PPE2 - AD GNS3 ET FS

09.02.2024

—

CRAMPON Nicolas

Dundermifflin.lan

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS SESSION 2024

Épreuve E5 - Administration des systèmes et des réseaux (option SISR)

ANNEXE 7-1-A : Fiche descriptive de réalisation professionnelle (recto)

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE

N° réalisation :

Nom, prénom : CRAMPON Nicolas

N° candidat :

Épreuve ponctuelle ☐ **Contrôle en cours de formation** ☒ **Date :** 07 / 03 / 2024

Organisation support de la réalisation professionnelle

Intitulé de la réalisation professionnelle

Période de réalisation : *février -> 07 mars* ***Lieu :*** *Senlis*

Modalité : ☒ *Seul(e)* ☐ *En équipe*

Compétences travaillées

- ☒ Concevoir une solution d'infrastructure réseau
- ☒ Installer, tester et déployer une solution d'infrastructure réseau
- ☐ Exploiter, dépanner et superviser une solution d'infrastructure réseau

Conditions de réalisation (ressources fournies, résultats attendus)

- 3 Serveur : 2 Active Directory et 1 Serveur de fichiers
- 7 Postes Windows 10
- 2 Routeurs
- 2 Switchs
- Réseau fonctionnel

Description des ressources documentaires, matérielles et logicielles utilisées

Ressources documentaires : Divers sites internet comme IT-Connect.

Ressource matérielle : Ordinateur portable avec 32 go de ram, Core i7, RTX4070.

Ressource logicielle : Tout mon environnement est virtualisé sur VMware® Workstation 17 Pro, et GNS3.

Modalités d'accès aux productions et à leur documentation

Page 11 pour tous les mots de passe de mon environnement.

Table des matières

1) PRÉAMBULE

- 1.1 - Introduction

2) CANEVAS

- 2.1 - Mise en situation
- 2.2 - Cahier des charges
- 2.3 - Solution
- 2.4 - Équipements et logiciels nécessaires
- 2.5 - Schéma réseau
- 2.6 - Tableau VLAN
- 2.7 - Tableau d'adressage
- 2.8 - Maquette Cisco
- 2.9 - Tableau utilisateurs / droits
- 2.10 - Tableau mots de passe

3) SOLUTION

- 3.1 - Création du domaine et ajout des serveurs et des clients au domaine
- 3.2 - DNS
- 3.3 - Création des utilisateurs dans l'Active Directory (AGDLP)
- 3.4 - Installation de AD FS sur le serveur FS
- 3.5 - Création du partage commun et du partage personnel caché
- 3.6 - Ajout de ces lecteurs réseau par GPO
- 3.7 - Configuration du DHCP
- 3.8 - Mise en place du DHCP FAILOVER
- 3.9 - GPO Longueur minimale du mot de passe
- 3.10 - GPO Restriction au panneau de configuration

1) PRÉAMBULE

1.1 - Introduction

La mise en place d'une infrastructure réseau robuste est devenue une priorité absolue pour Dunder Mifflin afin de soutenir efficacement ses opérations. Dans cette optique, une série de mesures stratégiques ont été envisagées pour garantir une connectivité stable et sécurisée, répondant ainsi aux besoins critiques de l'entreprise.

2) CANEVAS

2.1 - Mise en situation

Dunder Mifflin a exprimé le besoin critique d'une infrastructure réseau fiable pour soutenir ses opérations. La demande comprend l'installation de deux routeurs pour garantir une connectivité stable. La mise en place du routage dynamique pour gérer efficacement les chemins de communication et fournir un lien de secours en cas de défaillance.

De plus, des VLANS distincts seront configurés assurant ainsi une isolation sécurisée des ressources réseau des différents services.

Ensuite, le déploiement d'un serveur DHCP failover pour garantir la disponibilité continue des adresses IP, et l'implémentation d'un DNS secondaire pour renforcer la redondance.

Enfin, l'installation de l'AD FS permettra la configuration de partages réseau sécurisés, notamment un partage commun pour les utilisateurs et un partage personnel exclusif pour le directeur de l'entreprise.

Sans oublier la méthodologie AGDLP (Account, Global, Domain Local, Permission) et la configuration des GPO pour imposer des règles telles que la longueur minimale du mot de passe et les restrictions d'accès au panneau de configuration.

Dans notre cas, l'infrastructure sera émulée sur GNS3.

2.2 - Cahier des charges

- Ce que l'entreprise à besoin concrètement :
  - Routage dynamique entre 2 routeurs sur GNS3
  - 1 VLAN pour chaque services
  - Mise en place du domaine
  - AGDLP (Account, Global, Domain Local, Permission)
  - DHCP FAILOVER
  - DNS secondaire
  - Partage commun (ADFS)
  - Partage personnel caché (ADFS)
  - GPO (longueur minimale du mot de passe et restriction au panneau de configuration)
  - MD5 encryption

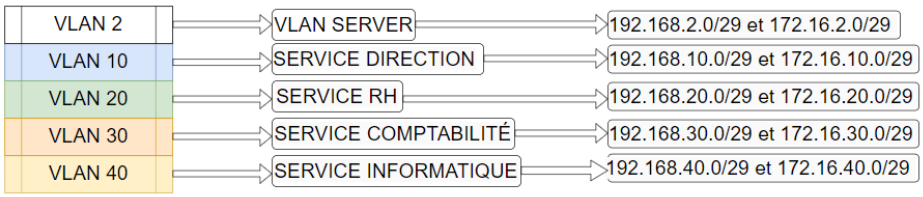
2.3 - Solution

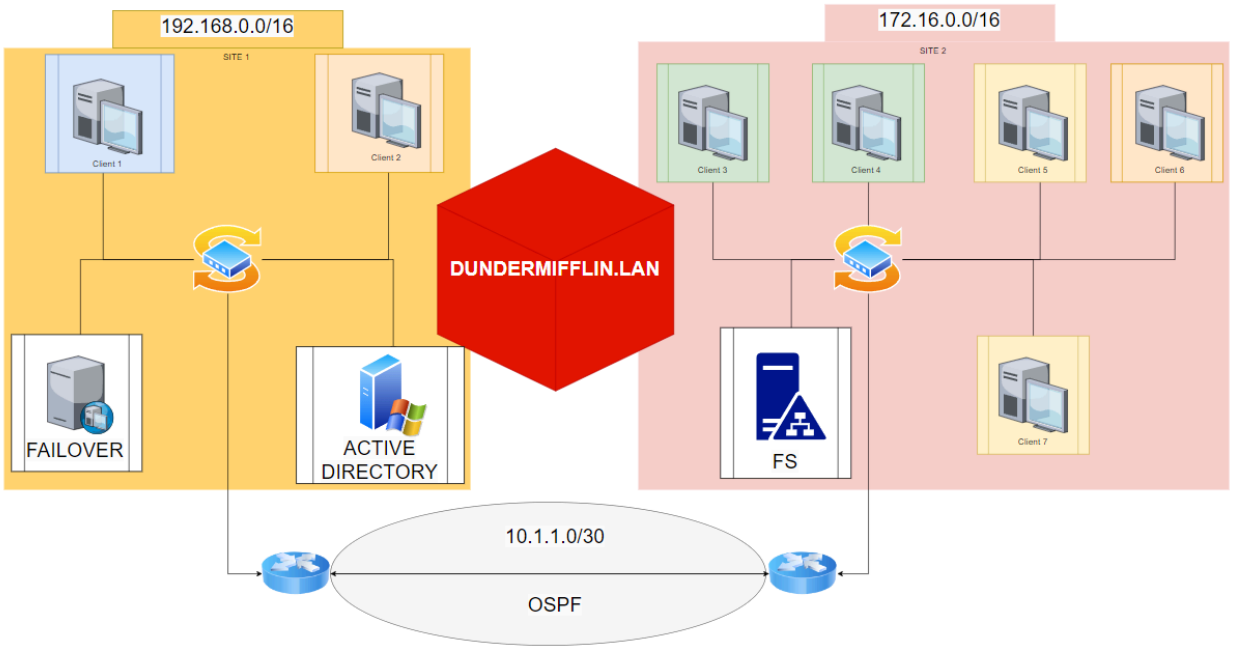
- Création du domaine et ajout des serveurs et des clients au domaine
- DNS
- Création des utilisateurs dans l'active directory
- Installation de AD FS sur le serveur FS
- Création du partage commun et du partage personnel caché
- Ajout de ces lecteurs réseau par GPO
- Configuration du DHCP
- Mise en place du DHCP FAILOVER
- GPO Longueur minimale du mot de passe
- GPO Restriction au panneau de configuration
- MD5 encryption

2.4 - Équipements et logiciels nécessaires

- 3 Windows Server 2022
- GNS3 2.2.45 (logiciel et machine virtuelle)
  - 2 Routeurs
  - 2 Switchs
  - 7 Postes
- 7 clients Windows 10

2.5 - Schéma réseau





En tout il y a 3 réseaux et 12 sous-réseaux (6 dans chaque site) :

- 10.1.1.0 /30
- 192.168.0.0 /16
  - 192.168.2.0 /29
  - 192.168.10.0 /29
  - 192.168.20.0 /29
  - 192.168.30.0 /29
  - 192.168.40.0 /29
  - 192.168.99.0 /29
- 172.16.0.0/16
  - 172.16.2.0 /29
  - 172.16.10.0 /29
  - 172.16.20.0 /29
  - 172.16.30.0 /29
  - 172.16.40.0 /29
  - 172.16.99.0 /29

2.6 - Tableau VLAN

	VLAN	SERVEURS / CLIENTS / INTERFACES
Serveurs	2	AD, DHCP FAILOVER, FS
Service de la Direction	10	Client 1
Service RH	20	Client 3 Client 4
Service Comptabilité	30	Client 2 Client 6
Service Informatique	40	Client 5 Client 7
TRUNK	99	SWITCH 1 INTERFACE SORTIE fa0/1 SWITCH 2 INTERFACE SORTIE fa0/1

2.7 - Tableau d'adressage

Routeurs Sortie	IP	MASQUE	BROADCAST	DNS	DNS2
ROUTEUR 1 Interface sortie se2/0	10.1.1.1	/30	X	X	X
ROUTEUR 2 Interface sortie se2/0	10.1.1.2	/30	X	X	X

Routeur 1 interfaces virtuelles	IP	MASQUE	BROADCAST	DNS	DNS2
fa0/1.2	192.168.2.6	/29	X	X	X
fa0/1.10	192.168.10.6	/29	X	X	X
fa0/1.20	192.168.20.6	/29	X	X	X
fa0/1.30	192.168.30.6	/29	X	X	X
fa0/1.40	192.168.40.6	/29	X	X	X
fa0/1.99	192.168.99.6	/29	X	X	X

Routeur 2 interfaces virtuelles	IP	MASQUE	BROADCAST	DNS	DNS2
fa0/1.2	172.16.2.6	/29	X	X	X
fa0/1.10	172.16.10.6	/29	X	X	X
fa0/1.20	172.16.20.6	/29	X	X	X
fa0/1.30	172.16.30.6	/29	X	X	X
fa0/1.40	172.16.40.6	/29	X	X	X
fa0/1.99	172.16.99.6	/29	X	X	X

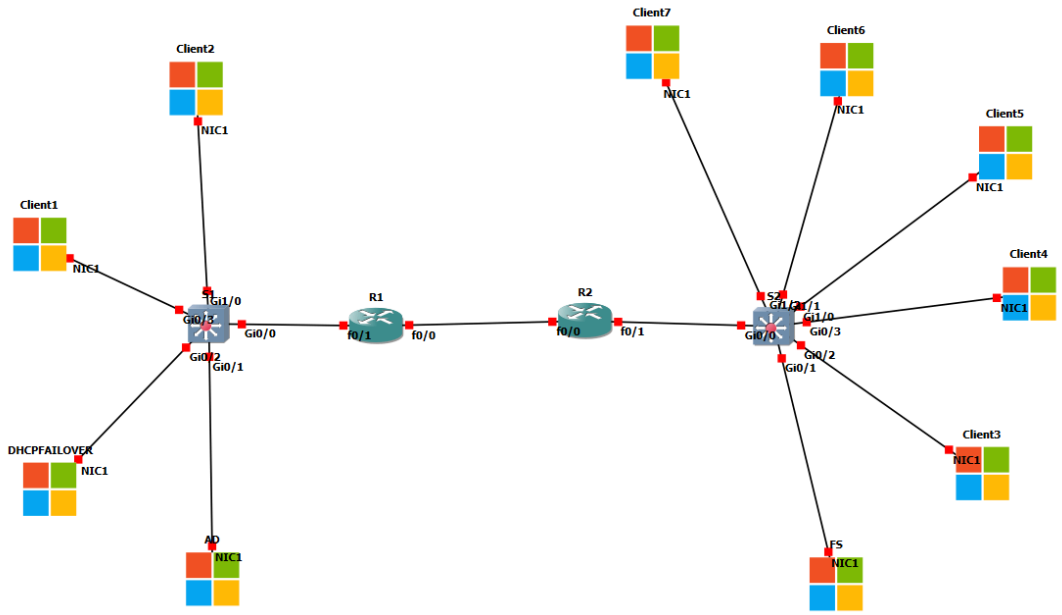
SITE 1

AD	192.168.2.1	/29	192.168.2.6	X	X
DHCP FAILOVER	192.168.2.2	/29	192.168.2.6	192.168.2.1	X
CLIENT 1	192.168.10.1	/29	192.168.10.6	192.168.2.1	X
CLIENT 2	192.168.30.1	/29	192.168.30.6	192.168.2.1	X

SITE 2

FS	172.16.2.1	/29	172.16.2.6	192.168.2.1	X
CLIENT 3	172.16.20.1	/29	172.16.20.6	192.168.2.1	X
CLIENT 4	172.16.20.2	/29	172.16.20.6	192.168.2.1	X
CLIENT 5	172.16.40.1	/29	172.16.40.6	192.168.2.1	X
CLIENT 6	172.16.30.1	/29	172.16.30.6	192.168.2.1	X
CLIENT 7	172.16.40.2	/29	172.16.40.6	192.168.2.1	X

2.8 - GNS



2.9 - Tableau utilisateurs \ Droits

	Service	Partage personnel caché Lecture / Modifier	Partage Commun Lecture / Modifier
Michael Scott	Direction	oui	oui
Jim Halpert	RH	X	oui
Dwight Schrute	RH	X	oui
Angela Martin	Compta	X	oui
Pam Beesly	Compta	X	oui
Ryan Howard	Informatique	X	oui
Kelly Kapoor	Informatique	X	oui

2.10 - Tableau Mots de passe

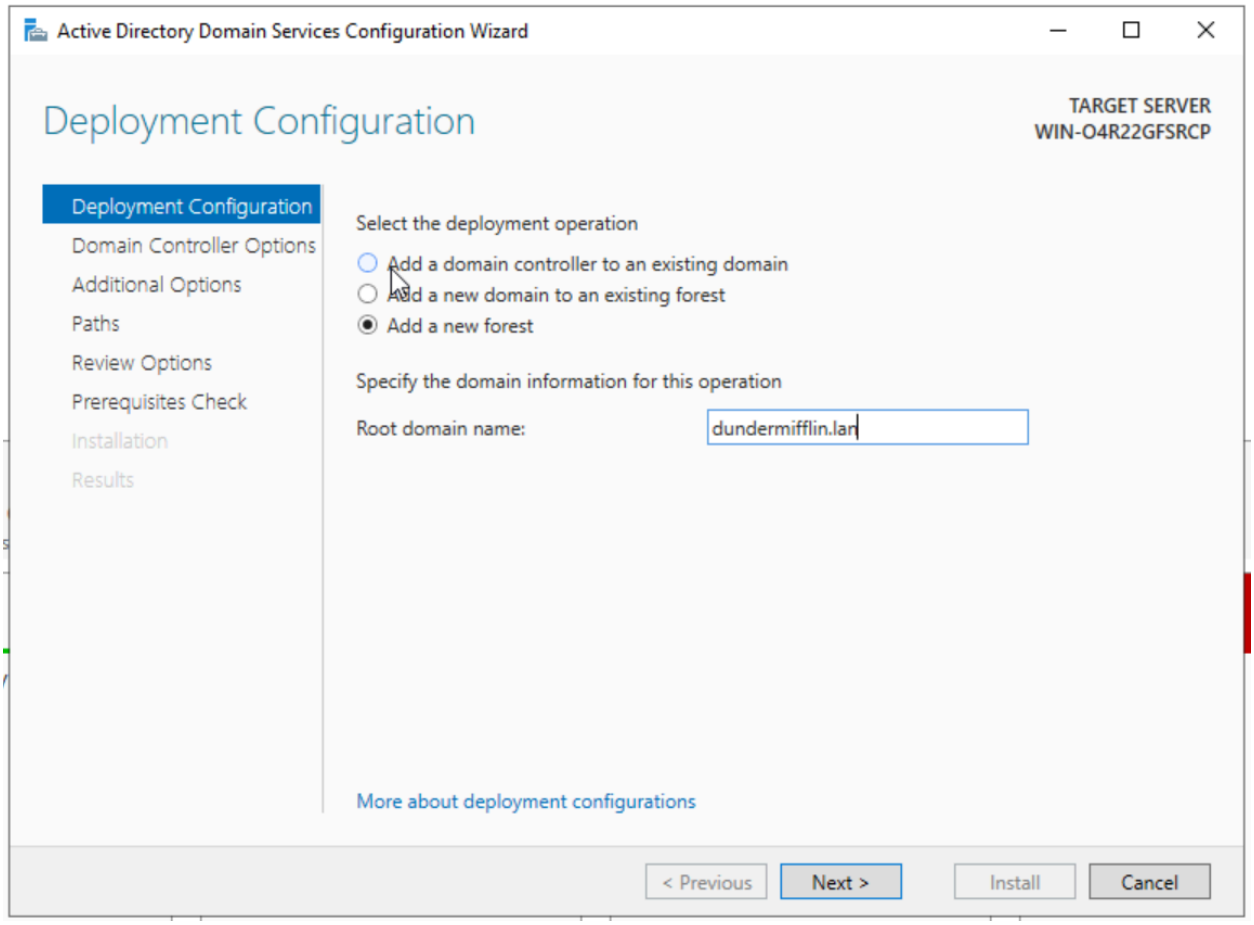
	Utilisateur	Mots de passe
AD	Administrator	Admin00
DHCP	Administrator	Admin00
FS	Administrator	Admin00
Client 1 (Michael Scott)	m.scott	Admin00
Client 2 (Jim Halpert)	j.halpert	Admin00
Client 3 (Angela Martin)	a.martin	Admin00
Client 4 (Pam Beesly)	p.beesly	Admin00
Client 5 (Ryan Howard)	r.howard	Admin00
Client 6 (Dwight Schrute)	d.schrute	Admin00
Client 7 (Kelly Kapoor)	k.kapoor	Admin00

La configuration des mots de passe n'est pas à reproduire !

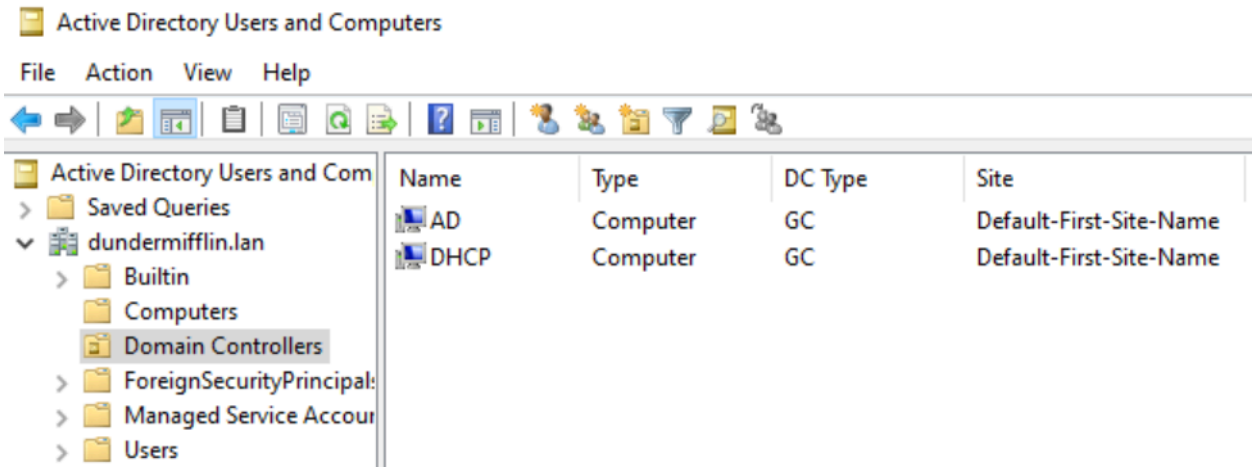
3) SOLUTION

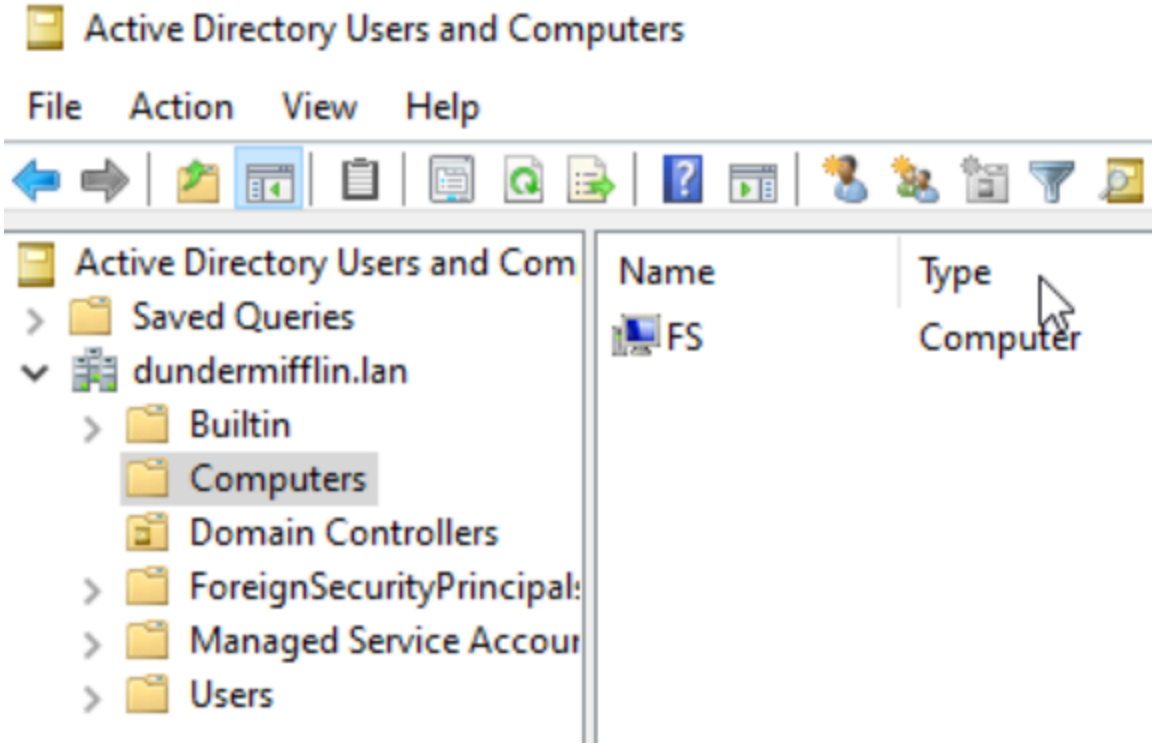
3.1 - Création du domaine et ajout des serveurs et des clients au domaine

J'ai modifié le nom du Windows Server en "AD" et puis j'ai créé le domaine.



Ensuite j'ai ajouté mon deuxième serveur (FS) au domaine et mon troisième (DHCP FAILOVER) que j'ai promu en contrôleur de domaine.

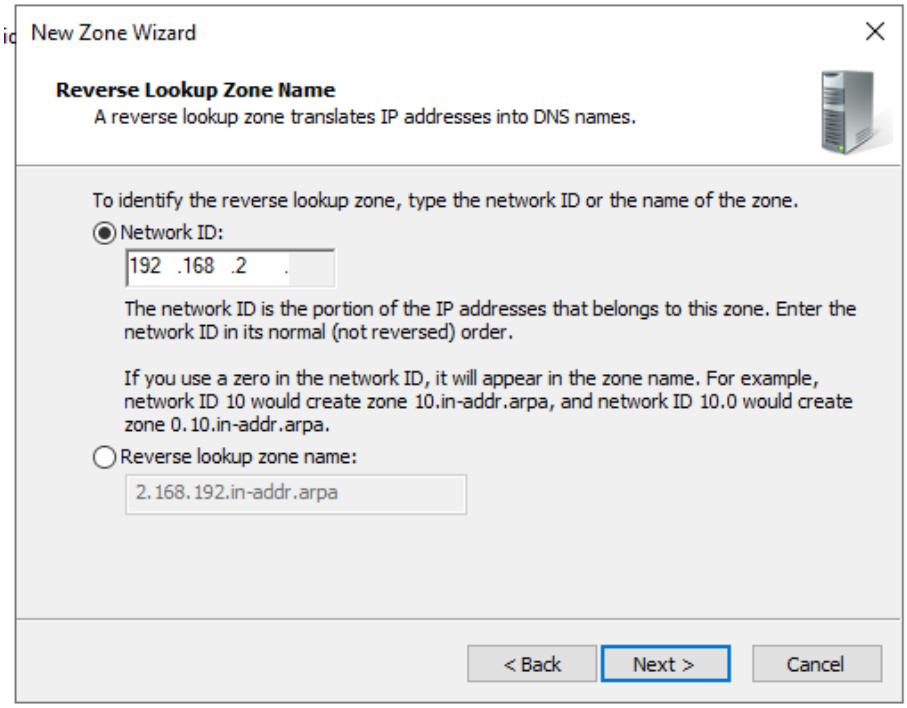


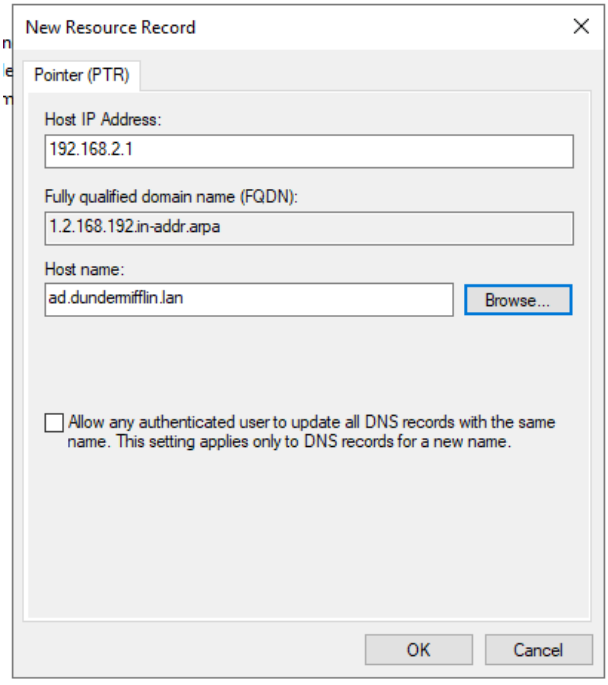


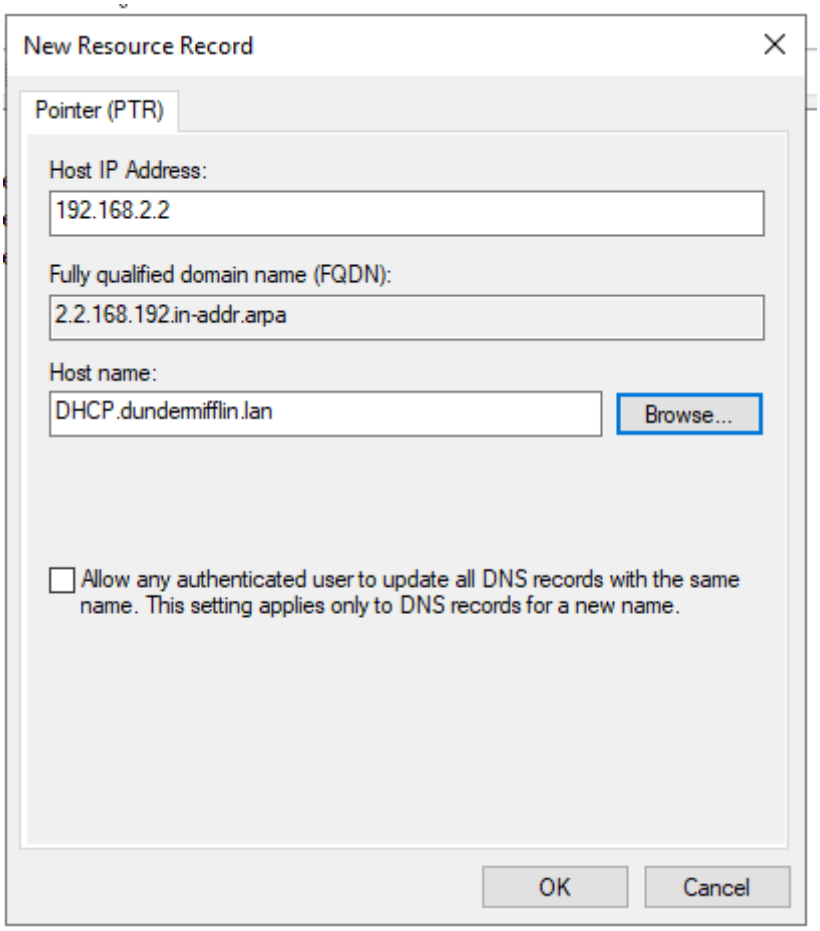
Et pour finir j'ai placé mes 7 clients dans le domaine.

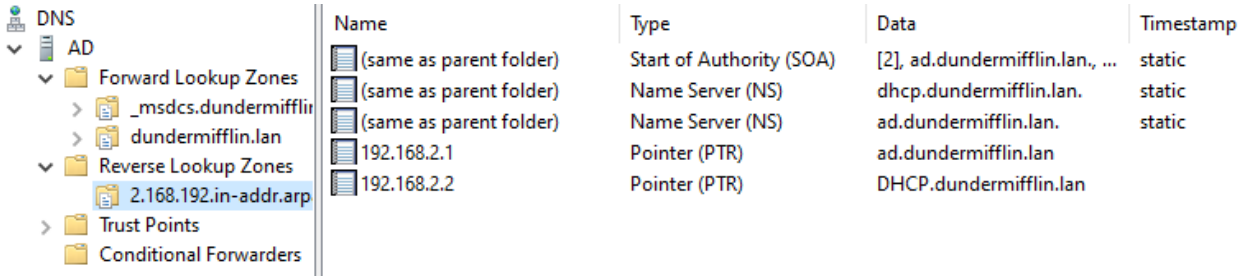
3.2 - DNS

Je vais créer une zone de recherche inversée pour mes deux serveurs afin de pouvoir convertir l'ip de mon serveur en nom d'hôte.










```
PS C:\Users\Administrator> nslookup 192.168.2.1
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  ::1

Name:    ad.dundermifflin.lan
Address:  192.168.2.1

PS C:\Users\Administrator> nslookup 192.168.2.2
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  ::1

Name:    DHCP.dundermifflin.lan
Address:  192.168.2.2

PS C:\Users\Administrator>
```

```
C:\Users\Administrator>ping dhcp

Pinging dhcp.dundermifflin.lan [192.168.2.2] with 32 bytes of data:
Reply from 192.168.2.2: bytes=32 time=14ms TTL=128
Reply from 192.168.2.2: bytes=32 time=5ms TTL=128
Reply from 192.168.2.2: bytes=32 time=10ms TTL=128
Reply from 192.168.2.2: bytes=32 time=20ms TTL=128

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 20ms, Average = 12ms
```

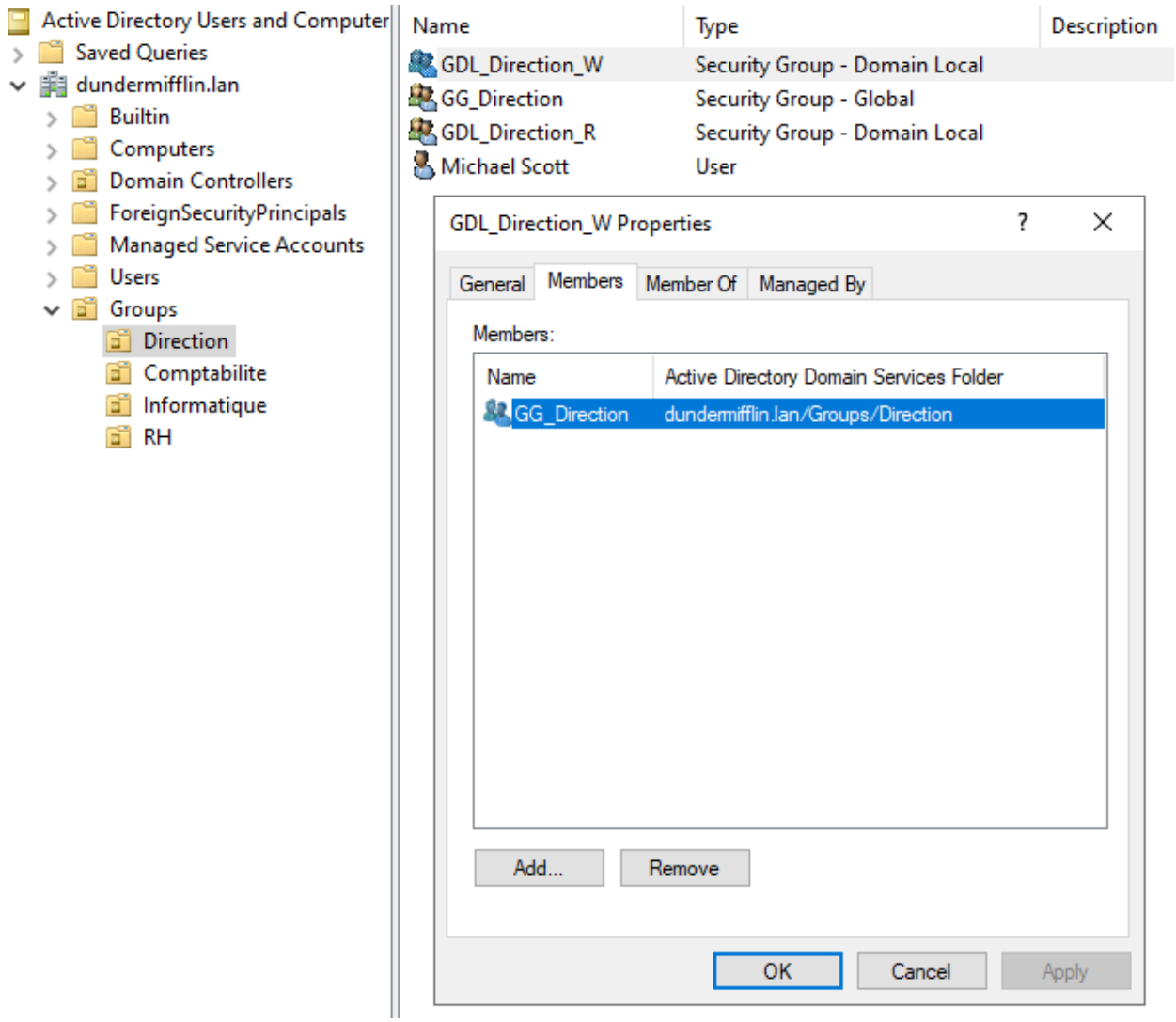
3.3 - Création des utilisateurs dans l'active directory

Je vais suivre la méthode AGLPD pour créer les utilisateurs concrètement ça donne ça :

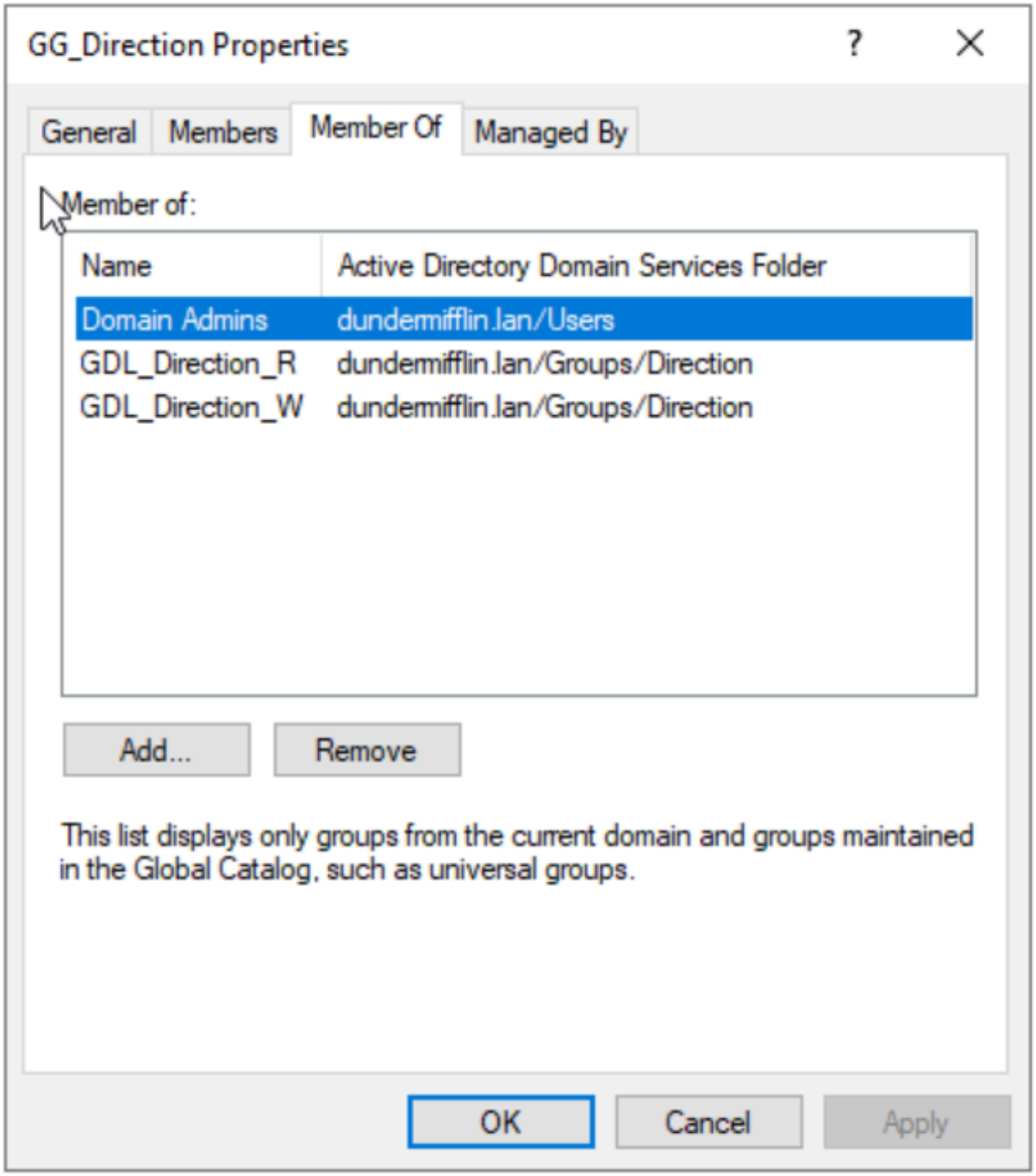
Users → GG → GDL_W (lecture et écriture)

Users → GG → GDL_R (lecture seulement)

Lorsque je vais donner les permissions à la direction par exemple, pour pouvoir lire et modifier le dossier, dans les autorisations j'ajouterais le groupe "GDL_Direction_W" avec "lecture" et "modifier" de cocher. Comme ça on saura directement que les utilisateurs dans le groupe "GDL_Direction_W" pourront modifier le dossier. À l'inverse si on aurait voulu donner l'accès au dossier mais qu'en lecture seulement, on aurait ajouté le groupe "GDL_Direction_R" avec les autorisations de "lecture" de cocher.

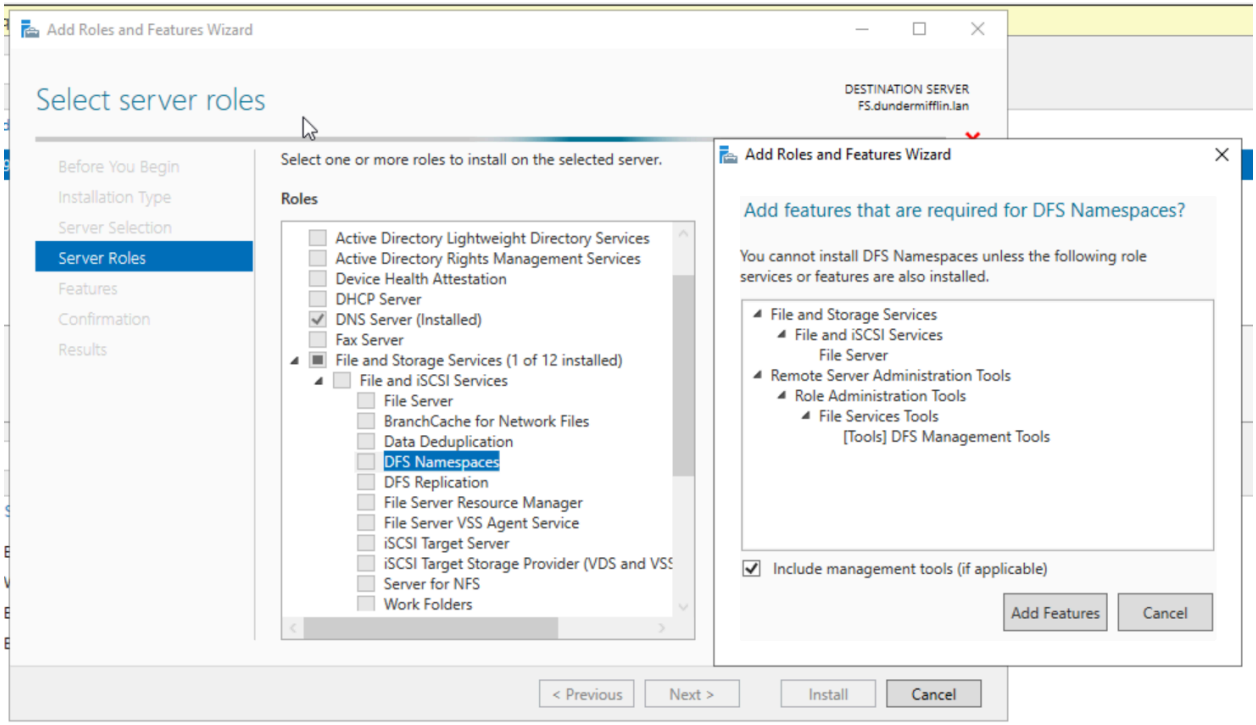


Je vais aussi ajouter les droits administrateurs au groupe de la direction “GG_Direction” afin que l’utilisateur Michael Scott puisse avoir tous les droits.



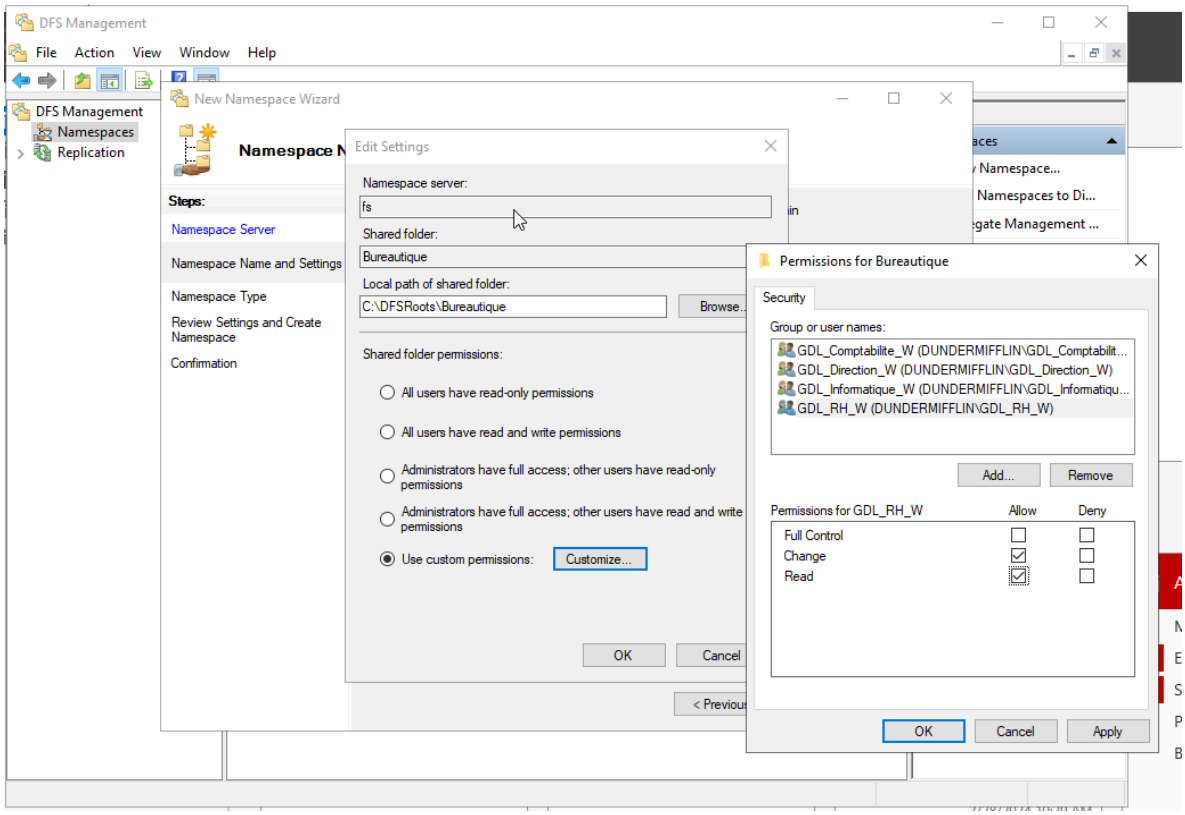
3.4 - Installation de AD FS sur le Serveur FS

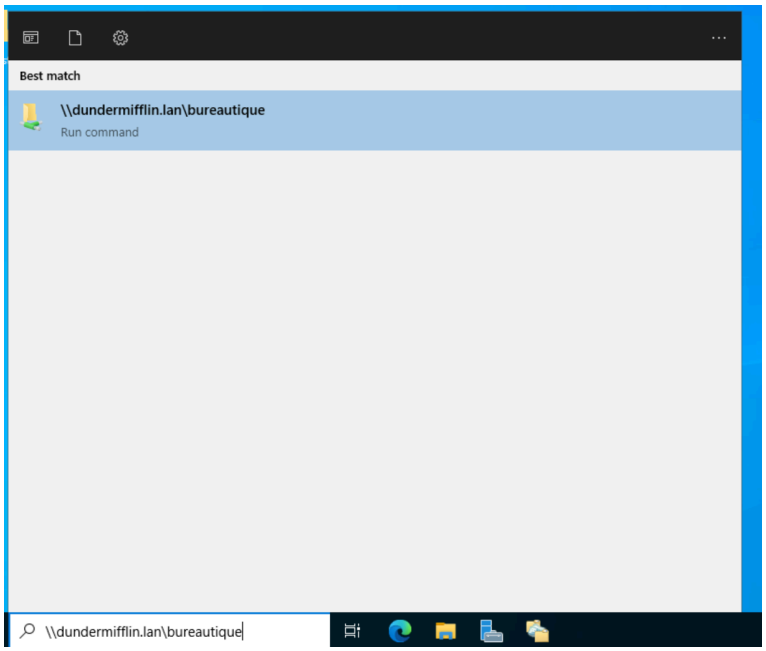
Je commence par installer les rôles et fonctionnalités AD FS.

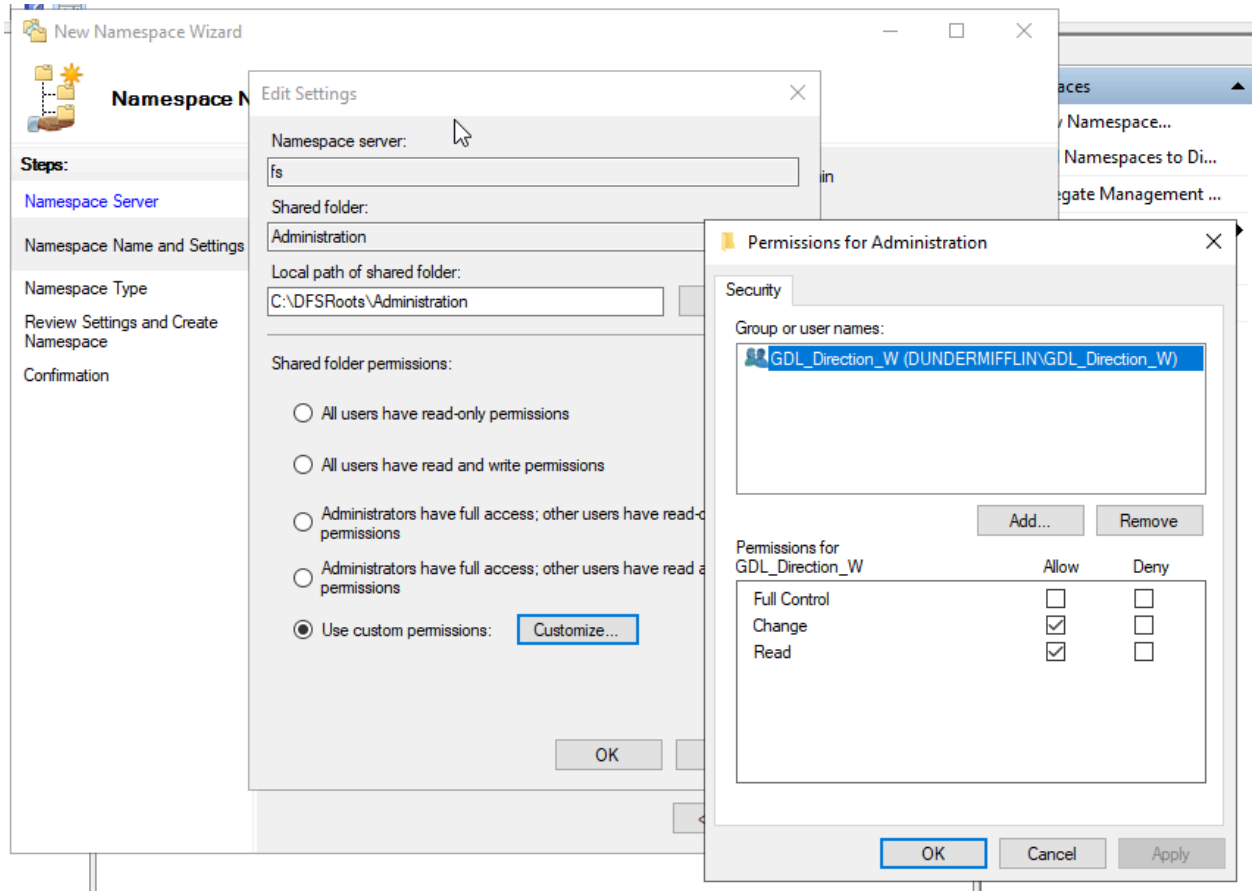


3.5 - Création du partage commun et du partage personnel caché

Le **dossier commun** s'appelle "**Bureautique**" et le **dossier caché** s'appelle "**Administration**".

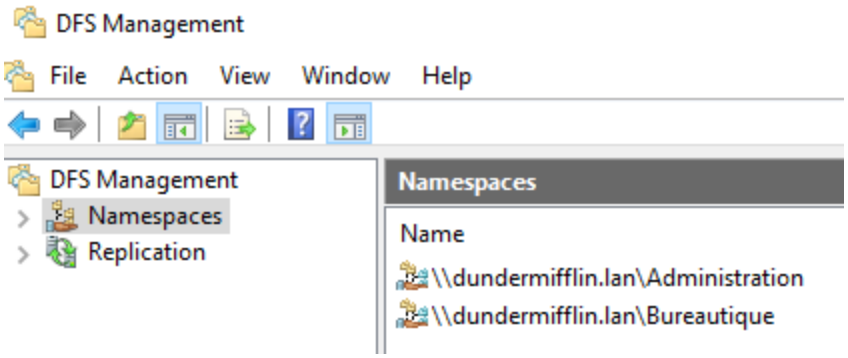




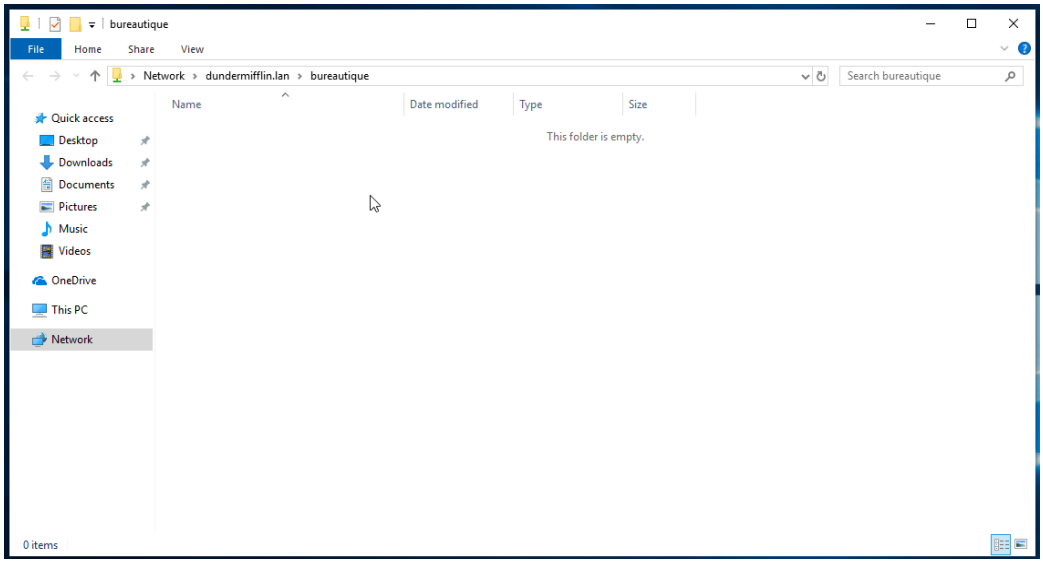


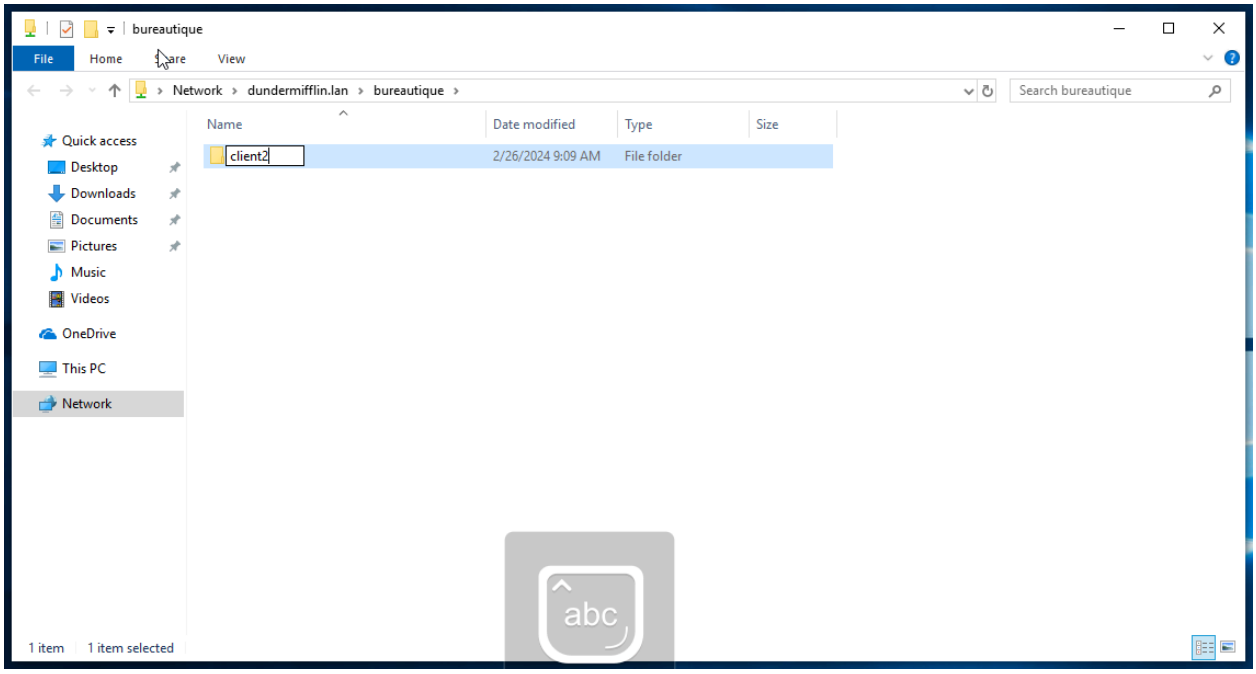
*Le directeur "**Michael Scott**" se trouve dans le groupe "**GDL_Direction_W**".*

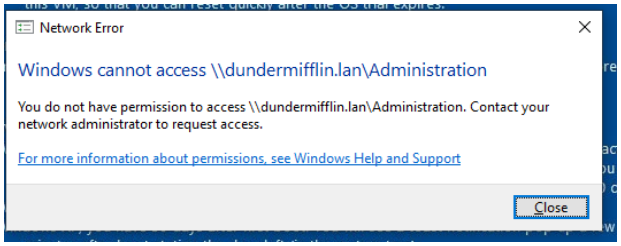
Étant donné que je n'ai pas encore fait de réplication, si le serveur FS n'est plus fonctionnel l'accès à ses dossier ne sera plus possible.



Maintenant on peut voir que sur mon client numéro 2, je peux créer un dossier dans le partage commun et je ne peux pas accéder au partage caché.

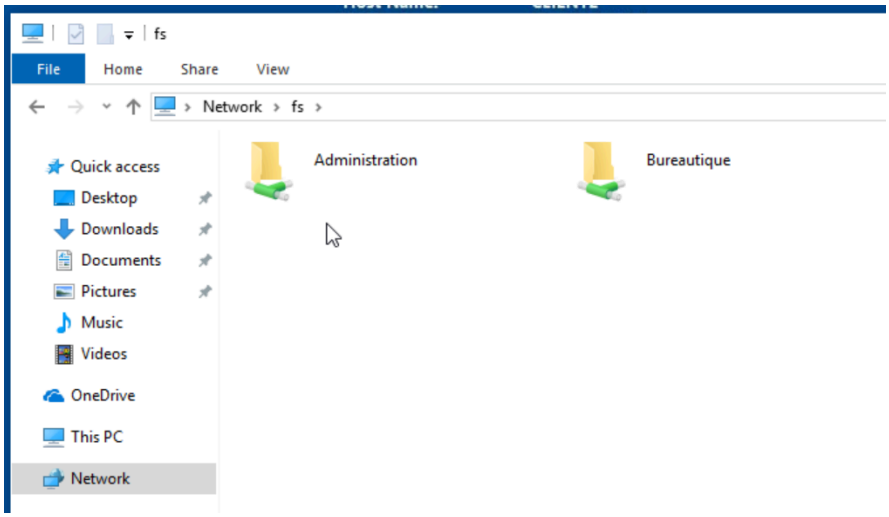




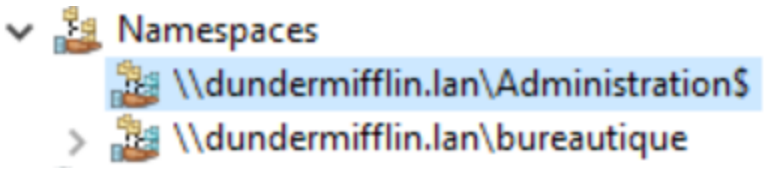


A l'inverse je peux le faire avec mon client 1 car il fait partie de la direction.

Mais à ce moment-là j'ai eu un problème car le dossier n'était pas caché car on pouvait le voir depuis le serveur fs directement.



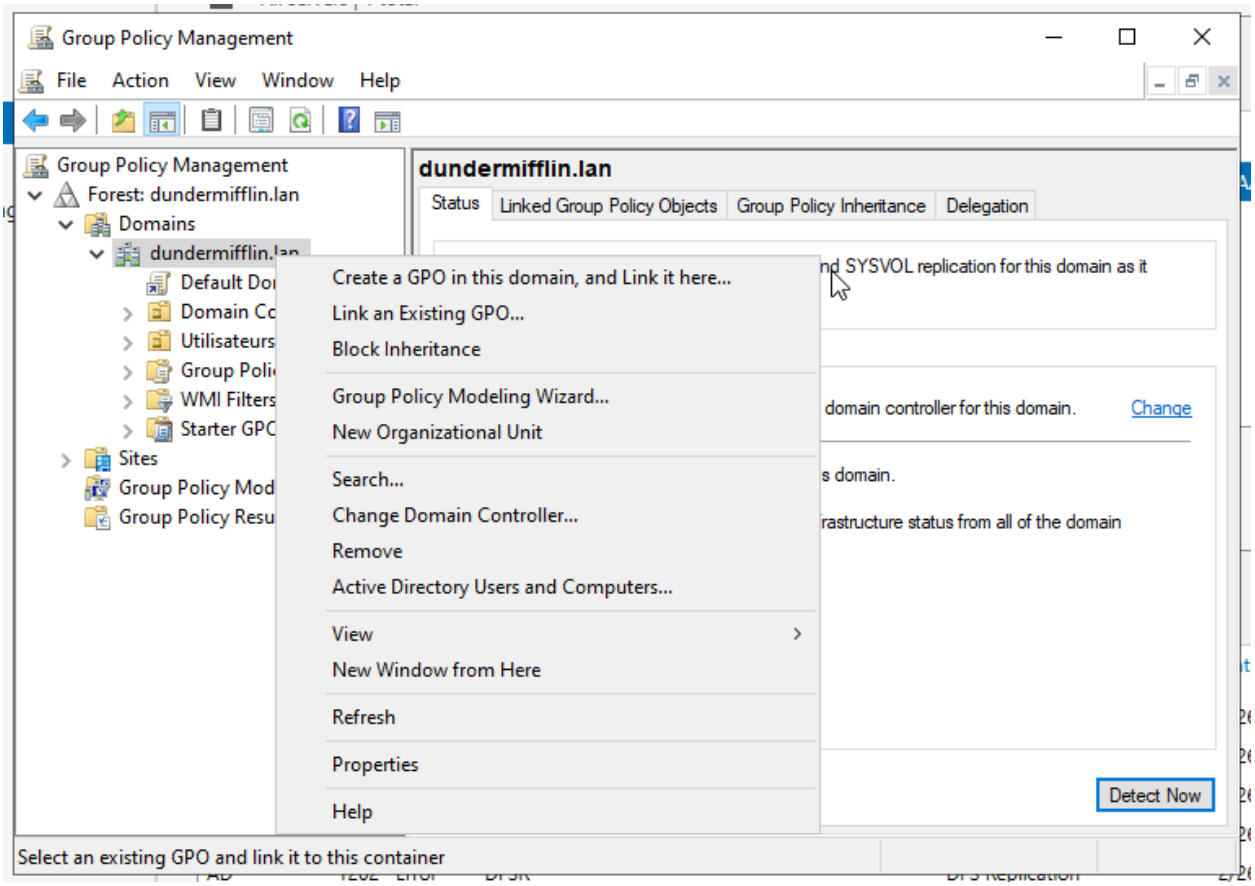
Donc j'ai recréé le dossier mais en ajoutant un $ à la fin.

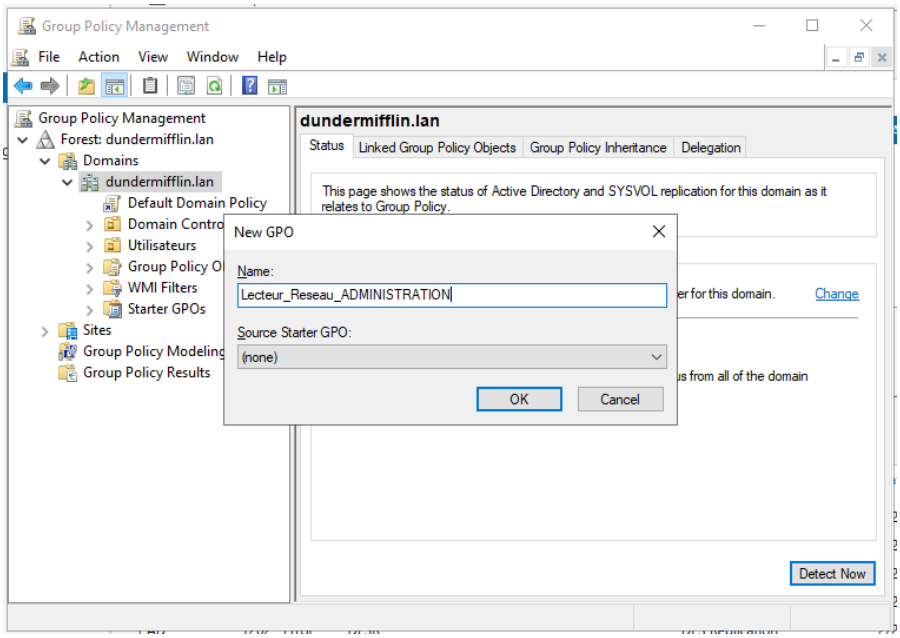


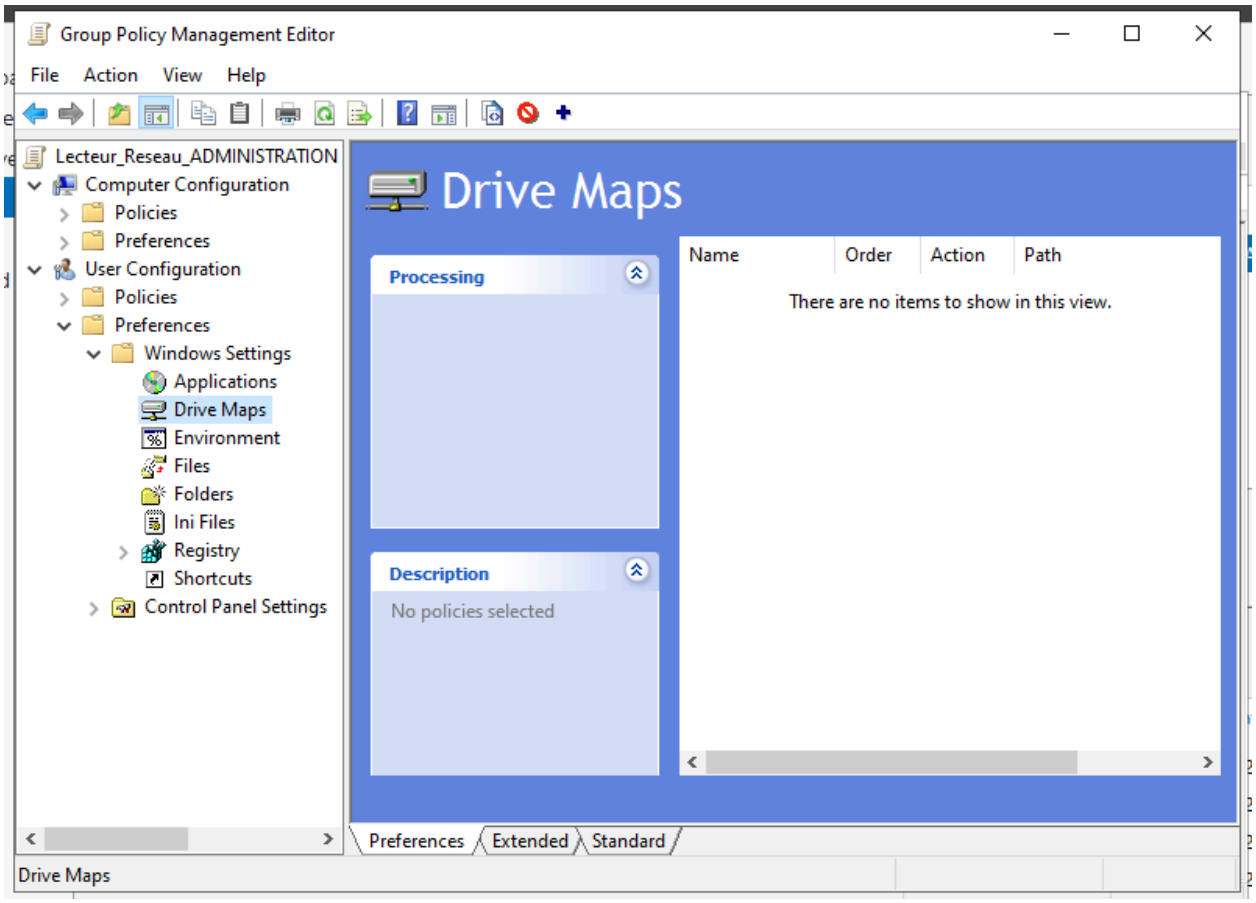
Maintenant je vais ajouter les lecteurs réseau sur un client par gpo.

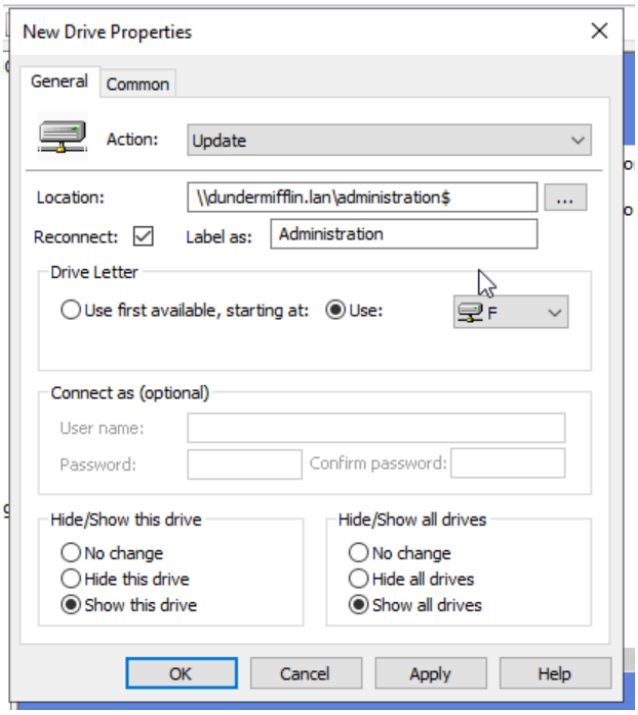
3.6 - Ajout de ces lecteurs réseau par GPO

Lecteur Administration :

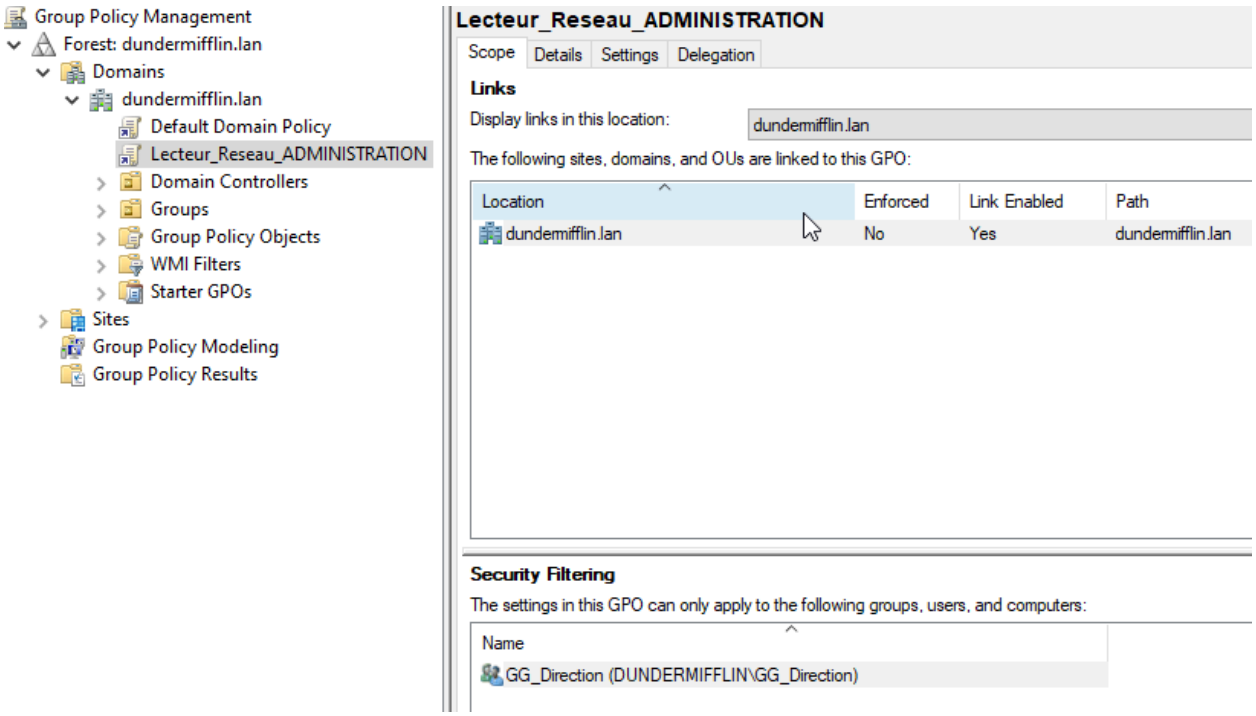




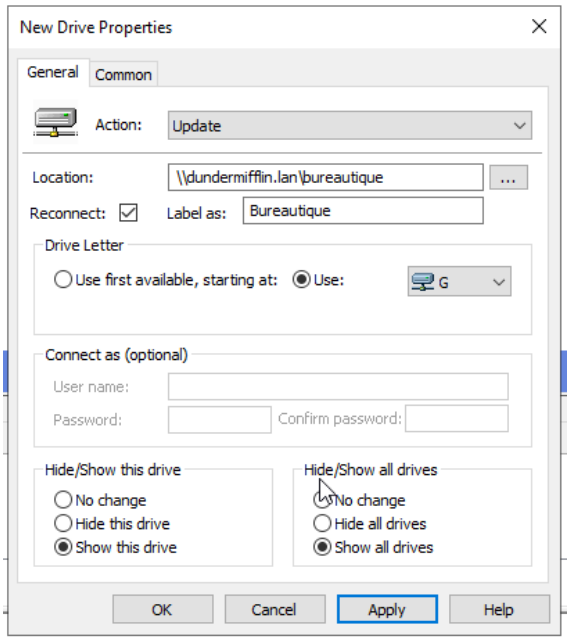

Group Policy Management Editor
File Action View Help
Lecteur_Reseau_ADMINISTRATION
Computer Configuration
Policies
Preferences
User Configuration
Policies
Preferences
Windows Settings
Applications
Drive Maps
Environment
Files
Folders
Ini Files
Registry
Shortcuts
Control Panel Settings
Drive Maps
Processing
Description
No policies selected
Name
Order
Action
Path
There are no items to show in this view.
Preferences
Extended
Standard
Drive Maps

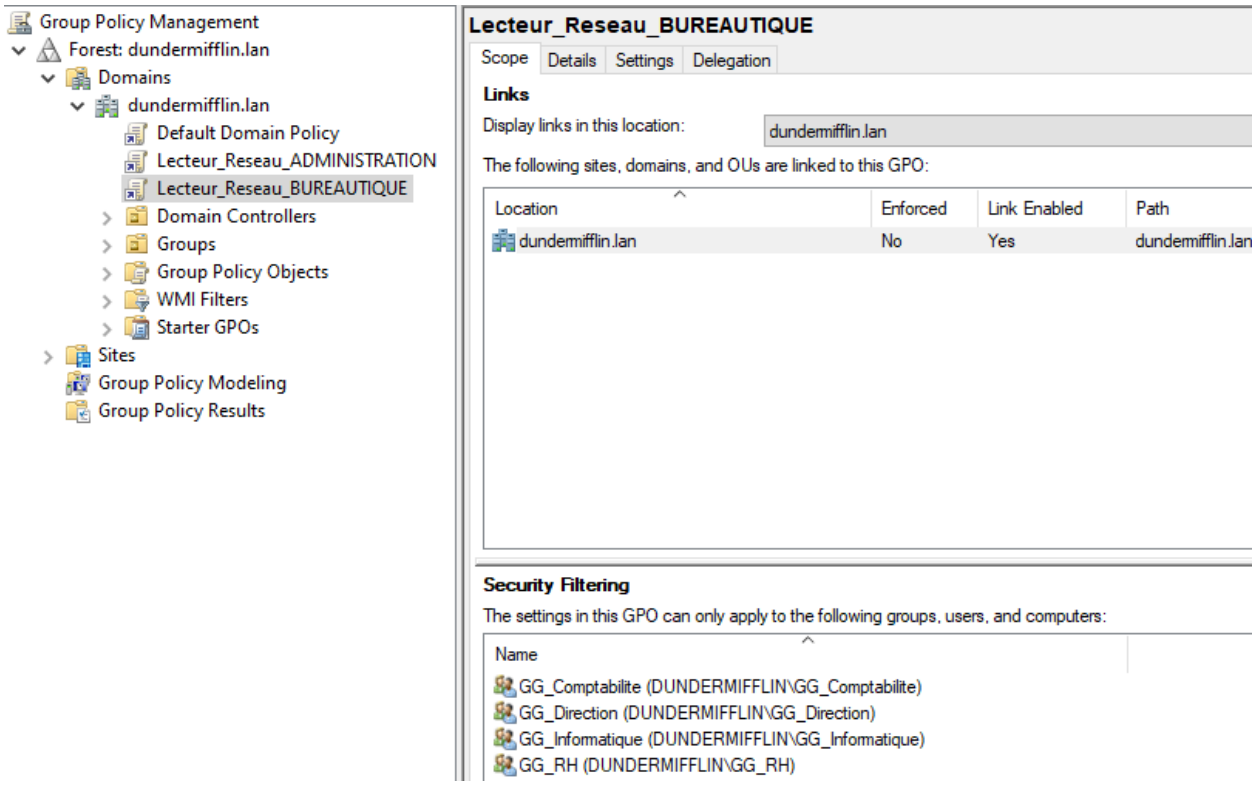

New Drive Properties
General
Common
Action:
Update
Location:
\\dundermifflin.lan\administration$
Reconnect:
Label as:
Administration
Drive Letter
Use first available, starting at:
Use:
F
Connect as (optional)
User name:
Password:
Confirm password:
Hide/Show this drive
No change
Hide this drive
Show this drive
Hide/Show all drives
No change
Hide all drives
Show all drives
OK
Cancel
Apply
Help

Et ici j'ai autorisé l'accès à cette gpo au groupe de la direction pour que seul la direction puisse avoir accès à ce lecteur réseau depuis l'explorateur de fichiers. Ainsi, pour les autres services il sera caché.



Et je créer la même gpo pour le lecteur "Bureautique" mais cette fois en donnant l'accès à tous les services.

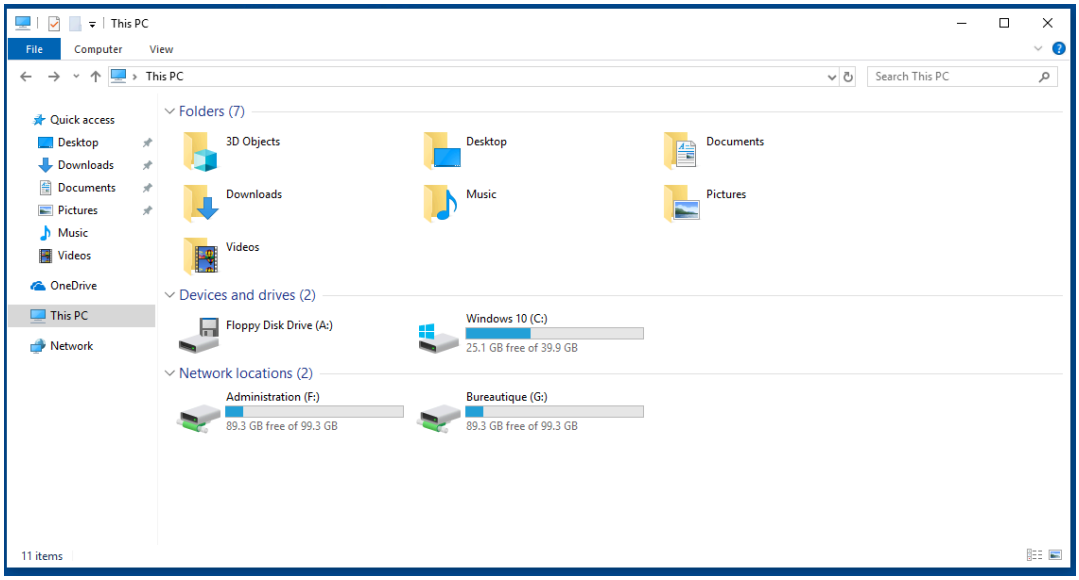




Et pour finir un gpupdate /force sur mes clients pour vérifier.

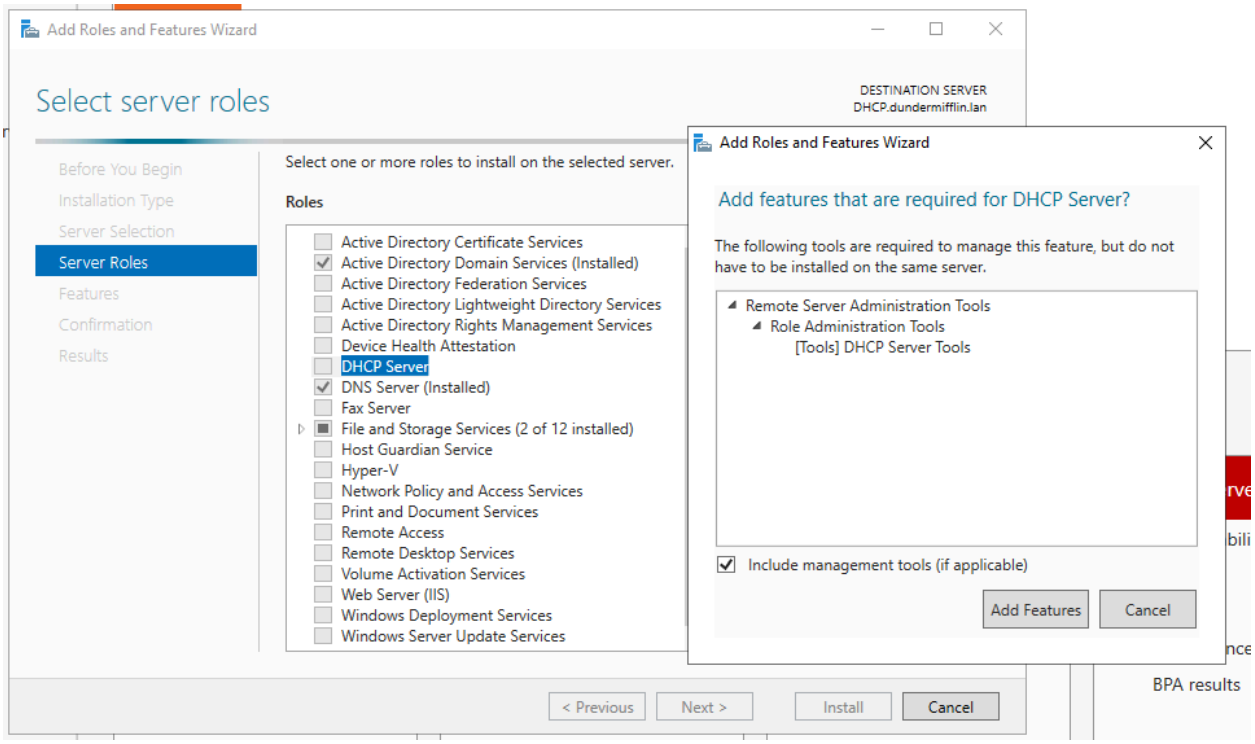
```
C:\Users\m.scott>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.
```

Client de la direction :

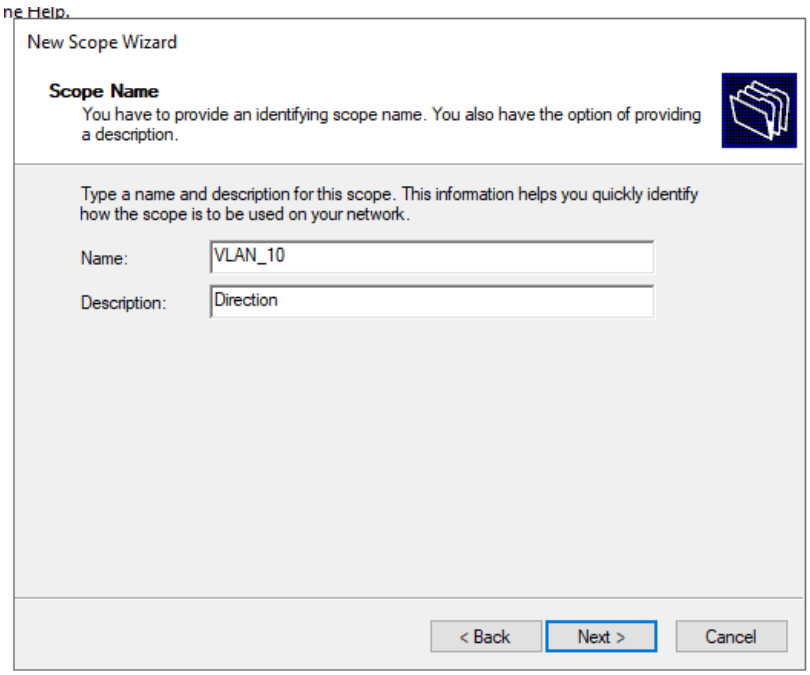


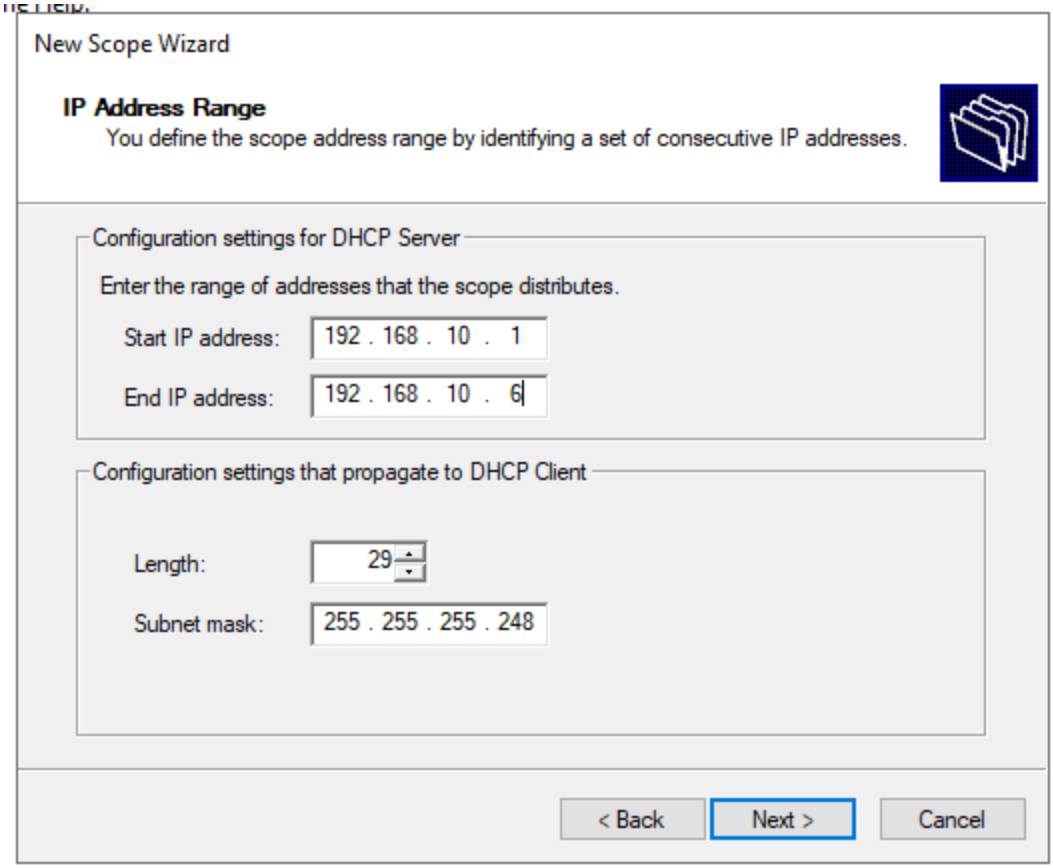
3.7 - Configuration du DHCP

Je commence par installer le rôle dhcp sur mon serveur dhcp.

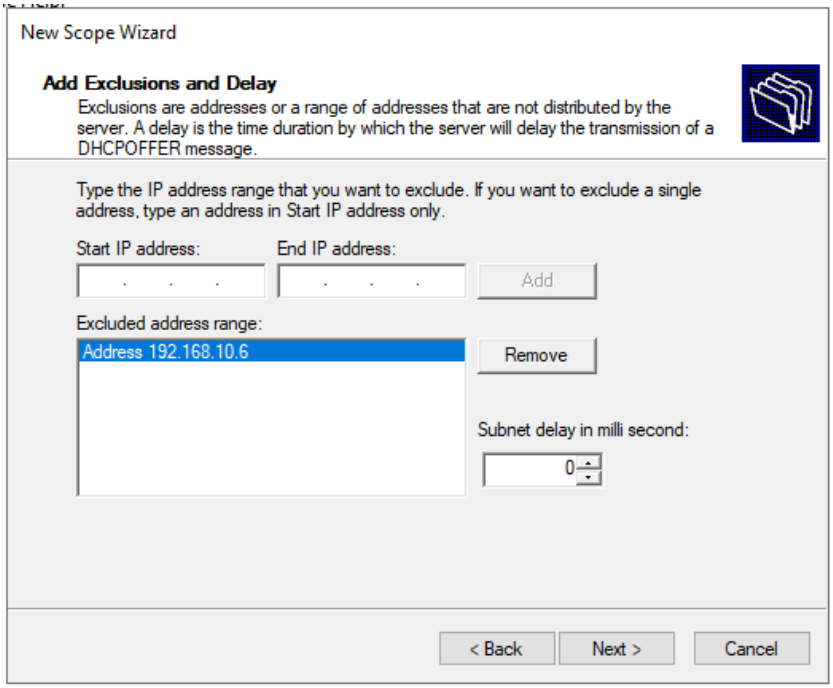


Et après je configure mes étendues dhcp en fonction des vlans, je n'en fait pas pour celui des serveurs car un serveur doit avoir une adresse IP physique.

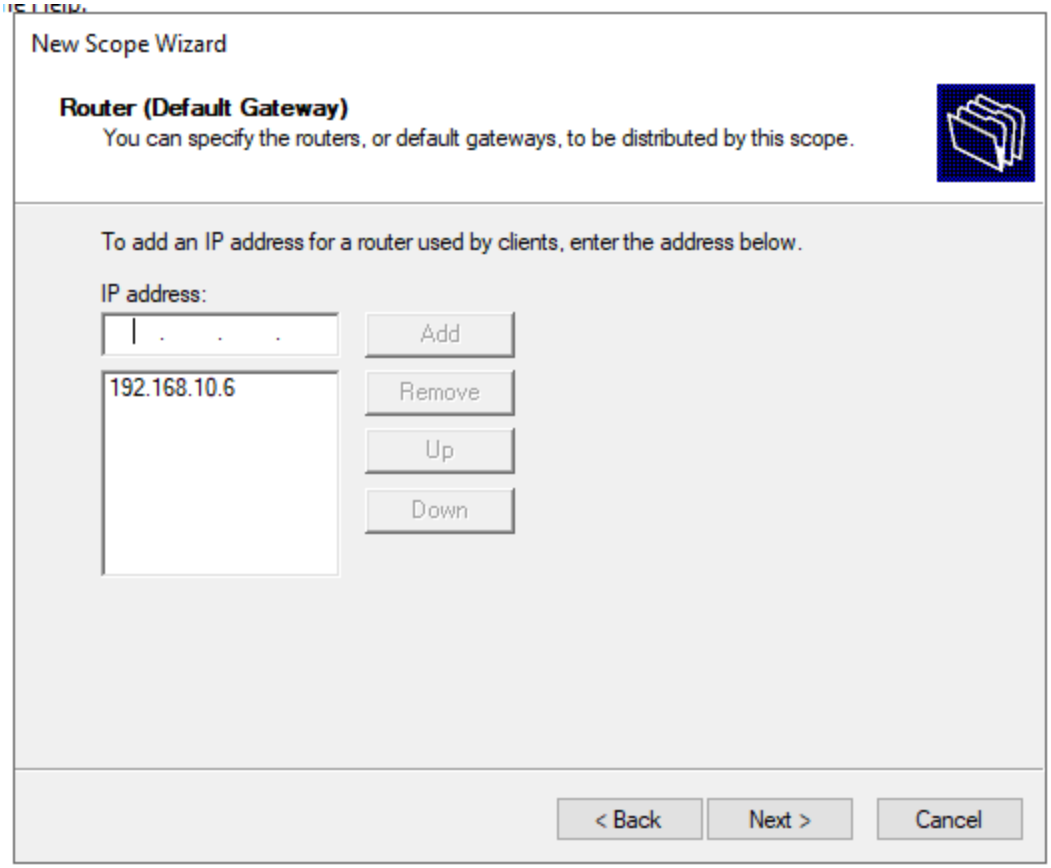




Et maintenant je vais exclure l'adresse "192.168.10.6" qui est l'adresse IP de l'interface virtuelle du sous-réseau du vlan 10 de mon routeur.



Ici j'ajoute l'adresse ip de mon routeur.



Avant de tester il faut que j'aille sur l'interface virtuelle du vlan 10 sur le routeur donc fa0/1.2 et que je tape cette commande "ip helper-address 192.168.2.2" qui va rediriger les paquets vers une adresse IP.

```
interface FastEthernet0/1.2
 encapsulation dot1Q 10
 ip address 192.168.10.6 255.255.255.248
 ip helper-address 192.168.2.2
```

Et je teste sur un client du vlan 10 si il prends bien une ip automatiquement avec cette commande.

```
ipconfig /renew
```

```
PS C:\Windows\system32> ipconfig /renew

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : dundermifflin.lan
   Link-local IPv6 Address . . . . . : fe80::8568:81e1:a64d:9ab6%5
   IPv4 Address. . . . . . . . . . . : 192.168.10.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.248
   Default Gateway . . . . . . . . . : 192.168.10.6
PS C:\Windows\system32>
```

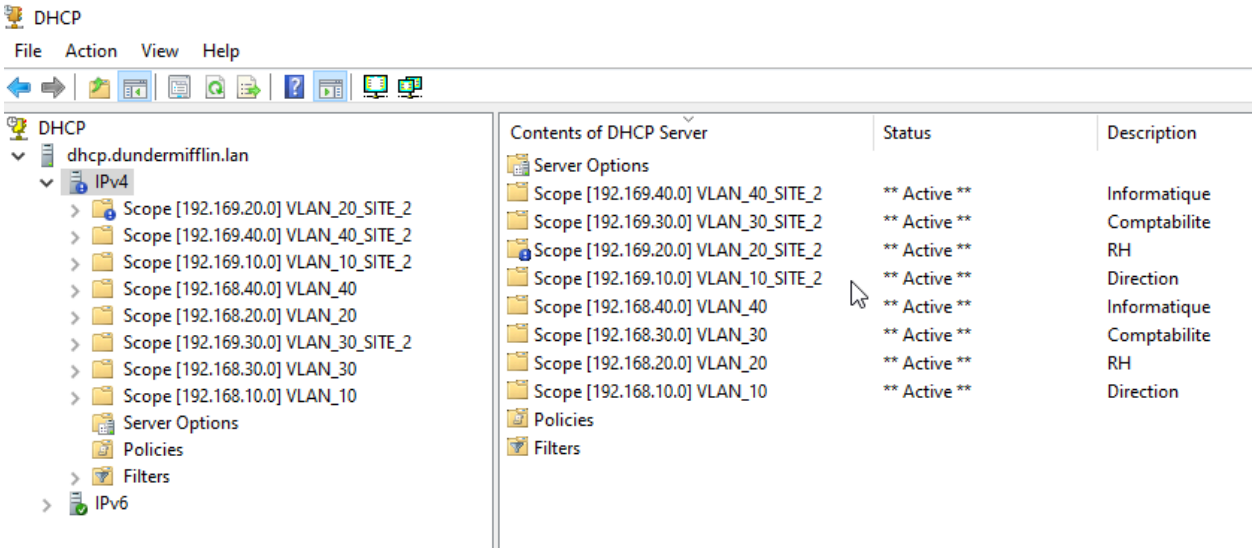
Je vais faire la même manipulation pour le vlan 30.

```
PS C:\Windows\system32> ipconfig /renew

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : dundermifflin.lan
   Link-local IPv6 Address . . . . . : fe80::59a8:f28f:feef:5b15%4
   IPv4 Address. . . . . . . . . . . : 192.168.30.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.248
   Default Gateway . . . . . . . . . :
PS C:\Windows\system32>
```

Mon dhcp est bien fonctionnel pour le vlan 30 du site 1.

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : dundermifflin.lan
   Link-local IPv6 Address . . . . . : fe80::b8dc:a3c6:53aa:951e%4
   IPv4 Address. . . . . . . . . . . : 192.169.30.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.248
   Default Gateway . . . . . . . . . : 192.169.30.6
PS C:\Windows\system32>
```

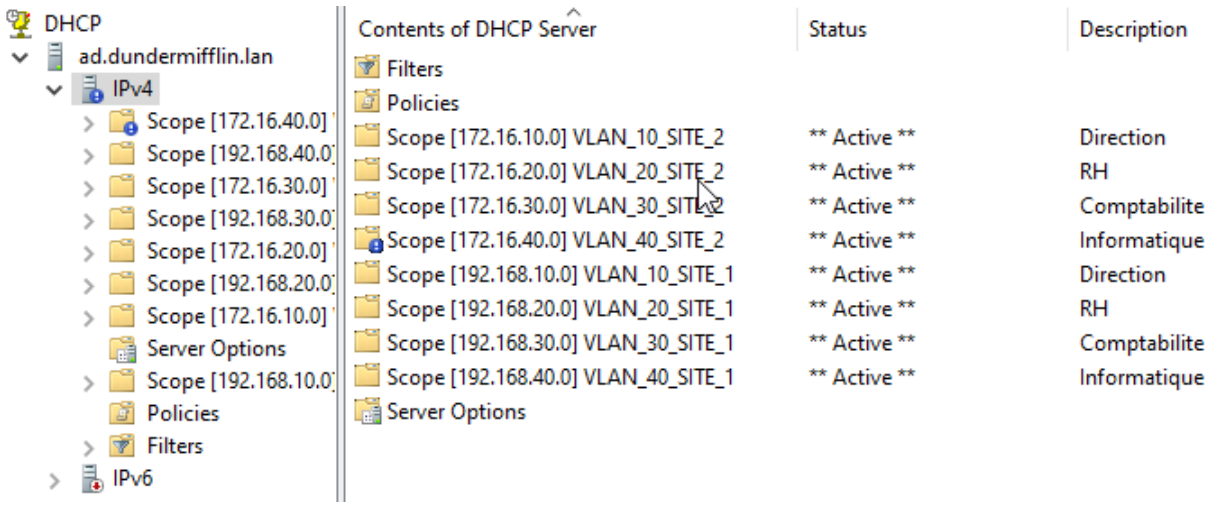
Test réussi pour le vlan 30 du site 2.



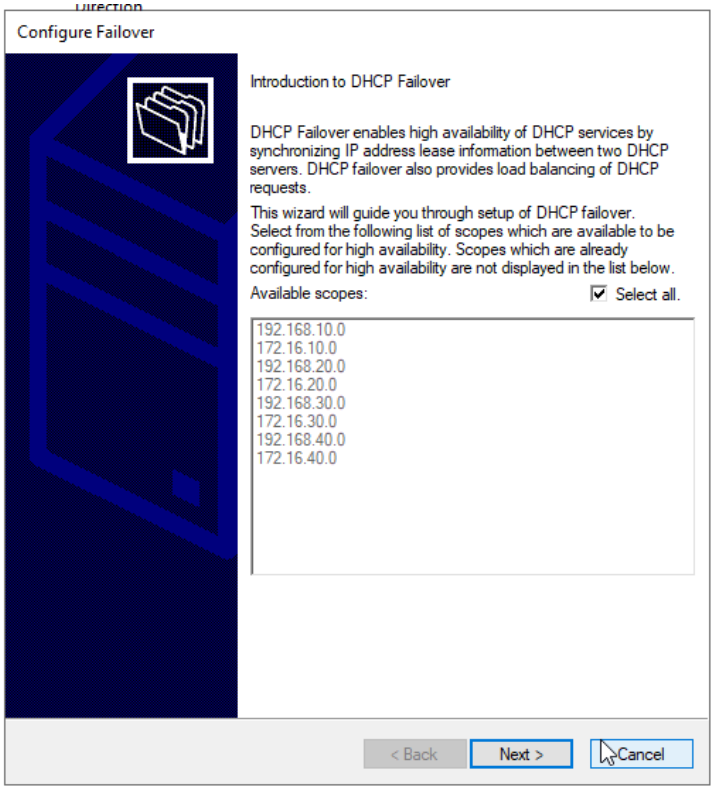
3.8 - Mise en place du DHCP FAILOVER

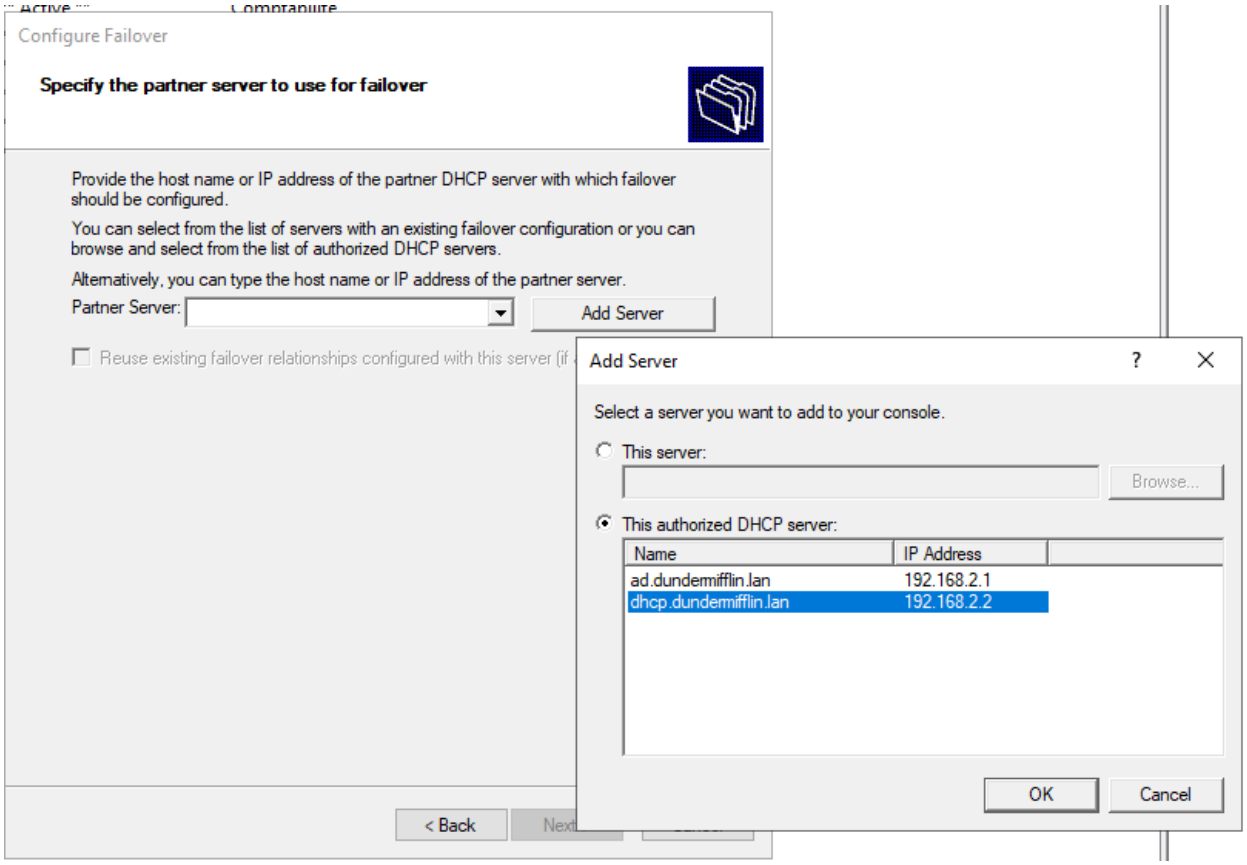
Déjà je vais refaire toutes mes pools dhcp sur mon serveur ad et les supprimer sur mon serveur dhcp. sans oublier la commande ip helper en changeant l'ip du serveur dhcp failover par celui de l'ad.

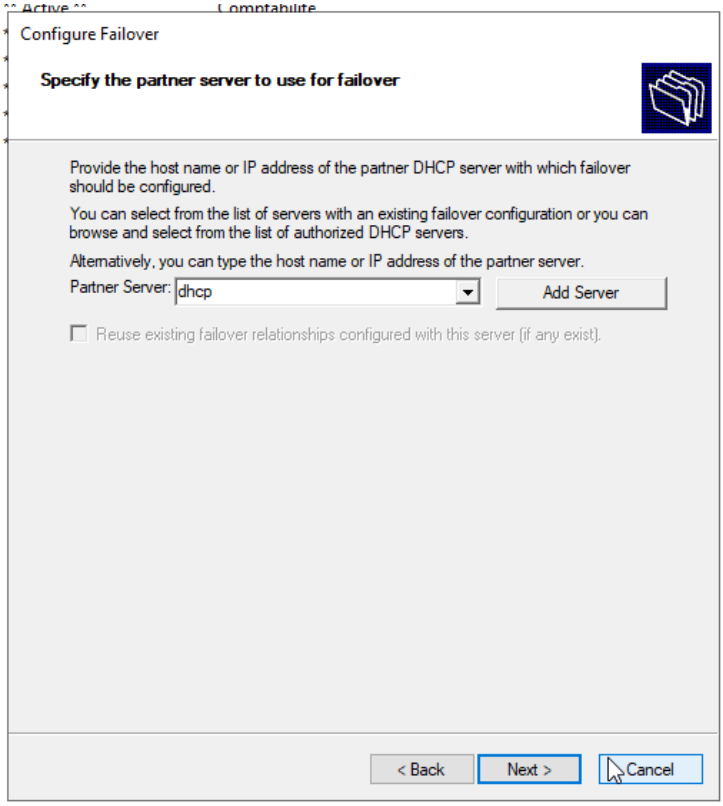
(Il faut déjà avoir installé le rôle dhcp sur mon serveur dhcp.)

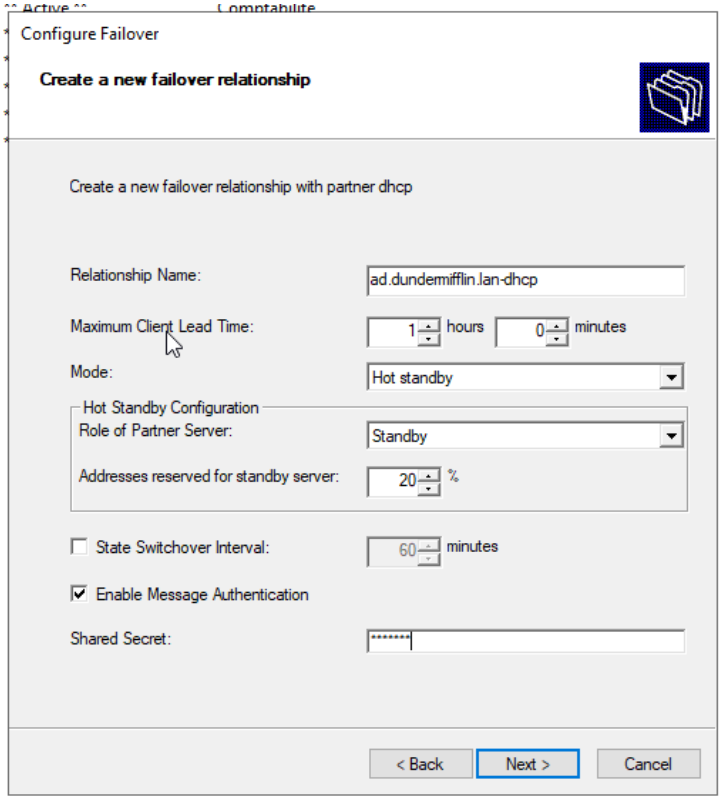


Pour redondé mon DHCP je vais procéder de la manière suivante.

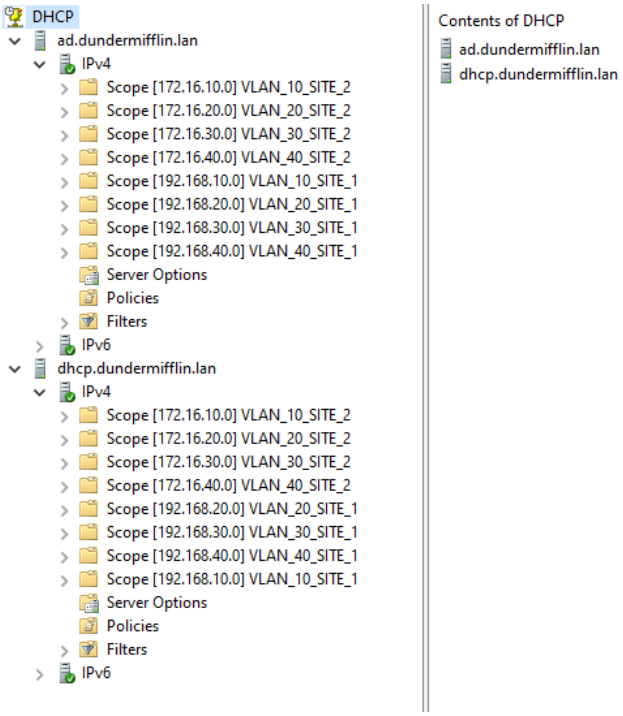



Configure Failover
Specify the partner server to use for failover
Provide the host name or IP address of the partner DHCP server with which failover should be configured.
You can select from the list of servers with an existing failover configuration or you can browse and select from the list of authorized DHCP servers.
Alternatively, you can type the host name or IP address of the partner server.
Partner Server:
Add Server
Reuse existing failover relationships configured with this server (if
< Back
Add Server
Select a server you want to add to your console.
This server:
Browse...
This authorized DHCP server:
Name
IP Address
ad.dundermifflin.lan
192.168.2.1
dhcp.dundermifflin.lan
192.168.2.2
OK
Cancel


Configure Failover
Specify the partner server to use for failover
Provide the host name or IP address of the partner DHCP server with which failover should be configured.
You can select from the list of servers with an existing failover configuration or you can browse and select from the list of authorized DHCP servers.
Alternatively, you can type the host name or IP address of the partner server.
Partner Server:
dhcp
Add Server
Reuse existing failover relationships configured with this server (if any exist).
< Back
Next >
Cancel



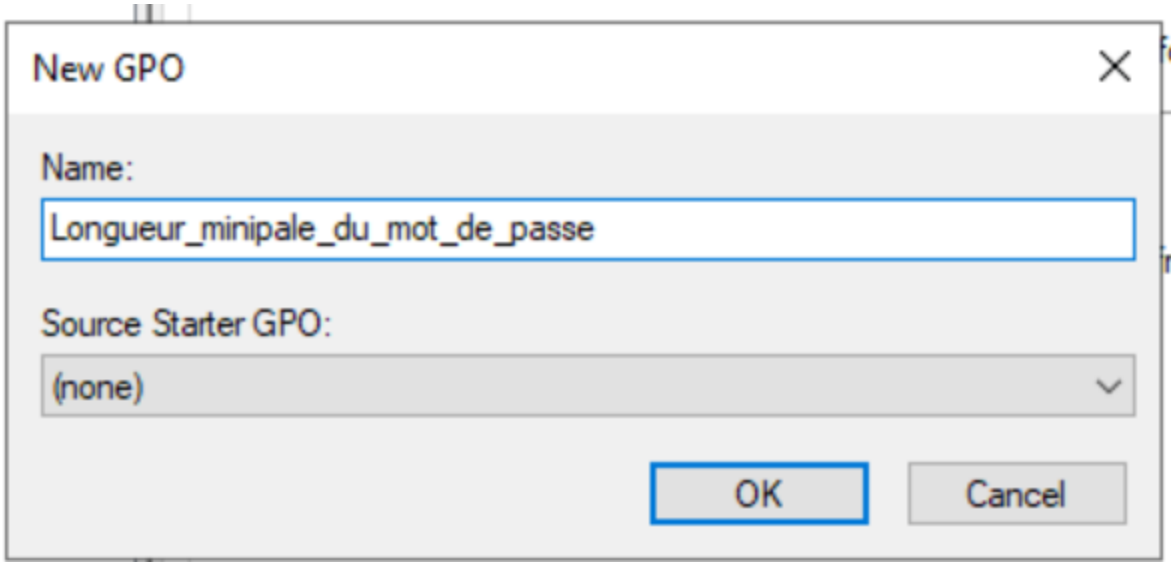
Le mot de passe est “Admin00”.

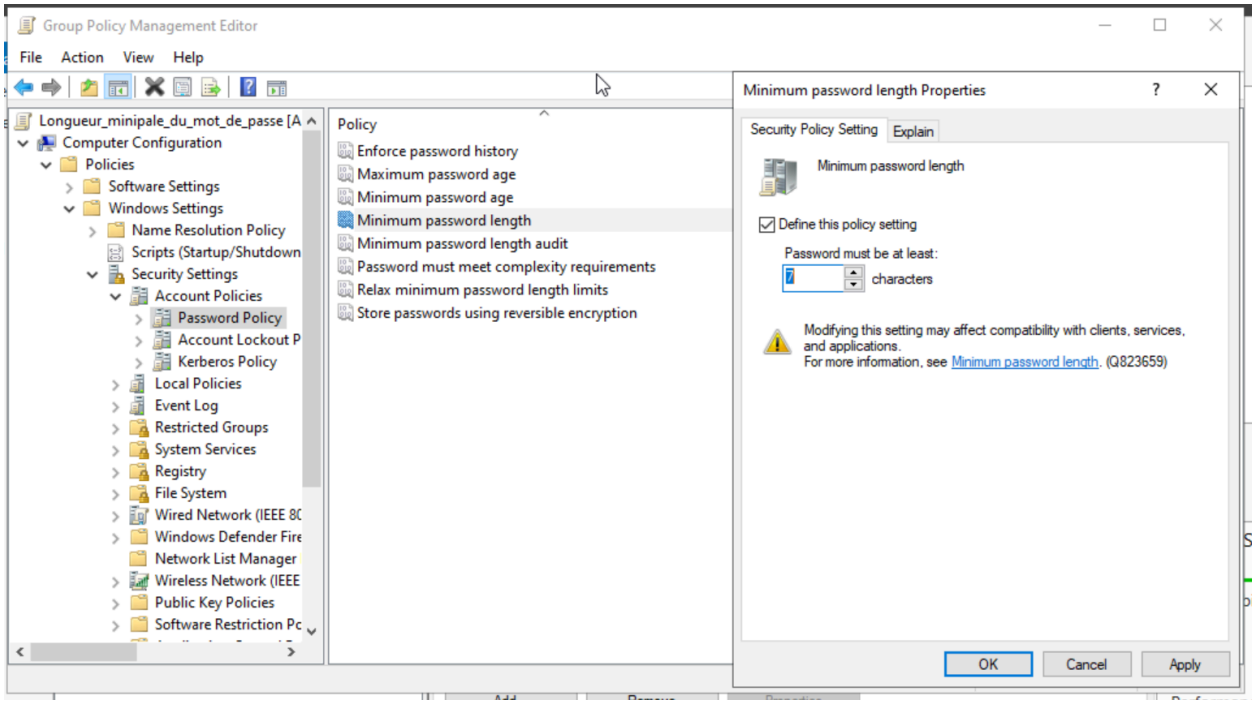


Voilà le FAILOVER est configuré, j’ai choisi de faire de la redondance à la place de l’équilibrage de charge.

3.9 - GPO Longueur minimale du mot de passe

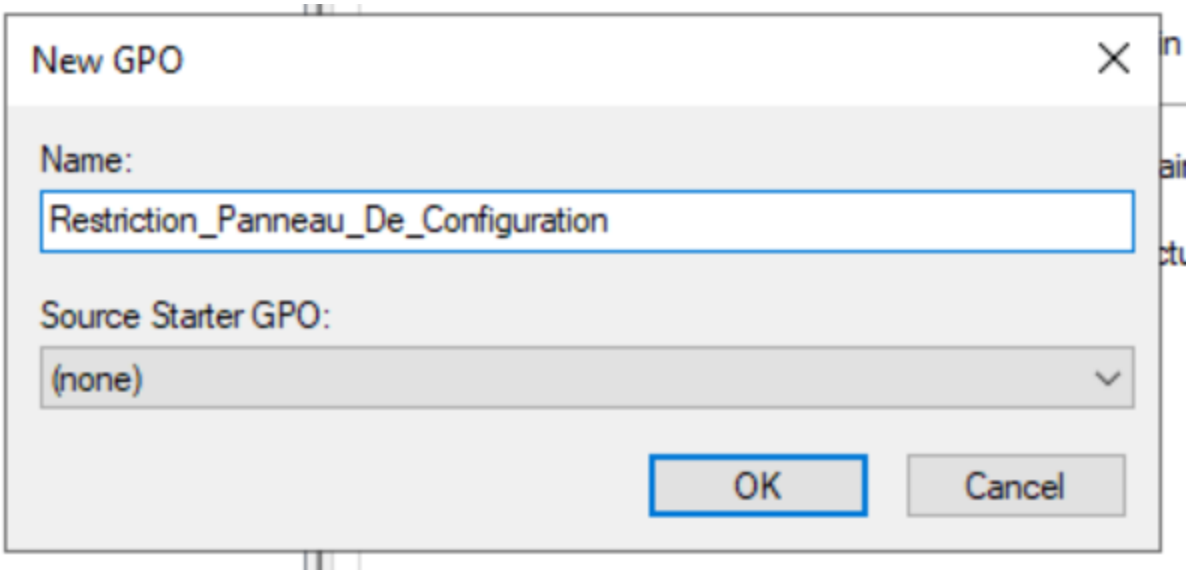
Ici je vais créer une gpo pour modifier la longueur minimale du mot de passe à 7 caractères..

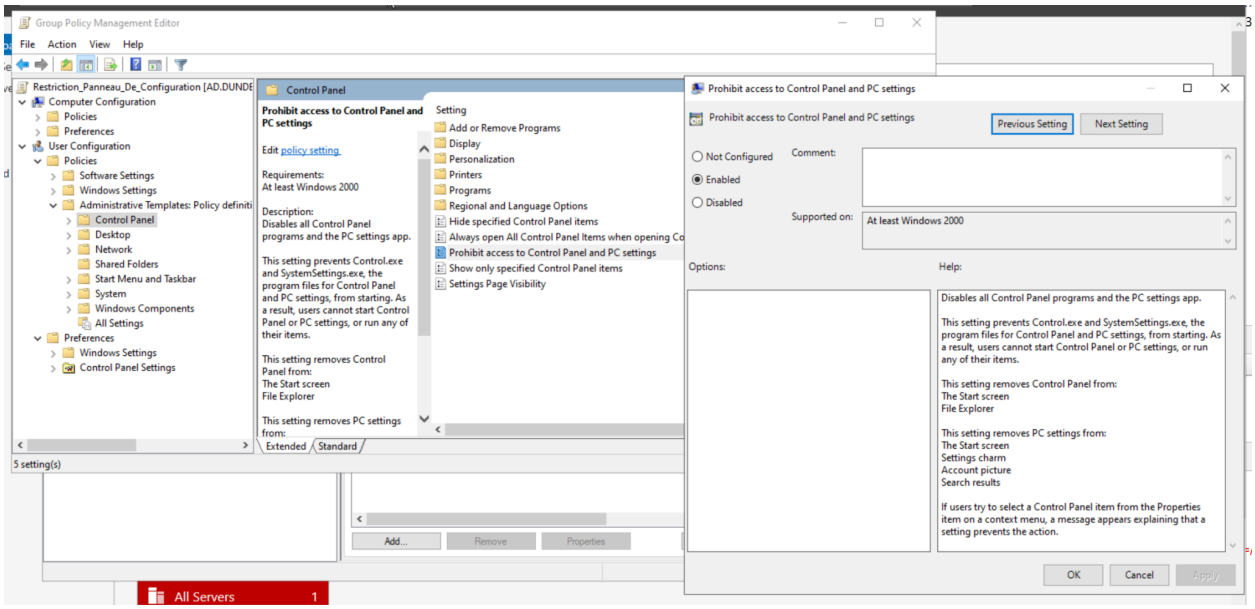




3.10 - GPO Restriction au panneau de configuration

Et ici je vais restreindre l'accès au panneau de configuration aux clients qui ne sont pas dans le groupe de la direction.

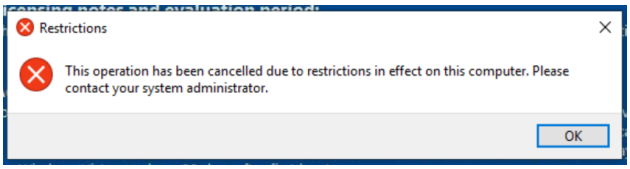




Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
GG_Comptabilite (DUNDERMIFFLIN\GG_Comptabilite)
GG_Informatique (DUNDERMIFFLIN\GG_Informatique)
GG_RH (DUNDERMIFFLIN\GG_RH)



3.11 - MD5 encryption

Pour finir, je vais activer l'authentification md5 sur le protocole de routage OSPF, l'interface fa0/0 entre les routeurs.

interface fa0/0

ip ospf message-digest-key 1 md5 aqw

exit

router ospf 1

area 0 authentication message-digest

end

```
!
interface FastEthernet0/0
 ip address 10.1.1.1 255.255.255.252
 ip ospf message-digest-key 1 md5 aqw
 duplex auto
 speed auto
!
```

4) PROBLÈMES RENCONTRÉS

Dans un premier temps, J'ai rencontré beaucoup de problèmes au niveau de GNS3 et de l'adressage, mais le plus gros était d'avoir utilisé une adresse IP Publique (192.169.0.0/16), une erreur de débutant que je n'avais pas prise en compte. Ensuite en ce qui concerne les tâches à faire pour ce ppe, j'ai dû refaire toutes les étendues dhcp sur mon ad car je les avais faites sur mon contrôleur de domaine et je ne parvenais pas à ajouter le failover afin de mettre en place la redondance. Et pour finir j'ai eu un problème au niveau du répertoire caché, pour qu'il soit totalement caché il fallait que j'ajoute un $ à la fin du nom lors de la création de l'espace de noms.

5) CONCLUSION

Dunder Mifflin a désormais son réseau opérationnel avec l'implémentation d'un Active Directory selon la méthode AGDLP, établissant ainsi une structure organisationnelle sécurisée. De plus, un partage commun a été configuré pour tous les utilisateurs, tandis qu'un partage personnel, accessible uniquement par le directeur, a été mis en place de manière discrète.

Le service DHCP est maintenant pleinement fonctionnel, avec une configuration de failover pour assurer la redondance grâce à un serveur dédié. De plus, des GPO ont été appliquées, imposant des normes telles qu'une longueur minimale pour les mots de passe et des restrictions d'accès au panneau de configuration, spécifiquement pour les utilisateurs n'appartenant pas au service de la direction.