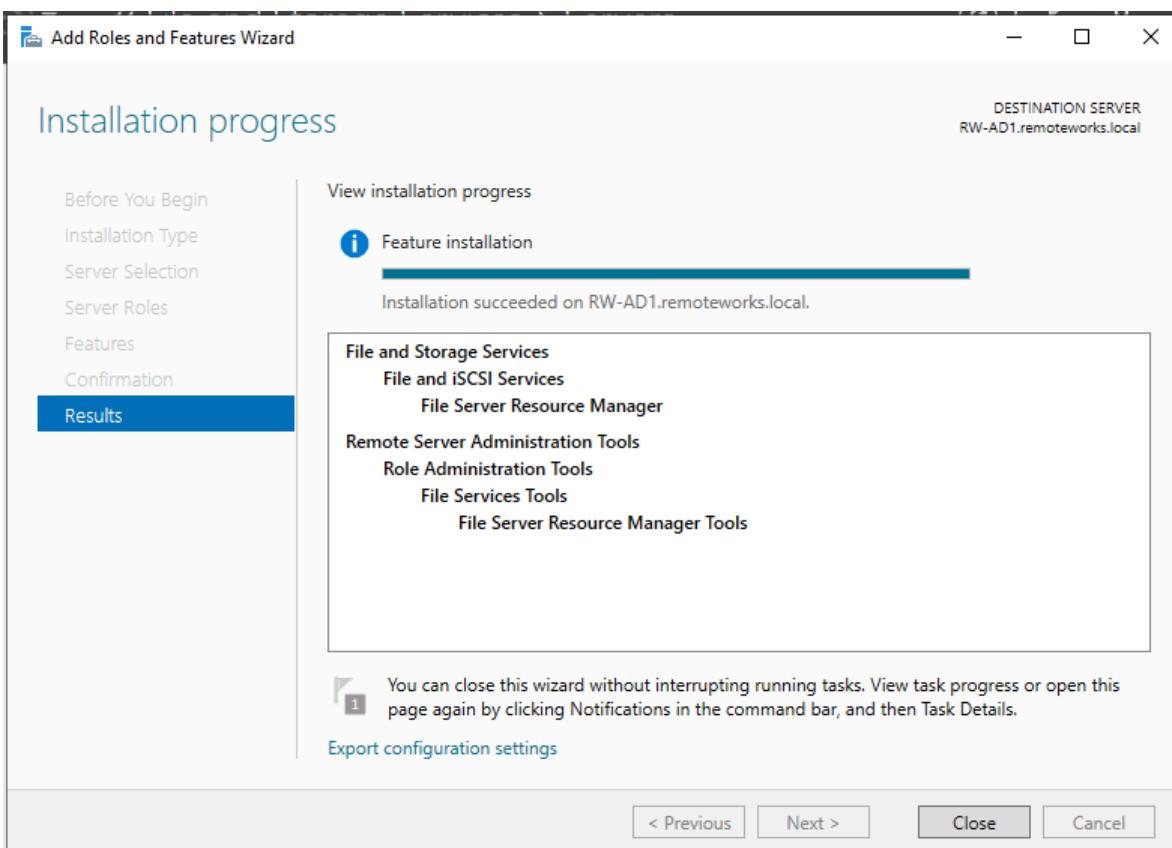
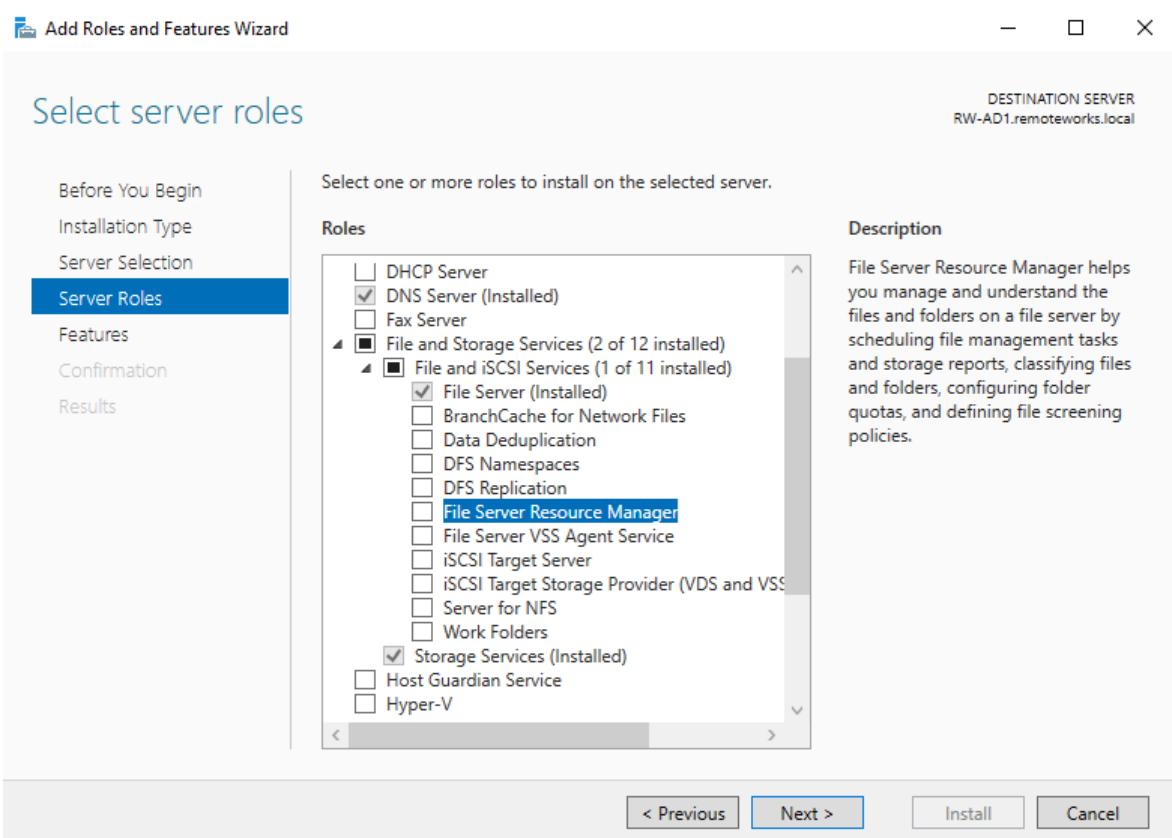
Créer une GPO pour configurer des profils itinérants

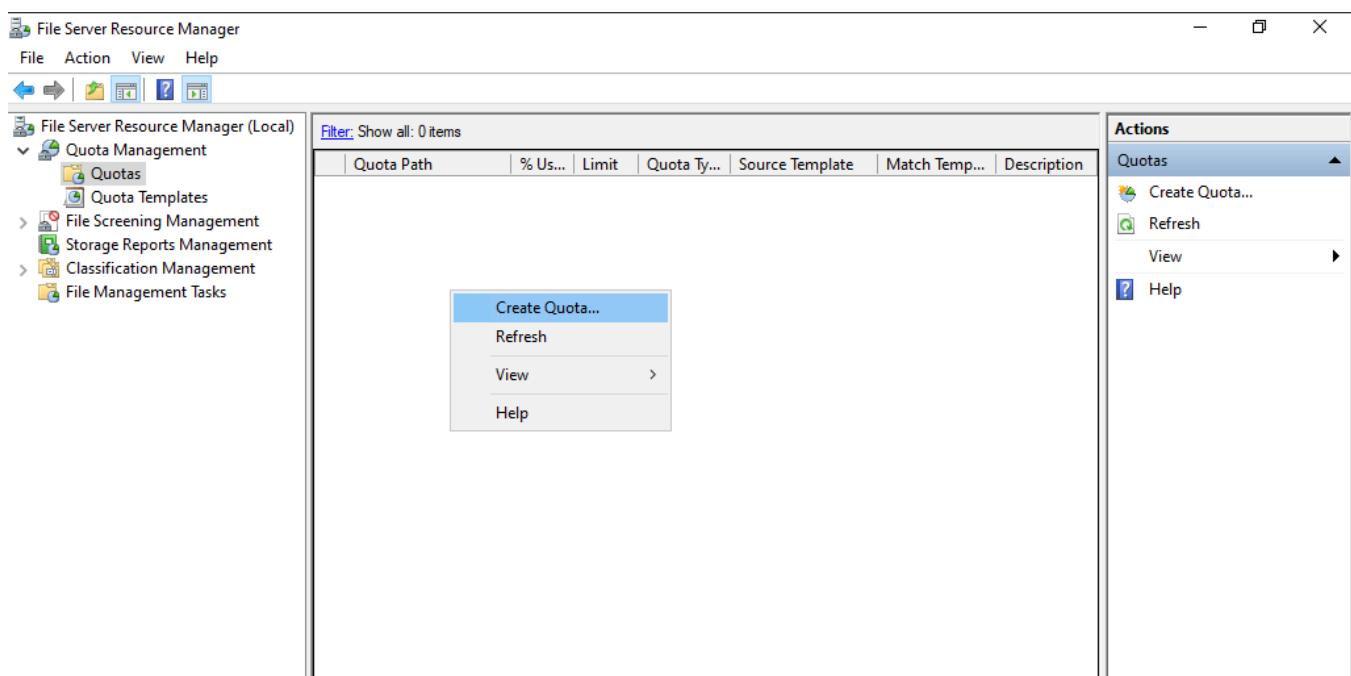
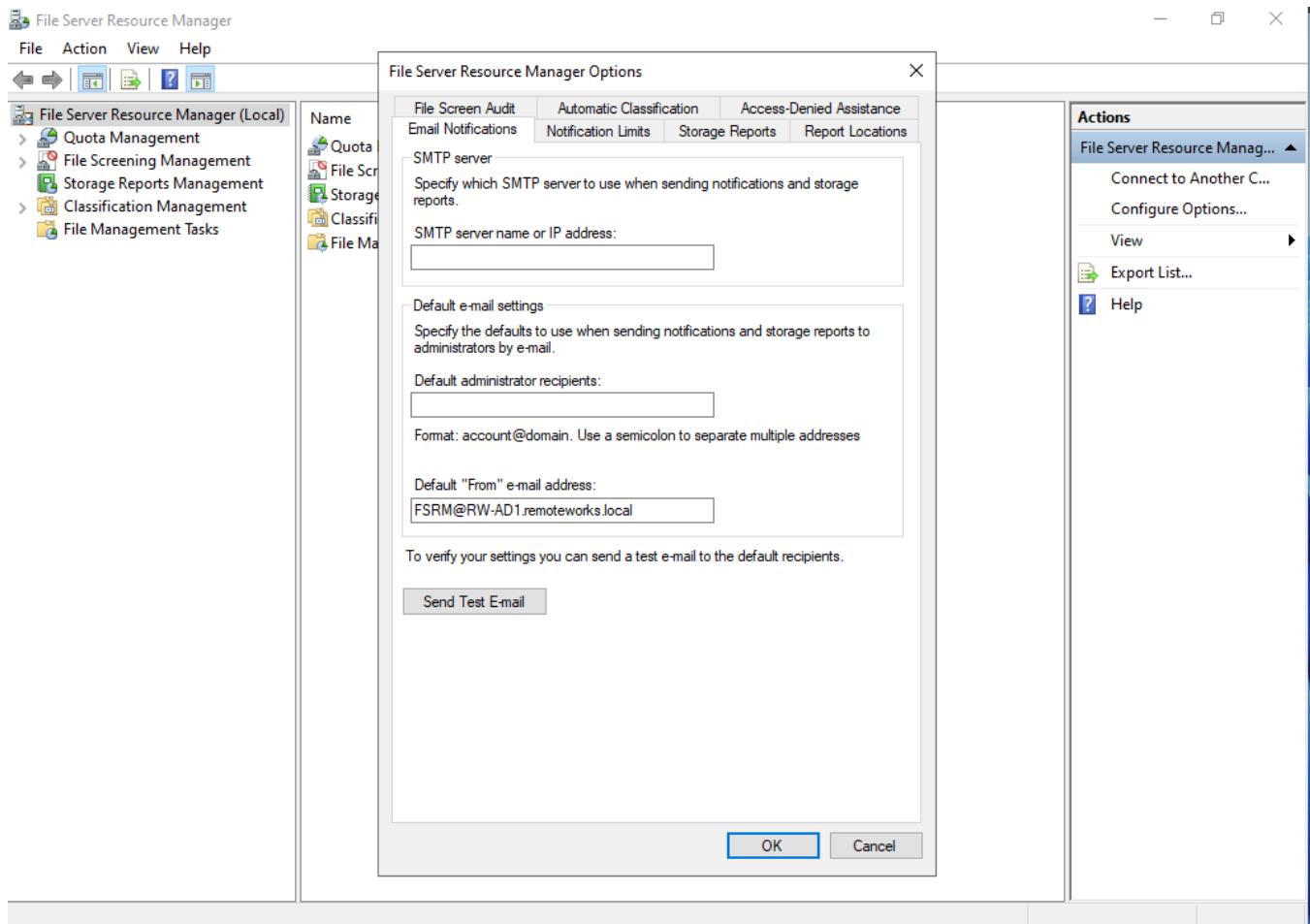
## Les quotas

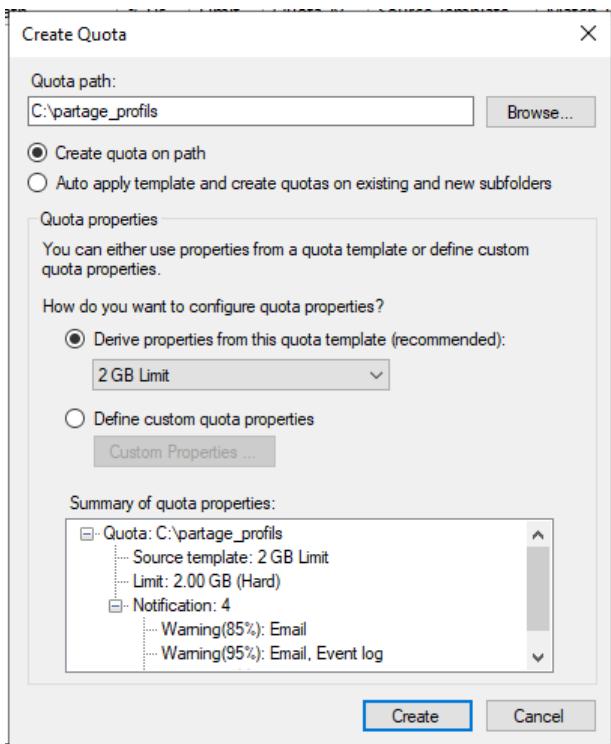
### Objectifs:

- Installer le rôle File Server Ressource Manager sur le serveur

- Ouvrir la console FSRM
- Configurer les Quotas







File Server Resource Manager

File Action View Help

File Server Resource Manager (Local)

Quota Management

Quotas

Quota Templates

File Screening Management

Storage Reports Management

Classification Management

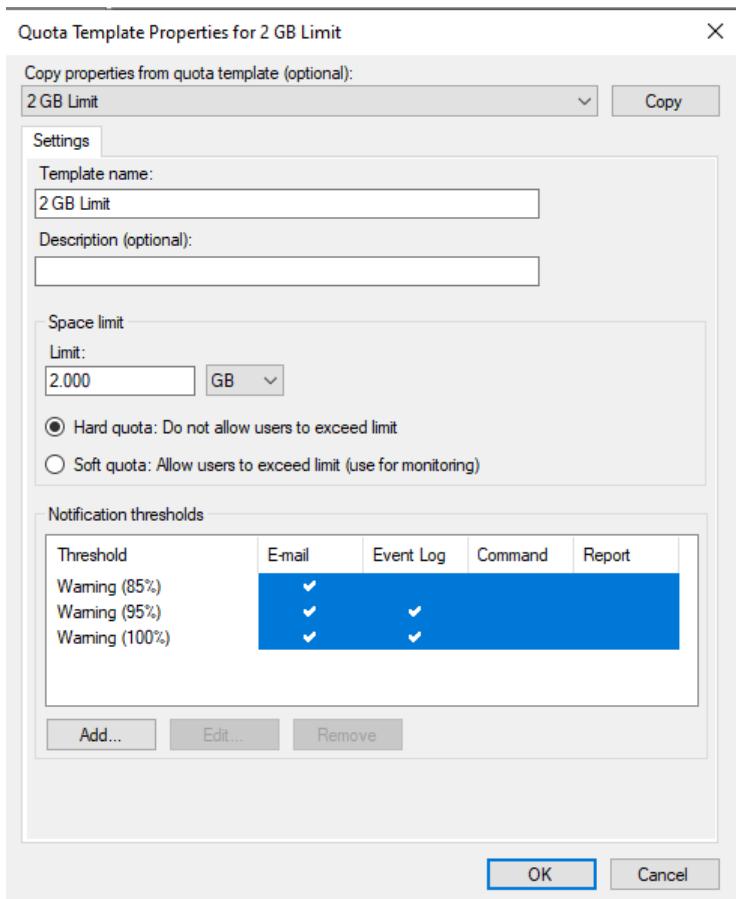
File Management Tasks

Quota Template	Limit	Quota Type	Description
10 GB Limit	10.0 GB	Hard	
100 MB Limit	100 MB	Hard	
2 GB Limit	2.00 GB	Hard	
200 MB Limit Reports to User	200 MB	Hard	
200 MB Limit with 50 MB Ext...	200 MB	Hard	
250 MB Extended Limit	250 MB	Hard	
5 GB Limit	5.00 GB	Hard	
Monitor 10 TB Volume Usage	10.0 TB	Soft	
Monitor 200 GB Volume Usage	200 GB	Soft	
Monitor 3 TB Volume Usage	3.00 TB	Soft	
Monitor 5 TB Volume Usage	5.00 TB	Soft	
Monitor 500 MB Share	500 MB	Soft	

Actions

Quota Templates

Selected Quota Templates



File Server Resource Manager

File Action View Help

Actions

Quotas

Create Quota... Refresh View Help

File Server Resource Manager (Local)

Quota Management

- Quotas
- Quota Templates

File Screening Management

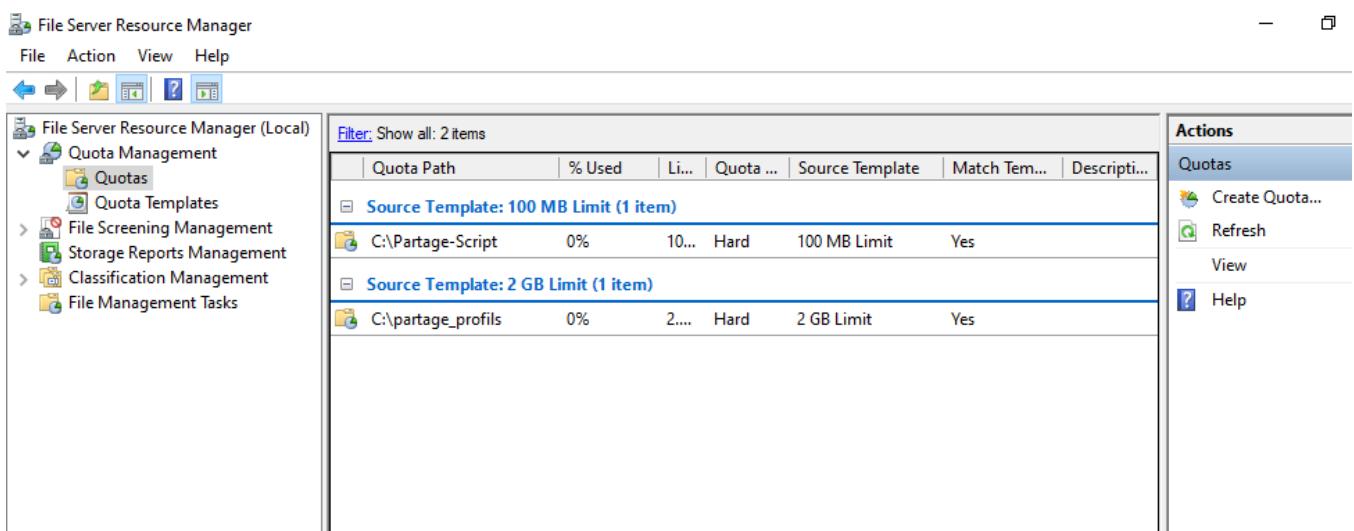
Storage Reports Management

Classification Management

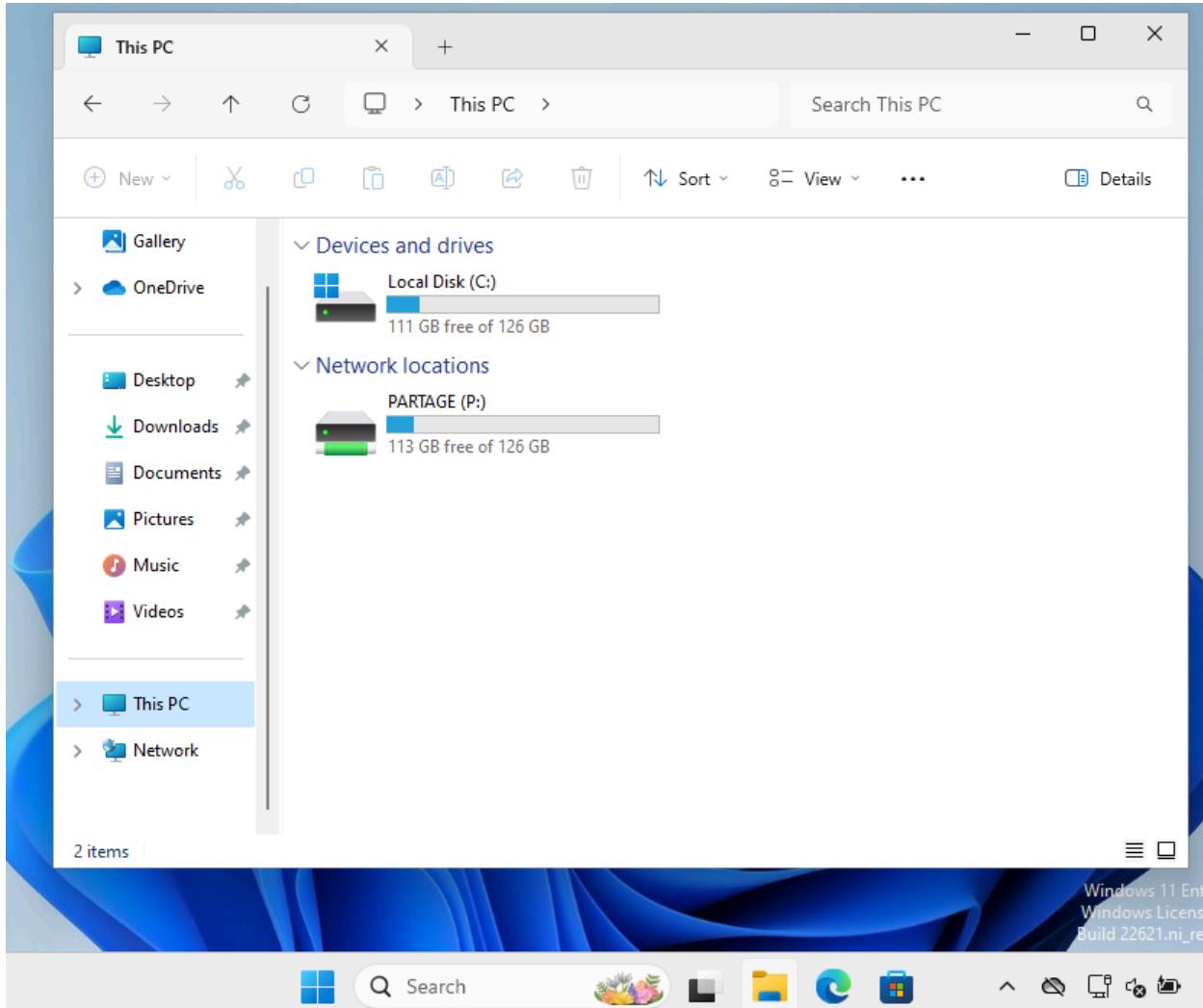
File Management Tasks

Filter: Show all: 2 items

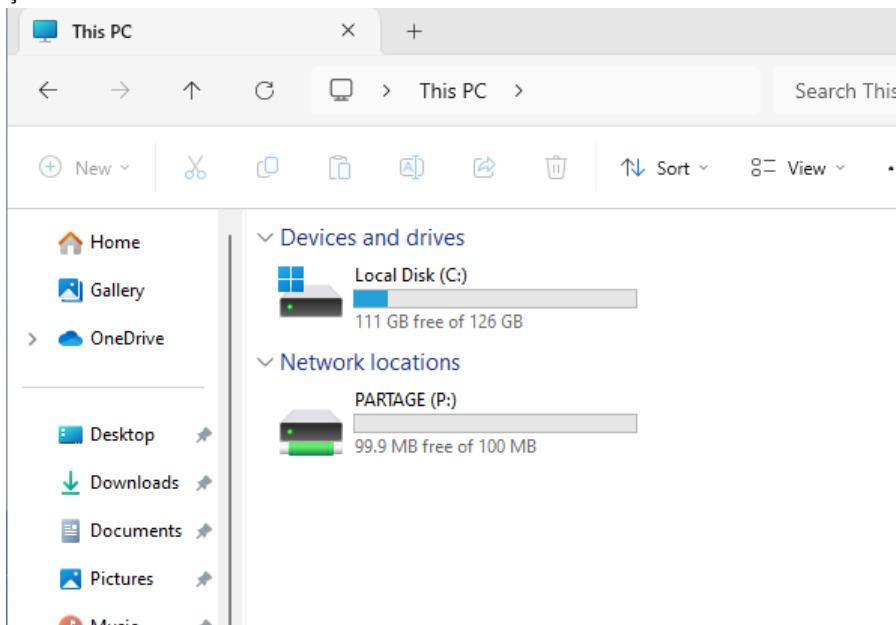
Quota Path	% Used	Li...	Quota ...	Source Template	Match Tem...	Descript...
C:\Partage-Script	0%	10...	Hard	100 MB Limit	Yes	
C:\partage_profil	0%	2....	Hard	2 GB Limit	Yes	



Originellement:



ça devient



## Les politiques de sécurité

Objectifs:

- Politique de mot de passe
  - Console DSAC.exe
- Politique de connexion

## DSAC.exe

Active Directory Administrative Center

System > Password Settings Container

Active Directory... < Password Settings Container (0)

Tasks

No results found.

Find in this column

Computers  
Domain Controllers  
ForeignSecurityPrincipals  
LostAndFound  
Managed Service Accounts  
NTDS Quotas  
Program Data  
Region Est  
Region Ouest  
Siege Social  
System  
TPM Devices  
Users

Find in this column

DomainUpdates  
File Replication Service  
FileLinks  
IP Security  
Meetings  
MicrosoftDNS  
Password Settings Container  
Policies  
PSPs  
RAS and IAS Servers Access  
RpcServices  
WinsockServices  
WMI Policy

Find in this column

>Password Settings Container

New  
Delete  
Search under this node  
Properties

Overview  
remoteworks (local)  
Dynamic Access Control  
Authentication  
Global Search

System > Password Settings Container

Active Directory... < Password Settings Container (0)

Tasks

New  
Delete  
Search under this node  
Properties

Find

Name	Precedence	Type	Description
New			Password Settings

Find in this column

Computers  
Domain Controllers  
ForeignSecurityPrincipals  
LostAndFound  
Managed Service Accounts  
NTDS Quotas  
Program Data  
Region Est  
Region Ouest  
Siege Social  
System  
TPM Devices  
Users

Find in this column

DomainUpdates  
File Replication Service  
FileLinks  
IP Security  
Meetings  
MicrosoftDNS  
Password Settings Container  
Policies  
PSPs  
RAS and IAS Servers Access  
RpcServices  
WinsockServices  
WMI Policy

Find in this column

>Password Settings Container

New  
Delete  
Search under this node  
Properties

Overview  
remoteworks (local)  
Dynamic Access Control  
Authentication  
Global Search

## Create Password Settings: politique mdp

TASKS ▾ SECTIONS ▾

**Password Settings**

**Directly Applies To**

Name	Mail
Groupe Marketing	

**OK** **Cancel**

**Active Directory...**

- Overview
- remoteworks (local)
  - ...\\Password Settings Contai...
- Dynamic Access Control
- Authentication
- Global Search

**Tasks**

- New
- Delete
- Search under this node
- Properties

**Filter**

Name	Precedence	Type	Description
politique mdp	10	Password S...	

## Les modèles utilisateurs

- Modèle basé sur les rôles** : Les permissions et accès sont attribués en fonction des rôles de travail spécifiques de l'utilisateur au sein de l'organisation, facilitant la gestion des droits d'accès selon les besoins professionnels.
- Modèle basé sur l'emplacement** : Les accès et les configurations sont définis en fonction de l'emplacement géographique de l'utilisateur, utile pour les organisations ayant plusieurs sites.
- Modèle basé sur le département** : Les utilisateurs sont organisés et gérés en fonction de leur appartenance à des départements spécifiques, avec des droits d'accès et des ressources allouées en fonction des besoins départementaux.
- Modèle hybride** : Combinaison des modèles ci-dessus pour répondre de manière flexible aux exigences complexes d'une organisation en termes de gestion des accès et des ressources.

Active Directory Users and Computers

File Action View Help

Active Directory Users and Com  
Saved Queries  
remoteworks.local  
Builtin  
Computers  
Domain Controllers  
ForeignSecurityPrincipal:  
Managed Service Accour  
Region Est  
Region Ouest  
Siege Social  
Administration  
Finance  
IT  
Marketing  
Ressources Humaine  
Support Technique  
Ventes  
Users

Name	Type	Description
UserMkt1	User	
UserMkt2	User	
UserMkt3	User	

New Object - User

Create in: remoteworks.local/Siege Social/Marketing

First name: \_marketingTemplate Initials:   
Last name:   
Full name: \_marketingTemplate

User logon name: marketingTemplate @remoteworks.local  
User logon name (pre-Windows 2000): REMOTEWORKS\marketingTemplate

< Back Next > Cancel

New Object - User

Create in: remoteworks.local/Siege Social/Marketing

Password:  Confirm password:

User must change password at next logon  
 User cannot change password  
 Password never expires  
 Account is disabled

< Back Next > Cancel

\_marketingTemplate Properties

Member Of	Dial-in	Environment	Sessions
Remote control	Remote Desktop Services Profile	COM+	
General	Address	Account	Profile
Address	Account	Profile	Telephones
Organization			

 \_marketingTemplate

First name:  Initials:   
Last name:   
Display name:   
Description:   
Office:   
  
Telephone number:  Other...  
E-mail:   
Web page:  Other...

OK Cancel Apply Help

\_marketingTemplate Properties

Member Of	Dial-in	Environment	Sessions
Remote control	Remote Desktop Services Profile	COM+	
General	Address	Account	Profile
Address	Account	Profile	Telephones
Organization			

User logon name:   
User logon name (pre-)   
Logon Hours...

Unlock account  
Account options:  
 User must change password  
 User cannot change password  
 Password never expires  
 Store password  
Account expires  Never  End of:

Logon Hours for \_marketingTemplate

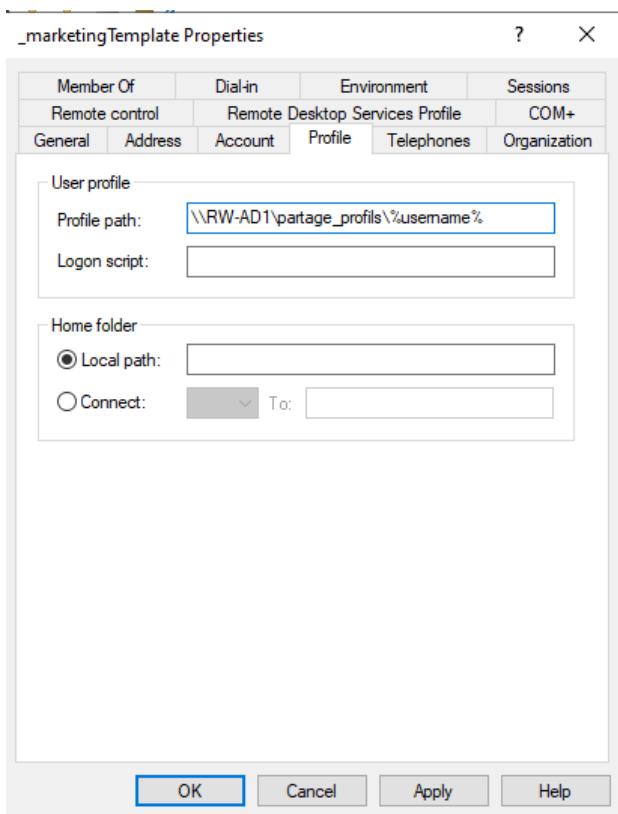
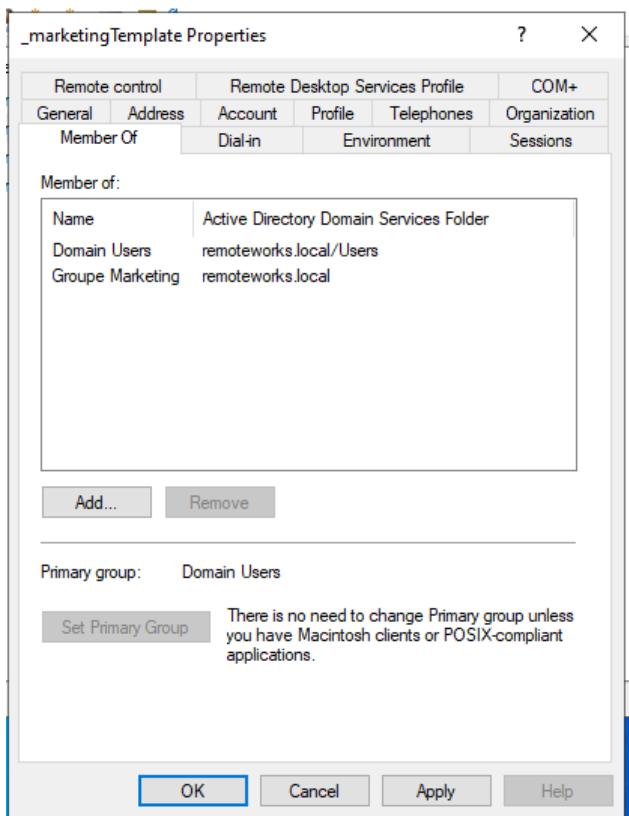
12	2	4	6	8	10	12	2	4	6	8	10	12
All												
Sunday												
Monday												
Tuesday												
Wednesday												
Thursday												
Friday												
Saturday												

OK Cancel Logon Permitted Logon Denied

Sunday through Saturday from 12:00 AM to 12:00 AM

Monday, April 11, 2024

OK Cancel Apply Help



The screenshot shows the Windows Active Directory Users and Computers management console. The left pane displays a tree view of the directory structure under 'remoteworks.local'. The right pane lists users with columns for Name, Type, and Description. A context menu is open over a user account named '\_markete' (Type: UserM). The menu includes options like Copy..., Add to a group..., Enable Account, Reset Password..., Move..., Open Home Page, Send Mail, All Tasks, Cut, Delete, Rename, Properties (which is bolded), and Help.

Copy Object - User X

---

 Create in: remoteworks.local/Siege Social/Marketing

---

First name:	<input type="text" value="user"/>	Initials:	<input type="text"/>
Last name:	<input type="text"/>		
Full name:	<input type="text" value="user"/>		

User logon name:  
  ▼

User logon name (pre-Windows 2000):

---

< Back Next > Cancel

**Copy Object - User**

---

 Create in: remoteworks.local/Siege Social/Marketing

---

Password:

Confirm password:

User must change password at next logon

User cannot change password

Password never expires

Account is disabled

---

< Back Next > Cancel

user Properties

Remote control    Remote Desktop Services Profile    COM+

Member Of	Dial-in	Environment	Sessions		
General	Address	Account	Profile	Telephones	Organization

 user

First name:  Initials:   
Last name:   
Display name:   
Description:   
Office:   
  
Telephone number:  Other...  
E-mail:   
Web page:  Other...

OK Cancel Apply Help

user Properties

Member Of    Dial-in    Environment    Sessions

Remote control	Remote Desktop Services Profile	COM+			
General	Address	Account	Profile	Telephones	Organization

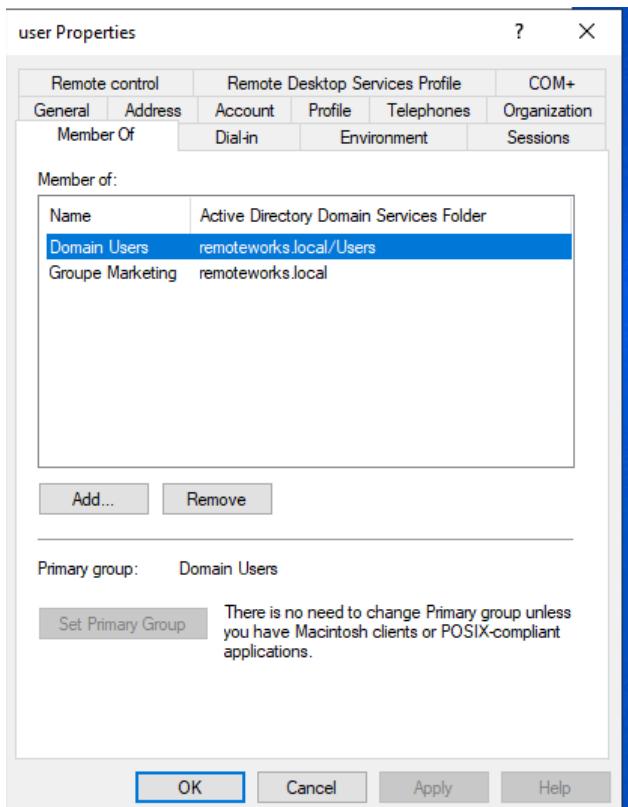
User profile

Profile path:   
Logon script:

Home folder

Local path:   
 Connect:  To:

OK Cancel Apply Help



## Les backups

### Utiliser l'outil Windows Server Backup

- **Installer Windows Server Backup** : Dans le gestionnaire de serveur, ajouter la fonctionnalité **Windows Server Backup**.
- **Configurer une tâche de sauvegarde planifiée** :
  - Ouvrir **Windows Server Backup**.
  - Sélectionner **Backup Schedule** pour créer une sauvegarde régulière.
  - Choisir une **sauvegarde complète** du volume, incluant le **System State** (nécessaire pour sauvegarder AD).
  - Indiquer un **emplacement de stockage** (disque dur externe, dossier partagé, etc.).

### Sauvegarde via PowerShell

Exécuter la commande suivante pour sauvegarder l'état du système, qui inclut les données de l'AD :

```
wbadmin start systemstatebackup -backupTarget:D:
```

- `wbadmin` est l'outil en ligne de commande pour les sauvegardes.
- `-backupTarget:D:` désigne le disque ou emplacement de stockage.

### Sauvegarde avec les Snapshots (VM)

- Si l'AD est virtualisé, utiliser les **snapshots de la machine virtuelle**.
- Cette méthode peut être pratique pour des environnements de tests ou pour un retour rapide, mais elle n'est pas recommandée pour une restauration complète en production.

### Configurer une Sauvegarde avec un Logiciel Tiers

- Utiliser des solutions de sauvegarde tierces (comme **Veeam**, **Acronis**, ou **Veritas**) qui prennent en charge les sauvegardes d'AD et permettent des restaurations granulaires.

### Points clés pour les backups d'AD

- **Planification régulière** : Pour des restaurations fiables, configurer des backups fréquents.
- **Emplacements redondants** : Stocker les backups dans des emplacements sécurisés et redondants.
- **Tests de restauration** : Valider régulièrement la qualité des backups par des restaurations tests.

## La sécurité

Les conseils de l'ANSSI

[https://cyber.gouv.fr/sites/default/files/document/anssi-guide-admin\\_securisee\\_si\\_ad\\_v1-0%20%283%29.pdf](https://cyber.gouv.fr/sites/default/files/document/anssi-guide-admin_securisee_si_ad_v1-0%20%283%29.pdf)

Un article sur les bonnes pratiques:

<https://www.it-connect.fr/comment-creer-un-domaine-active-directory-respectueux-des-bonnes-pratiques-de-securite/>

Un outil pour analyser vos GPO:

<https://www.it-connect.fr/gpozaurr-outil-ultime-pour-audit-analyser-gpo/>

Ping Castle, un outil pour auditer votre AD

<https://www.pingcastle.com/download/>

Harden.net, hardening de différents produits microsofts donc Active Directory

<https://hardenad.net/>

## Exercice 8

Mettez en place l'outil PingCastle ou HardenAD. Au choix (ou les deux).