

# **TP Active Directory parent et enfant avec relation d'approbation bidirectionnelle**

## **Objectifs**

L'objectif de ce TP est de créer un domaine racine et un domaine enfant sur deux serveurs distincts, et de créer des relations d'approbation entre les deux domaines.

## **Matériel**

- Un serveur EXSi
- Deux serveurs virtuels Windows Server 2022
- Une station Windows 11 avec hyper V
- 2 VM Windows 11
- Un routeur cisco
- Un switch cisco

## **Étapes**

### **Configuration du routage**

1. Faire un schéma du routage.
2. Faire la configuration du routeur.
3. Faire la configuration du switch.

### Création d'un domaine racine

1. Activez le serveur et rejoignez le domaine Active Directory local.
2. Créez un domaine racine avec le nom et .local.
3. Créez des GPO pour appliquer des stratégies de sécurité et de configuration.
4. Créez des utilisateurs et des groupes.

### Intégration des VM W11

1. Activez la station et rejoignez le domaine Active Directory.
2. Vérifiez l'appartenance au domaine.

### Création d'un domaine enfant

1. Activez le serveur et rejoignez le domaine Active Directory racine.
2. Créez un domaine enfant avec le nom de votre choix.
3. Créez des GPO pour appliquer des stratégies de sécurité et de configuration.
4. Créez des utilisateurs et des groupes.

### Intégration des VM W11

1. Activez la station et rejoignez le domaine Active Directory.
2. Vérifiez l'appartenance au domaine.

### Relation d'approbation

1. Routage sur Windows
2. Faire la relation d'approbation

### Partage de données

1. Faire le partage de données

### **Définition :**

**Le routage** est le processus de sélection d'un chemin à travers un ou plusieurs réseaux pour acheminer les données d'un expéditeur jusqu'à un ou plusieurs destinataires.

Dans les réseaux informatiques, le routage est effectué par des routeurs, qui sont des périphériques réseaux spécialisés. Les routeurs utilisent des protocoles de routage pour échanger des informations sur les réseaux et les chemins disponibles.

Il existe **deux types de routage** :

**Le routage statique** est un processus manuel qui nécessite la configuration de chaque routeur individuellement.

**Le routage dynamique** est un processus automatique qui permet aux routeurs d'échanger des informations sur les réseaux et les chemins disponibles.

**Le routage** est un processus essentiel pour le fonctionnement des réseaux informatiques. Il permet aux données de circuler d'un point à un autre, même si les réseaux sont interconnectés.

**Active Directory**, un domaine parent est un domaine qui contient un ou plusieurs domaines enfants. Un domaine enfant est un domaine qui est subordonné à un domaine parent.

**Les domaines parent et enfant** sont liés par une relation d'approbation. L'approbation permet aux utilisateurs et aux ordinateurs du domaine enfant d'accéder aux ressources du domaine parent.

**Un domaine parent** est généralement créé pour regrouper des ressources et des utilisateurs appartenant à une même organisation. **Les domaines enfants** sont généralement créés pour regrouper des ressources et des utilisateurs appartenant à une même division ou département de l'organisation.

Par exemple, une entreprise peut avoir **un domaine parent** pour regrouper tous ses utilisateurs et ses ordinateurs. L'entreprise peut ensuite créer **des domaines enfants** pour regrouper les utilisateurs et les ordinateurs de ses différentes divisions, telles que la vente, le marketing et les finances.

### **Fonctionnalités**

**Les domaines parent et enfant** offrent les mêmes fonctionnalités que les domaines autonomes. Ces fonctionnalités incluent :

Gestion centralisée des utilisateurs et des ordinateurs

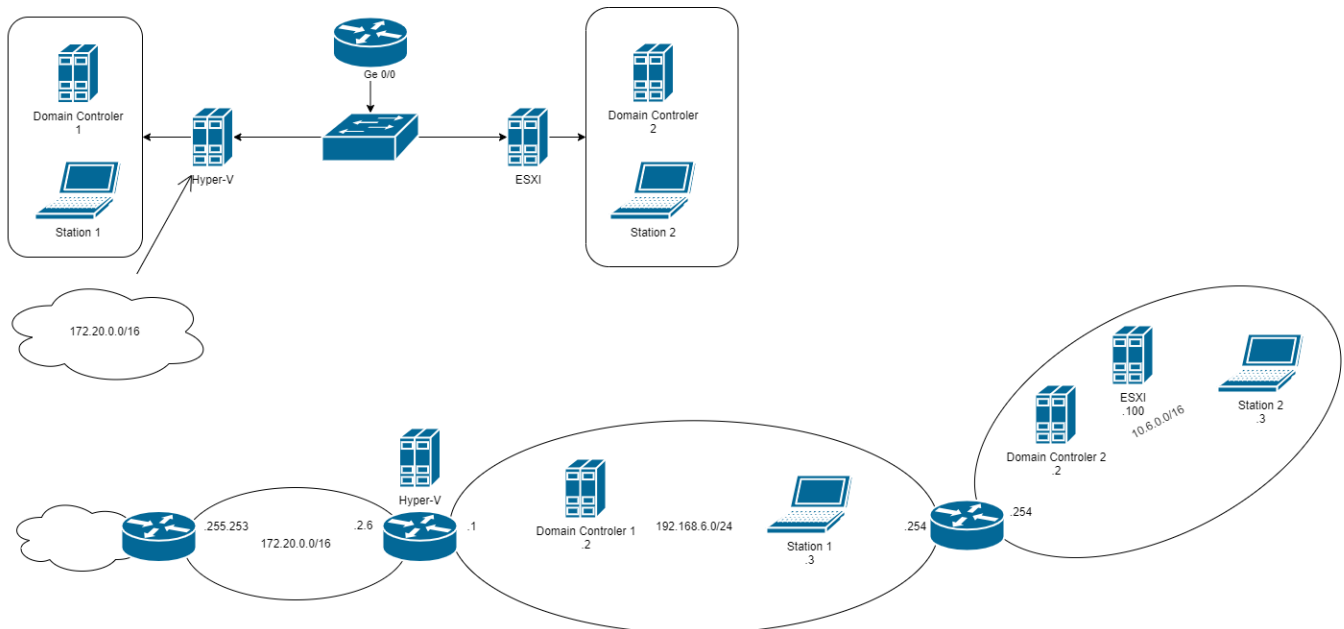
Authentification et autorisation des utilisateurs

Partage de ressources

Gestion de la sécurité

## Configuration du routage

### 1. Faire un schéma du routage.



### 2. Faire la configuration du routeur.

Voici un aperçu de notre configuration :

**en**

**conf t**

Cela entre dans le mode de configuration global du routeur.

**ip route 0.0.0.0 0.0.0.0 192.168.6.1**

Cela configure une route statique vers le routeur par défaut (192.168.6.1) sur l'interface interne.

**interface GigabitEthernet0/1**

**no ip address**

**no sh**

Cela désactive l'interface GigabitEthernet0/1 et désactive le mode de désactivation.

**interface GigabitEthernet0/0**

**no ip address**

**duplex auto**

**speed auto**

**no sh**

Cela désactive l'interface GigabitEthernet0/0, définit le mode duplex sur auto, définit le mode de vitesse sur auto et désactive le mode de désactivation.

#### **interface GigabitEthernet0/0.10**

**encapsulation dot1Q 10**

**ip address 192.168.6.254 255.255.255.0**

Cela configure l'interface GigabitEthernet0/0.10 en tant qu'interface de jonction VLAN avec VLAN 10. Elle attribue également l'adresse IP 192.168.6.254/24 à l'interface.

#### **interface GigabitEthernet0/0.20**

**encapsulation dot1Q 20**

**ip address 10.6.0.254 255.255.0.0**

Cela configure l'interface GigabitEthernet0/0.20 en tant qu'interface de jonction VLAN avec VLAN 20. Elle attribue également l'adresse IP 10.6.0.254/24 à l'interface.

**end**

**write mem**

Cela quitte le mode de configuration global du routeur et enregistre la configuration en mémoire.

### **3. Faire la configuration du switch.**

Voici un aperçu de notre configuration :

**conf t**

Cela entre dans le mode de configuration global du commutateur.

**vlan 10**

**vlan 20**

**exit**

Ceci crée VLAN 10 et VLAN 20.

**interface range FastEthernet0/1-12**

**switchport mode access**

**switchport access vlan 10**

Ceci configure les interfaces FastEthernet 0/1 à 0/12 en tant que ports d'accès affectés à VLAN 10.

**interface range FastEthernet0/13-24**

**switchport mode access**

**switchport access vlan 20**

Ceci configure les interfaces FastEthernet 0/13 à 0/24 en tant que ports d'accès affectés à VLAN 20.

**interface GigabitEthernet0/1**

**switchport mode trunk**

Ceci configure l'interface GigabitEthernet 0/1 en tant que port de liaison.

**interface vlan 10**

**ip address 192.168.6.253 255.255.255.0**

**no shutdown**

**ip default-gateway 192.168.6.254**

Ceci configure VLAN 10 avec l'adresse IP 192.168.6.253/24 et définit la passerelle par défaut sur 192.168.6.254.

**line vty 0 4**

**password cisco**

**login**

**exec-timeout 15 0**

Ceci configure les lignes VTY 0-4 avec le mot de passe "cisco" et l'authentification activée. Il définit également le délai d'exécution de l'invite à 15 minutes.

**end**

**write mem**

Ceci quitte le mode de configuration global du commutateur et enregistre la configuration en mémoire.

Voici quelques commentaires spécifiques sur notre configuration :

Nous avons configuré VLAN 10 et VLAN 20 avec des plages d'adresses IP différentes. Cela permet de séparer les trafics des deux VLAN.

Nous avons configuré les interfaces FastEthernet 0/1 à 0/12 en tant que ports d'accès affectés à VLAN 10. Cela signifie que les appareils connectés à ces interfaces seront membres de VLAN 10.

Nous avons configuré les interfaces FastEthernet 0/13 à 0/24 en tant que ports d'accès affectés à VLAN 20. Cela signifie que les appareils connectés à ces interfaces seront membres de VLAN 20.

Nous avons configuré l'interface GigabitEthernet 0/1 en tant que port de liaison. Cela signifie que l'interface peut transporter des trames de plusieurs VLAN.

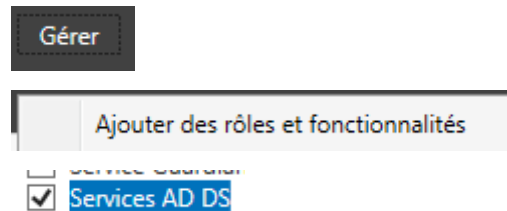
Nous avons configuré VLAN 10 avec l'adresse IP 192.168.6.253/24. Cela permet aux appareils membres de VLAN 10 d'accéder à Internet via la passerelle par défaut.

Pour finir on a fait du Nat de la carte réseau Intel vers la carte broadcom à l'aide de la technologie partage de windows sur la station windows 11.

## Création d'un domaine racine

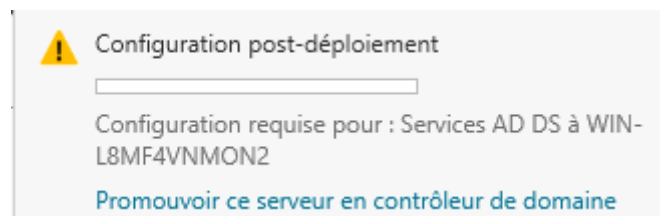
1. Activez le serveur et rejoignez le domaine Active Directory local.

Pour commencer on installe active directory dans les roles :

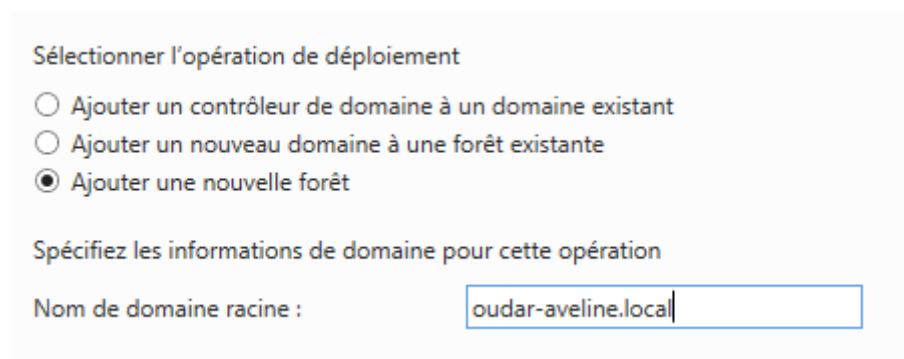


2. Créez un domaine racine avec le nom et .local.

Ensuite on va promouvoir le serveur en contrôleur de domaine :



Puis on ajoute une nouvelle forêt avec le nom de domaine racine (nom + local) :



Pour la suite on ajoute un mot de passe :

Sélectionner le niveau fonctionnel de la nouvelle forêt et du domaine racine

Niveau fonctionnel de la forêt :

Niveau fonctionnel du domaine :

Spécifier les fonctionnalités de contrôleur de domaine

☒ Serveur DNS (Domain Name System)

☒ Catalogue global (GC)

☐ Contrôleur de domaine en lecture seule (RODC)

Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)

Mot de passe :

Confirmer le mot de passe :

On a laissé l'emplacement par défaut de la base de données de l'AD :

Spécifier l'emplacement de la base de données AD DS, des fichiers journaux et de SYSVOL

Dossier de la base de données :  ...

Dossier des fichiers journaux :  ...

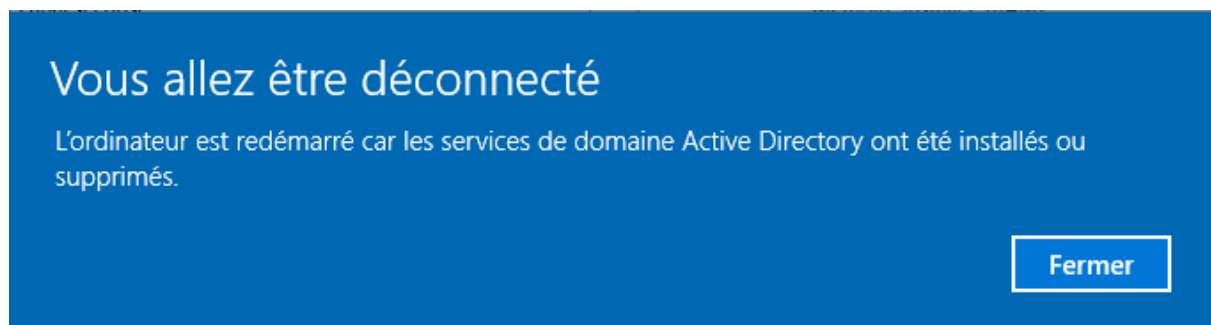
Dossier SYSVOL :  ...

Ensuite on a laissé le nom de domaine NetBIOS suggérer.

Vérifiez le nom NetBIOS attribué au domaine et modifiez-le si nécessaire.

Le nom de domaine NetBIOS :

Pour finir on va être déconnecté :





Et on vérifie si le serveur windows est bien connecté au domaine :

Domaine	oudar-aveline.local
Serveur DNS préféré :	127 . 0 . 0 . 1

3. Créez des GPO pour appliquer des stratégies de sécurité et de configuration.

### **Définition :**

**Une stratégie de groupe (GPO)** est un ensemble de paramètres de configuration et de gestion des systèmes d'exploitation, ainsi que des paramètres d'ordinateur et d'utilisateur dans un environnement informatique Microsoft.

**Les GPO** sont gérées à travers **des objets de stratégie de groupe (GPO)** communément appelés **GPO (Group Policy Objects)**. Chaque GPO contient deux parties, ou nœuds : **une configuration utilisateur** et **une configuration ordinateur**.

La configuration utilisateur définit les paramètres qui s'appliquent aux utilisateurs, tels que les **paramètres de bureau**, les **paramètres de sécurité** et les **paramètres d'applications**.

La **configuration ordinateur** définit les paramètres qui s'appliquent aux ordinateurs, tels que les paramètres de démarrage, les paramètres de réseau et les paramètres d'applications.

**Les GPO** sont utilisées pour centraliser la gestion des ordinateurs et des utilisateurs dans un environnement **Active Directory**. Elles permettent aux administrateurs informatiques de configurer et de gérer les ordinateurs et les utilisateurs en masse.

### **Exemples d'utilisation des GPO**

- Pour configurer les paramètres de bureau, tels que le fond d'écran, les polices et les couleurs.
- Pour configurer les paramètres de sécurité, tels que les droits d'accès aux fichiers et aux dossiers.
- Pour configurer les paramètres d'applications, tels que les paramètres d'installation et de désinstallation.

- Pour configurer les paramètres d'imprimantes, tels que les paramètres d'impression et les paramètres de sécurité.

### Avantages des GPO

Les GPO offrent plusieurs avantages, notamment :

- Simplifie la gestion des ressources
- Améliore la sécurité
- Facilite la croissance de l'organisation

### Inconvénients des GPO

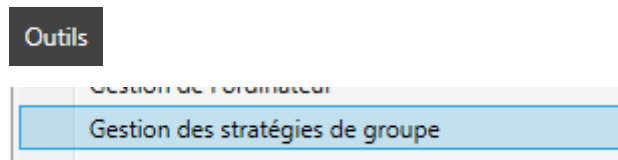
Les GPO présentent quelques inconvénients, notamment :

- Peut être complexe à configurer
- Peut avoir un impact sur les performances

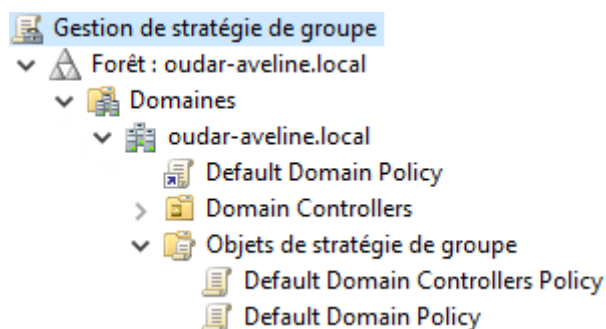
### Conclusion

Les GPO sont un outil puissant qui peut être utilisé pour centraliser la gestion des ordinateurs et des utilisateurs dans un environnement informatique Microsoft.

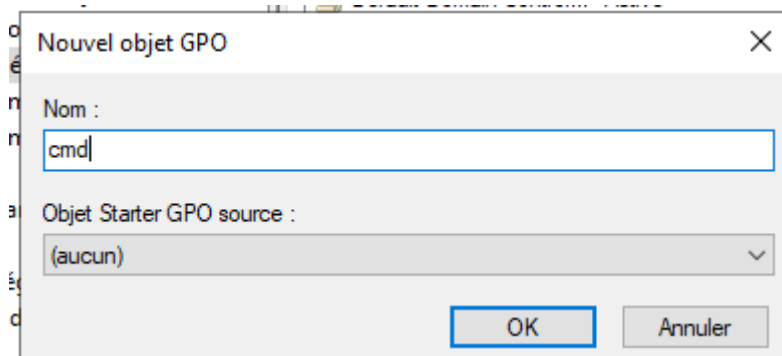
Pour créer des GPO il faut aller dans outils, gestion des stratégies de groupe :



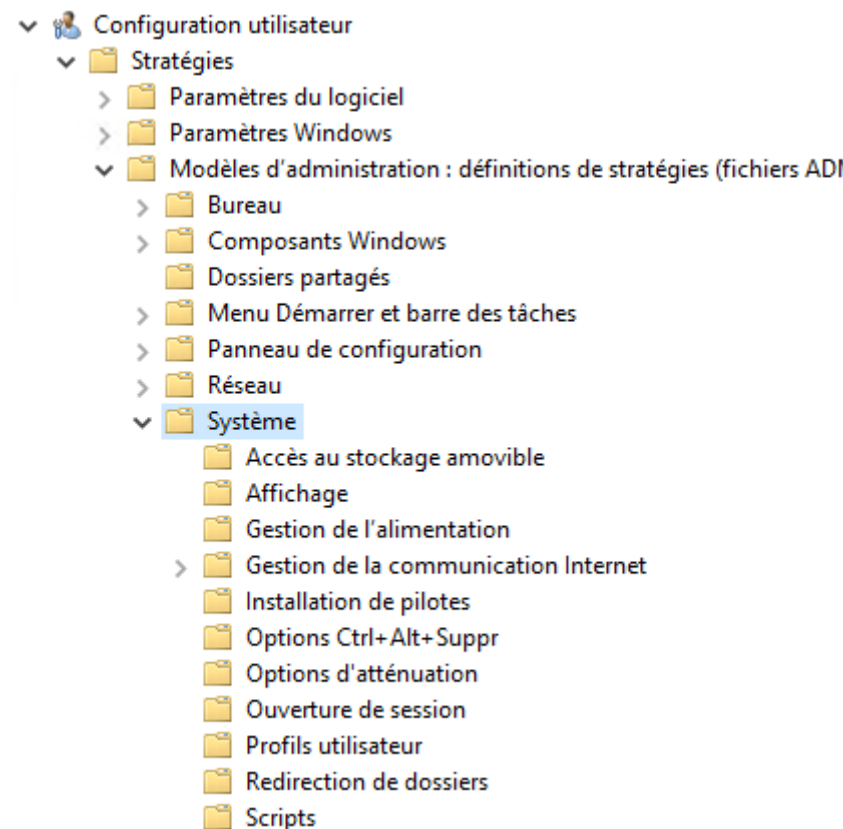
Puis dans gestion de stratégie de groupe, la forêt que vous souhaitez, dans domaines, choisissez le domaine souhaitez puis dans Objets de stratégie de groupe :



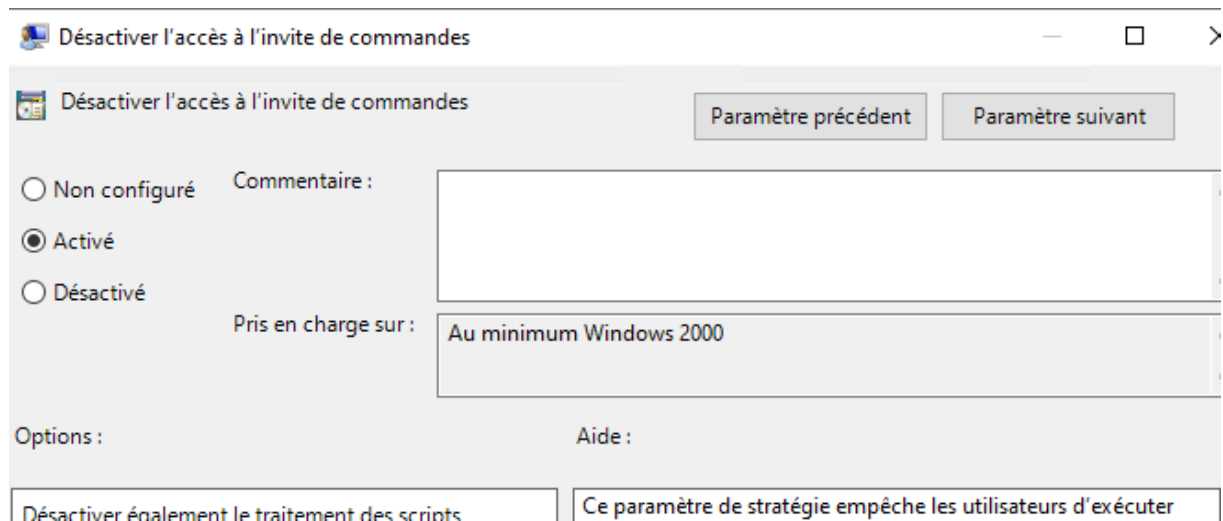
Ensuite on crée un nouvel GPO pour notre part on va créer un GPO qui bloque le cmd :



Ensuite on modifie le GPO qu'on vient de créer. Puis on va dans la configuration de l'utilisateur, dans Stratégie, puis dans modèle d'administration et dans Système :

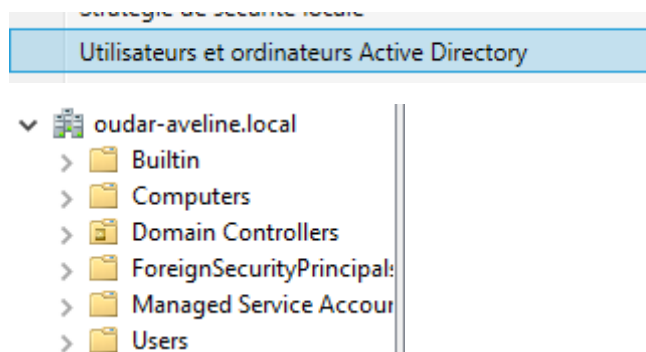


Pour la suite on choisit la règle qu'on veut pour notre part on a choisi « désactiver l'accès à l'invite de commandes et on l'active :



#### 4. Créez des utilisateurs et des groupes.

Pour créer des utilisateurs et des groupes on va dans « Utilisateurs et ordinateurs Active Directory » et dans le domaine souhaiter :




Puis on a créé une nouvelle unité d'organisation :



Puis on a créé un nouveau groupe qu'on va nommer « GPOuser »

Nouvel objet - Groupe ×

 Créer dans : oudar-aveline.local/Utilisateurs

---

Nom du groupe :


Nom de groupe (antérieur à Windows 2000) :

Étendue du groupe	Type de groupe
<input type="radio"/> Domaine local	<input checked="" type="radio"/> Sécurité
<input checked="" type="radio"/> Globale	<input type="radio"/> Distribution
<input type="radio"/> Universelle	

---

Et on a créé un nouvel utilisateur :

Nouvel objet - Utilisateur ×

 Créer dans : oudar-aveline.local/Utilisateurs

---

Prénom :  Initiales :

Nom :

Nom complet :


Nom d'ouverture de session de l'utilisateur :  
 @oudar-aveline.local ▼

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :

---

Nouvel objet - Utilisateur X

---

 Créer dans : oudar-aveline.local/Utilisateurs

---

Mot de passe :

Confirmer le mot de passe :

☐ L'utilisateur doit changer le mot de passe à la prochaine ouverture de session  
☒ L'utilisateur ne peut pas changer de mot de passe  
☒ Le mot de passe n'expire jamais  
☐ Le compte est désactivé

---


< Précédent    Suivant >    Annuler

Qu'on va ajouté dans le groupe qu'on a créé juste avant :

Propriétés de : GPOuser

Général    Membres    Membre de    Géré par

Membres :





Nom	Dossier Services de domaine Active Dire
 Nicolas OUDAR	oudar-aveline.local/Utilisateurs

Pour finir on fait une délégation des GPO :

**Objets de stratégie c**

Contenu    Délégation

Et on ajoute le groupe qu'on a créé qui regroupe l'utilisateur qu'on a créé :

-  Admins du domaine (OUDAR-AVELINE\Admins du domaine) |
-  **GPOuser (OUDAR-AVELINE\GPOuser)** |
-  Propriétaires créateurs de la stratégie de groupe (OUDAR-AVELI... |
-  Système |

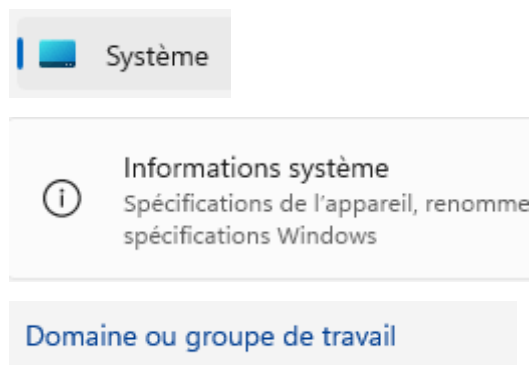
## Intégration des VM W11

1. Activez la station et rejoignez le domaine Active Directory.

Pour connecter la station W11 au domaine de l'active directory il faut dans les paramètres IP mettre en DNS l'IP du serveur Active directory donc pour nous c'est 10.6.0.4 :

### DNS préféré

Ensuite dans les paramètres on va dans système, information système, Domaine ou groupe de travail :



Puis on modifie le domaine en mettant le domaine du serveur Active directory :

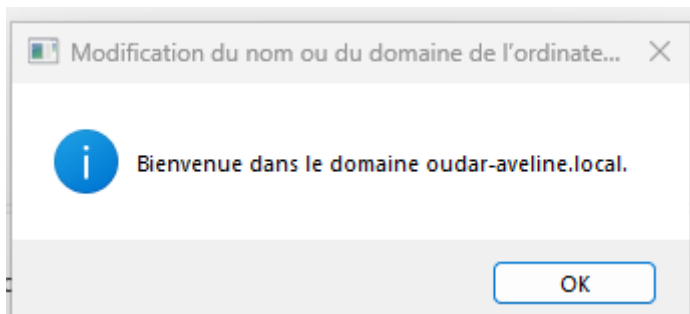
This is a screenshot of the 'Membre d'un' (Member of) settings window. The 'Domaine :' (Domain) option is selected with a blue radio button, and the text 'oudar-aveline.local' is entered in the adjacent text field.

Ensuite on se connecte avec le compte autorisé à joindre le domaine pour notre part on mit le compte Administrateur :

## Modification du nom ou du domaine de l'ordinateur

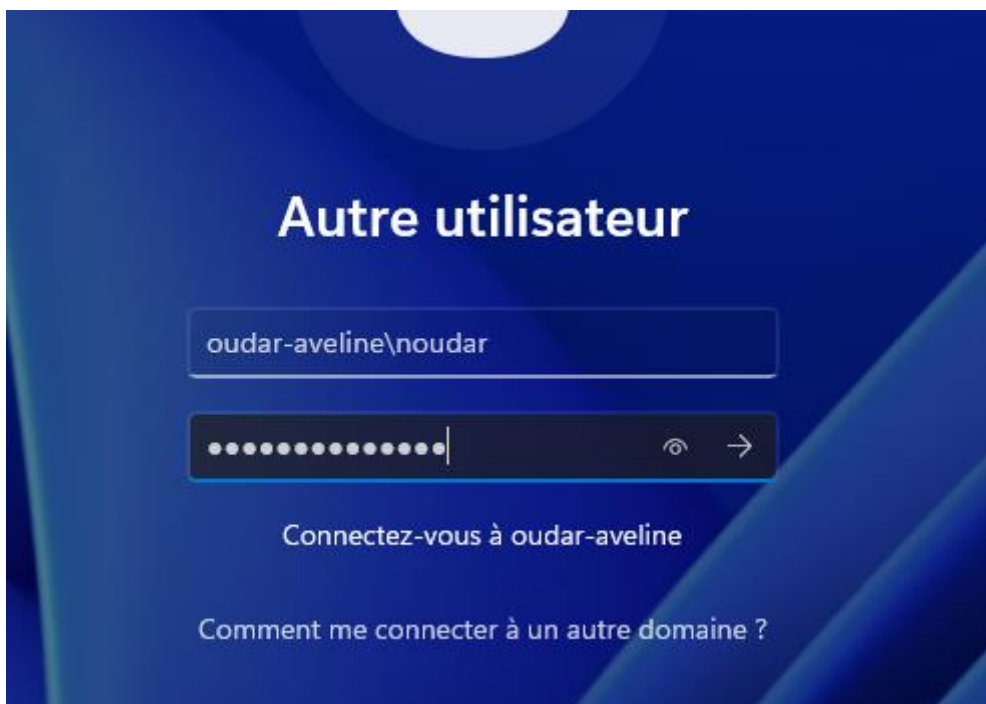
Entrez le nom et le mot de passe d'un compte autorisé à joindre le domaine.

Puis on remarque qu'on est bien dans le domaine de l'Active directory :



2. Vérifiez l'appartenance au domaine.

Pour finir on se connecte au compte qu'on a créé dans l'active directory :



Et on remarque qu'on n'a pas accès au cmd.

### Création d'un domaine enfant

1. Activez le serveur et rejoignez le domaine Active Directory racine.

Pour commencer on connecte le serveur windows à l'active directory parent.

Pour le connecter au domaine de l'AD parent on met l'IP de l'AD parent.

Serveur DNS préféré :

Puis on va dans paramètres, système, à propos de et renommer ce PC (avancé) :







## Système

Affichage, son, notifications,  
alimentation

À propos de

[Renommer ce PC \(avancé\)](#)

Enfin on ajoute le domaine d'AD parent :

☒ Domaine :

Et on se connecte avec un compte autorisé à joindre le domaine :

Sécurité Windows


### Modification du nom ou du domaine de l'ordinateur

Entrez le nom et le mot de passe d'un compte autorisé à joindre le domaine.

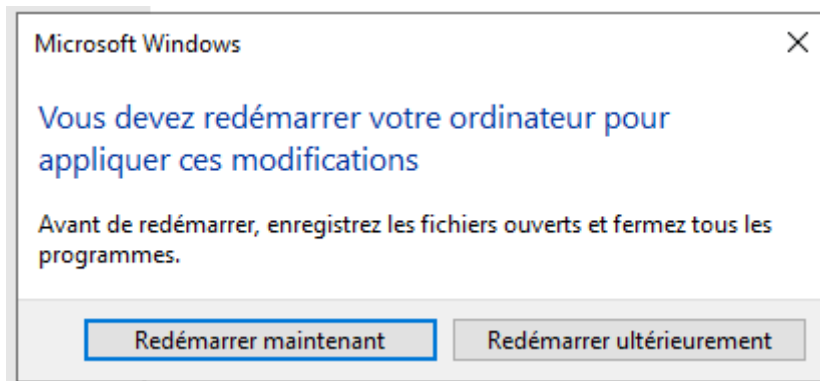
OK Annuler

On remarque qu'on est bien connecté au domaine :

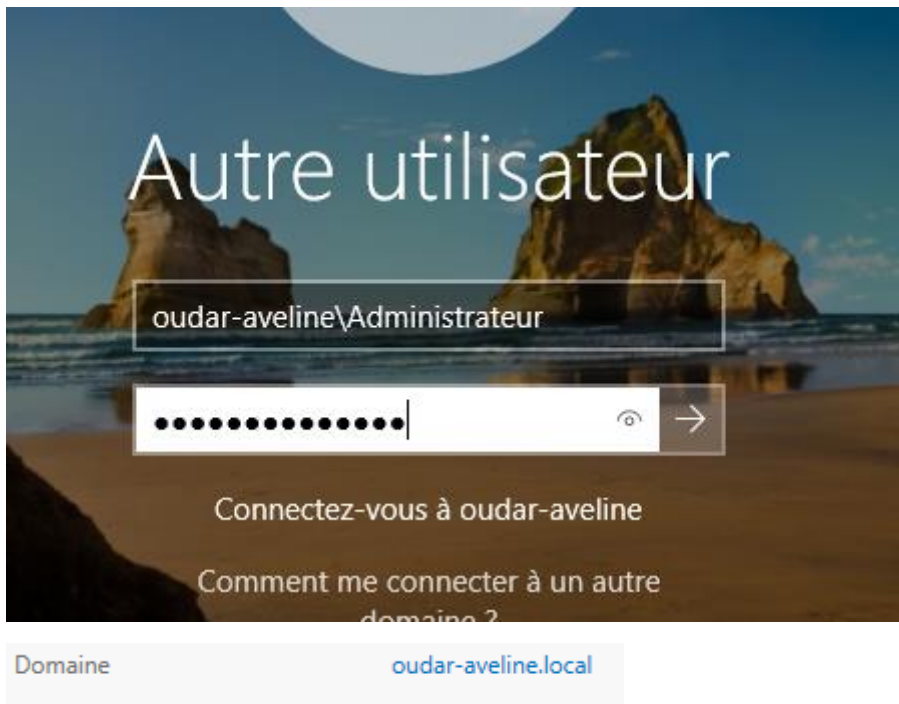
Modification du nom ou du domaine de l'ordinateur

 Bienvenue dans le domaine oudar-aveline.local.

OK

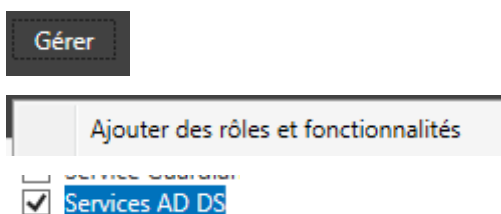


Puis on se connecte au domaine en le mettant de l'ID de l'utilisateur :

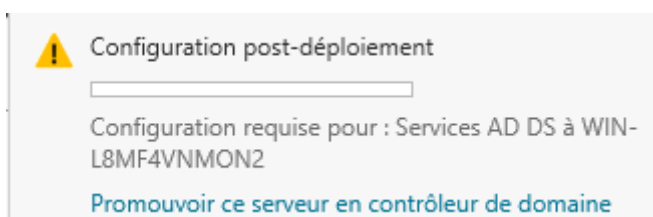


2. Créez un domaine enfant avec le nom de votre choix.

Puis on installe Active directory :



Ensuite on va promouvoir ce serveur en contrôleur de domaine :



Pour la suite on ajoute un nouveau domaine à une forêt existante, on sélectionne le type de domaine (domaine enfant) (le nom du domaine parent et les informations d'identification se met automatiquement) :

Sélectionner l'opération de déploiement

☐ Ajouter un contrôleur de domaine à un domaine existant

☒ Ajouter un nouveau domaine à une forêt existante

☐ Ajouter une nouvelle forêt

Spécifiez les informations de domaine pour cette opération

Sélectionnez le type du domaine : Domaine enfant

Nom du domaine parent : oudar-aveline.local Sélectionner...

Nouveau nom de domaine : sio

Fournir les informations d'identification pour effectuer cette opération

OUДАР-AVELINE\Administrateur (Utilisateur actuel) Modifier...

Pour la suite on ajoute un mot de passe :

Sélectionner le niveau fonctionnel du nouveau domaine

Niveau fonctionnel du domaine : Windows Server 2016

Spécifier les capacités du contrôleur de domaine et les informations sur le site

☒ Serveur DNS (Domain Name System)

☒ Catalogue global (GC)

☐ Contrôleur de domaine en lecture seule (RODC)

Nom du site : Default-First-Site-Name

Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)

Mot de passe : .....

Confirmer le mot de passe : .....

On va créer une délégation DNS :

Spécifier les options de délégation DNS

☒ Créer une délégation DNS

Informations d'identification pour la création de délégation

OUDAR-AVELINE\Administrateur (Utilisateur actuel)

Modifier...

Comme nom de domaine netBIOS on a mis SIO :

Vérifiez le nom NetBIOS attribué au domaine et modifiez-le si nécessaire.

Le nom de domaine NetBIOS :

SIO

On a laissé l'emplacement par défaut de la base de données de l'AD enfant :

Spécifier l'emplacement de la base de données AD DS, des fichiers journaux et de SYSVOL

Dossier de la base de données :

C:\Windows\NTDS

Dossier des fichiers journaux :

C:\Windows\NTDS

Dossier SYSVOL :

C:\Windows\SYSVOL

## Vous allez être déconnecté

L'ordinateur est redémarré car les services de domaine Active Directory ont été installés ou supprimés.

Fermer

Pour finir on vérifie si on est bien connecté au domaine enfant :

Domaine

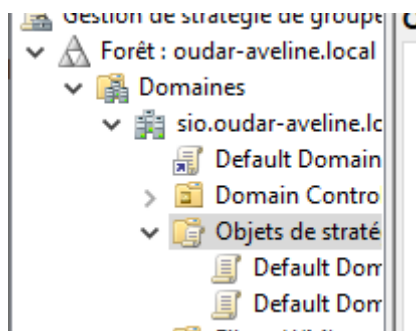
sio.oudar-aveline.local

3. Créez des GPO pour appliquer des stratégies de sécurité et de configuration.

Pour créer des GPO il faut aller dans outils, gestion des stratégies de groupe :

Gestion des stratégies de groupe

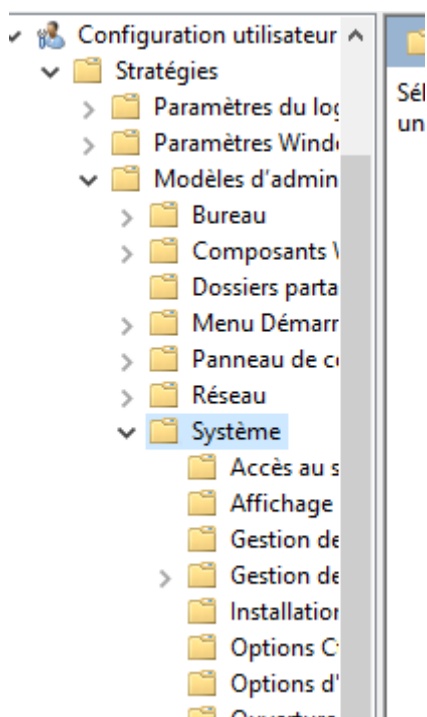
Puis dans gestion de stratégie de groupe, la forêt que vous souhaitez, dans domaines, choisissez le domaine souhaitez puis dans Objets de stratégie de groupe :



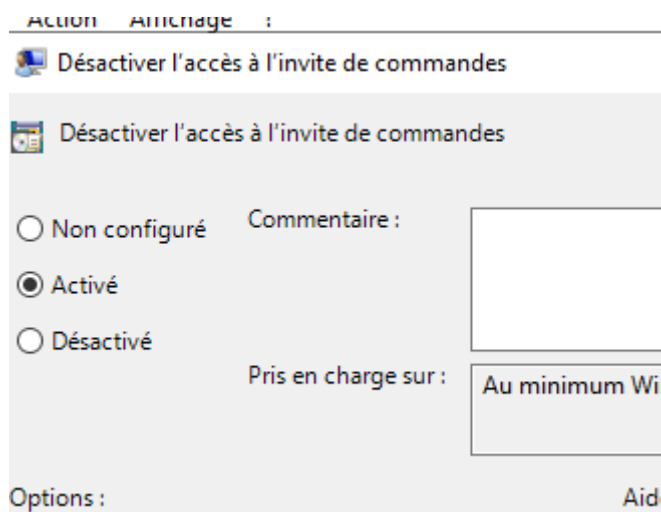
Ensuite on crée un nouvel GPO pour notre part on va créer un GPO qui bloque le cmd :

Nom	Etat GPO
cmd	Activé
Default Domain Control...	Activé
Default Domain Policy	Activé

Ensuite on modifie le GPO qu'on vient de créer. Puis on va dans la configuration de l'utilisateur, dans Stratégie, puis dans modèle d'administration et dans Système :

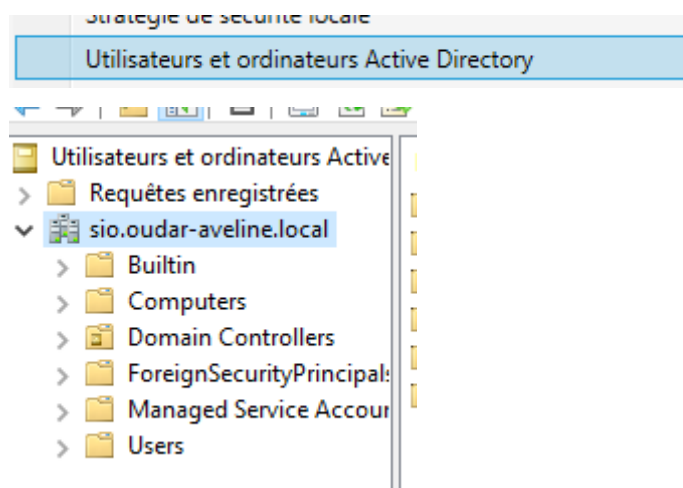


Pour la suite on choisit la règle qu'on veut pour notre part on a choisi « désactiver l'accès à l'invite de commandes et on l'active :

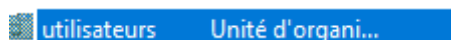


1. Créez des utilisateurs et des groupes.

Pour créer des utilisateurs et des groupes on va dans « Utilisateurs et ordinateurs Active Directory et dans le domaine souhaiter :



Puis on a créé une nouvelle unité d'organisation :



Et on a créé un nouvel utilisateur :

Nouvel objet - Utilisateur

Créer dans : sio.oudar-aveline.local/utilisateurs

Prénom :  Initiales :

Nom :

Nom complet :

Nom d'ouverture de session de l'utilisateur :  
 @sio.oudar-aveline.local

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :

< Précédent Suivant > Annuler

Nouvel objet - Utilisateur

Créer dans : sio.oudar-aveline.local/utilisateurs

Mot de passe :

Confirmer le mot de passe :

☐ L'utilisateur doit changer le mot de passe à la prochaine ouverture de session

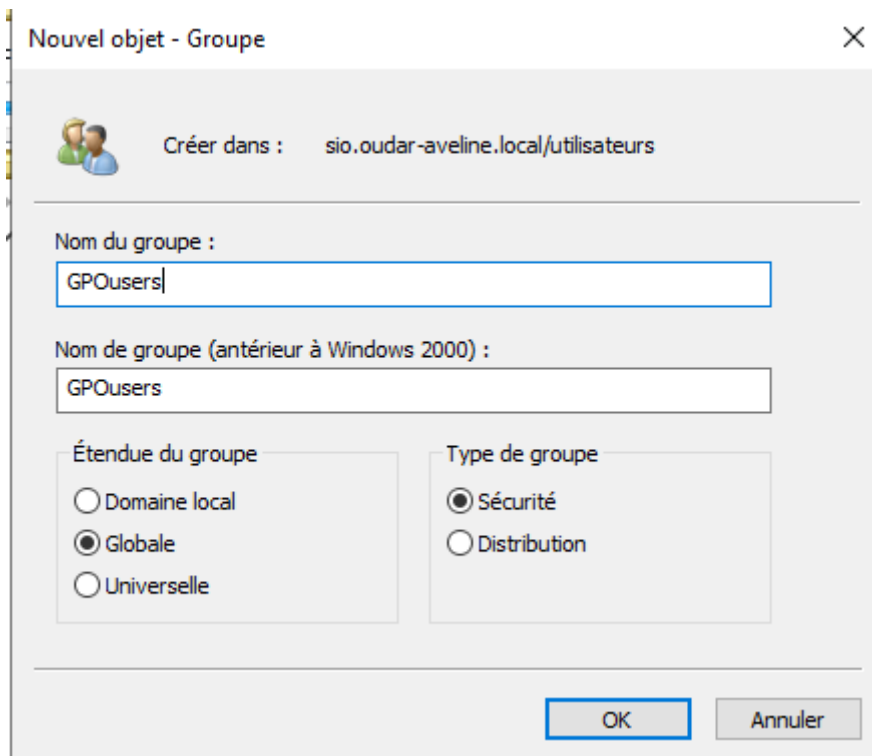
☒ L'utilisateur ne peut pas changer de mot de passe

☒ Le mot de passe n'expire jamais

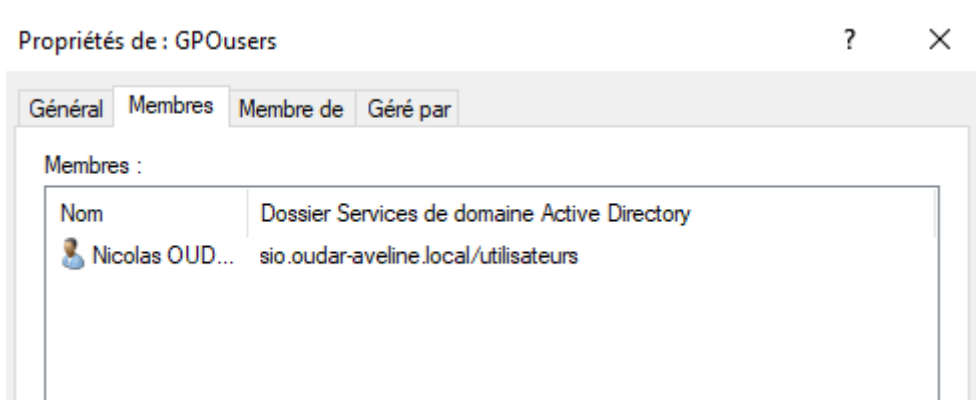
☐ Le compte est désactivé

< Précédent Suivant > Annuler

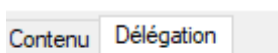
Puis on a créé un nouveau groupe qu'on va nommer « GPOuser » :



On ajoute l'utilisateur qu'on vient de créer dans le groupe qu'on vient de créer :



Puis on fait une délégation dans le GPO :



Les groupes et utilisateurs su

Groupes et utilisateurs :

Pour finir on ajoute le groupe qu'on a créé :

Nom

- Admins du domaine (SIO\Admins du domaine)
- GPOusers (SIO\GPOusers)**
- Propriétaires créateurs de la stratégie de groupe (SIC)
- Système



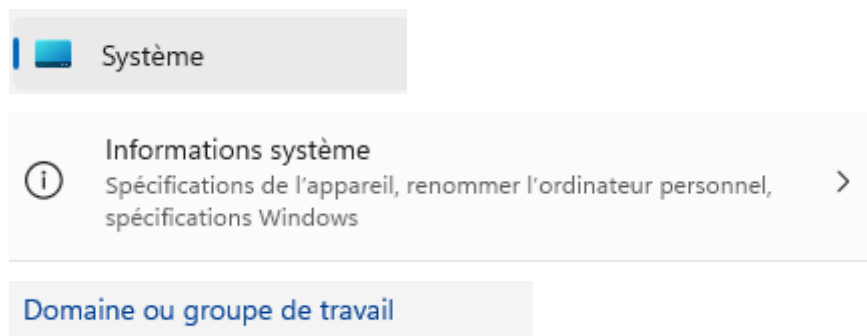
## Intégration des VM W11

1. Activez la station et rejoignez le domaine Active Directory.

Pour connecter la station W11 au domaine enfant de l'active directory il faut dans les paramètres IP mettre en DNS l'IP du serveur Active directory enfant donc pour nous c'est 192.168.6.4 :

### DNS préféré

Ensuite dans les paramètres on va dans système, information système, Domaine ou groupe de travail :



Puis on modifie le domaine en mettant le domaine du serveur Active directory enfant:

The image shows the 'Domaine ou groupe de travail' settings screen. The 'Domaine' option is selected with a blue circle, and the text 'sio.oudar-aveline.local' is entered in the adjacent text box.

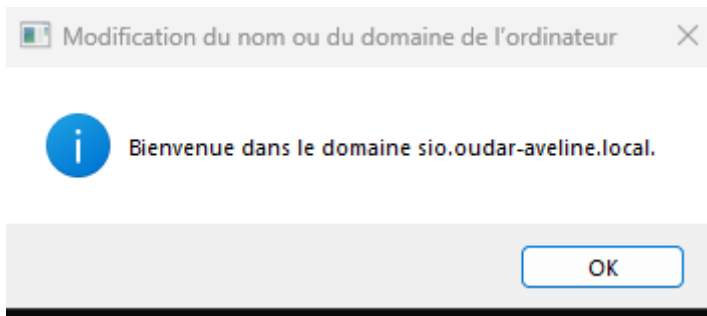
Ensuite on se connecte avec le compte autorisé à joindre le domaine pour notre part on mit le compte Administrateur :

## Modification du nom ou du domaine de l'ordinateur

Entrez le nom et le mot de passe d'un compte autorisé à joindre le domaine.

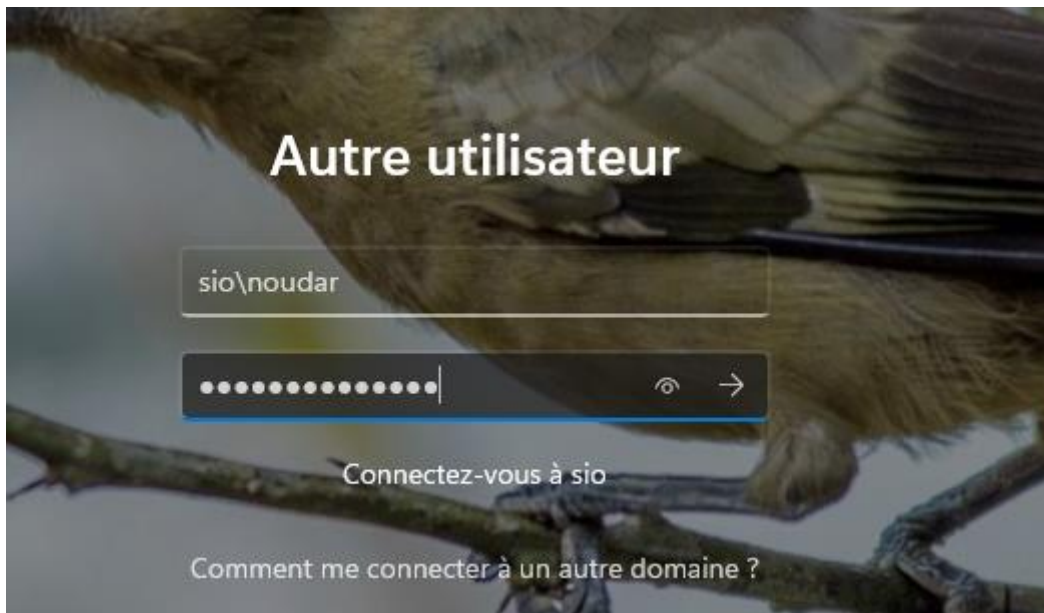
The image shows the 'Join a domain' dialog box in Windows. The 'Username' field contains 'Administrateur'. The 'Password' field is masked with dots. At the bottom, there are two buttons: 'OK' (highlighted in blue) and 'Annuler'.

On remarque qu'on est bien connecté au domaine enfant :



2.Vérifiez l'appartenance au domaine.

Pour finir on se connecte au compte qu'on a créé dans l'active directory :



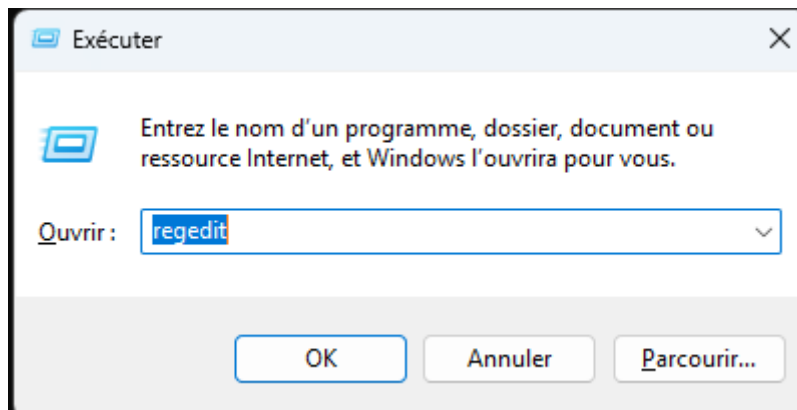
Et on remarque qu'on n'a pas accès au cmd.

## Relation d'approbation

### 1. Routage sur Windows

Pour commencer le routage il faut activer le routage car sur Windows le routage n'est pas activé par défaut.

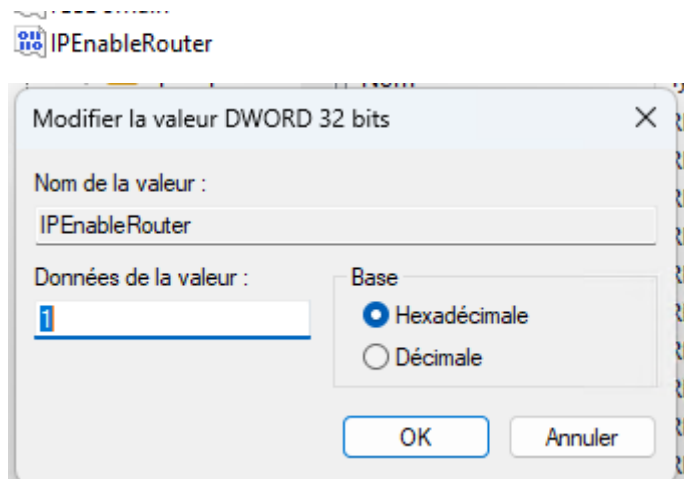
Pour cela il existe deux façon pour activer le routage sur Windows dont la première est d'aller dans le registre (Windows+R et mon écrit regedit) :



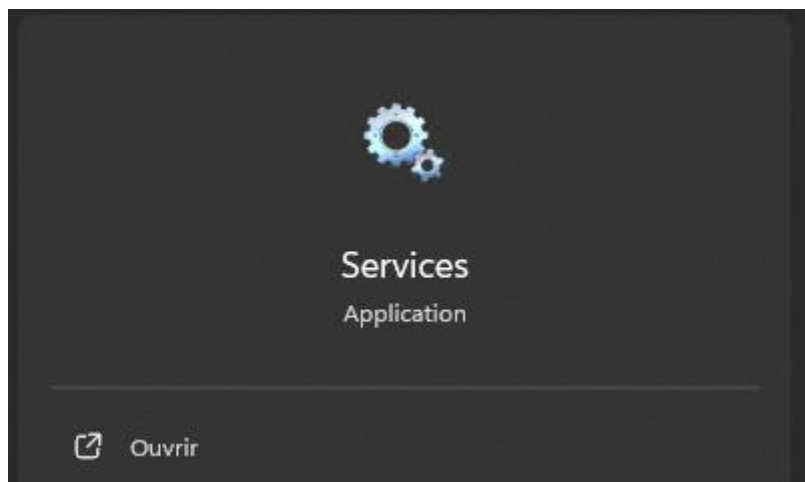
Puis on va dans le répertoire ci-dessous :

Ordinateur\HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

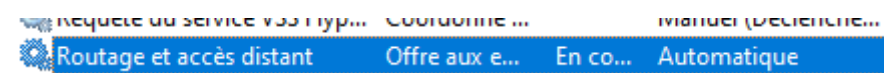
Puis on va dans IPEnableRouter et on remplace le 0 (qui signifie désactiver) par un 1 (qui signifie activer) :



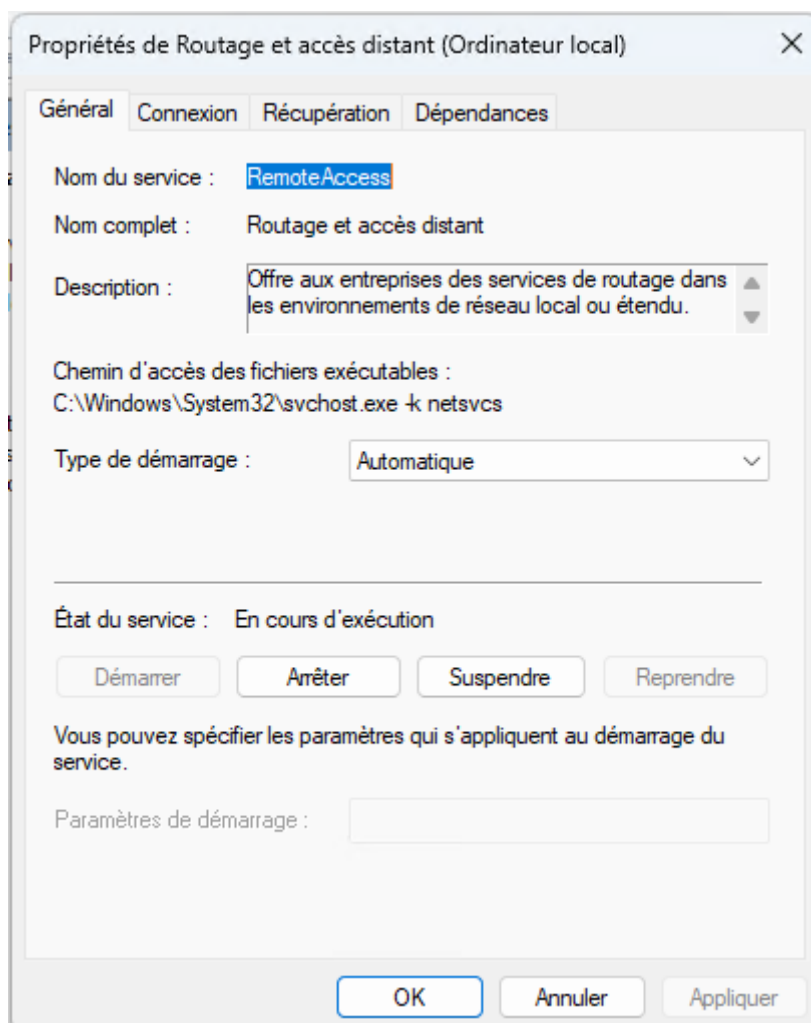
Et la deuxième façon est d'aller dans le service :



Puis aller dans Routage et accès distant (pour aller vite pour chercher appuyer sur R et cela mettra tout les Services commençant par la lettre R) :



Puis on mets le type de démarrage en automatique et on le démarre :



Pour la suite il ne faut pas oublier de désactiver le NAT (avec le partage) et de redémarrer l'ordinateur.

Après avoir redémarrer ne pas oublier de vérifier si le routage est toujours activé puis on va dans le terminal en Administrateur et on tape la commande suivante :

La ligne suivante est une commande Windows pour ajouter une route statique à la table de routage d'un routeur :

**route -p ADD 192.168.2.0 MASK 255.255.255.0 172.20.2.2**

Cette commande a les effets suivants :

- Ajoute une route statique(permanente) à la table de routage.
- La route statique indique que les paquets destinés au réseau 192.168.2.0 doivent être envoyés à la passerelle 172.20.2.2.

Explication de la commande

La commande est composée des éléments suivants :

- route : Le nom de la commande.
- -p : L'option pour rendre la route statique permanente.
- ADD : L'option pour ajouter une route à la table de routage.
- 192.168.2.0 : L'adresse IP de destination du réseau.
- MASK : L'option pour spécifier le masque réseau.
- 255.255.255.0 : Le masque réseau.
- 172.20.2.2 : L'adresse IP de la passerelle pour le réseau.

Exemple

Supposons que nous souhaitons ajouter une route statique pour le réseau 192.168.2.0 à un routeur avec une adresse IP de 192.168.1.1. La passerelle pour le réseau est 172.20.2.2. Nous pourrions utiliser la commande suivante pour ajouter cette route :

**route -p ADD 192.168.2.0 MASK 255.255.255.0 172.20.2.2**

Après avoir exécuté cette commande, le routeur acheminera les paquets destinés au réseau 192.168.2.0 vers la passerelle 172.20.2.2.

## Conclusion

La commande **route -p ADD** est utilisée pour ajouter une route statique à la table de routage d'un routeur. Cette commande peut être utilisée pour fournir un chemin d'accès aux réseaux qui ne sont pas accessibles via des protocoles de routage dynamiques.

Ensuite on avait fait cette table de routage (donc une route pour chaque poste (plus précisément deux route pour une route vers l'EXSI et une route vers l'hyper V))

IPv4 Table de routage				
=====				
Itinéraires actifs :				
Destination réseau	Masque réseau	Adr. passerelle	Adr. interface	Métrique
0.0.0.0	0.0.0.0	172.20.255.253	172.20.2.6	281
10.2.0.0	255.255.0.0	172.20.2.2	172.20.2.6	26
10.3.0.0	255.255.0.0	172.20.2.3	172.20.2.6	26
10.4.0.0	255.255.0.0	172.20.2.4	172.20.2.6	26
10.5.0.0	255.255.0.0	172.20.2.5	172.20.2.6	26
10.6.0.0	255.255.0.0	192.168.6.254	192.168.6.1	36
10.7.0.0	255.255.0.0	172.20.2.7	172.20.2.6	26
10.8.0.0	255.255.0.0	172.20.2.8	172.20.2.6	26
10.9.0.0	255.255.0.0	172.20.2.9	172.20.2.6	26
10.10.0.0	255.255.0.0	172.20.2.10	172.20.2.6	26
10.11.0.0	255.255.0.0	172.20.2.11	172.20.2.6	26
127.0.0.0	255.0.0.0	On-link	127.0.0.1	331
127.0.0.1	255.255.255.255	On-link	127.0.0.1	331
127.255.255.255	255.255.255.255	On-link	127.0.0.1	331
172.18.128.0	255.255.240.0	On-link	172.18.128.1	5256
172.18.128.1	255.255.255.255	On-link	172.18.128.1	5256
172.18.143.255	255.255.255.255	On-link	172.18.128.1	5256
172.20.0.0	255.255.0.0	On-link	172.20.2.6	281
172.20.2.6	255.255.255.255	On-link	172.20.2.6	281
172.20.255.255	255.255.255.255	On-link	172.20.2.6	281
192.168.2.0	255.255.255.0	172.20.2.2	172.20.2.6	26
192.168.3.0	255.255.255.0	172.20.2.3	172.20.2.6	26
192.168.4.0	255.255.255.0	172.20.2.4	172.20.2.6	26
192.168.5.0	255.255.255.0	172.20.2.5	172.20.2.6	26
192.168.6.0	255.255.255.0	On-link	192.168.6.1	291
192.168.6.1	255.255.255.255	On-link	192.168.6.1	291
192.168.6.255	255.255.255.255	On-link	192.168.6.1	291
192.168.7.0	255.255.255.0	172.20.2.7	172.20.2.6	26
192.168.8.0	255.255.255.0	172.20.2.8	172.20.2.6	26
192.168.9.0	255.255.255.0	172.20.2.9	172.20.2.6	26
192.168.10.0	255.255.255.0	172.20.2.10	172.20.2.6	26
192.168.11.0	255.255.255.0	172.20.2.11	172.20.2.6	26
224.0.0.0	240.0.0.0	On-link	127.0.0.1	331
224.0.0.0	240.0.0.0	On-link	172.20.2.6	281
224.0.0.0	240.0.0.0	On-link	192.168.6.1	291
224.0.0.0	240.0.0.0	On-link	172.18.128.1	5256
255.255.255.255	255.255.255.255	On-link	127.0.0.1	331
255.255.255.255	255.255.255.255	On-link	172.20.2.6	281
255.255.255.255	255.255.255.255	On-link	192.168.6.1	291
255.255.255.255	255.255.255.255	On-link	172.18.128.1	5256
=====				

Itinéraires persistants :

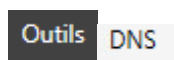
Adresse réseau	Masque réseau	Adresse passerelle	Métrique
0.0.0.0	0.0.0.0	172.20.255.253	Par défaut
10.6.0.0	255.255.0.0	192.168.6.254	1
192.168.2.0	255.255.255.0	172.20.2.2	1
192.168.3.0	255.255.255.0	172.20.2.3	1
192.168.4.0	255.255.255.0	172.20.2.4	1
192.168.5.0	255.255.255.0	172.20.2.5	1
192.168.7.0	255.255.255.0	172.20.2.7	1
192.168.8.0	255.255.255.0	172.20.2.8	1
192.168.9.0	255.255.255.0	172.20.2.9	1
192.168.10.0	255.255.255.0	172.20.2.10	1
192.168.11.0	255.255.255.0	172.20.2.11	1
10.2.0.0	255.255.0.0	172.20.2.2	1
10.3.0.0	255.255.0.0	172.20.2.3	1
10.4.0.0	255.255.0.0	172.20.2.4	1
10.5.0.0	255.255.0.0	172.20.2.5	1
10.7.0.0	255.255.0.0	172.20.2.7	1
10.8.0.0	255.255.0.0	172.20.2.8	1
10.9.0.0	255.255.0.0	172.20.2.9	1
10.10.0.0	255.255.0.0	172.20.2.10	1
10.11.0.0	255.255.0.0	172.20.2.11	1

Mais nous avons remarqué que cela avait beaucoup de problème donc on a tous fait une route vers le poste 9 qui nous redirige vers les autres postes.

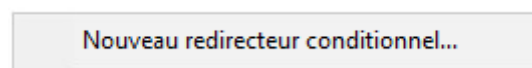
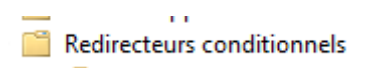
## 2. Faire la relation d'approbation

Pour commencer la relation d'approbation il faut d'abord ajouter un redirecteur conditionnel car l'AD parent ne connaît pas les autres DNS donc il faut un redirecteur conditionnel pour dire que s'il veut joindre ce DNS il faut qu'il passe par cette adresse IP.

Donc pour faire un redirecteur conditionnel il faut aller dans Outils puis dans DNS :



Ensuite il faut aller dans Redirecteurs conditionnels et faire Nouveau redirecteur conditionnel :



Pour la suite on mets le DNS qu'on veut joindre et son adresse IP et pour notre part on a choisi de stocker ce redirecteur conditionnel dans Active Directory et le répliquer dans tous les serveurs DNS de cette forêt (donc le répliquer sur l'AD enfant) :

Nouveau redirecteur conditionnel

Domaine DNS :  
chateau-senhadjji.local

Adresses IP des serveurs maîtres :

Adresse IP	Nom de domaine compl...	Validé
<Cliquez ici pour ajo...		
192.168.9.2	<Tentative de résolutio...	Validation en cours...

☒ Stocker ce redirecteur conditionnel dans Active Directory, et le répliquer comme suit :

Tous les serveurs DNS de cette forêt

⚠ La réplication n'aura pas lieu sur les serveurs DNS qui sont des contrôleurs de domaine antérieurs à Windows Server 2003.

Délai d'expiration des requêtes de redirection (en secondes) : 5

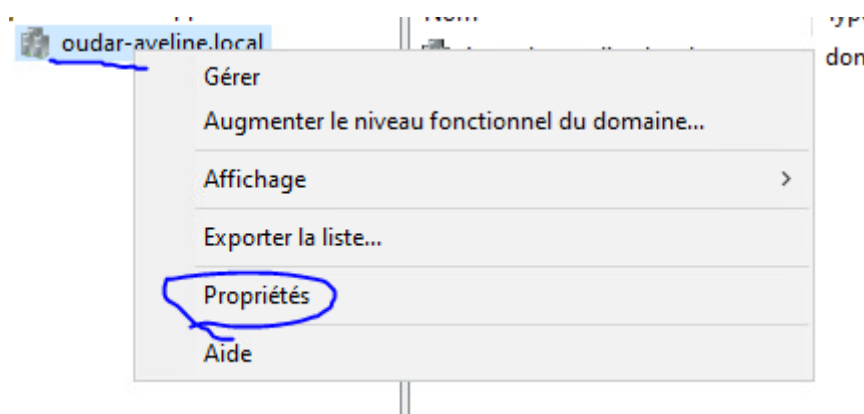
Le nom de domaine complet du serveur n'est pas disponible si les entrées et les zones de recherche inversée appropriées ne sont pas configurées.

OK Annuler

Ensuite on ajoute une approbation dans Outils et Domaines et approbation Active Directory :

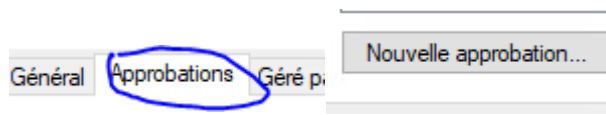
Outils Domaines et approbations Active Directory

Ensuite on fait propriétés dans le domaine de l'AD parent :





Puis on va dans Approbation et on fait nouvelle approbation :



Pour la suite on mets le domaine qu'on va faire l'approbation :

A screenshot of the 'Assistant Nouvelle approbation' dialog box. The title bar says 'Assistant Nouvelle approbation'. The main heading is 'Nom d'approbation' with a gold medal icon. Below it, the text says 'Vous pouvez créer une approbation en utilisant un nom NetBIOS ou DNS.' The instructions state: 'Entrez le nom d'un domaine, d'une forêt ou d'un domaine Kerberos pour cette approbation. Si vous entrez un nom de forêt, vous devez entrer un nom DNS.' Examples are provided: 'Exemple de nom NetBIOS : fournisseur01-int' and 'Exemple de nom DNS : fournisseur01-interne.microsoft.com'. A text field labeled 'Nom :' contains the value 'chateau-senhadjilocal'. At the bottom, there are three buttons: '< Précédent', 'Suivant >', and 'Annuler'.

Remarque : il détecte directement que c'est un domaine Windows server avec AD.

Puis on sélectionne Approbation de forêt :

A screenshot of the 'Assistant Nouvelle approbation' dialog box. The title bar says 'Assistant Nouvelle approbation'. The main heading is 'Type d'approbation' with a gold medal icon. Below it, the text says 'Ce domaine est un domaine racine de forêt. Si le domaine spécifié est approprié, vous pouvez créer une approbation de forêt.' The instructions state: 'Sélectionnez le type d'approbation que vous voulez créer.' There are two radio button options: 'Approbation externe' (unselected) and 'Approbation de forêt' (selected). Descriptions are provided for each: 'Une approbation externe est une approbation non transitive entre un domaine et un autre domaine en dehors de la forêt. Une approbation non transitive est liée par les domaines dans la relation.' and 'Une approbation de forêt est une approbation transitive entre deux forêts permettant à des utilisateurs dans n'importe quel domaine d'une forêt d'être authentifiés dans n'importe quel domaine de l'autre forêt.'

Puis on choisit Bidirectionnel :

Assistant Nouvelle approbation ×

**Direction de l'approbation**  
Vous pouvez créer des approbations à sens unique ou bidirectionnelle.

Sélectionnez le sens de cette approbation.

☒ Bidirectionnel  
Les utilisateurs présents dans ce domaine peuvent être authentifiés dans le domaine spécifié, le domaine Kerberos ou la forêt, et les utilisateurs dans le domaine spécifié, le domaine Kerberos et la forêt peuvent être authentifiés dans ce domaine.

☐ Sens unique : en entrée  
Les utilisateurs présents dans ce domaine peuvent être authentifiés dans le domaine spécifié, le domaine Kerberos, ou la forêt.

☐ Sens unique : en sortie  
Les utilisateurs présents dans le domaine spécifié, le domaine Kerberos ou la forêt peuvent être authentifiés dans ce domaine.

< Précédent Suivant > Annuler

Ensuite on coche « ce domaine et le domaine spécifié » :

Assistant Nouvelle approbation ×

**Sens de l'approbation**  
Si vous avez les autorisations appropriées dans les deux domaines, vous pouvez créer les deux côtés de la relation d'approbation.

Pour utiliser une approbation, vous devez créer les deux sens de la relation d'approbation. Par exemple, si vous créez une approbation unilatérale entrante dans le domaine local, vous devez également créer une approbation sortante dans le domaine spécifié pour que le trafic d'authentification circule au sein de l'approbation.

Créer l'approbation pour le ou les domaines suivants :

☐ Ce domaine uniquement  
Cette option crée la relation d'approbation dans le domaine local.

☒ Ce domaine et le domaine spécifié  
Cette option crée une relation d'approbation dans le domaine local et dans le domaine spécifié. Vous devez disposer des privilèges de création d'approbations dans le domaine spécifié.

< Précédent Suivant > Annuler

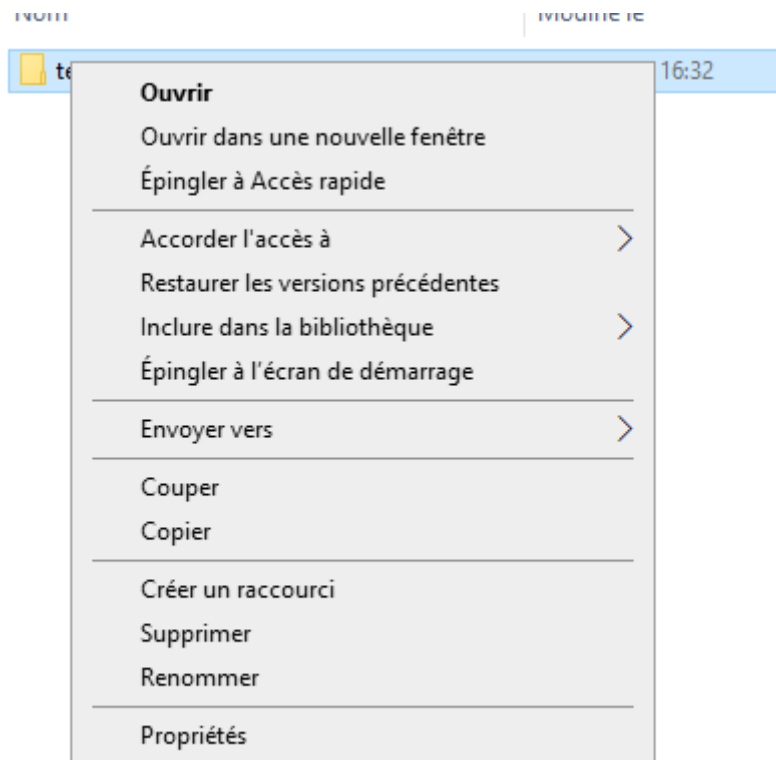
Puis on met le nom d'utilisateur et le mot de passe Admin pour se connecter au domaine :

Et on remarque que l'approbation a fonctionné :

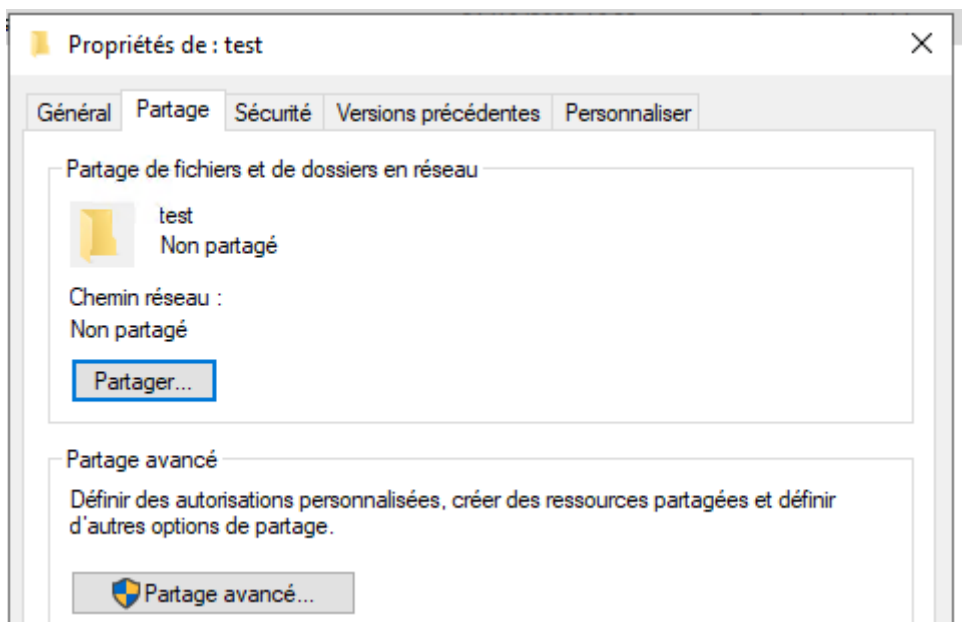
## Partage de données

### 1. Faire le partage de données

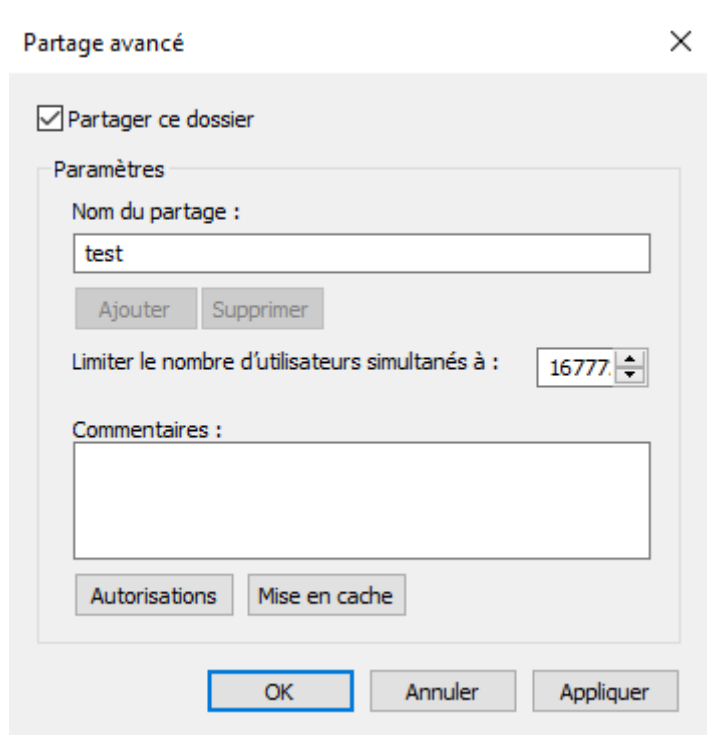
Pour commencer le partage de données on sélectionne le dossier qu'on veut et on va dans les propriétés :



Ensuite on va dans Partage avancé :



Ensuite on met le nom du partage et on va dans Autorisations :



Partage avancé

☒ Partager ce dossier

Paramètres

Nom du partage :

test

Ajouter Supprimer

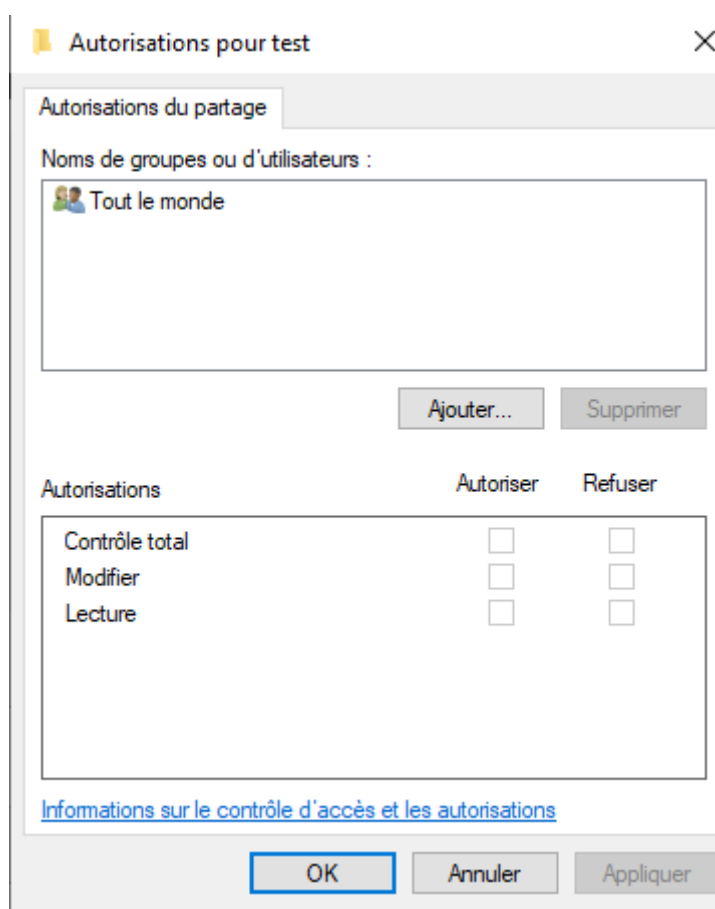
Limiter le nombre d'utilisateurs simultanés à : 16777

Commentaires :

Autorisations Mise en cache

OK Annuler Appliquer

Puis on ajoute un Utilisateur :



Autorisations pour test

Autorisations du partage

Noms de groupes ou d'utilisateurs :

Tout le monde

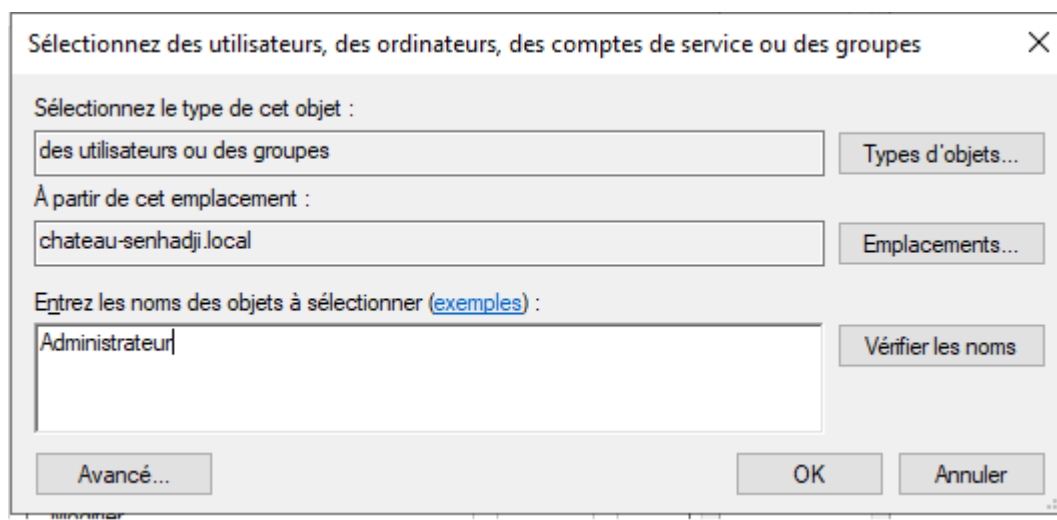
Ajouter... Supprimer

Autorisations	Autoriser	Refuser
Contrôle total	<input type="checkbox"/>	<input type="checkbox"/>
Modifier	<input type="checkbox"/>	<input type="checkbox"/>
Lecture	<input type="checkbox"/>	<input type="checkbox"/>

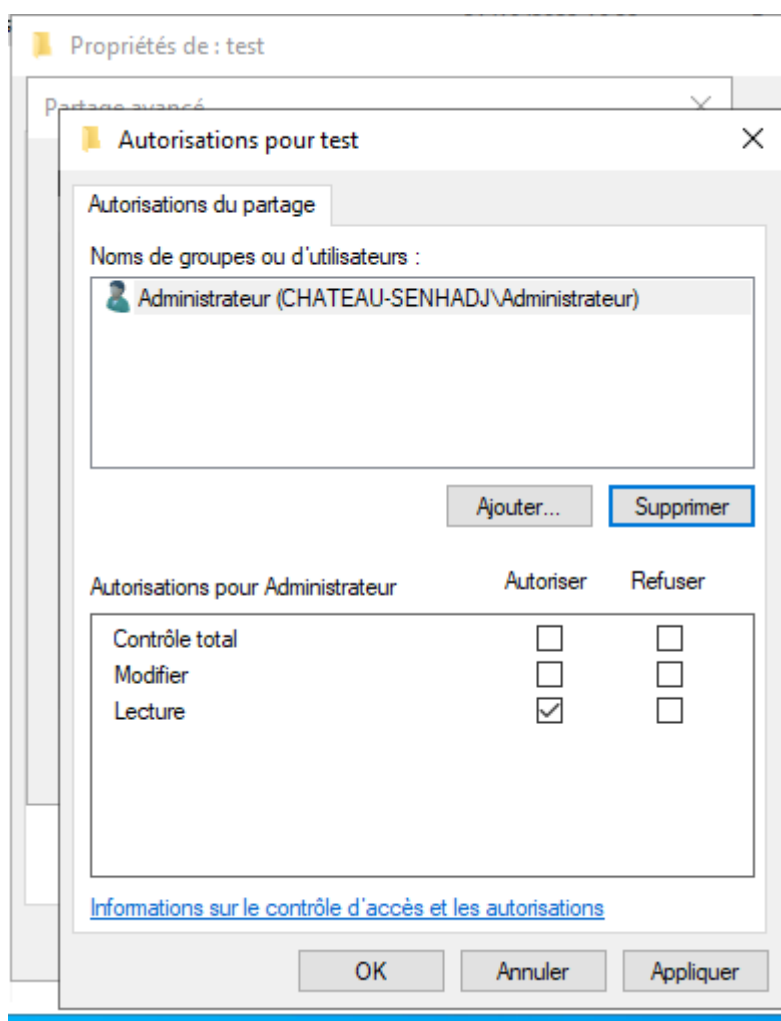
[Informations sur le contrôle d'accès et les autorisations](#)

OK Annuler Appliquer

Pour la suite on mets le domaine dans l'emplacement et on entre le nom de l'utilisateur qu'on veut :



Puis on applique et on remarque que cela fonctionne :



## **Conclusion**

Ce TP a permis de mettre en pratique les concepts de vlan, de routeur virtuel et de switch virtuel. Il a également permis de voir comment ces technologies peuvent être utilisées pour séparer le trafic réseau entre les différents domaines.

Puis à faire des relations d'approbation entre différent domaine et faire des partages suivant les utilisateurs de chaque domaine d'active directory.

## **Remarques**

Il est important de bien comprendre les concepts de vlan, de routeur et de switch avant de commencer ce TP.