PRINCE TOGBLE

REALISATION

MISE EN PLACE ET ADMINISTRATION DES SERVICES INFORMATIQUES

Microsoft
Active Directory

Introduction – Le rôle d'Hermes dans StadiumCompany

Hermes est le **contrôleur de domaine principal (AD DS)** et **DNS primaire** de l'infrastructure StadiumCompany.

Dans l'architecture :

- Il est dans le **VLAN 10 – Administration**
- Son IP est **172.20.1.2**
- Son nom complet est **hermes.stadiumcompany.local**
- Il porte le **domaine Active Directory : stadiumcompany.local**

🎯 Besoin dans la structure StadiumCompany

StadiumCompany a besoin :

- d'un **annuaire centralisé** pour gérer :
  - les utilisateurs
  - les groupes
  - les ordinateurs
  - les droits
- d'un **DNS interne fiable** pour :
  - résoudre les noms des serveurs (hermes, kratos1, zimbra, glpi…)
  - permettre l'authentification AD
  - permettre les services (GLPI, Nagios, Zimbra, HAProxy, etc.)
- d'un **point central de sécurité** :
  - GPO
  - politiques de mot de passe
  - restrictions machines
  - scripts de connexion

Hermes est donc :

- **le cerveau logique** du réseau
- **le référentiel d'identité** (qui est qui, qui a droit à quoi)
- **le pivot DNS** de tout le SI

Sans Hermes, ton projet StadiumCompany n'existe pas vraiment.

Partie 1 - Préparation de la VM Hermes

1.1 Création de la VM dans VMware Workstation

Paramètres recommandés :

- **Nom de la VM :** `Hermes`
- **Emplacement :** `C:\VM\StadiumCompany\Hermes\`
- **Type :** Custom (avancé)
- **Compatibilité :** Workstation 16.x
- **OS invité :**
  - Microsoft Windows
  - Windows Server 2022 (ou 2019 si besoin)

Ressources :

- **CPU :** 2 vCPU
- **RAM :** 4 Go (minimum 2 Go, mais 4 c'est confortable)
- **Disque :** 60 Go (ou plus si tu veux stocker des profils/dossiers)
- **Type de disque :** SCSI, disque unique ou scindé (comme tu préfères)

1.2 Carte réseau de Hermes

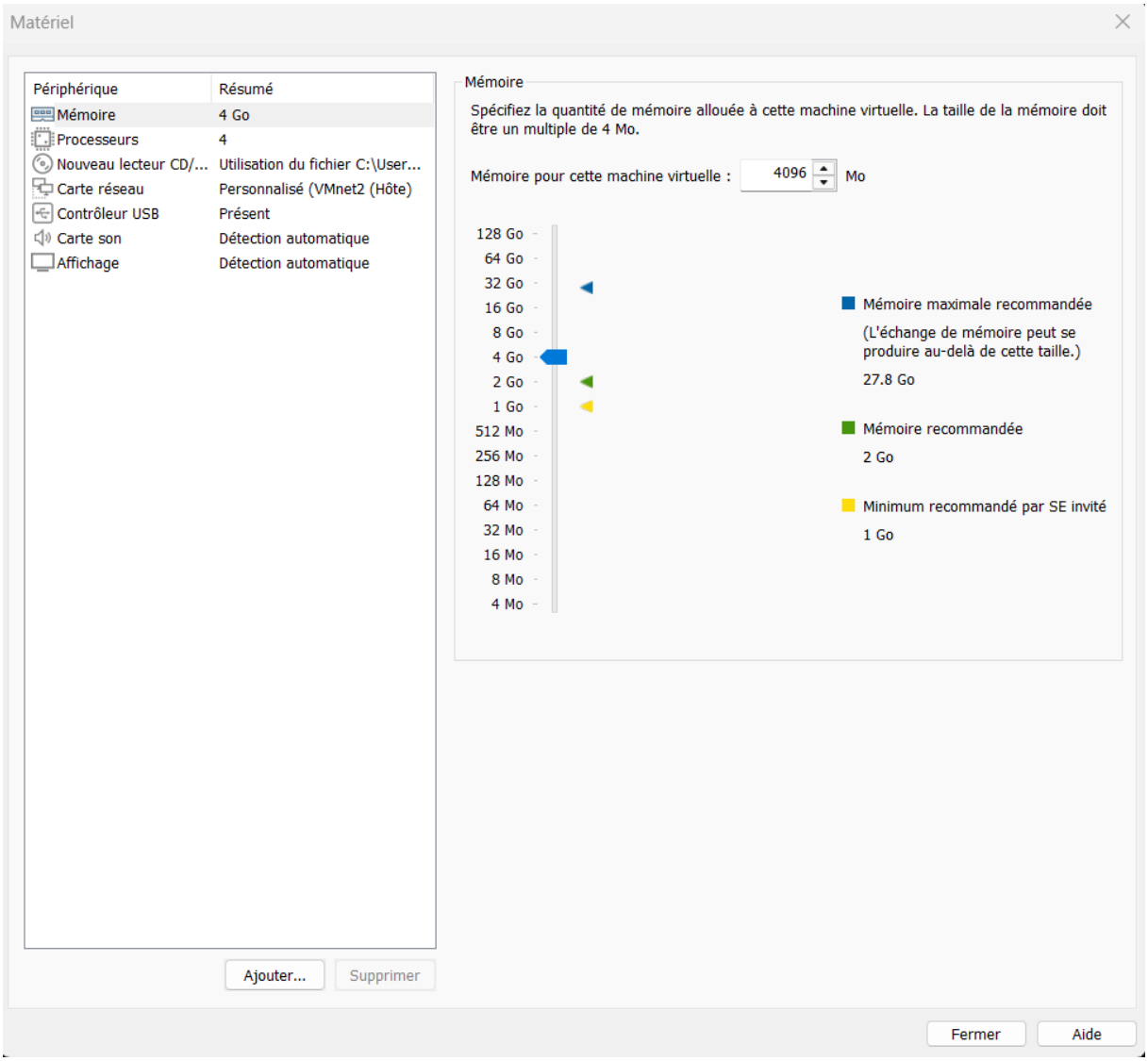
Hermes doit être dans le **VLAN 10 – Administration**, donc sur le même réseau que :

- pfSense (172.20.1.254)
- Kratos1/2
- GLPI
- Nagios
- Ares
- etc.

Dans **VM Settings > Network Adapter** :

- **Type :** Custom
- **Réseau :** VMnet correspondant au VLAN 10 (celui relié à 172.20.1.0/24)
- Exemple si tu as mappé :
  - VLAN 10 → VMnet2
  - VLAN 20 → VMnet3
  - VLAN 30 → VMnet4
  - VLAN 40 → VMnet5

Alors Hermes → **VMnet2**


Matériel
Périphérique
Résumé
Mémoire
4 Go
Processeurs
4
Nouveau lecteur CD/...
Utilisation du fichier C:\User...
Carte réseau
Personnalisé (VMnet2 (Hôte)
Contrôleur USB
Présent
Carte son
Détection automatique
Affichage
Détection automatique
Ajouter...
Supprimer
Mémoire
Spécifiez la quantité de mémoire allouée à cette machine virtuelle. La taille de la mémoire doit être un multiple de 4 Mo.
Mémoire pour cette machine virtuelle :
4096
Mo
128 Go
64 Go
32 Go
16 Go
8 Go
4 Go
2 Go
1 Go
512 Mo
256 Mo
128 Mo
64 Mo
32 Mo
16 Mo
8 Mo
4 Mo
Mémoire maximale recommandée
(L'échange de mémoire peut se produire au-delà de cette taille.)
27.8 Go
Mémoire recommandée
2 Go
Minimum recommandé par SE invité
1 Go
Fermer
Aide

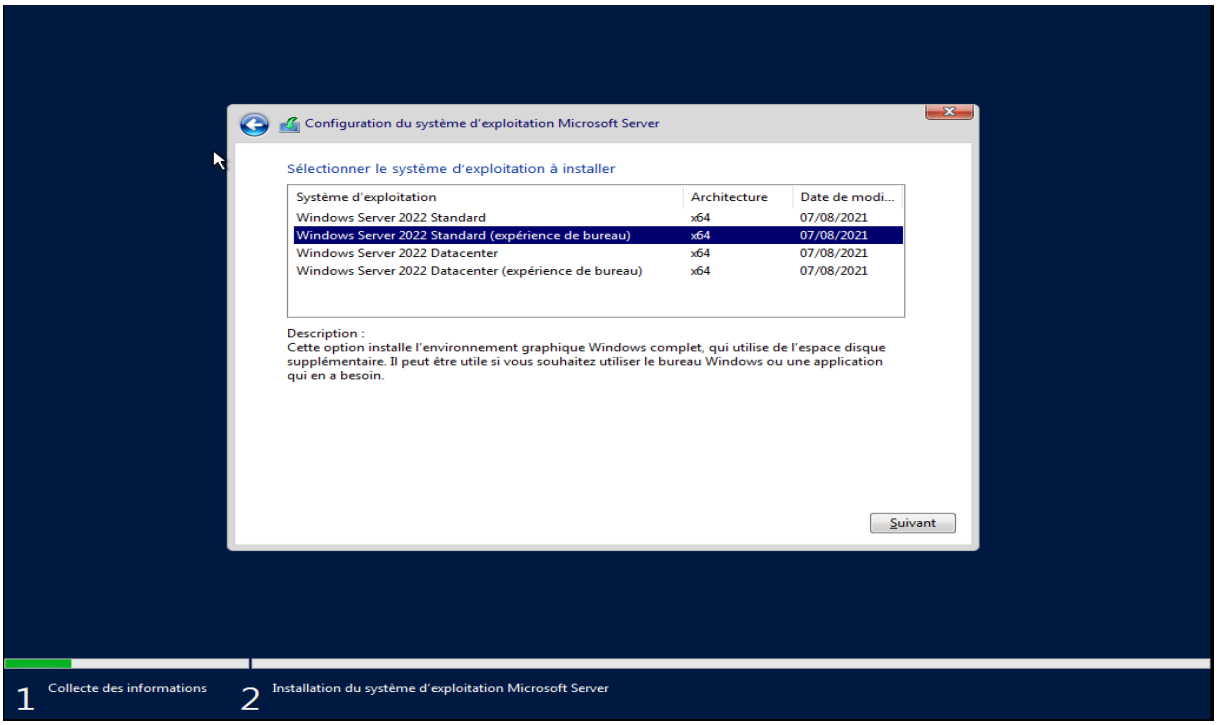
Partie 2 – Installation de Windows Server sur Hermes

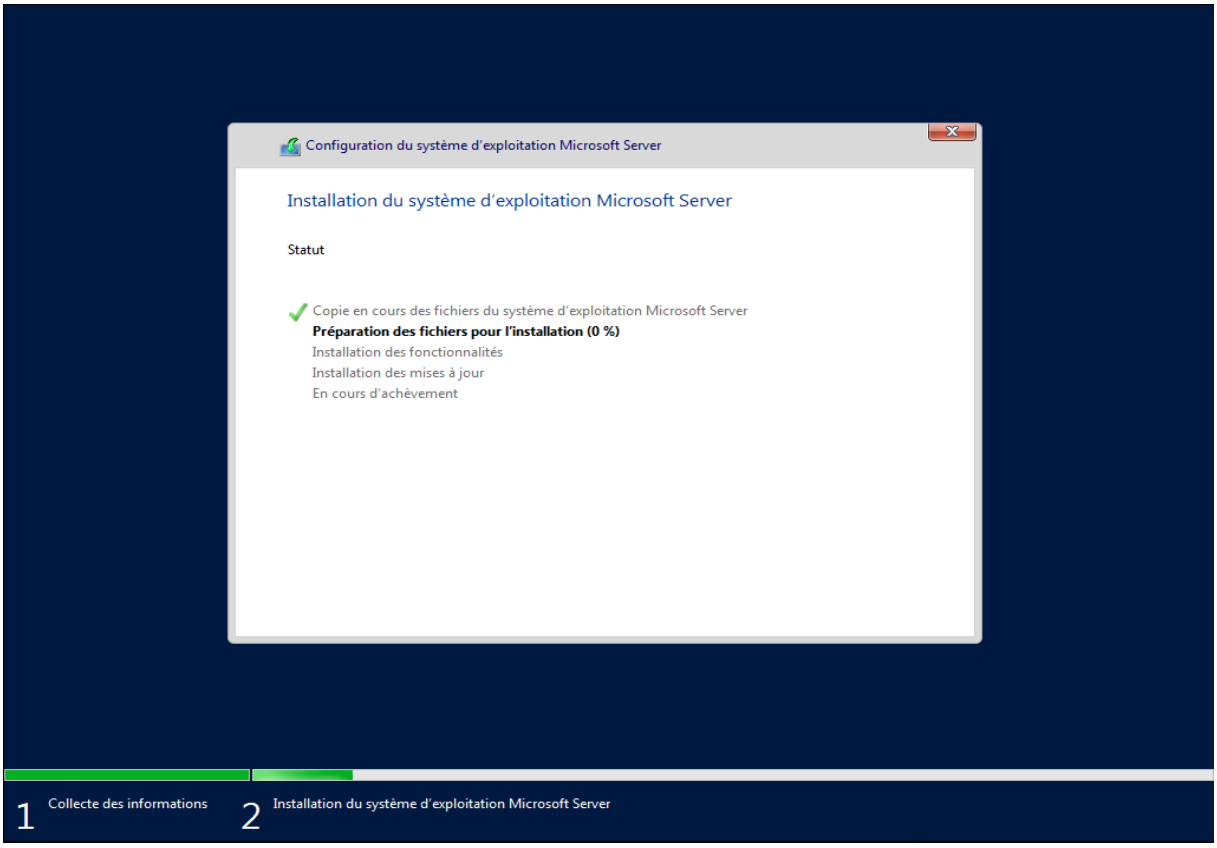
2.1 Démarrage sur l'ISO

1. Dans les paramètres de la VM Hermes :
   - CD/DVD → **Use ISO image**
   - Choisir l'ISO de **Windows Server 2022**
2. Démarrer la VM
3. Appuyer sur une touche pour booter sur le CD

2.2 Installation de base

1. Choisir la langue : **Français (France)**
2. Clavier : **Français**
3. Cliquer sur **Installer maintenant**
4. Choisir l'édition :
   - **Windows Server 2022 Standard (Expérience Desktop)**
5. Accepter la licence
6. Type d'installation : **Personnalisée**
7. Sélectionner le disque → **Nouveau** → Appliquer → Suivant
8. Laisser l'installation se faire
9. Redémarrage
10. Définir le mot de passe Administrateur :
    - `Bts2024@` (conforme à ton environnement)



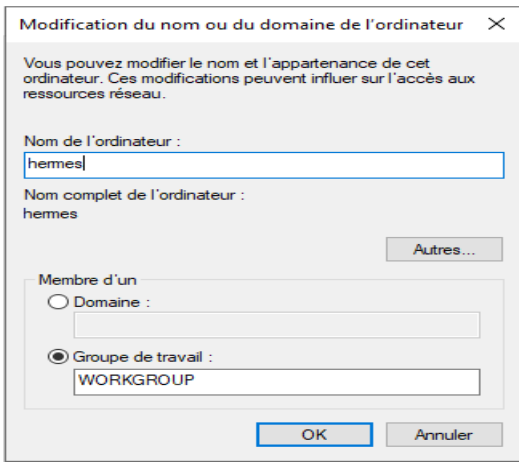


Partie 3 – Configuration réseau de Hermes

Une fois Windows installé et connecté en Administrateur :

3.1 Renommer la machine

1. Clic droit sur **Ce PC** → Propriétés
2. **Renommer ce PC**
3. Nom : `Hermes`
4. Redémarrer



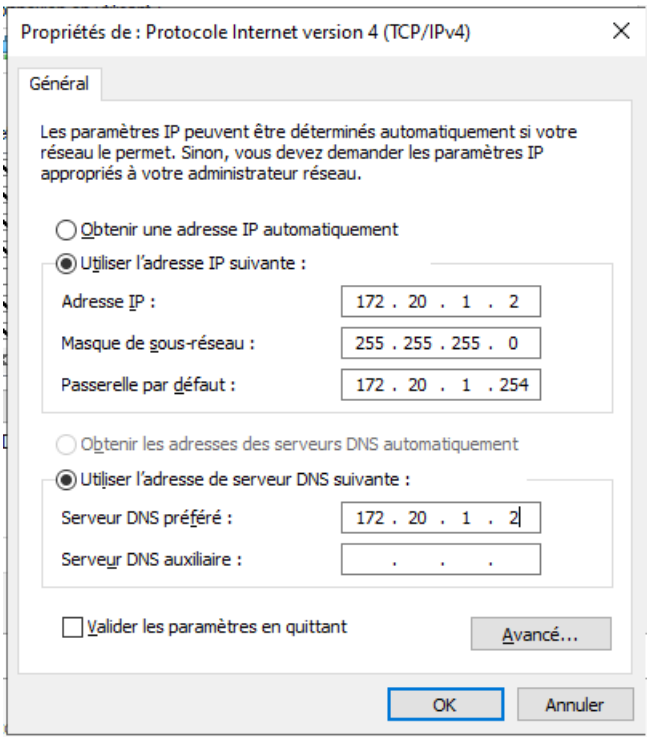
3.2 Configurer l'adresse IP

Aller dans :

- **Panneau de configuration > Réseau et Internet > Centre Réseau et partage > Modifier les paramètres de la carte**
- Clic droit sur la carte réseau → Propriétés
- Double clic sur **Protocole Internet version 4 (TCP/IPv4)**

Configurer :

- **Adresse IP :** `172.20.1.2`
- **Masque :** `255.255.255.0`
- **Passerelle :** `172.20.1.254` (pfSense – interface Admin)
- **DNS préféré :** `172.20.1.2` (lui-même)
- **DNS alternatif :** (vide pour l'instant, tu mettras Ares plus tard)



Tester :

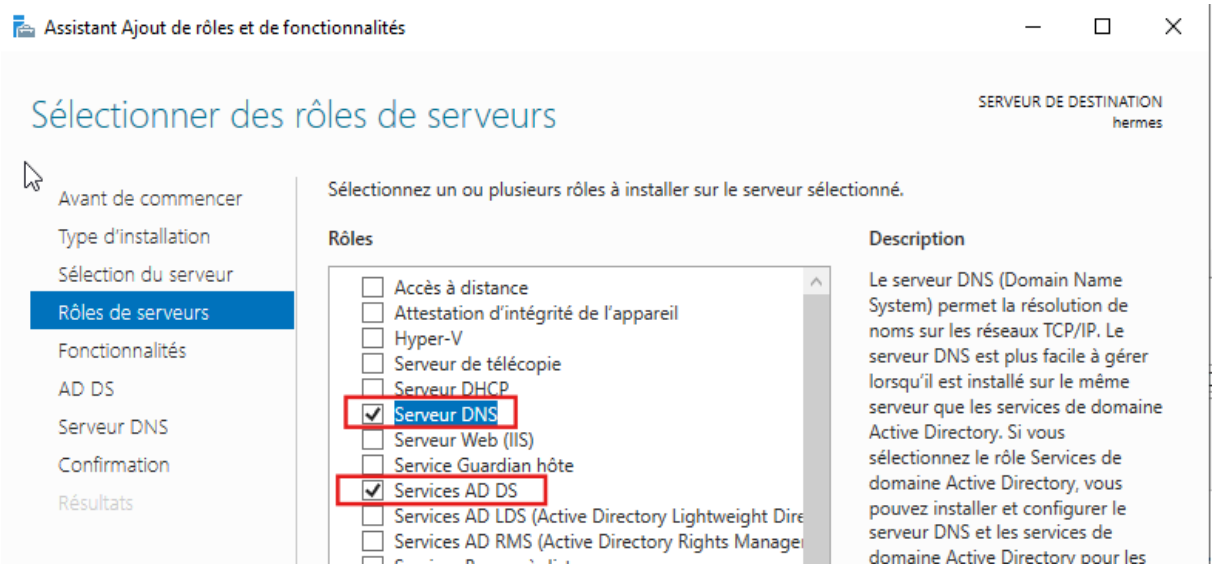
- `ping 172.20.1.254` → pfSense
- `ping 8.8.8.8` → Internet (si NAT OK)
- `ping google.fr` → test DNS (fonctionnera après installation DNS)

```
PS C:\Users\Administrateur> ping 172.20.1.254

Envoi d'une requête 'Ping'  172.20.1.254 avec 32 octets de données :
Réponse de 172.20.1.254 : octets=32 temps<1ms TTL=64
Réponse de 172.20.1.254 : octets=32 temps<1ms TTL=64
Réponse de 172.20.1.254 : octets=32 temps=1 ms TTL=64
Réponse de 172.20.1.254 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 172.20.1.254:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms
PS C:\Users\Administrateur> ping 8.8.8.8

Envoi d'une requête 'Ping'  8.8.8.8 avec 32 octets de données :
Réponse de 8.8.8.8 : octets=32 temps=8 ms TTL=115
Réponse de 8.8.8.8 : octets=32 temps=5 ms TTL=115
Réponse de 8.8.8.8 : octets=32 temps=9 ms TTL=115
Réponse de 8.8.8.8 : octets=32 temps=6 ms TTL=115

Statistiques Ping pour 8.8.8.8:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 5ms, Maximum = 9ms, Moyenne = 7ms
```

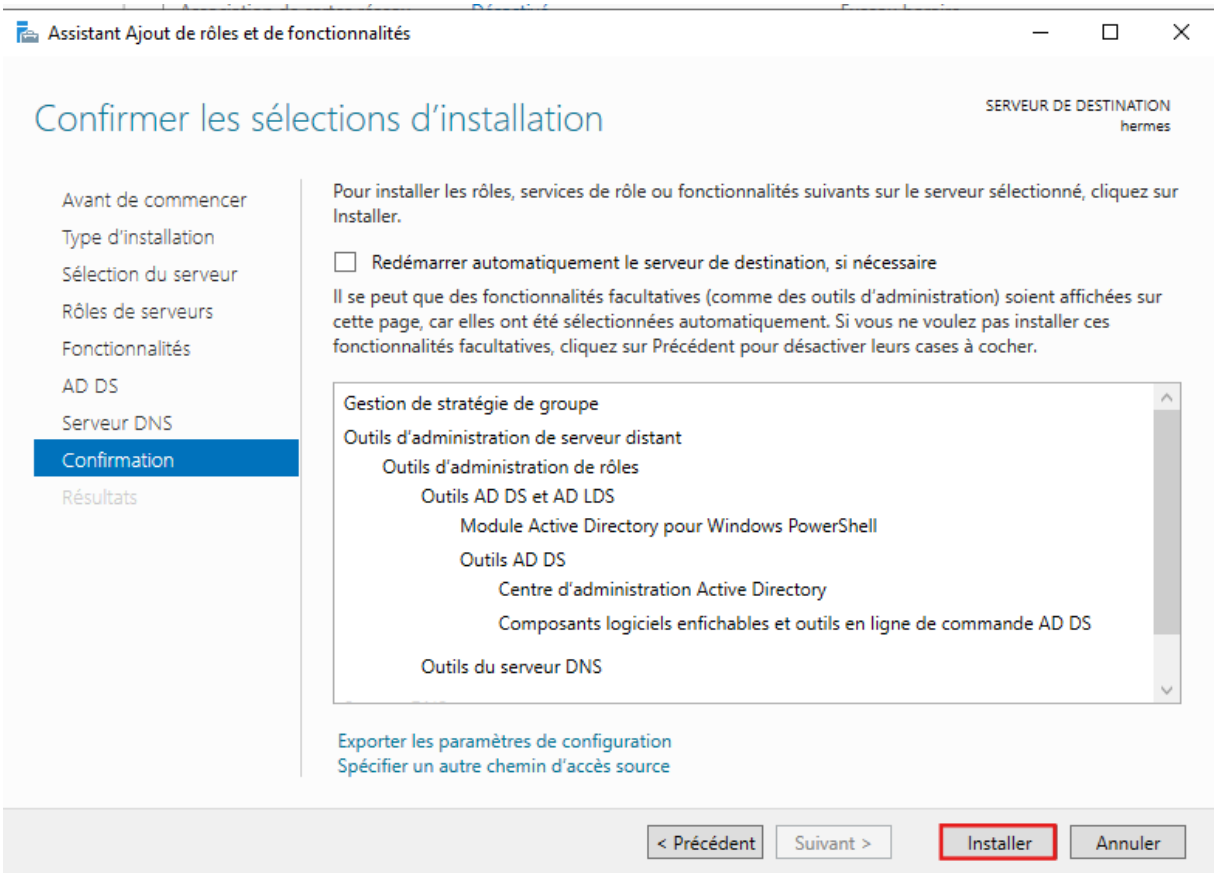
Partie 4 – Promotion de Hermes en contrôleur de domaine (AD DS)

4.1 Installation du rôle AD DS + DNS

1. Ouvrir **Gestionnaire de serveur**
2. Cliquer sur **Ajouter des rôles et fonctionnalités**
3. Type d'installation : **Installation basée sur un rôle ou une fonctionnalité**
4. Serveur : Hermes (local)
5. Rôles :
    - **Services de domaine Active Directory**
    - **Serveur DNS**



6. Accepter les fonctionnalités supplémentaires
7. Suivant → Installer



8. Redémarrer si demandé

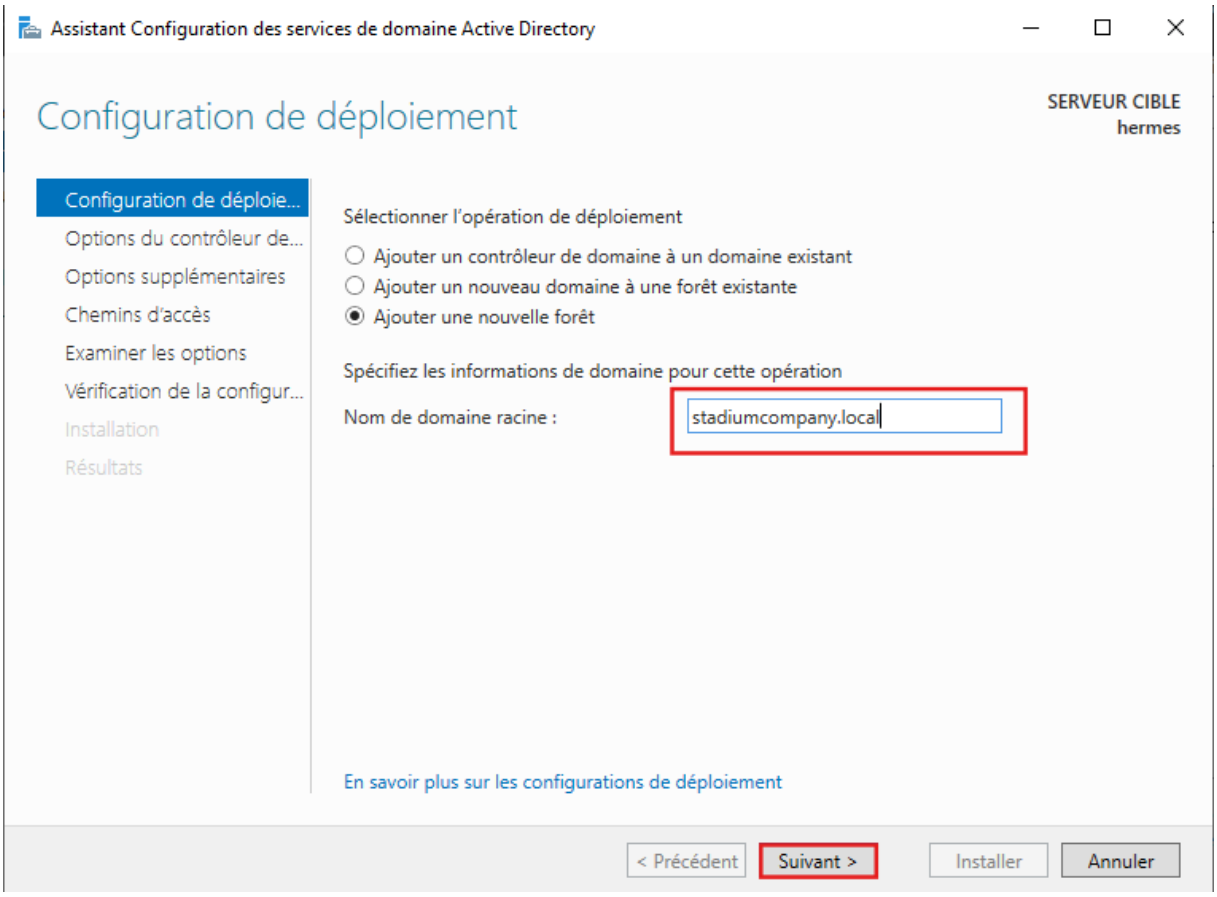
4.2 Promotion en contrôleur de domaine

Après l'installation, en haut à droite dans le Gestionnaire de serveur :

- Un drapeau jaune apparaît → **Promouvoir ce serveur en contrôleur de domaine**

Choisir :

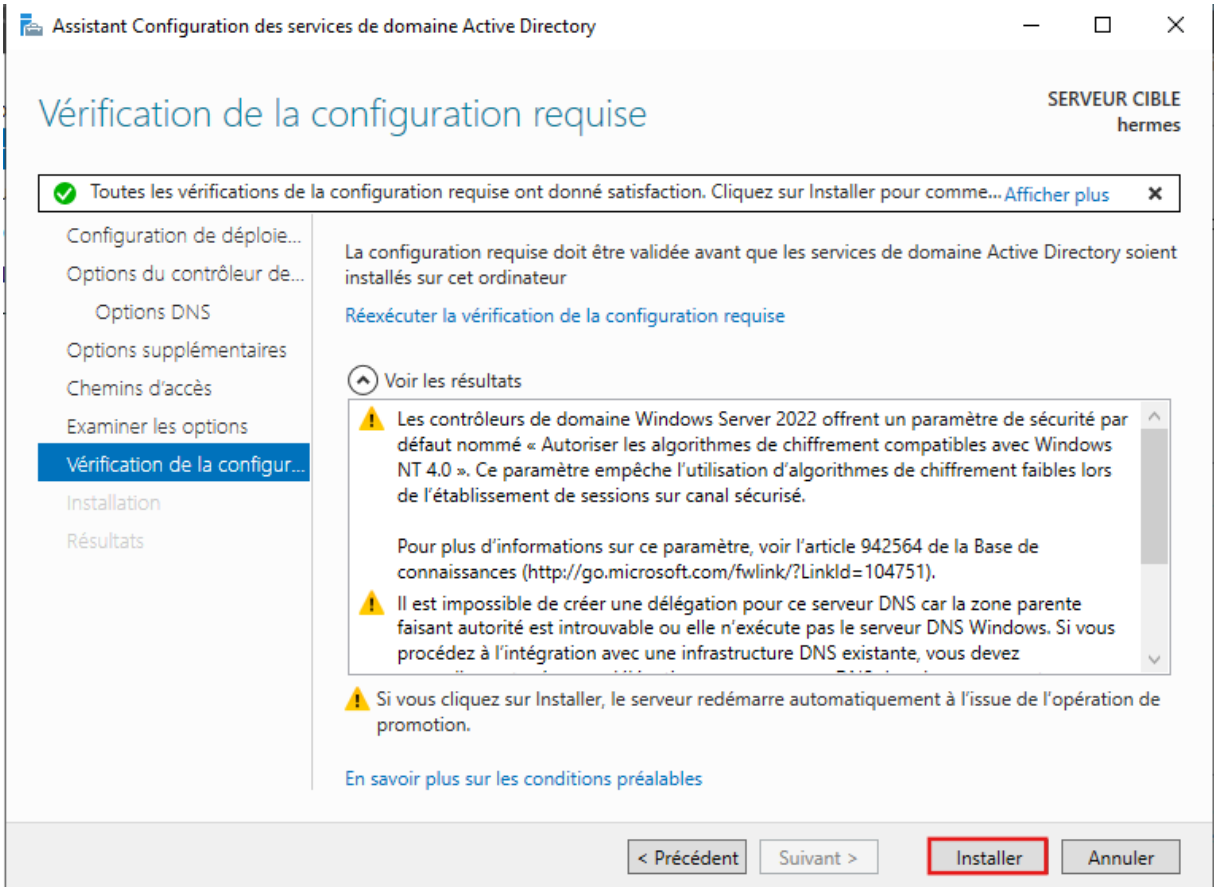
- **Ajouter une nouvelle forêt**
  - Nom de domaine racine : `stadiumcompany.local`



Paramètres :

- Niveau fonctionnel forêt : Windows Server 2016/2019/2022
- Niveau fonctionnel domaine : idem
- Cocher **Serveur DNS**
- Mot de passe du mode de restauration (DSRM) : `Bts2024@` (par exemple)

Suivant → Suivant → Installer



Le serveur redémarre.

Partie 5 – Configuration DNS sur Hermes

Une fois Hermes redémarré, se connecter avec :

- Domaine : `STADIUMCOMPANY`
- Utilisateur : `Administrateur`
- Mot de passe : `Bts2024@`

5.1 Vérifier la zone DNS

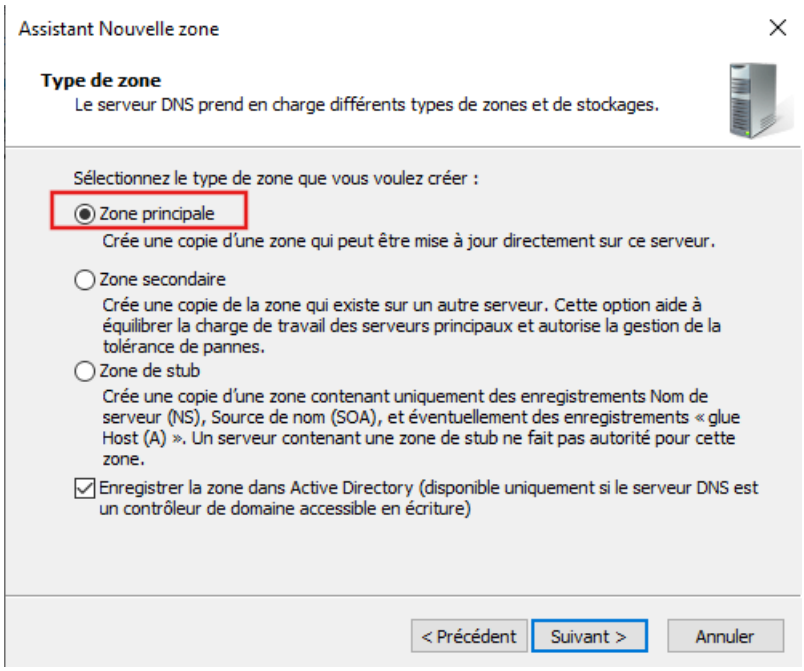
Ouvrir **Outils > DNS**

- Zone de recherche directe :
  - `stadiumcompany.local`
  - Tu dois voir :
    - `hermes` (A → 172.20.1.2)

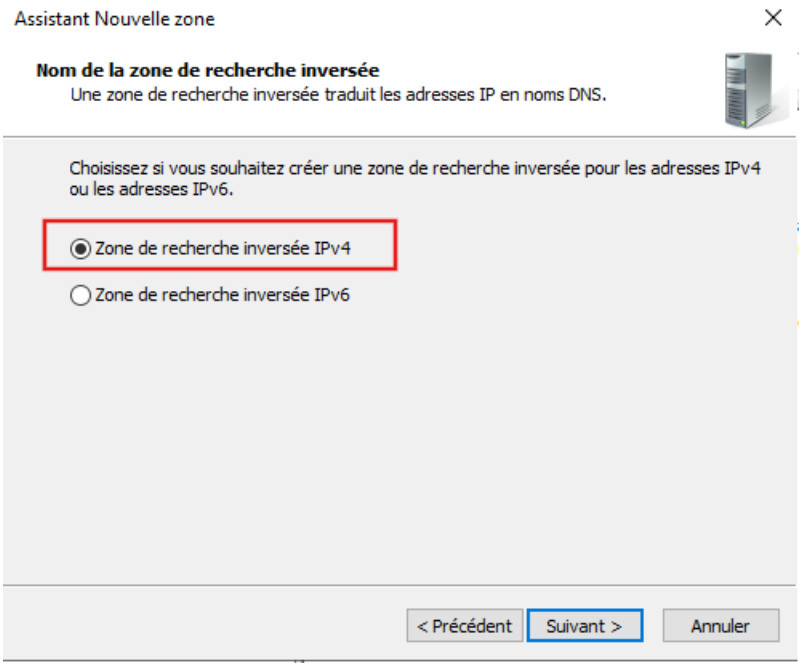
5.2 Créer la zone de recherche inversée

Toujours dans DNS :

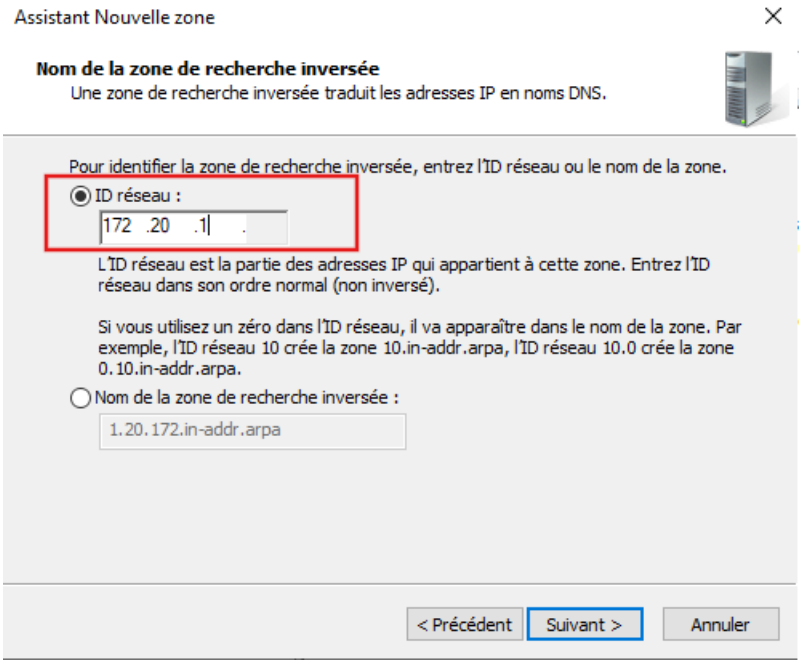
1. Clic droit sur **Zones de recherche inversée** → Nouvelle zone
2. Zone principale



3. Réseau IPv4

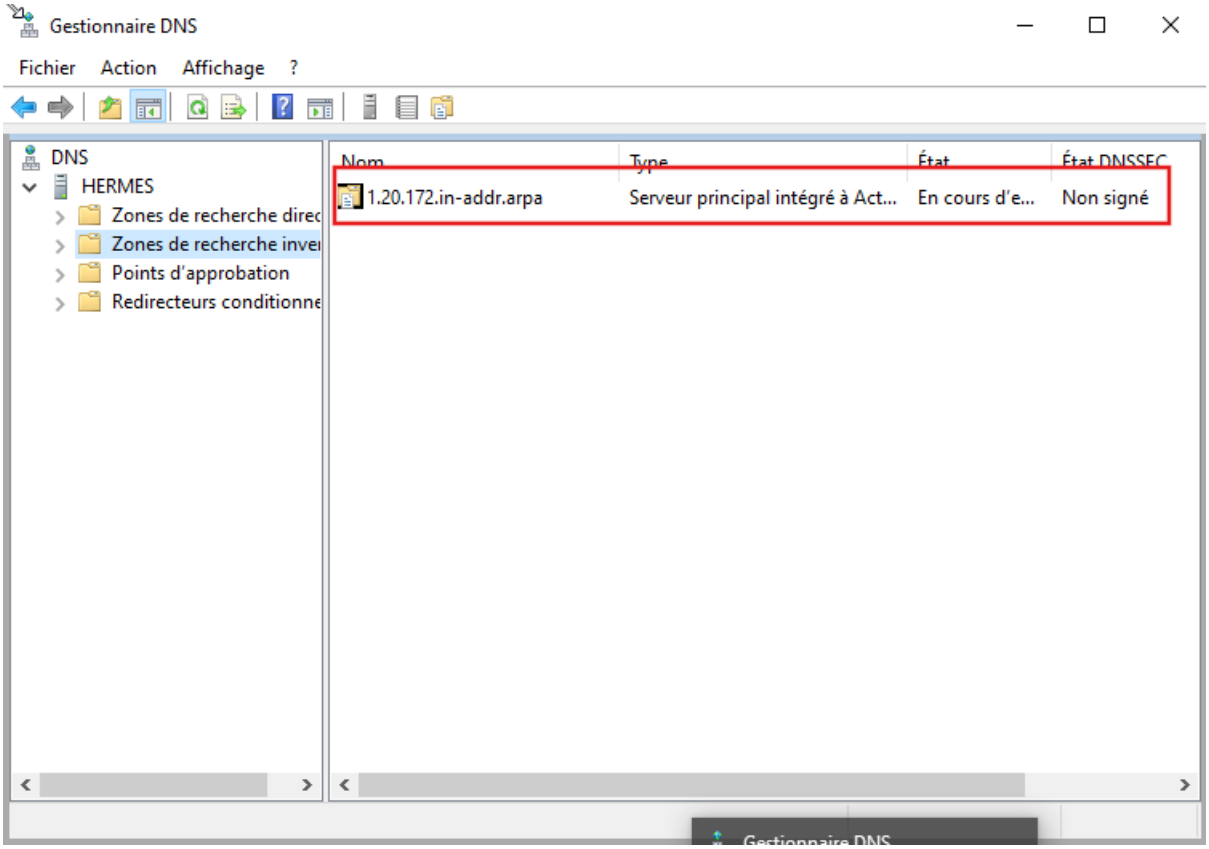


4. ID réseau : `172.20.1`
5. Nom de zone : `1.20.172.in-addr.arpa`



6. Terminer

Vérifier que Hermes a un enregistrement PTR.



PARTIE 6 – STRUCTURE ACTIVE DIRECTORY (SUITE ET VERSION AMÉLIORÉE)

Après la promotion d'Hermes en contrôleur de domaine, il est nécessaire de structurer l'annuaire Active Directory afin d'organiser les utilisateurs, les groupes, les ordinateurs et les stratégies de sécurité.

Cette étape est essentielle pour :

- séparer les services
- appliquer des GPO ciblées
- préparer l'arrivée des serveurs Kratos (DHCP), Ares (DNS secondaire), GLPI, OCS, Nagios, etc.
- respecter le cahier des charges StadiumCompany

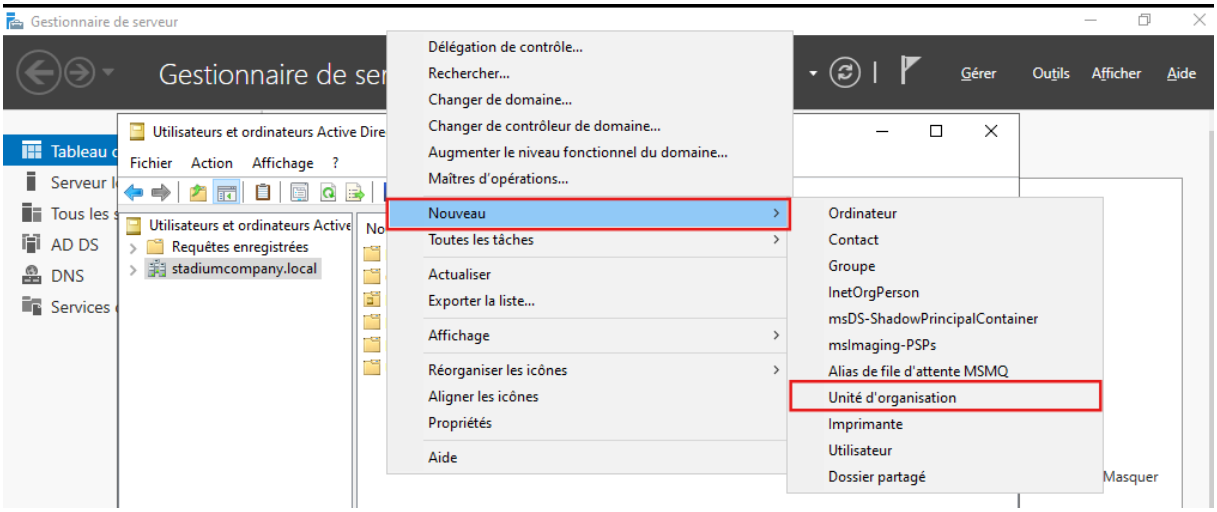
6.1 Création des Unités d'Organisation (UO)

📌 Objectif

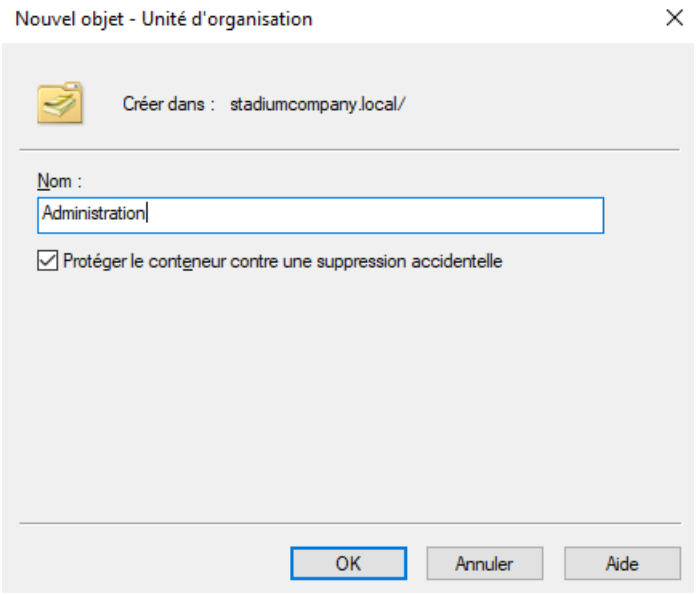
Organiser l'annuaire en fonction des services de StadiumCompany.

🔧 Étapes

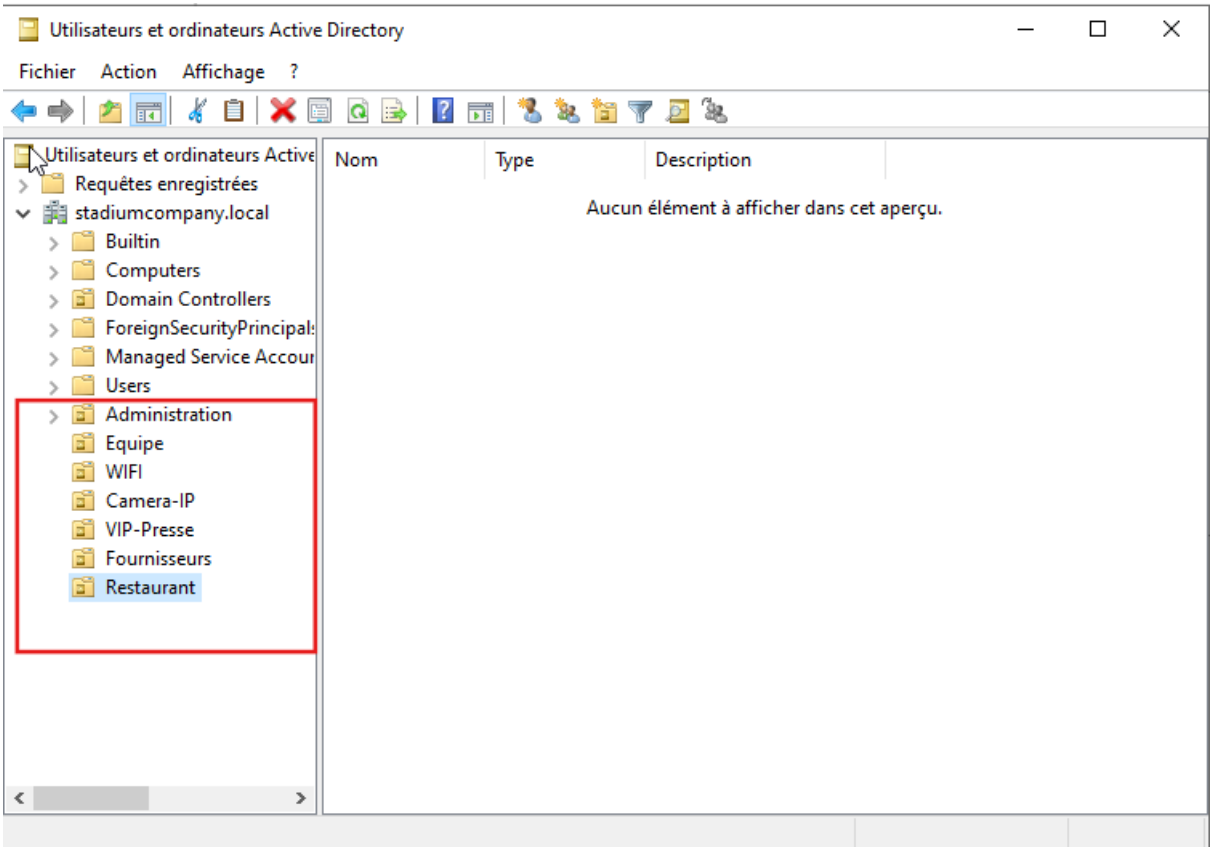
1. Ouvrir :
   Gestionnaire de serveur → Outils → Utilisateurs et ordinateurs Active Directory
2. Dans le domaine :
   stadiumcompany.local
3. Clic droit → **Nouveau → Unité d'organisation**



4. Créer les UO principales suivantes :

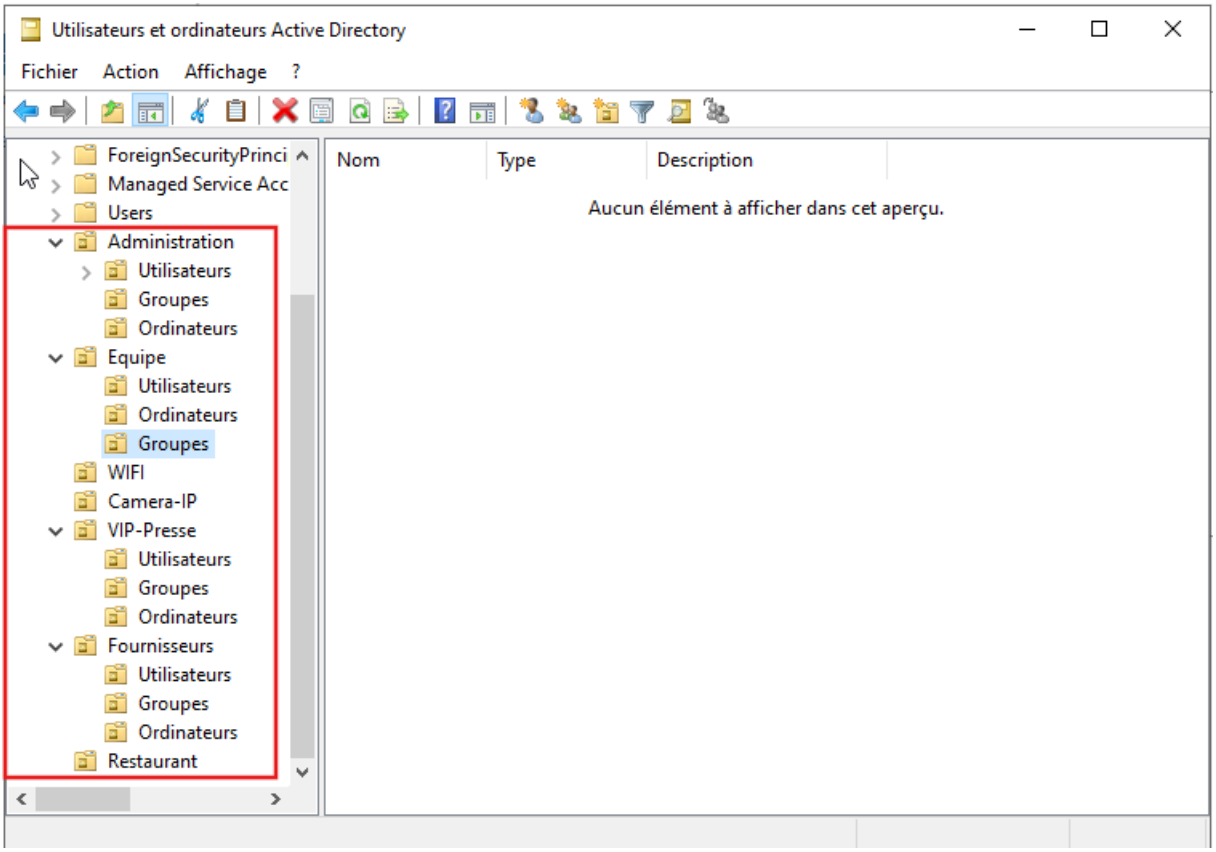


Administration
Équipe
WiFi
Caméra-IP
VIP-Presse
Fournisseurs
Restaurant



5. Dans les UO qui contiennent du personnel (Administration, Équipe, Fournisseurs, Restaurant, VIP-Presse), créer les sous-UO :

```
Utilisateurs
Groupes
Ordinateurs
```



☞ Cette structure respecte parfaitement le cahier des charges du projet StadiumCompany.

6.2 Création des GPO (Stratégies de groupe)

Les GPO permettent d'appliquer des règles automatiques aux utilisateurs et aux ordinateurs du domaine.

Nous allons créer :

- une GPO pour **déployer un fond d'écran**
- une GPO pour **mapper un lecteur réseau**
- une GPO pour **bloquer l'accès au panneau de configuration**

6.2.1 GPO – Déploiement du fond d'écran

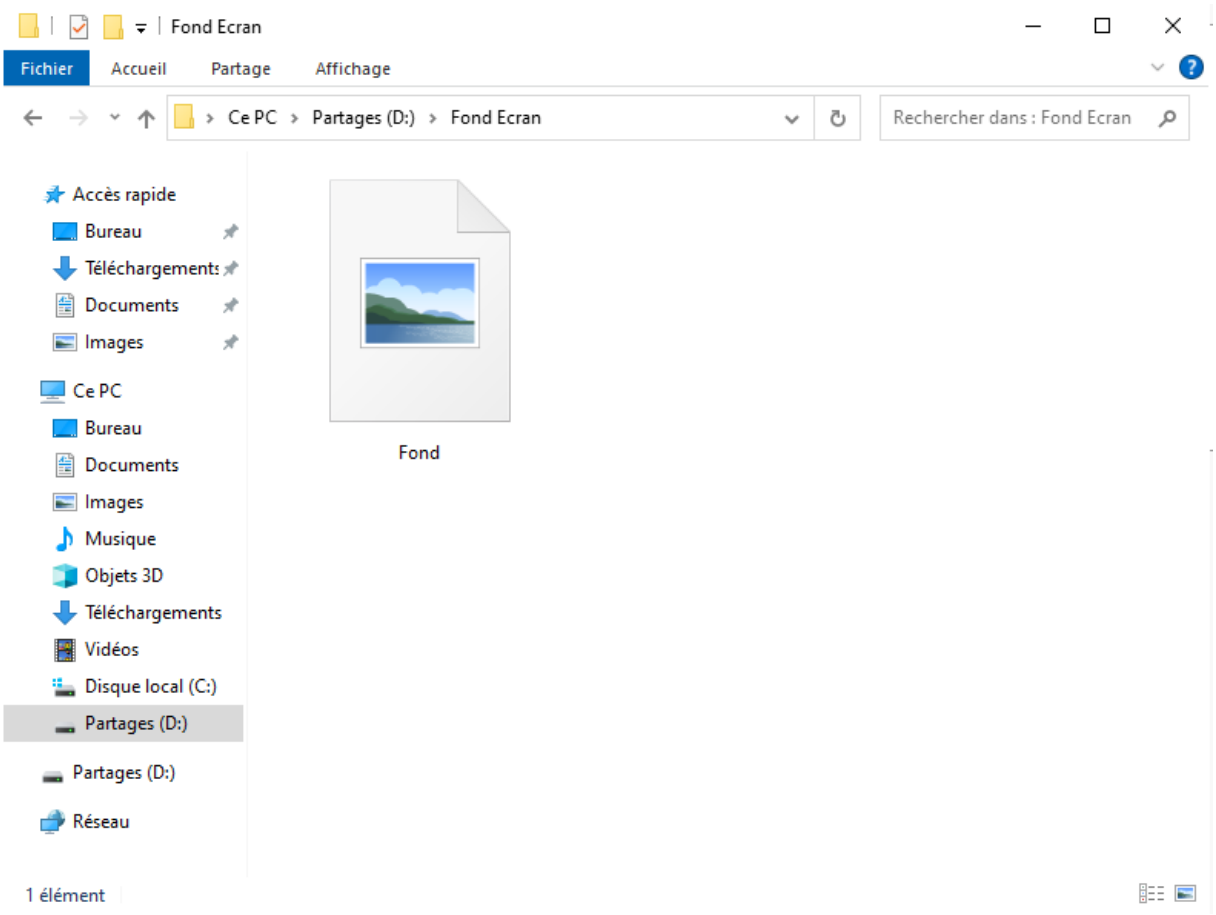
📌 Objectif

Imposer un fond d'écran corporatif StadiumCompany sur tous les postes.

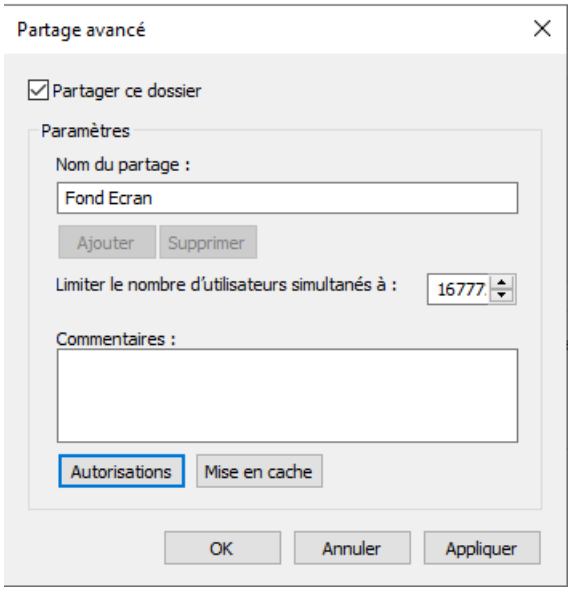
🔧 Étapes

1. Préparation du dossier partagé

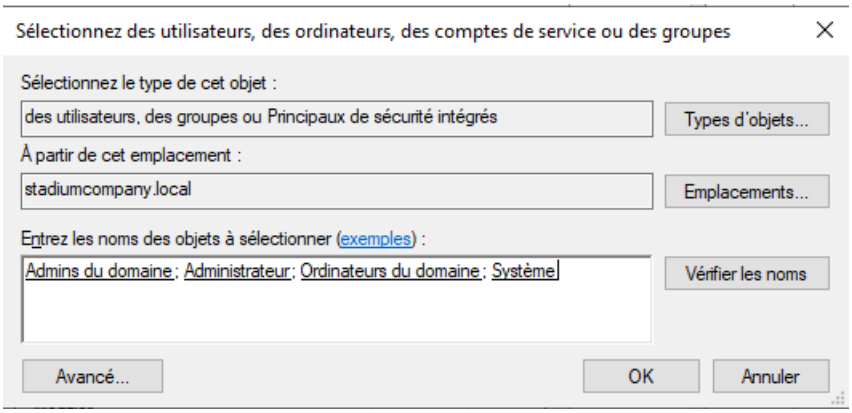
1. Aller sur le **deuxième disque** du serveur Hermes (ex : `D:\Partages`)
2. Créer un dossier :
   Fond d'écran
3. Ajouter l'image (ex : `Fond.png`)



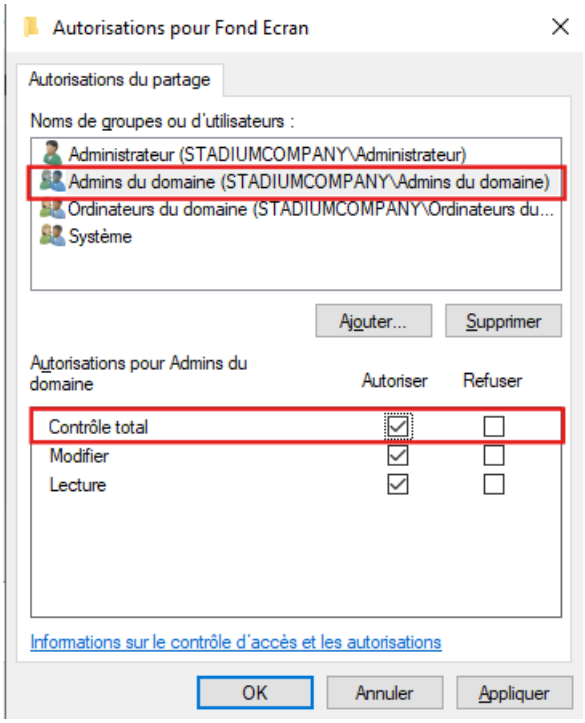
4. Clic droit → **Propriétés → Partage avancé**
5. Cocher **Partager ce dossier**



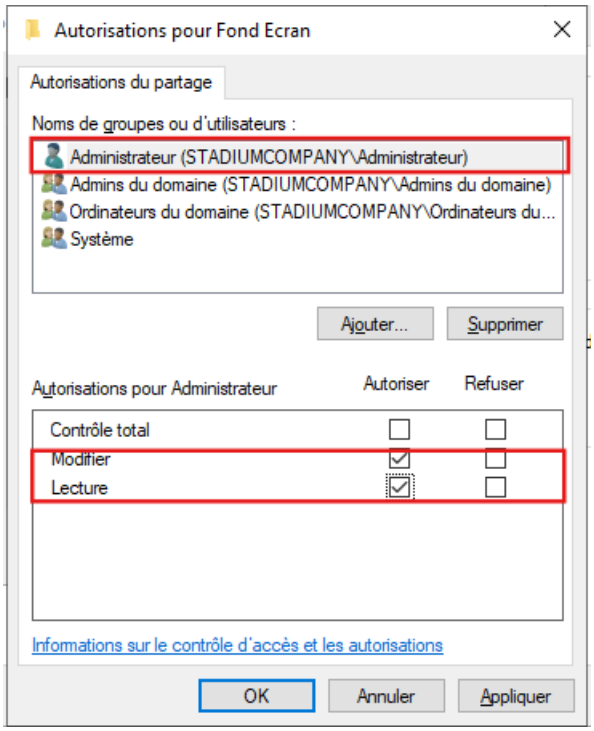
6. Autorisations :
   - Supprimer **Tout le monde**
   - Ajouter :
   - `Ordinateurs du domaine`
   - `Admins du domaine`
   - `Administrateurs`
   - `Système`



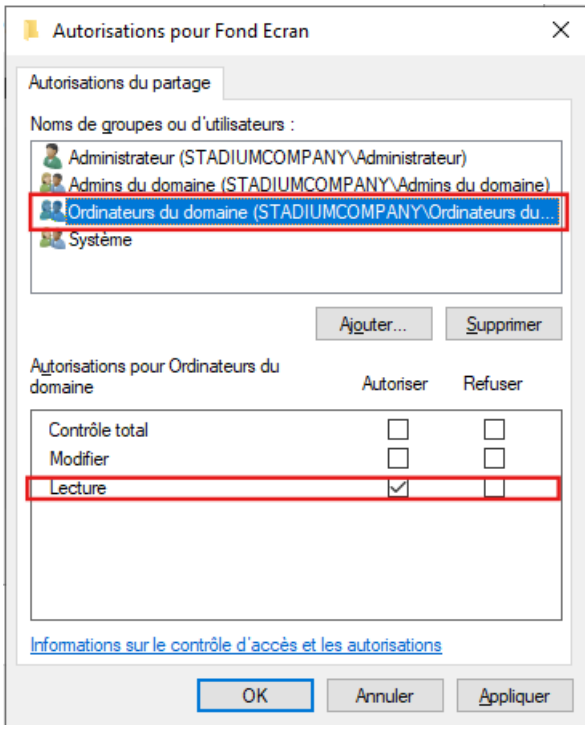
- Droits :
  - Admins du domaine → Contrôle total



  - Administrateurs → Modification



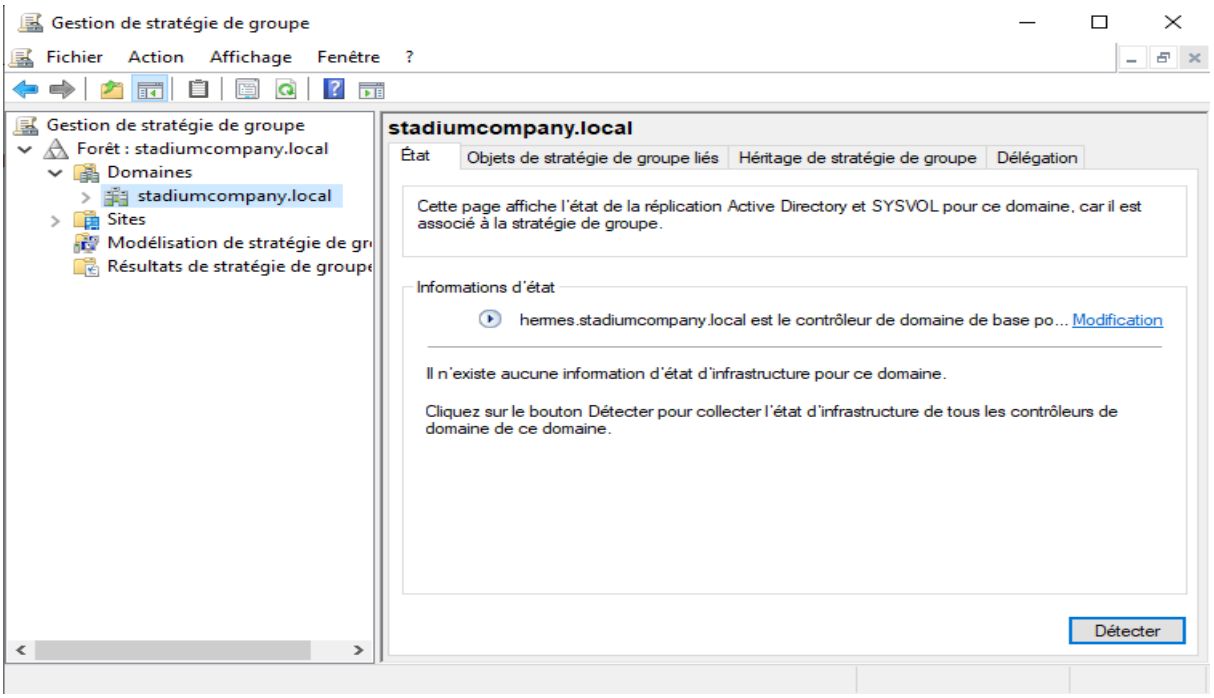
- Ordinateurs du domaine → Lecture



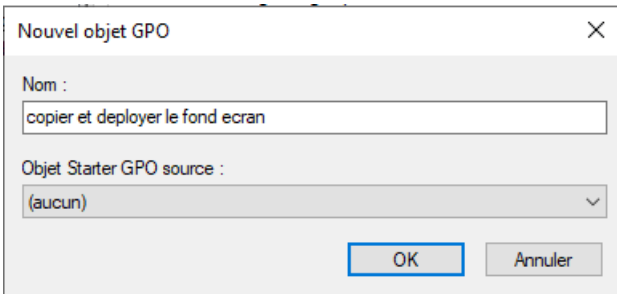
- Système → Lecture

2. Création de la GPO

1. Ouvrir :
   Gestionnaire de serveur → Outils → Gestion des stratégies de groupe
2. Domaine : **stadiumcompany.local**



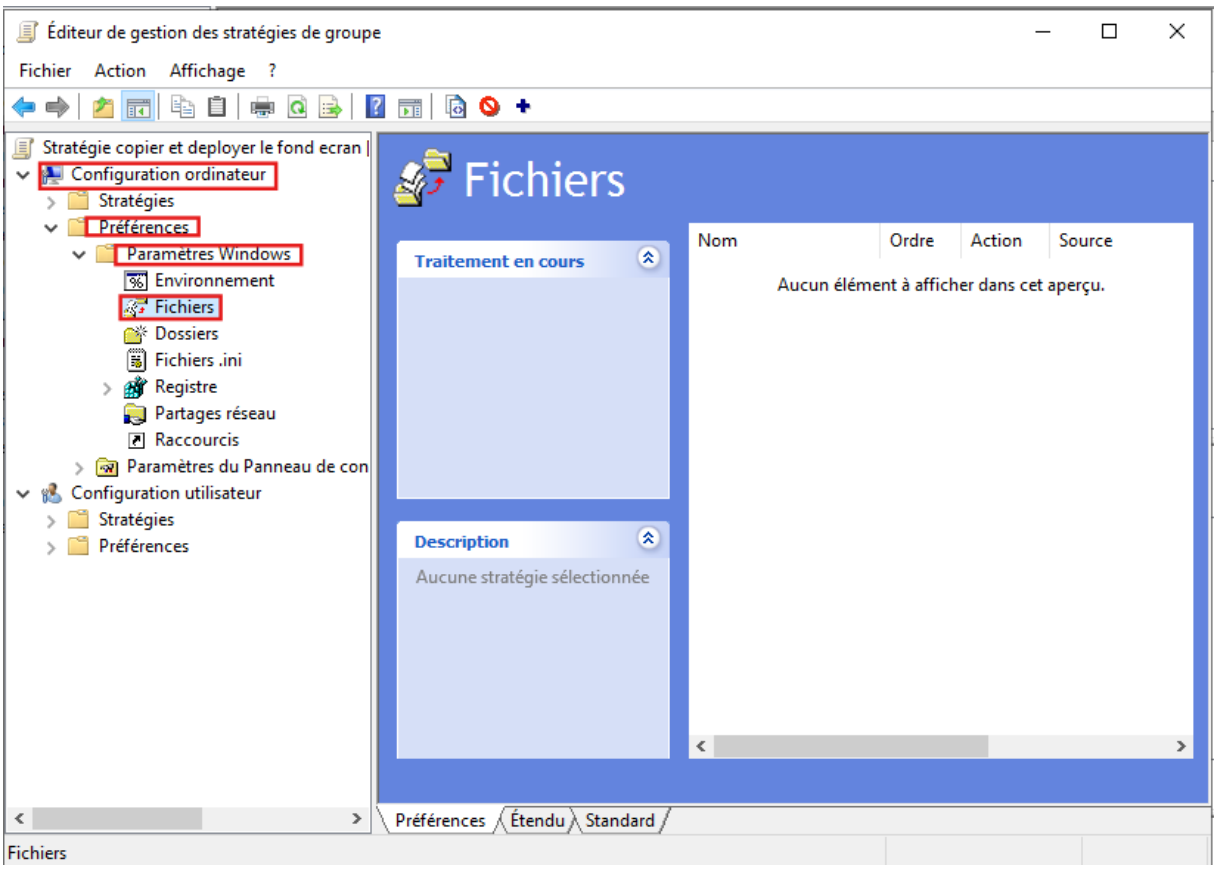
3. Clic droit → **Créer un objet GPO dans ce domaine**
4. Nom :
   Copier et déployer le fond d'écran



3. Configuration de la GPO

a) Copier le fichier en local

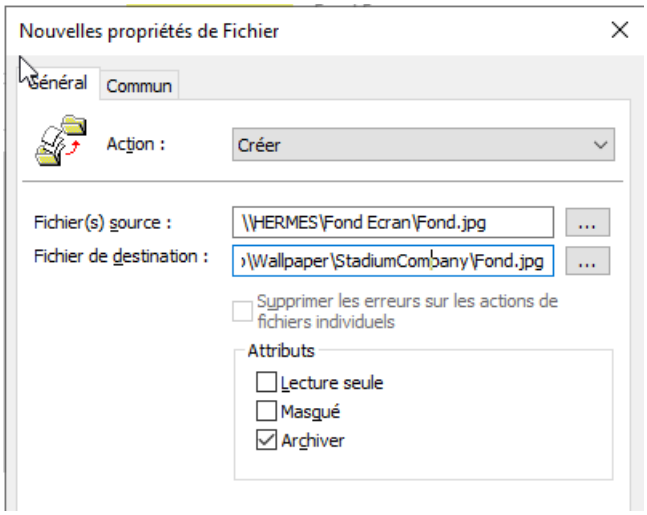
Chemin : clique droit sur la GPO et option modifier
Configuration ordinateur → Préférences → Paramètres Windows → Fichiers



Créer un nouvel élément :

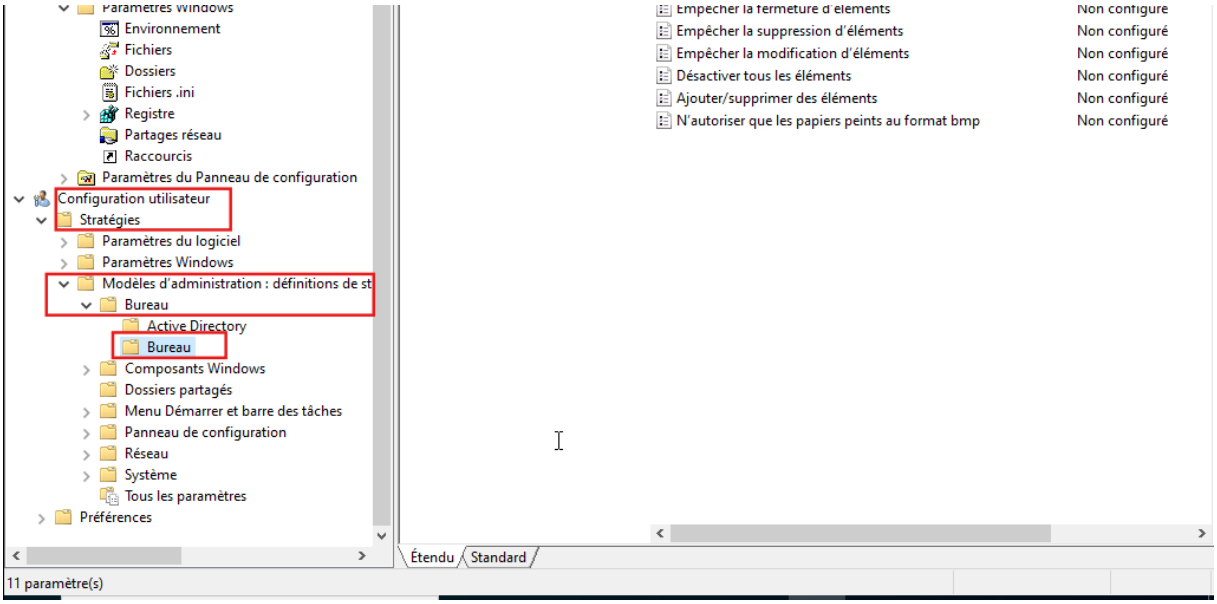
Clic droit dans le panneau de droite (là où c'est vide) -- **Nouveau** -- **Fichier**

- Action : **Créer**
- Source : `\\HERMES\Fond d'écran\Fond.png`
- Destination : `C:\Windows\Web\Wallpaper\StadiumCompany\Fond.png`
- Options :
  Appliquer une fois et ne pas réappliquer



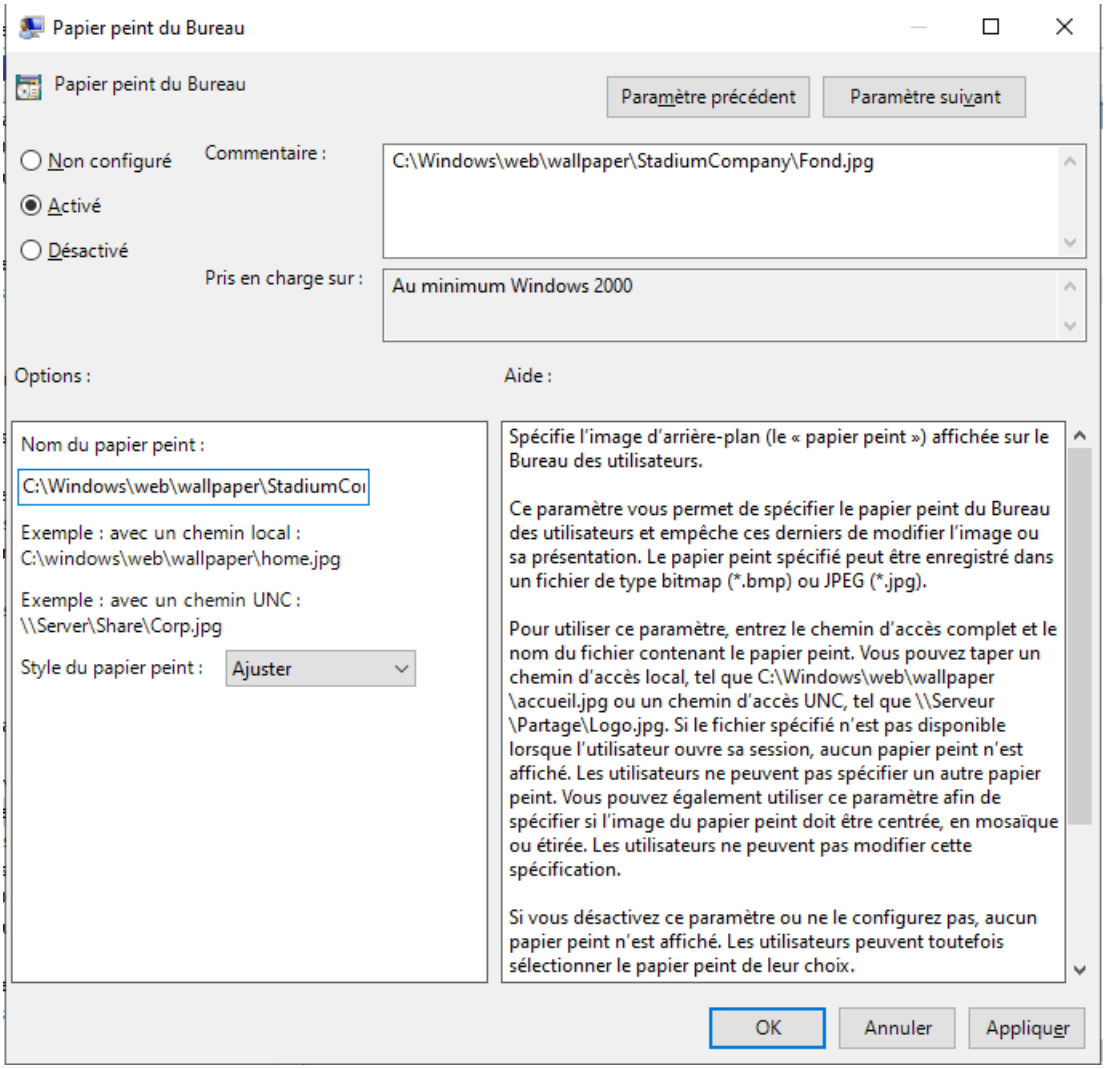
b) Définir le fond d'écran

Chemin :
Configuration utilisateur → Stratégies → Modèles d'administration → Bureau → Bureau



Paramètre : **Papier peint du Bureau**

- Activé
- Chemin :
  `C:\Windows\Web\Wallpaper\StadiumCompany\Fond.png`



4. Appliquer la GPO

Clic droit → **Appliqué**

6.2.2 GPO – Mappage automatique d'un lecteur réseau

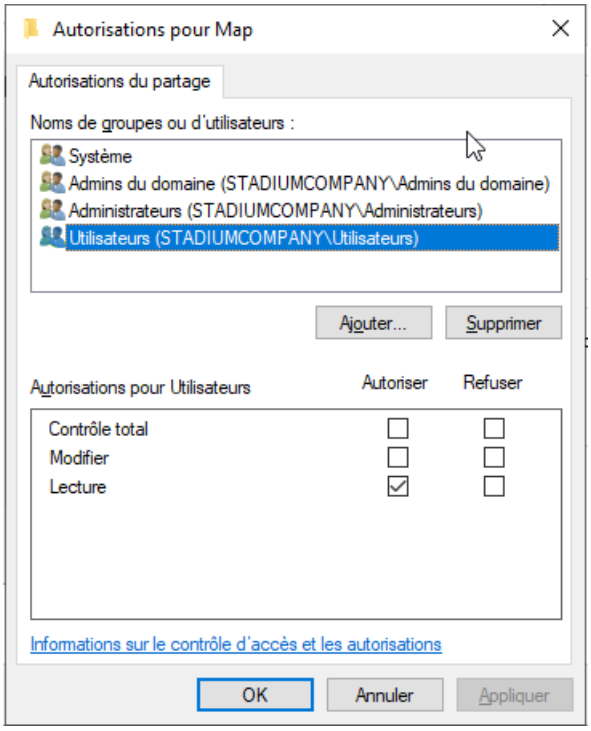
📌 Objectif

Créer un lecteur réseau M:\ pour tous les utilisateurs.

🔧 Étapes

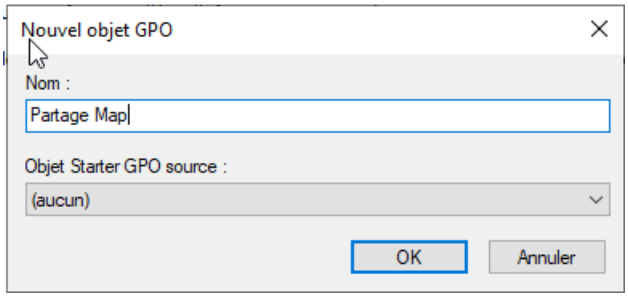
1. Préparation du dossier partagé

1. Sur le disque partagé → créer un dossier :
   Map
2. Partage avancé → Autorisations :
   - Supprimer **Tout le monde**
   - Ajouter :
   - `Admins du domaine`
   - `Administrateurs`
   - `Système`
   - `Utilisateurs`
   - Droits :
     - Admins du domaine → Contrôle total
     - Administrateurs → Modification
     - Utilisateurs → Lecture
     - Système → Lecture



2. Création de la GPO

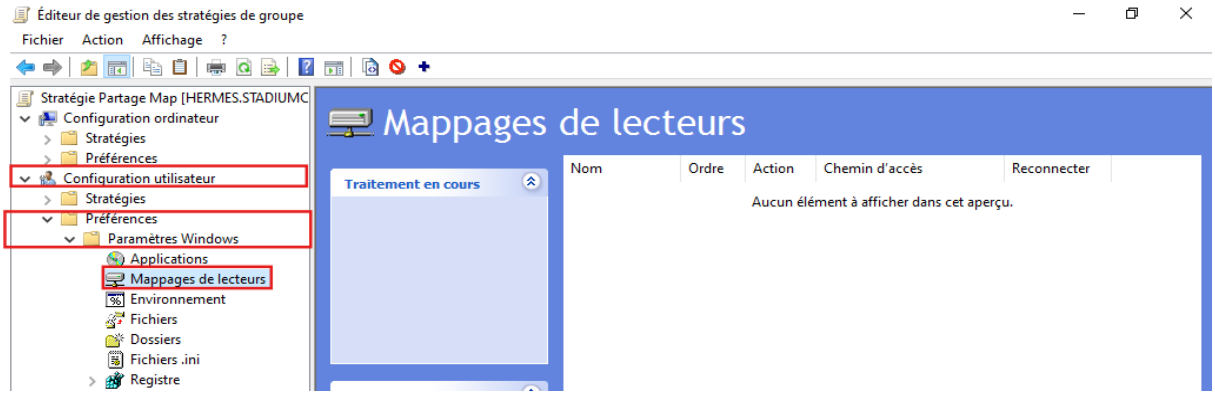
1. Gestion des stratégies de groupe
2. Créer une GPO :
   Partage Map



3. Configuration

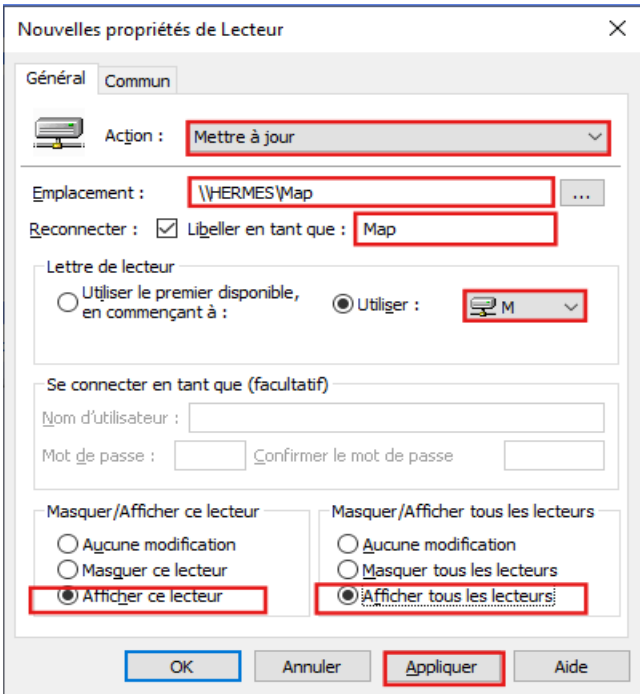
Clique droit -- Modifier

Chemin :
Configuration utilisateur → Préférences → Paramètres Windows → Mappages de lecteurs



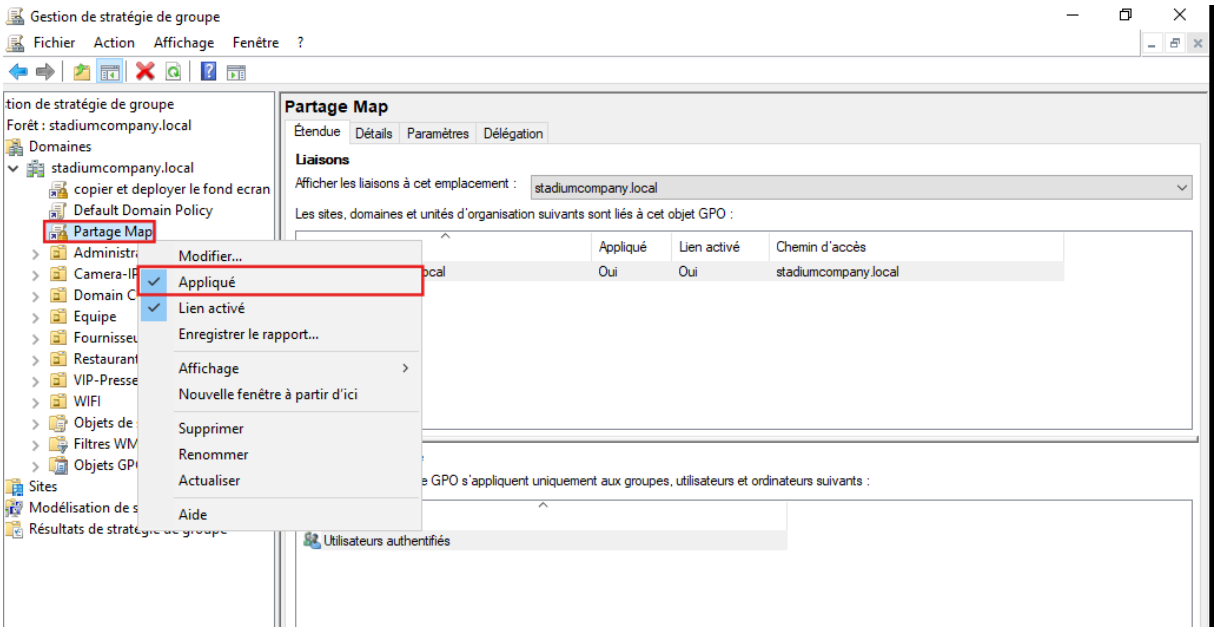
Créer un lecteur mappé : clique droit – nouveau -- lecteur mappé

- Action : **Mettre à jour**
- Emplacement : `\\HERMES\Map`
- Libellé : **Map**
- Lettre : **M**
- Options :
  - Afficher ce lecteur
  - Afficher tous les lecteurs



4. Appliquer la GPO

Clic droit → **Appliqué**



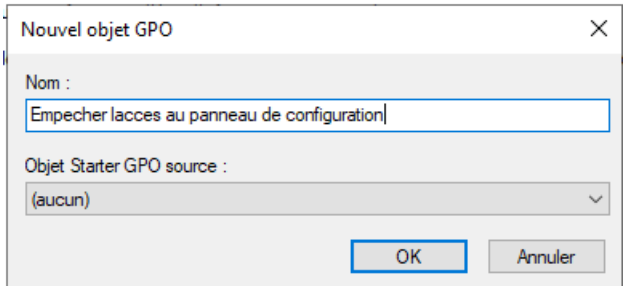
6.2.3 GPO – Bloquer l'accès au panneau de configuration

📌 Objectif

Empêcher les utilisateurs standards de modifier les paramètres système.

🔑 Étapes

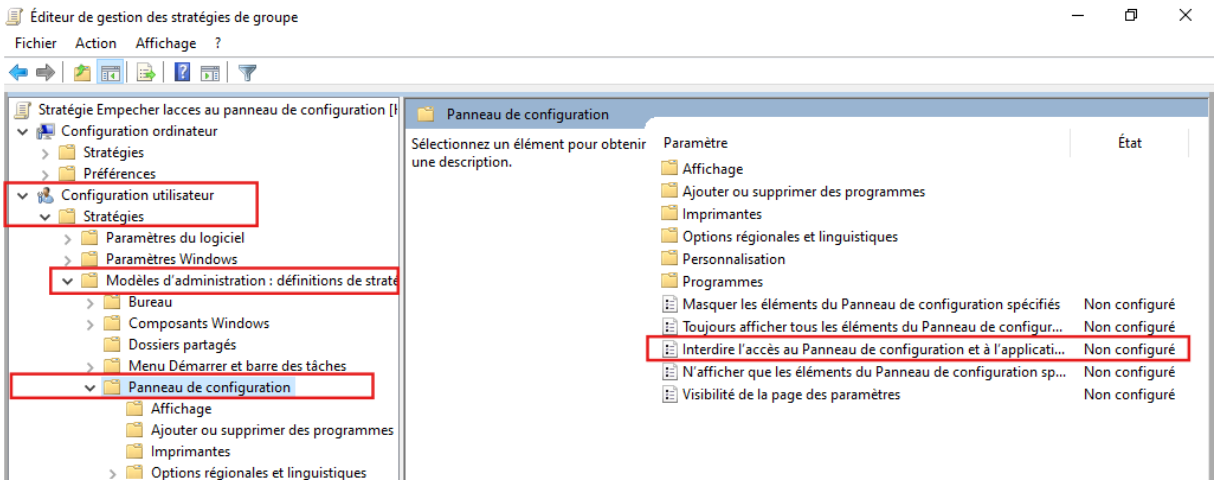
1. Créer une GPO :
   Empêcher l'accès au panneau de configuration



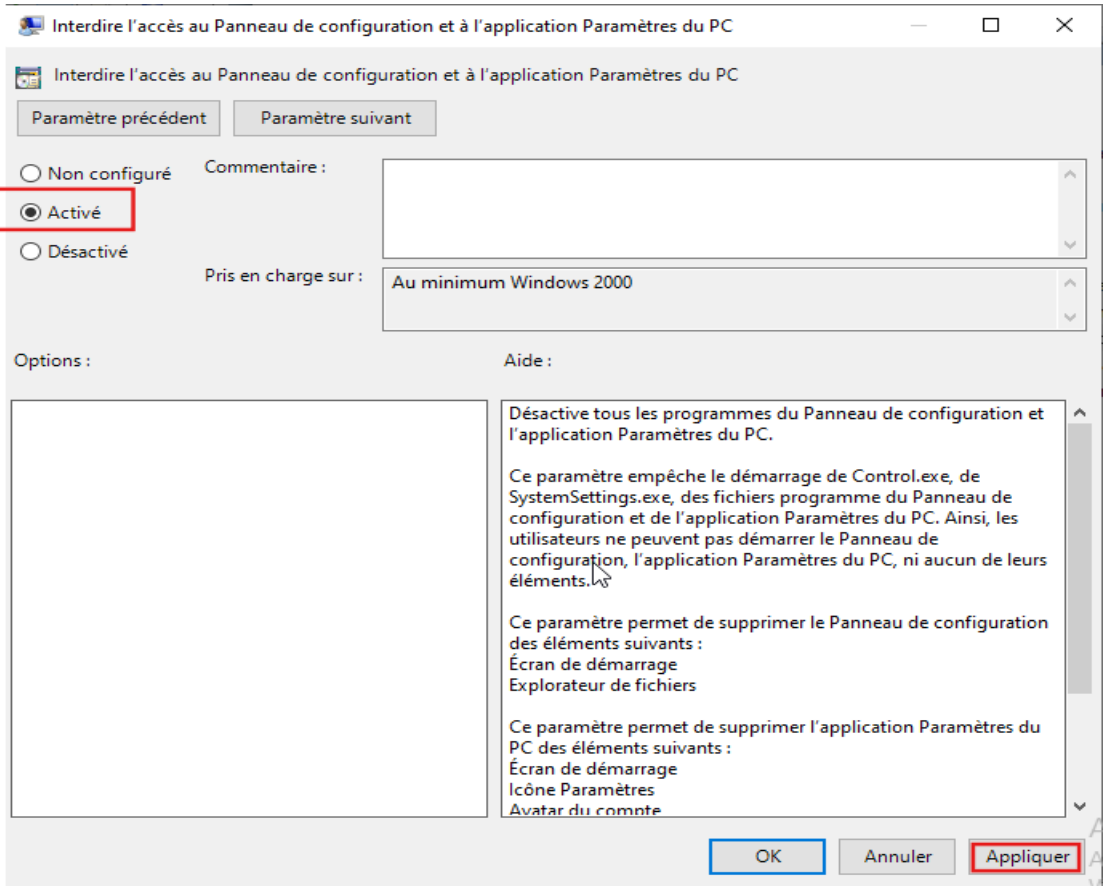
2. Modifier la GPO :

Chemin :
Configuration utilisateur → Stratégies → Modèles d'administration → Panneau de configuration

Paramètre :
Interdire l'accès au Panneau de configuration et à l'application Paramètres du PC



- Activé



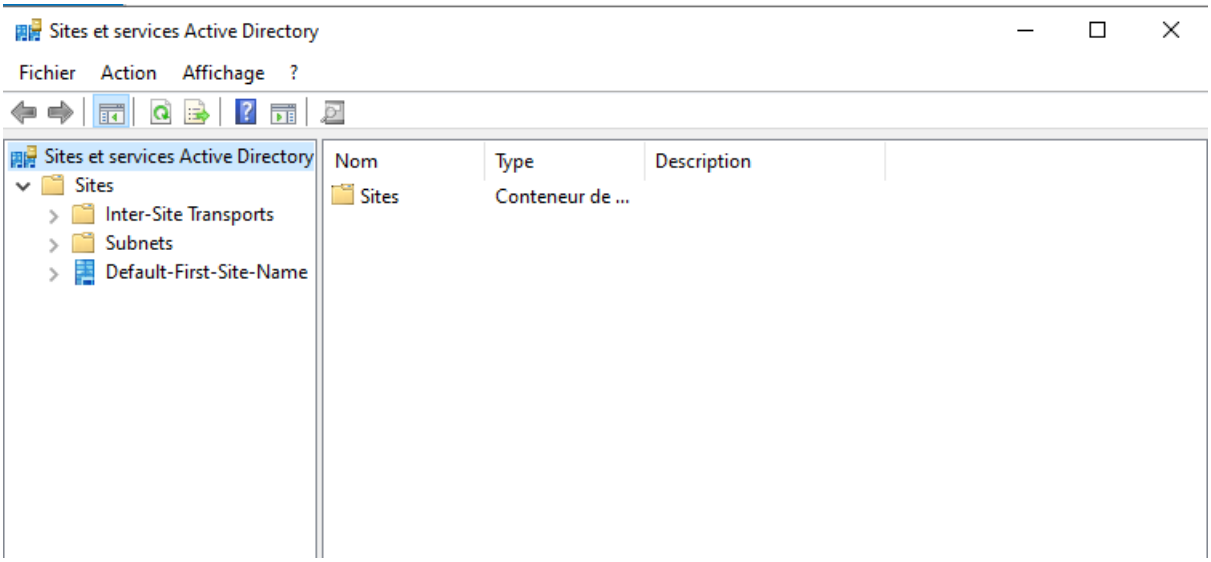
3. Appliquer la GPO

6.3 – Configuration des Sites Active Directory (version adaptée)

L'objectif est de définir la topologie réseau logique de StadiumCompany dans Active Directory.
Cela permet d'optimiser la réplication entre les contrôleurs de domaine et de représenter les différents sites géographiques.

6.3.1 – Accès à la console "Sites et services Active Directory"

1. Se connecter au serveur **Hermes**
   - Utilisateur : `STADIUMCOMPANY\Administrator`
   - Mot de passe : `Bts2024@`
2. Ouvrir la console :
   Démarrer → Outils d'administration Windows → Sites et services Active Directory



6.3.2 – Renommer le site par défaut

Dans l'arborescence :

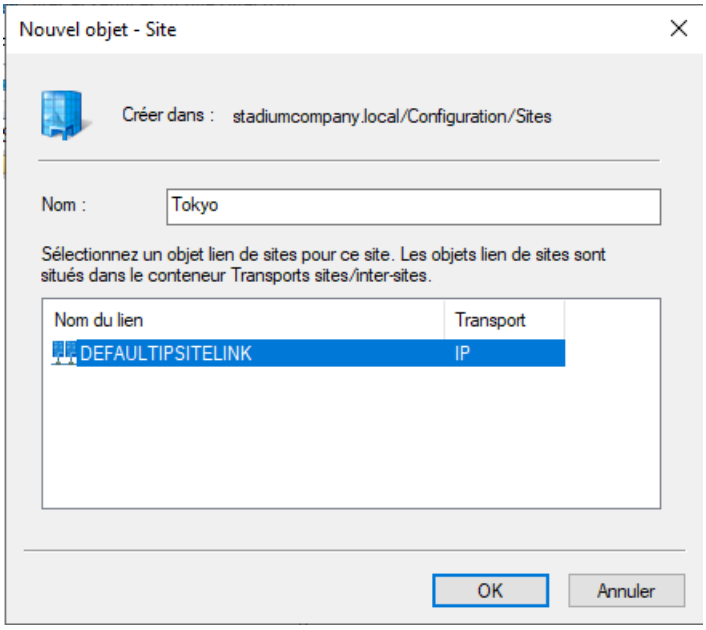
1. Développer **Sites**
2. Clic droit sur **Default-First-Site-Name**
3. Sélectionner **Renommer**
4. Entrer :
   Paris

Le site principal devient :
Sites → Paris

6.3.3 – Création des sites distants

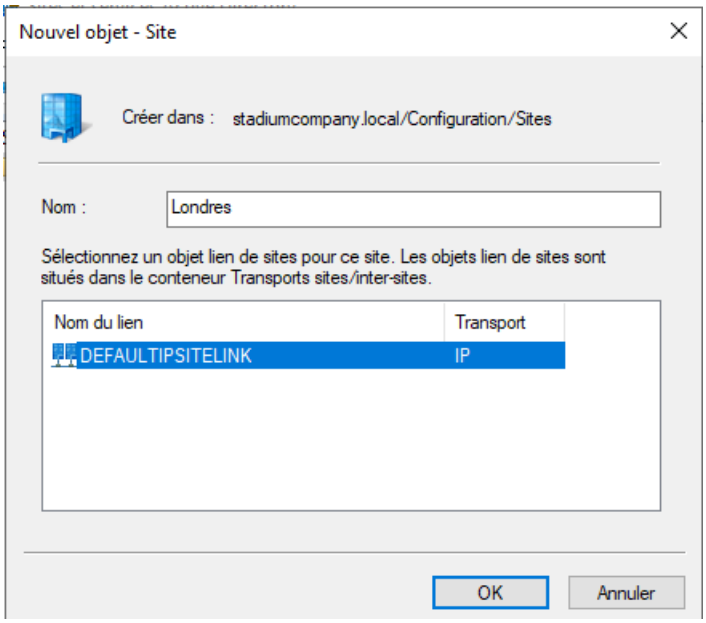
● Création du site Tokyo

1. Clic droit sur **Sites**
2. **Nouveau site**
3. Nom : **Tokyo**
4. Lien de site : **DEFAULTIPSITELINK**
5. Valider

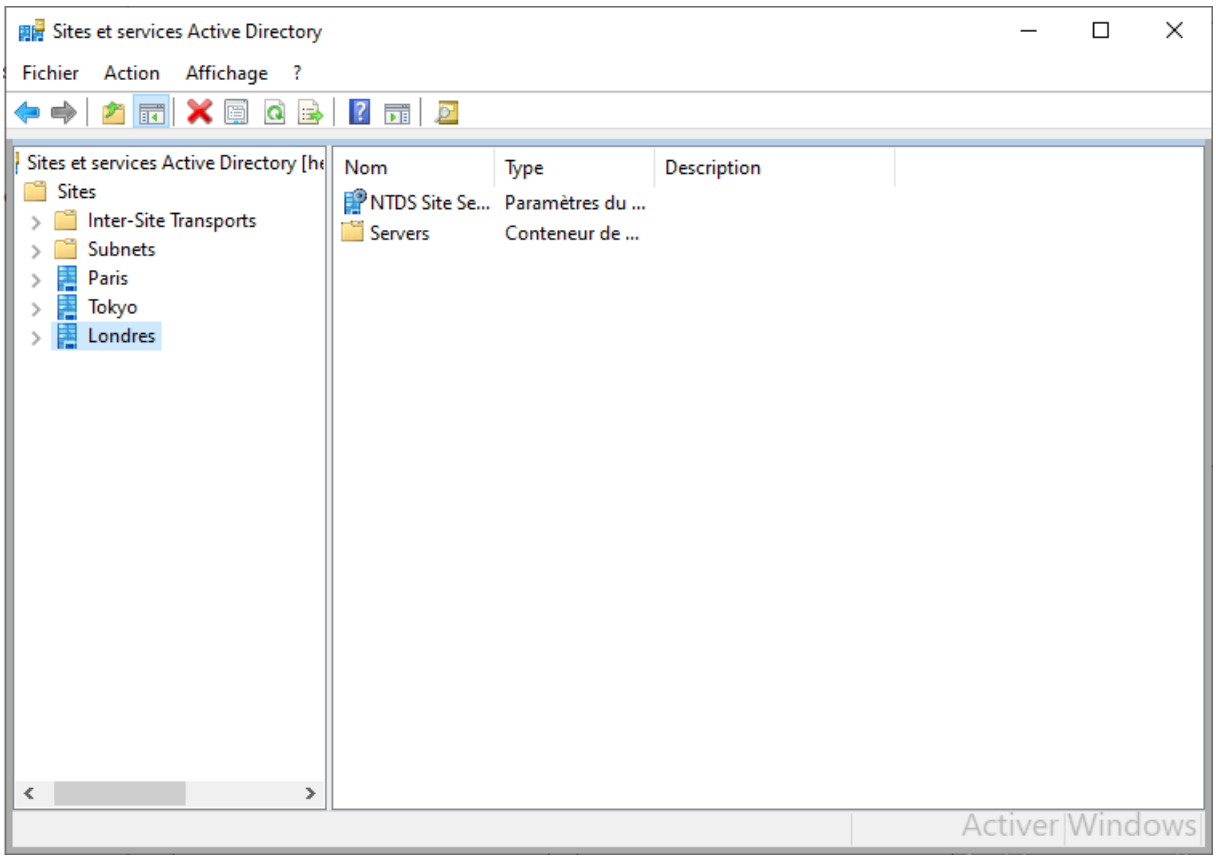


● Création du site Londres

1. Clic droit sur **Sites**
2. **Nouveau site**
3. Nom : **Londres**
4. Lien de site : **DEFAULTIPSITELINK**
5. Valider



Tu dois maintenant avoir :
Paris – Tokyo – Londres

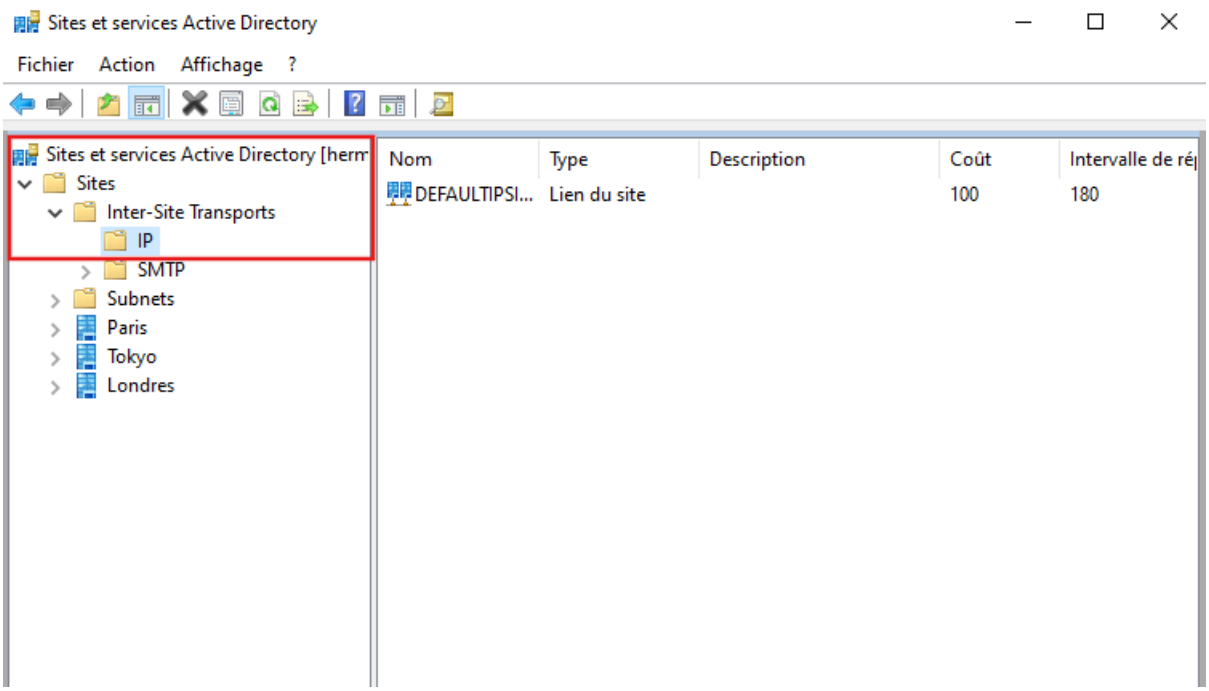


6.3.4 – Création des liens de sites (réplication inter-sites)

Les liens de sites définissent comment les sites AD communiquent entre eux.

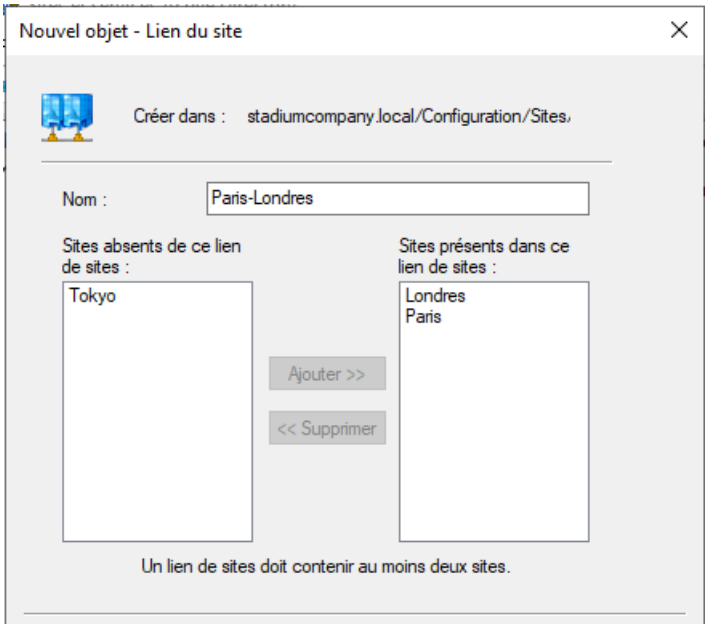
● Accéder aux liens

1. Développer : **Inter-Site Transports**
2. Cliquer sur : **IP**



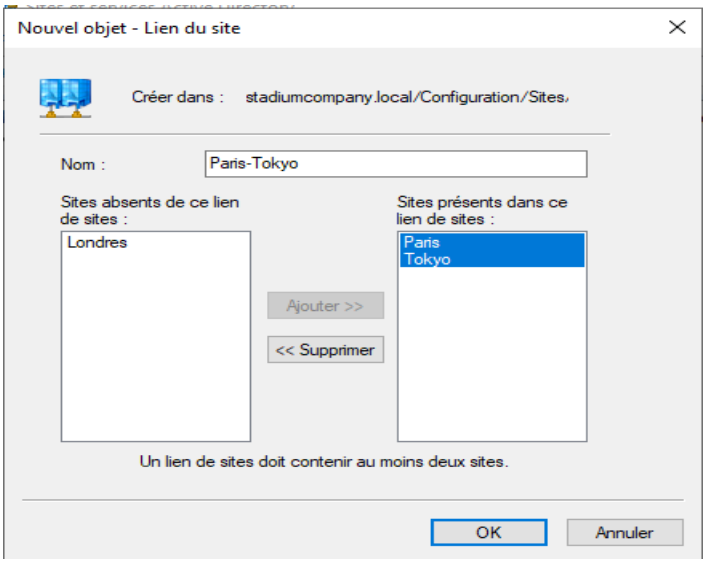
● Lien Paris – Londres

1. Clic droit dans la zone vide → **Nouveau lien de sites**
2. Nom : **Paris-Londres**
3. Ajouter :
   - Paris
   - Londres
4. OK



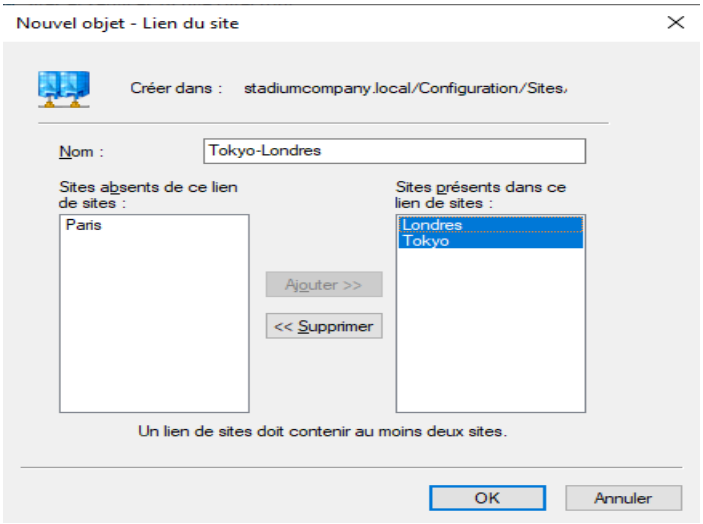
● Lien Paris – Tokyo

1. Nouveau lien de sites
2. Nom : **Paris-Tokyo**
3. Ajouter :
    - Paris
    - Tokyo
4. OK



● Lien Tokyo – Londres

1. Nouveau lien de sites
2. Nom : **Tokyo-Londres**
3. Ajouter :
    - Tokyo
    - Londres
4. OK

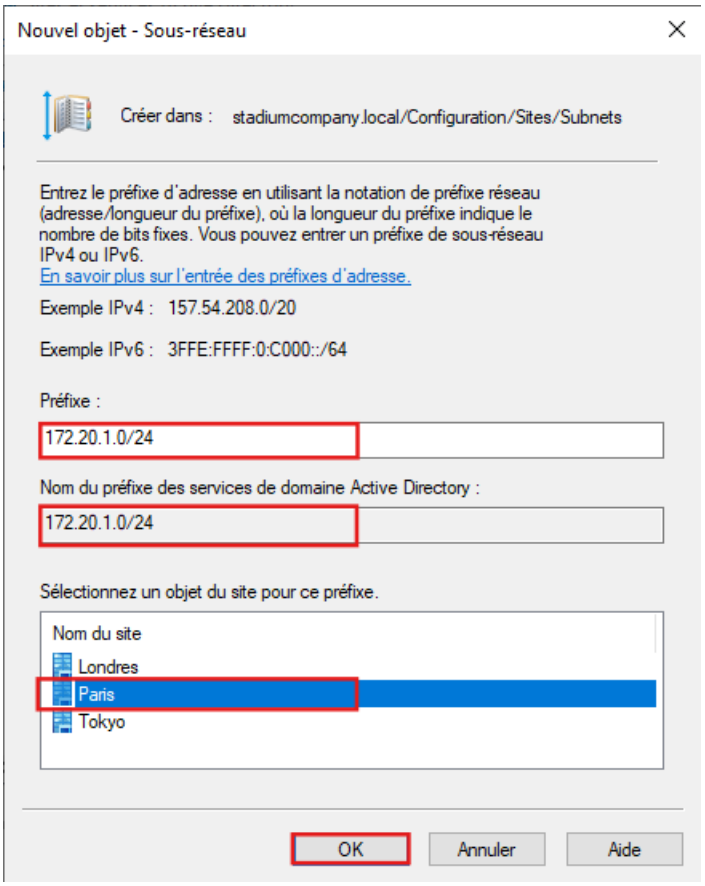


6.3.5 - Création des sous-réseaux

Les sous-réseaux permettent d'associer automatiquement les machines à leur site AD.

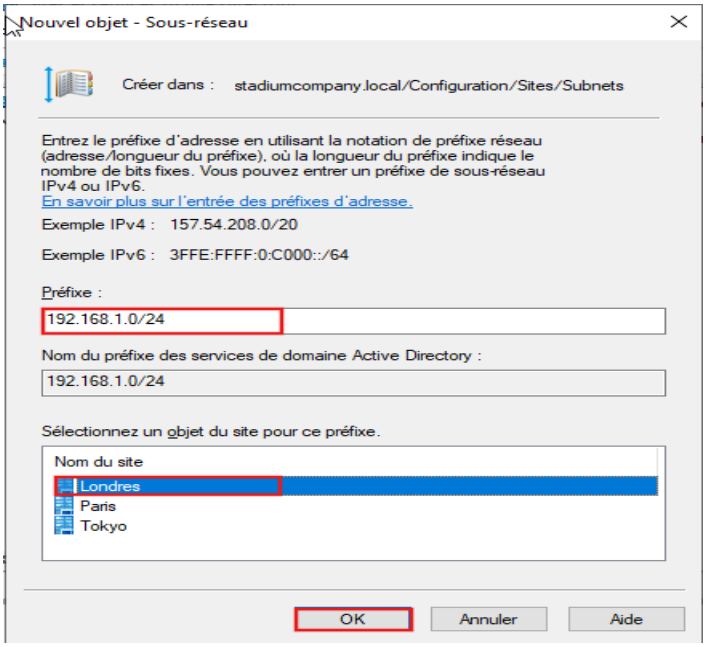
● Sous-réseau Paris

1. Clic sur **Sous-réseaux**
2. Clic droit → **Nouveau sous-réseau**
3. Préfixe : `172.20.1.0/24`
4. Associer au site : **Paris**
5. OK



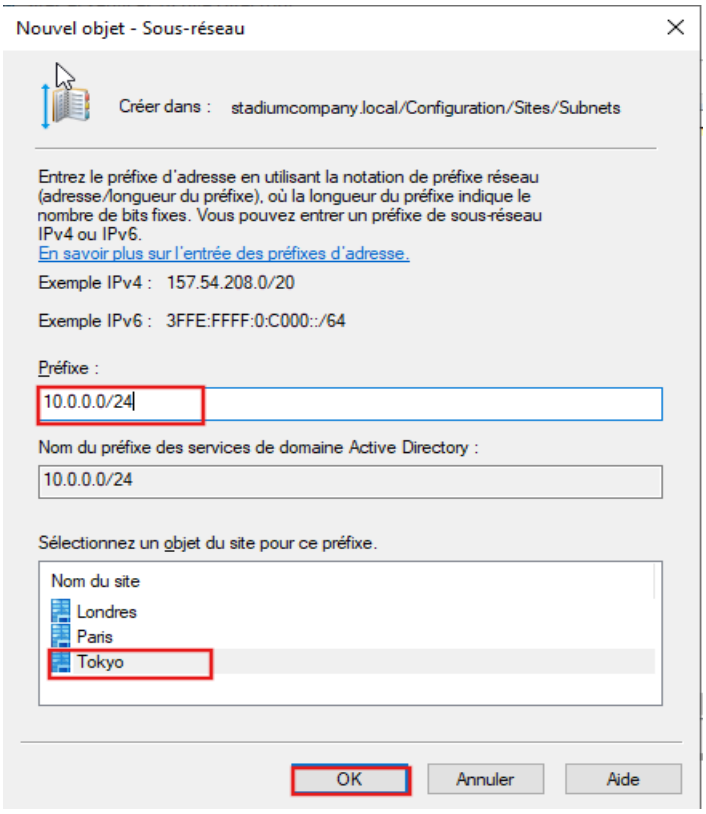
● Sous-réseau Londres

1. Nouveau sous-réseau
2. Préfixe : `192.168.1.0/24`
3. Associer au site : **Londres**
4. OK



● Sous-réseau Tokyo

1. Nouveau sous-réseau
2. Préfixe : `10.0.0.0/24`
3. Associer au site : **Tokyo**
4. OK



6.3.6 – Vérifications

À la fin, tu dois avoir :

✓ Dans “Sites” :

- Paris
- Tokyo
- Londres

✓ Dans “IP” :

- Paris-Londres
- Paris-Tokyo
- Tokyo-Londres

✓ Dans “Sous-réseaux” :

- 172.20.1.0/24 → Paris
- 192.168.1.0/24 → Londres
- 10.0.0.0/24 → Tokyo

6.4 – Automatisation : Script PowerShell de création d’utilisateurs

🎯 Objectif

Automatiser la création des comptes utilisateurs Active Directory à partir d’un fichier CSV.

Cette méthode permet de créer rapidement des dizaines d’utilisateurs avec leurs informations, leur service, leur login et leur appartenance aux groupes.

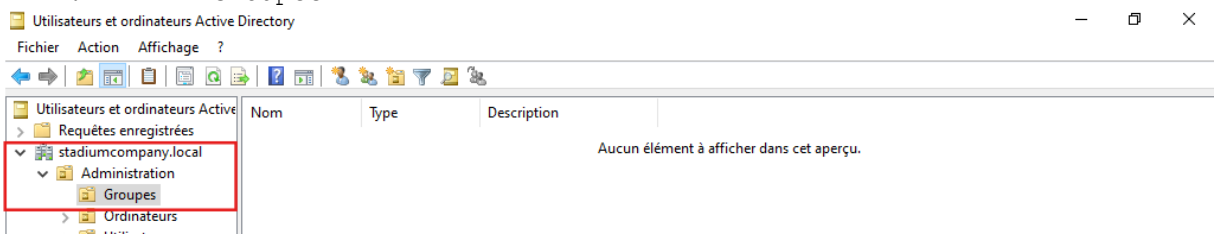
6.4.0 - Création des groupes Active Directory (préparation du script)

🎯 Objectif
Créer les groupes AD correspondant aux services de StadiumCompany, afin que le script PowerShell puisse ajouter automatiquement les utilisateurs dans le bon groupe.

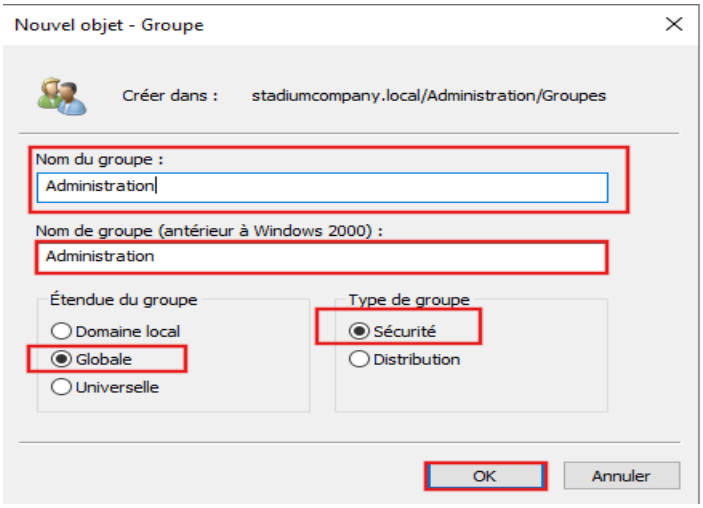
🔑 Étapes

Pour chaque UO (Administration, Équipe, Fournisseurs, Restaurant, VIP-Presse, Caméra-IP, WiFi) :

1. Ouvrir :
   Gestionnaire de serveur → Outils → Utilisateurs et ordinateurs Active Directory
2. Dans l'arborescence, aller dans :
3. `<Nom de l'UO>`
4. `└── Groupes`



5. Clic droit sur **Groupes → Nouveau → Groupe**
6. Renseigner :
   - **Nom du groupe :**
     doit être exactement le nom de l'UO parent
     (important pour le script PowerShell)
   - **Type :** Sécurité
   - **Portée :** Globale
7. Valider



📌 **Groupes à créer :**

UO	Groupe à créer
Administration	Administration
Équipe	Equipe
Fournisseurs	Fournisseurs
Restaurant	Restaurant
VIP-Presse	VIP-Presse
Caméra-IP	Caméra-IP
WiFi	WiFi

☞ Ces groupes seront utilisés par le script PowerShell pour attribuer automatiquement les droits aux utilisateurs.

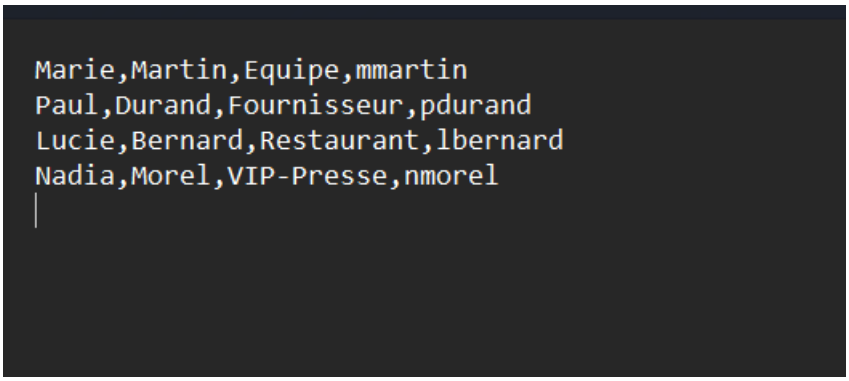
6.4.1 - Création du fichier CSV

Créer un fichier nommé par exemple :

`utilisateurs.csv`

Contenu du fichier (en-tête obligatoire) :

```
Prenom,Nom,Service,Login
Jean,Dupont,Administration,jdupont
Marie,Martin,Equipe,mmartin
Paul,Durand,Fournisseur,pdurand
Lucie,Bernard,Restaurant,lbernard
Nadia,Morel,VIP-Presse,nmorel
```



☞ Tu peux ajouter autant de lignes que nécessaire.

6.4.2 - Script PowerShell d'automatisation

Créer un fichier :

```
Create-Users.ps1
```

Et y mettre le script suivant :

```
# Import du fichier CSV
$users = Import-Csv -Path "C:\Scripts\utilisateurs.csv"

foreach ($user in $users) {
    Write-Host "Création de $($user.Prenom) $($user.Nom)..." -
ForegroundColor Cyan

    # Correction du nom
    $ServiceAD = $user.Service
    if ($ServiceAD -eq "Fournisseurs") {
        $ServiceAD = "Fournisseur"
    }

    $OU = "OU=Utilisateurs,OU=$ServiceAD,DC=stadiumcompany,DC=local"

    # Créer l'utilisateur
    New-ADUser `
        -Name "$($user.Prenom) $($user.Nom)" `
        -GivenName $user.Prenom `
        -Surname $user.Nom `
        -SamAccountName $user.Login `
        -UserPrincipalName "$($user.Login)@stadiumcompany.local" `
        -Path $OU `
        -AccountPassword (ConvertTo-SecureString "@azerty1234" -AsPlainText
-Force) `
        -Enabled $true `
        -ChangePasswordAtLogon $true

    Write-Host "OK" -ForegroundColor Green
    Start-Sleep -Seconds 1
}

Write-Host "`nTous les utilisateurs ont été créés !" -ForegroundColor Green
```

Fichier Modifier Affichage H1

```powershell
# Import du fichier CSV
$users = Import-Csv -Path "C:\Scripts\utilisateurs.csv"

foreach ($user in $users) {
    Write-Host "Création de $($user.Prenom) $($user.Nom)..." -ForegroundColor Cyan

    # Correction du nom
    $ServiceAD = $user.Service
    if ($ServiceAD -eq "Fournisseurs") {
        $ServiceAD = "Fournisseur"
    }

    $OU = "OU=Utilisateurs,OU=$ServiceAD,DC=stadiumcompany,DC=local"

    # Créer l'utilisateur
    New-ADUser `
        -Name "$($user.Prenom) $($user.Nom)" `
        -GivenName $user.Prenom `
        -Surname $user.Nom `
        -SamAccountName $user.Login `
        -UserPrincipalName "$($user.Login)@stadiumcompany.local" `
        -Path $OU `
        -AccountPassword (ConvertTo-SecureString "@azerty1234" -AsPlainText -Force) `
        -Enabled $true `
        -ChangePasswordAtLogon $true

    Write-Host "OK" -ForegroundColor Green
    Start-Sleep -Seconds 1
}

Write-Host "`nTous les utilisateurs ont été créés !" -ForegroundColor Green
```

Enregistrer le fichier sous : `Create-Users.ps1`

Explication rapide du script

Ligne / Commande	Fonction
Import-Csv	Charge les utilisateurs depuis le fichier CSV. Chaque ligne devient un objet PowerShell.
foreach ($user in $users)	Boucle sur chaque utilisateur du CSV pour les traiter un par un.
Write-Host	Affiche dans la console le nom de l'utilisateur en cours de création (feedback visuel).
Correction du nom du service	Permet d'adapter automatiquement les valeurs du CSV aux noms exacts des UO dans Active Directory (ex : "Fournisseurs" → "Fournisseur").
$OU = "OU=Utilisateurs,OU=$ServiceAD,DC=stadiumcompany,DC=local"	Construit dynamiquement le chemin LDAP de l'UO où sera créé l'utilisateur.

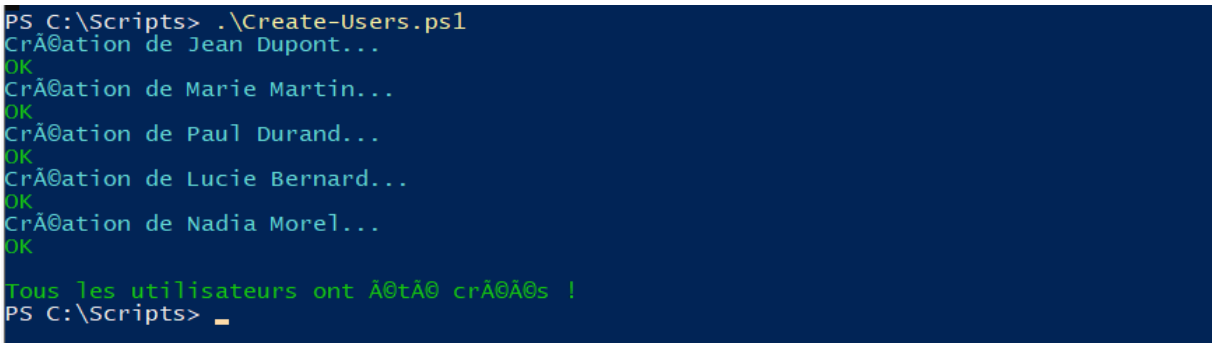
New-ADUser	Crée le compte utilisateur dans Active Directory avec : nom, prénom, login, UPN, mot de passe, OU cible, activation du compte.
-ChangePasswordAtLogon $true	Force l'utilisateur à changer son mot de passe lors de sa première connexion.
Start-Sleep	Petite pause d'une seconde pour rendre l'affichage plus lisible.
Write-Host "Tous les utilisateurs ont été créés !"	Message final confirmant la fin du script.

6.4.3 - Exécution du script

Dans PowerShell (en administrateur) :

```
cd C:\Scripts
.\Create-Users.ps1
```

Les utilisateurs sont automatiquement créés dans l'OU définie.



6.5 – Mise en place du service FTP sur Hermes

📌 Objectif

Permettre l'échange de fichiers via le protocole FTP (port 21) depuis le serveur Hermes.

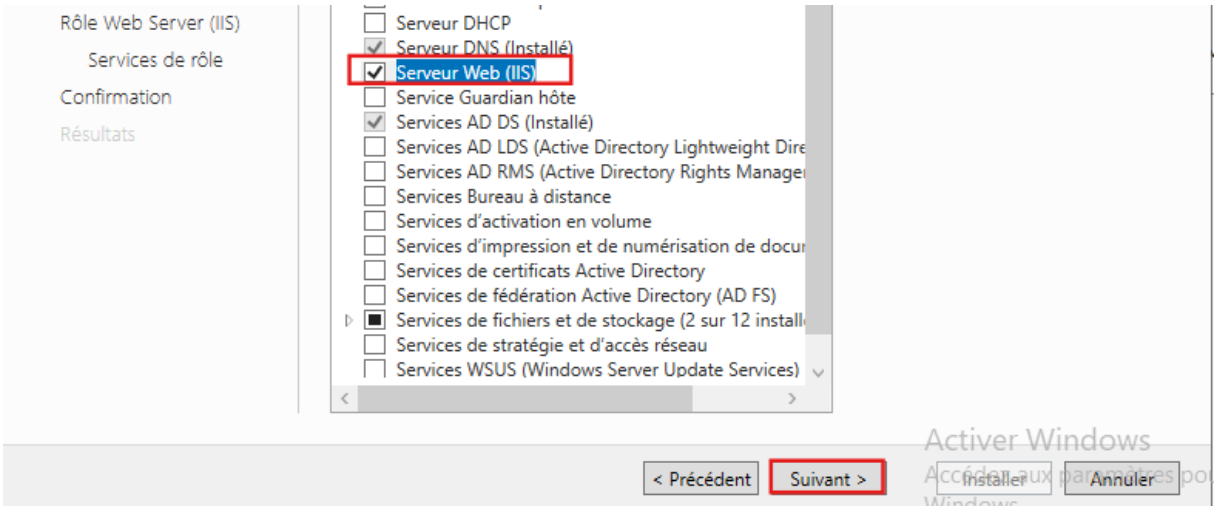
🔑 Étapes

1. Installation du rôle IIS + modules FTP

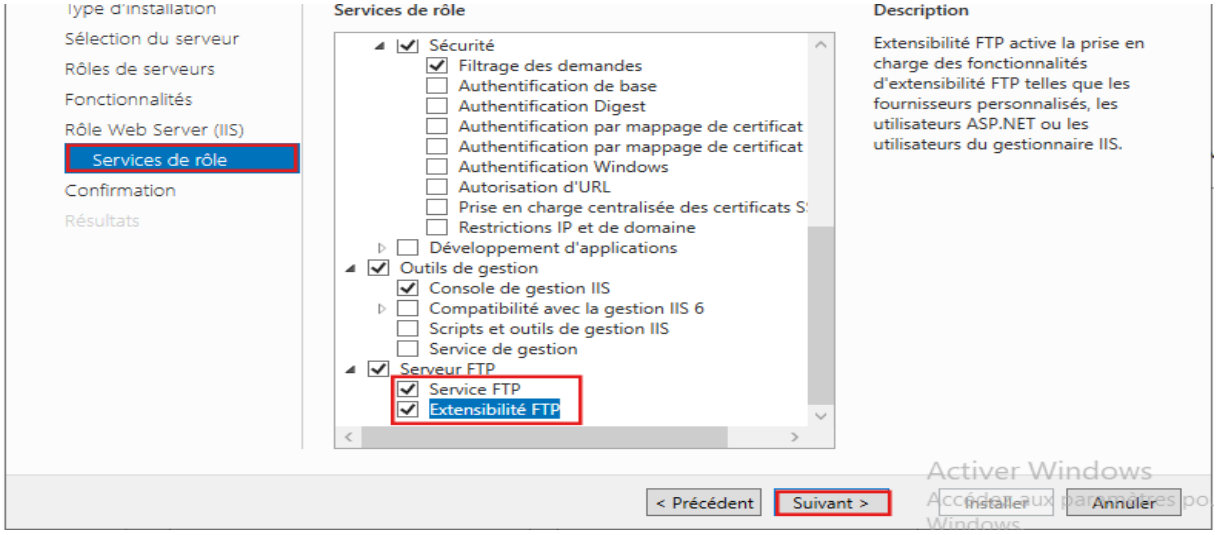
⚠ **Important :**
Le FTP n'apparaît pas dans *Rôles de serveurs*.
Il se trouve dans **Services de rôle** du rôle **Serveur Web (IIS)**.

✓ Procédure

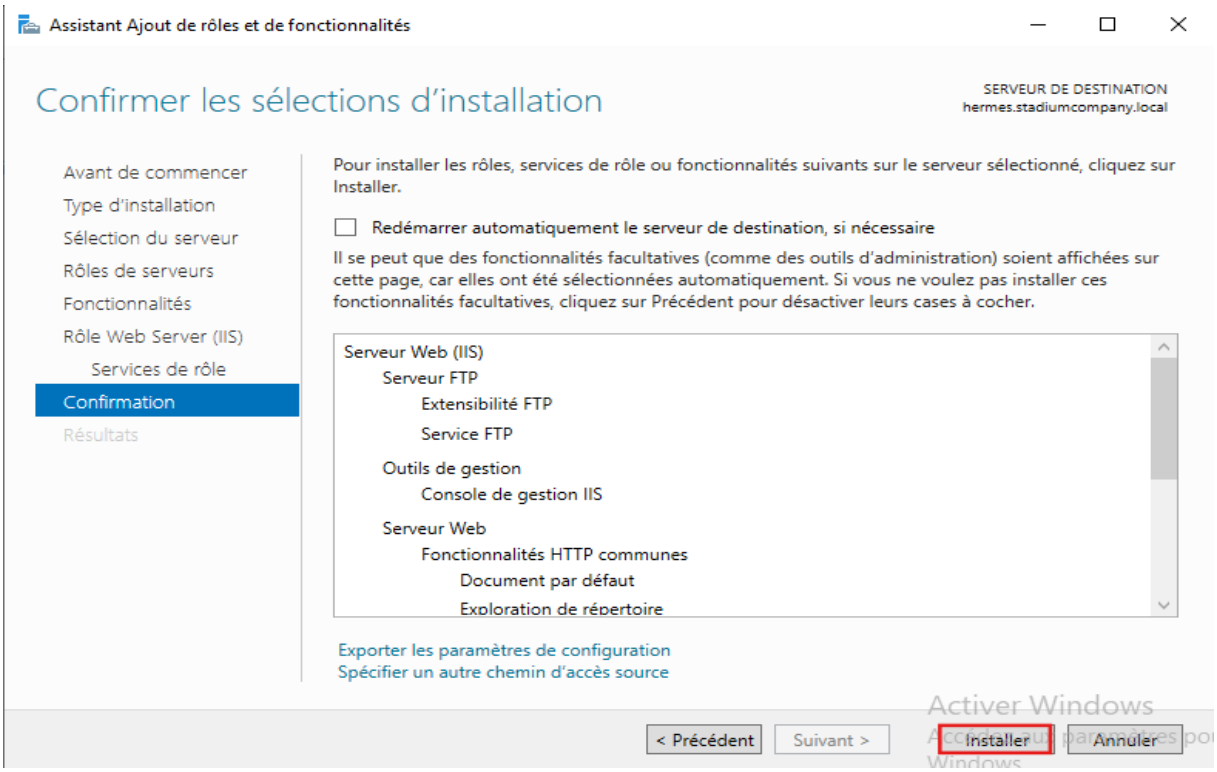
1. Ouvrir **Gestionnaire de serveur**
2. Cliquer sur **Ajouter des rôles et fonctionnalités**
3. Type d'installation :
   Installation basée sur un rôle ou une fonctionnalité
4. Sélectionner le serveur :
   hermes.stadiumcompany.local
5. Dans **Rôles de serveurs**, cocher :
   - **Serveur Web (IIS)**
     (si déjà installé, laisser coché)



6. Cliquer **Suivant** jusqu'à la page **Services de rôle**
7. Dérouler :
8. `Serveur Web (IIS)`
9. `└── Serveur FTP`
10. Cocher :
    - **Service FTP**
    - **Extensibilité FTP**

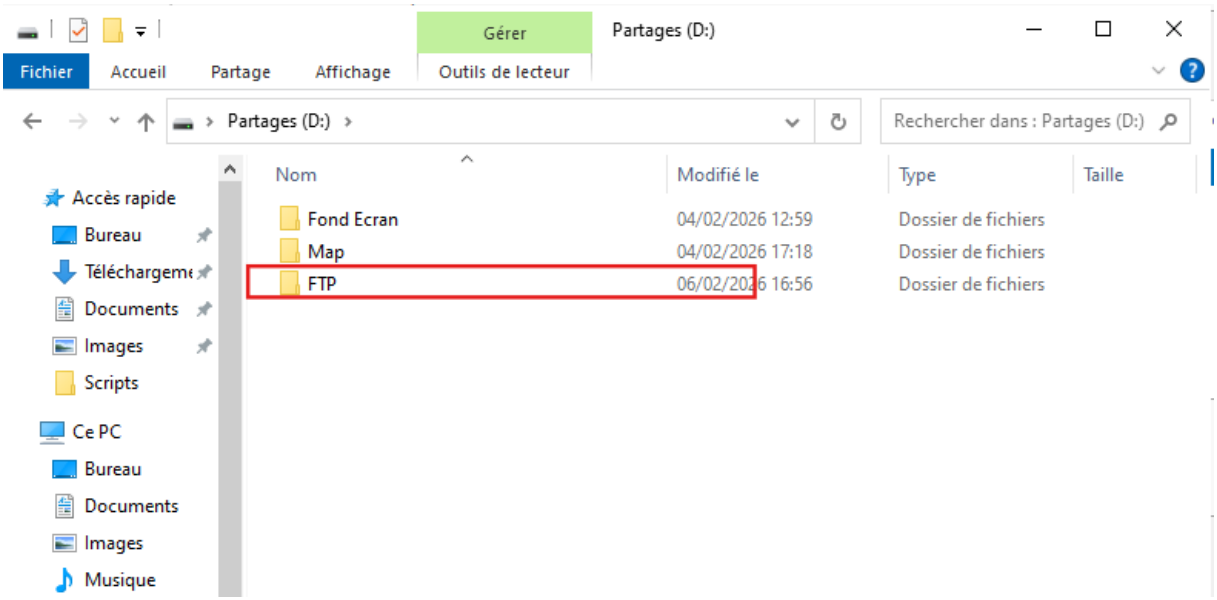


11. Valider et installer



2. Création du dossier FTP

1. Créer un dossier local sur Hermes, par exemple :
2. `D:\FTP`

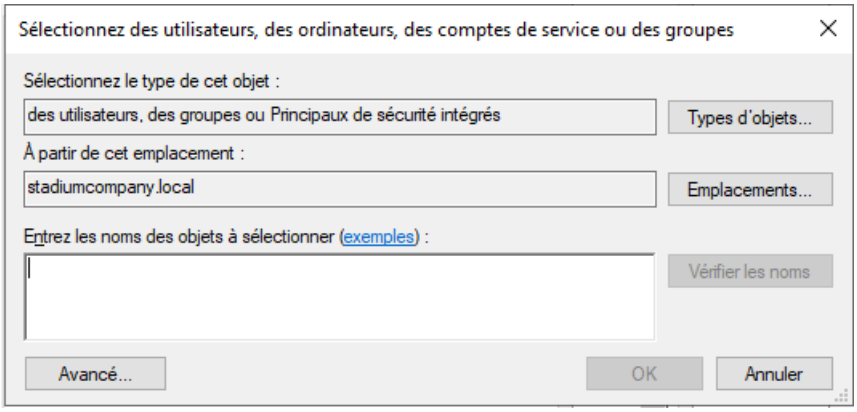


3. Configurer les permissions NTFS

L'objectif est de permettre uniquement aux utilisateurs du domaine (AD) d'accéder au dossier FTP. Pour cela, on utilise les **groupes Active Directory** déjà créés (Administration, Equipe, Fournisseur, Restaurant, VIP-Presse).

✓ Étapes

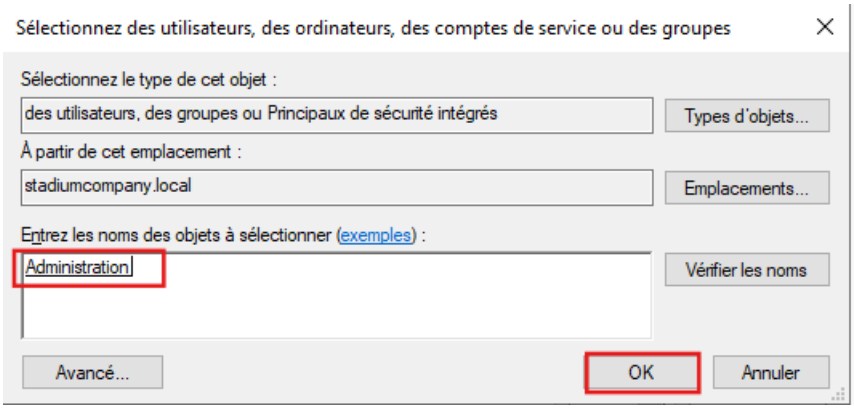
1. Clic droit sur le dossier **D:\FTP**
2. Sélectionner **Propriétés**
3. Aller dans l'onglet **Sécurité**
4. Cliquer sur **Modifier…**
5. Cliquer sur **Ajouter…**



6. Dans la zone de saisie, entrer le nom du groupe AD souhaité, par exemple :

   ```
   Administration
   ```

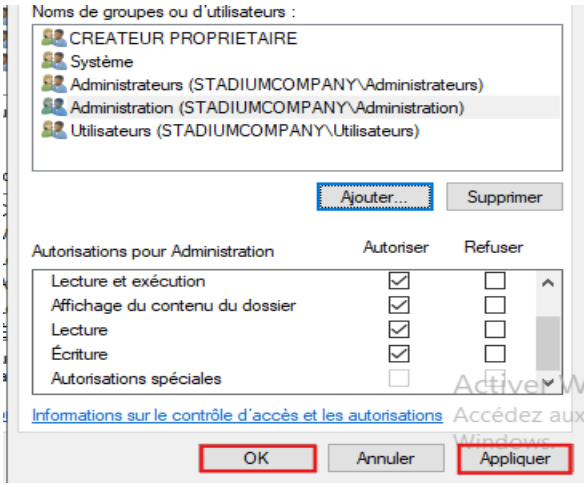
7. Cliquer sur **Vérifier les noms** (le nom doit se souligner → cela confirme qu'il existe dans l'AD)
8. Valider avec **OK**



9. Dans la liste des permissions, cocher :
   - **Lecture** → si les utilisateurs doivent seulement consulter/télécharger
   - **Lecture / Écriture** → si les utilisateurs doivent déposer des fichiers
10. Répéter l'opération pour chaque groupe AD autorisé :
    - Administration
    - Equipe
    - Fournisseur
    - Restaurant
    - VIP-Presse

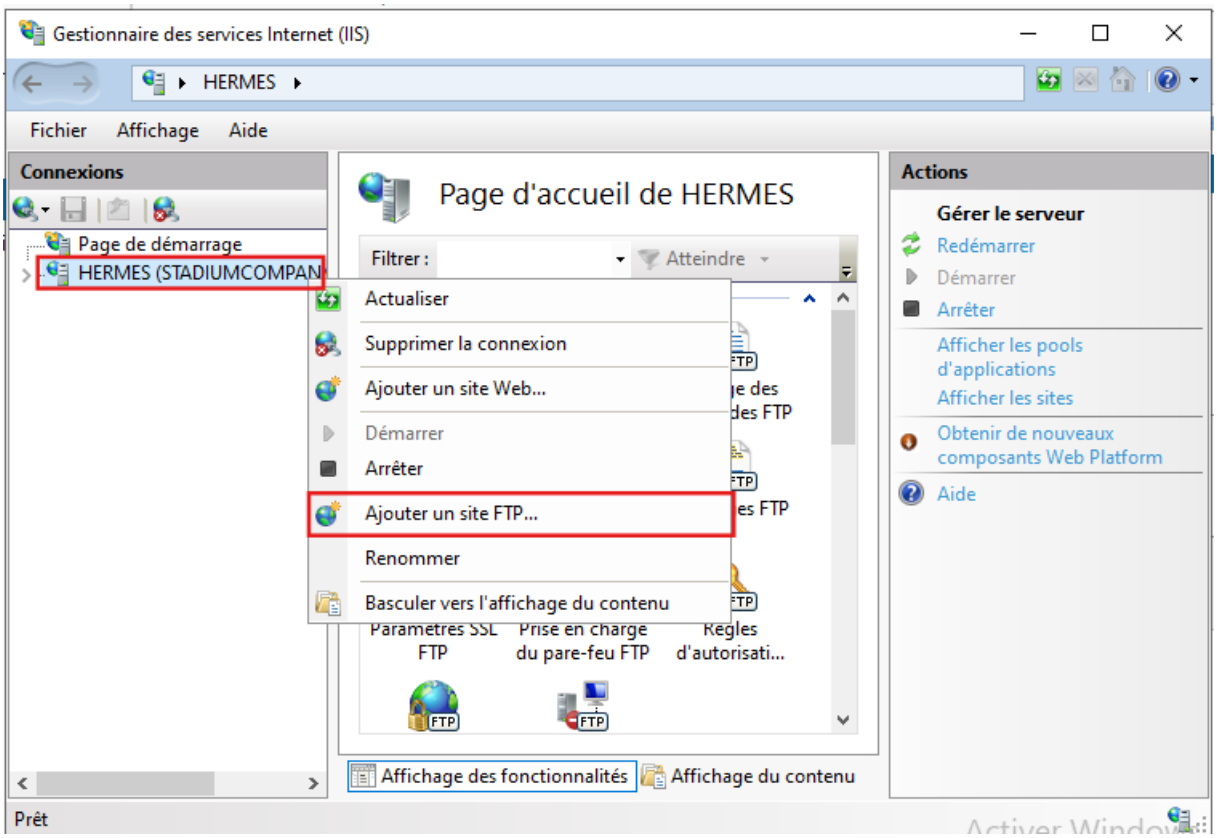
✓ Résultat

Seuls les utilisateurs appartenant à ces groupes AD pourront accéder au FTP. Les permissions sont gérées **centralement** via Active Directory, ce qui est propre, sécurisé et professionnel.

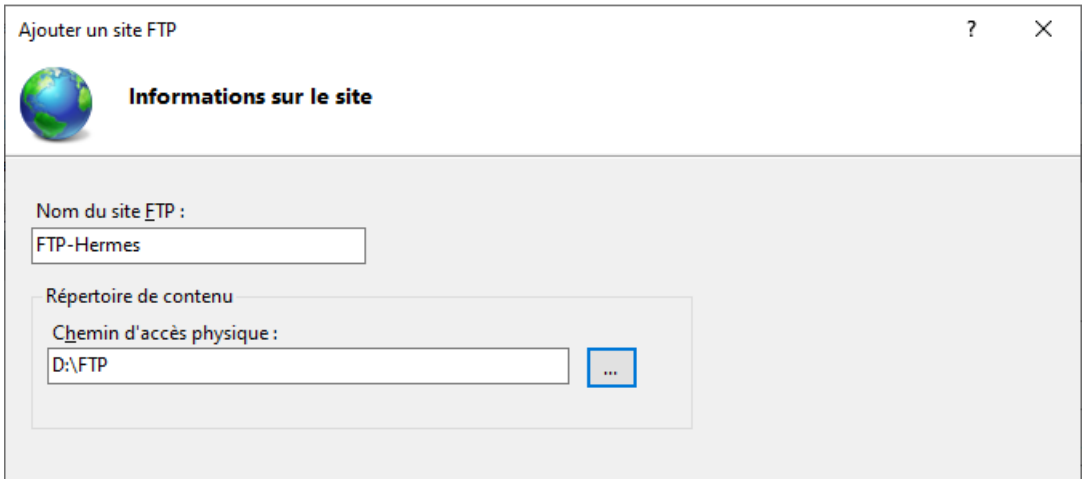


3. Création du site FTP dans IIS

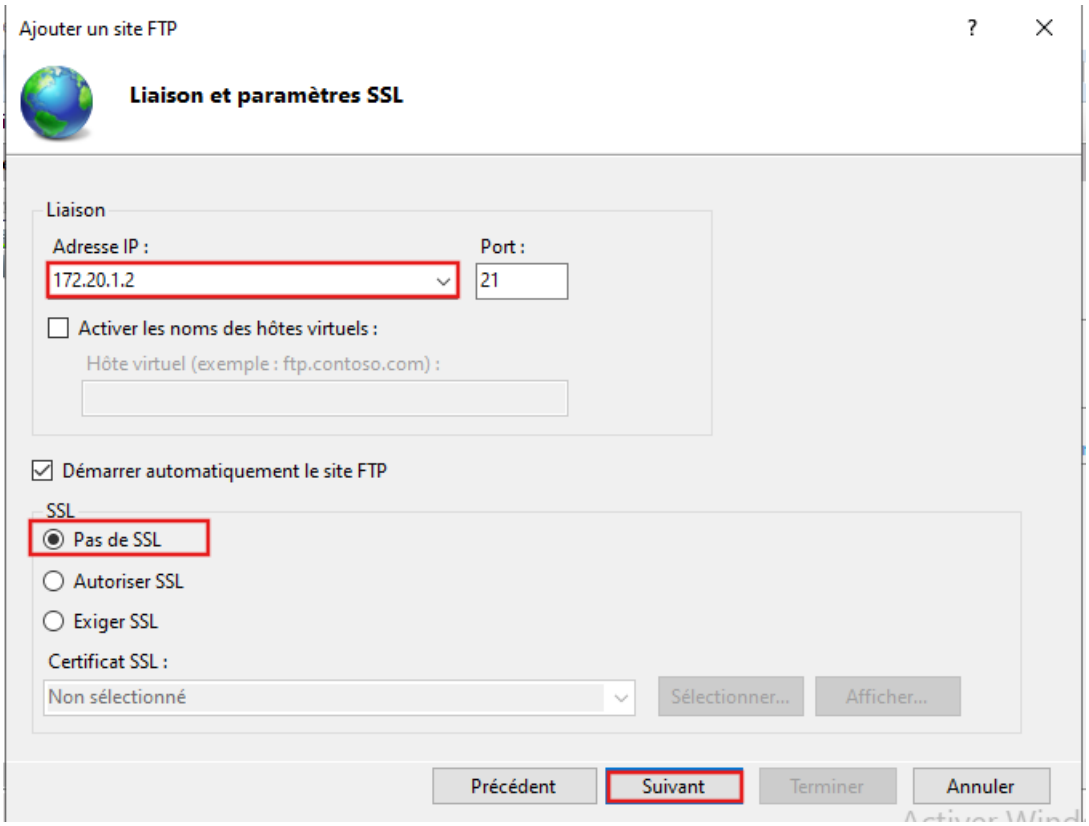
1. Ouvrir **Gestionnaire IIS**
2. Clic droit sur **HERMES → Ajouter un site FTP**



3. Renseigner les paramètres :
   - **Nom du site :**
     `FTP-Hermes`
   - **Chemin physique :**
     `D:\FTP`



- **Adresse IP :**
  `172.20.1.2`
- **Port :**
  `21`
- **SSL :**
  Désactivé (aucun certificat pour l'instant)



4. Configuration de l'authentification

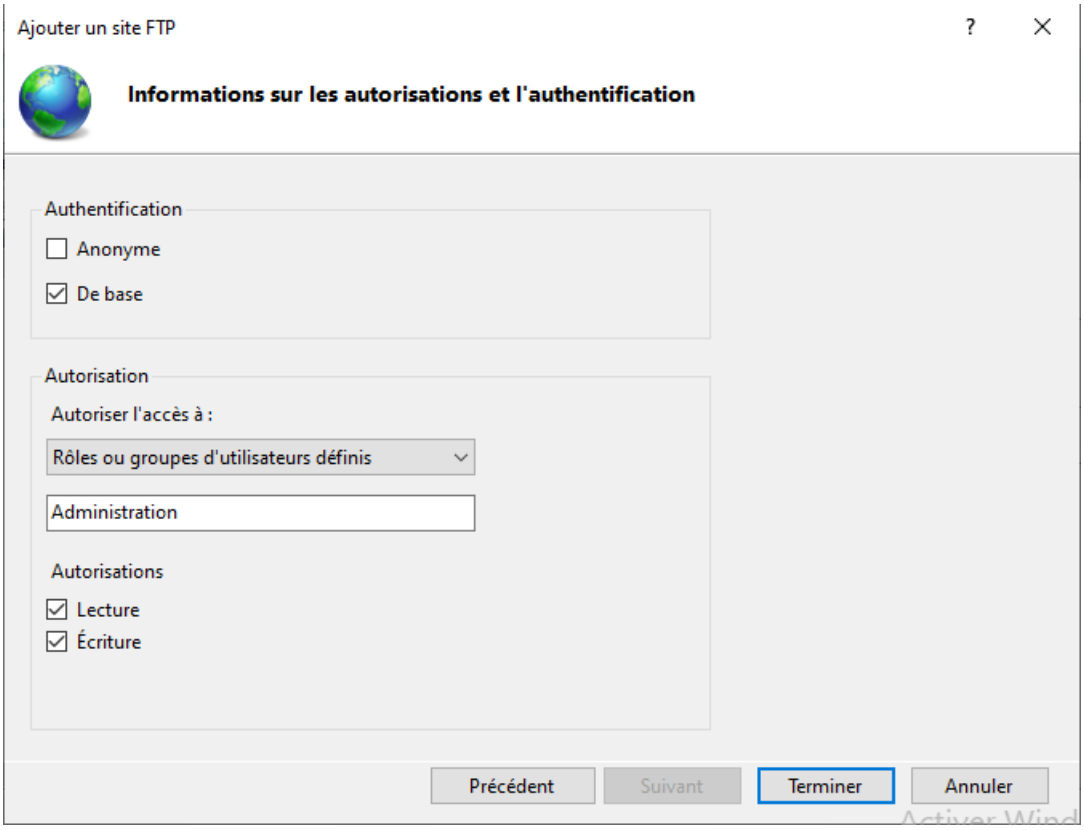
Deux modes possibles :

✓ Authentification anonyme

- Accès public
- Pas de compte AD requis
- Permissions NTFS doivent autoriser *IUSR*

✓ Authentification de base

- Nécessite un **compte Active Directory**
- Plus sécurisé
- Permissions NTFS doivent autoriser les groupes AD

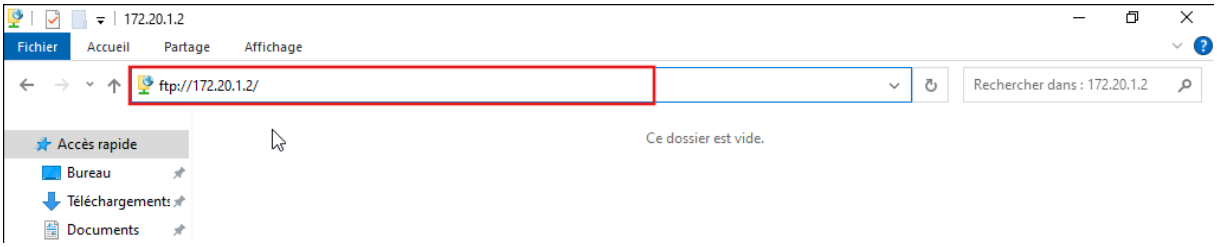


5. Test depuis un poste client

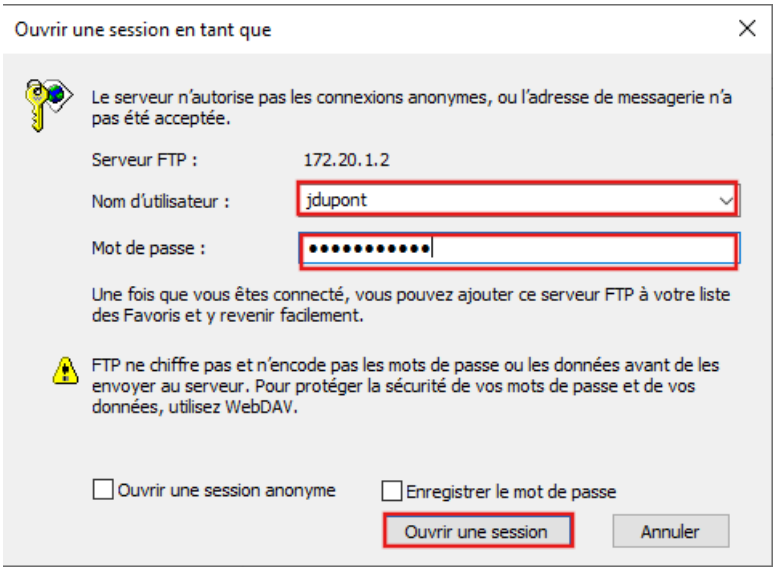
Dans l'explorateur Windows :

`ftp://172.20.1.2`

Si authentification de base :



Entrer un **login AD** (ex : jdupont).

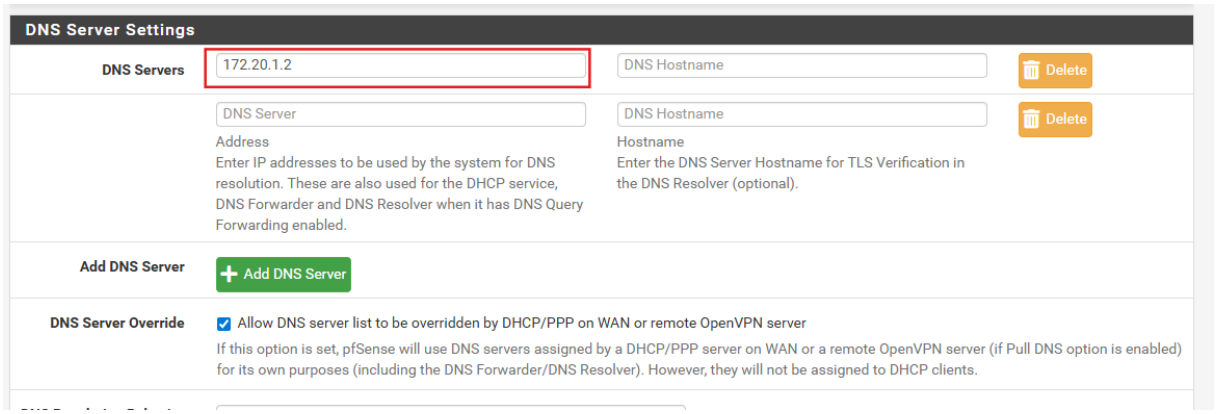


Partie 8 – Intégration avec pfSense (DNS / routage)

8.1 Configurer pfSense pour utiliser Hermes comme DNS

Dans pfSense :

- **System > General Setup**
  - DNS Server 1 : `172.20.1.2` (Hermes)
  - DNS Server 2 : (plus tard Ares)
  - Cocher : **Do not use the DNS Forwarder/Resolver as a DNS server for the firewall** si tu veux forcer Hermes



8.2 DHCP (plus tard avec Kratos)

Quand Kratos1/2 seront installés, leurs étendues DHCP devront distribuer :

- **DNS : 172.20.1.2**
- **Passerelle : 172.20.1.254 (pfSense)**

Partie 9 – Tests essentiels

Sur Hermes :

- `ping 172.20.1.254` → pfSense
- `ping hermes.stadiumcompany.local` → lui-même
- `nslookup hermes.stadiumcompany.local` → doit répondre 172.20.1.2
- `nslookup google.fr` → doit passer par la chaîne DNS (Hermes → pfSense → Internet)

Plus tard, depuis un poste client joint au domaine :

- `ping hermes`
- `ping glpi.stadiumcompany.local` (quand GLPI sera installé)
- `ping zimbra.stadiumcompany.local` (quand Zimbra sera installé)