

Résumé de l'infra :

- 3 pc sur un VLAN (VLAN10)
- Un hyperviseur contenant 3 VM (VLAN20)
- Une DMZ et un serveur Web (VLAN30)
- Un routeur
- Un switch

ROUTEUR

Configuration du routeur :

Le nom :

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname routeur-cisco
routeur-cisco(config)#ip domain-name clemanet.com
routeur-cisco(config)#^Z
routeur-cisco#wr
Building configuration...
```

Pour supprimer un nom :

```
routeur-cisco(config)#no hostname
Router(config)#no ip domain-name
Router(config)#+
```

ADRESSAGE IP DU ROUTEUR

SWITCH

Configuration du nom du switch, du domaine DNS, puis enregistrement de la configuration.

Dans l'exemple, le nom du switch est : 9200-RG et le domaine est mondomaine.local.

En fonction de la date du firmware, la commande pour le nom de domaine est soit "ip domain-name" soit "ip domain name".

```
Switch#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#

Switch(config)#hostname SwitchNINI

SwitchNINI(config)#ip domain-name clemanet.com

SwitchNINI(config)#end

SwitchNINI#wr

Building configuration...

[OK]

SwitchNINI#

Pour supprimer le nom du commutateur et le nom de domaine, il faut saisir les commandes suivantes.

SwitchNINI(config)#no hostname

Switch(config)#no ip domain-name

Switch(config)#

Adressage IP du switch:

L'adressage IP du switch va nous servir à superviser celui ci à distance. Un vlan dédié au management du switch est configuré (dans l'exemple: vlan2). L'adresse IP sera donc associée au vlan 2.

La configuration IP choisie est:

- **Adresse IP : 192.168.100.25**
- **Masque de sous-réseau : 255.255.255.0**

- Passerelle par défaut : 10.20.5.254

```
SwitchNINI(config)#vlan 2
```

```
SwitchNINI(config-vlan)#exit
```

```
SwitchNINI(config)#interface vlan2
```

```
SwitchNINI(config-if)#ip address 192.168.100.25 255.255.255.0
```

```
SwitchNINI(config-if)#ex
```

```
SwitchNINI(config)#ip default-gateway 192.168.100.1
```

Vérification de la configuration du vlan d'administration

```
SwitchNINI#sh run int vlan2
```

```
Building configuration...
```

```
Current configuration : 64 bytes
```

```
!
```

```
interface Vlan2
```

```
ip address 192.168.100.25 255.255.255.0
```

```
end
```

```
SwitchNINI#
```

Suppression de l'adresse IP et de la passerelle par défaut:

```
SwitchNINI(config)#interface vlan2
```

```
SwitchNINI(config-if)#no ip address
```

```
SwitchNINI(config-if)#ex
```

```
SwitchNINI(config)#no ip default-gateway
```

Ajout de mot de passe pour l'authentification

La connexion au switch s'effectue par le port console en utilisant la ligne associée à ce port ou bien à distance en utilisant les lignes virtuelles (appelées VTY).

Par défaut, il n'y a pas de compte créé pour l'authentification.

Il faut créer au minimum un mot de passe pour l'accès aux différents terminaux (console et virtuel) et un mot de passe pour l'accès au mode privilégié (enable).

Le mode d'administration par défaut est telnet.

Par défaut, les mots de passe apparaissent en clair lors de l'affichage du fichier de configuration. Nous allons donc tout d'abord activer le service encryption-password, les mots de passe apparaîtront alors chiffrés lorsque les commandes d'affichage de la configuration sont entrées.

Activation du service password-encryption

```
Switch(config)#service password-encryption
```

Affichage des lignes disponibles.

On notera la ligne accessible par la console (CTY) et les lignes virtuelles (VTY) pour l'accès distant au switch.

```
SwitchNINI#sh line
```

| Tty | Typ | Tx/Rx | A Modem | Roty | Acc0 | AccI | Uses | Noise | Overruns | Int |
|-----|-------|-----------|---------|------|------|------|------|-------|----------|-----|
| * | 0 CTY | - - - - - | 0 0 | 0/0 | - | | | | | |
| 1 | VTY | - - - - - | 0 0 | 0/0 | - | | | | | |
| 2 | VTY | - - - - - | 0 0 | 0/0 | - | | | | | |
| 3 | VTY | - - - - - | 0 0 | 0/0 | - | | | | | |
| 4 | VTY | - - - - - | 0 0 | 0/0 | - | | | | | |
| 5 | VTY | - - - - - | 0 0 | 0/0 | - | | | | | |
| 6 | VTY | - - - - - | 0 0 | 0/0 | - | | | | | |
| 7 | VTY | - - - - - | 0 0 | 0/0 | - | | | | | |
| 8 | VTY | - - - - - | 0 0 | 0/0 | - | | | | | |
| 9 | VTY | - - - - - | 0 0 | 0/0 | - | | | | | |
| 10 | VTY | - - - - - | 0 0 | 0/0 | - | | | | | |

Création des mots de passe et configuration de la console et des lignes virtuelles.

Un mot de passe est créé pour se loguer au différentes lignes.

```
SwitchNINI(config)#enable secret M02p@55
```

```
SwitchNINI(config)#line con 0
```

```
SwitchNINI(config-line)#password P@55w0rd
```

```
SwitchNINI(config-line)#login
```

```
SwitchNINI(config-line)#exit
```

```
SwitchNINI(config)#line vty 0 15
```

```
SwitchNINI(config-line)#password P@55w0rd
```

```
SwitchNINI(config-line)#login
```

```
SwitchNINI(config-line)#end
```

```
SwitchNINI#
```

Il y a maintenant un mot de passe à saisir pour l'accès au switch et un mot de passe à saisir pour l'accès au mode avec privilège.

```
User Access Verification
```

Password:

```
SwitchNINI>en
```

Password:

```
SwitchNINI#
```

Configuration et affichage de l'heure

On configure l'heure, puis le fuseau horaire et le moment de passer à l'heure d'été (dans l'exemple: pour la France).

```
switch#clock set 15:19:00 4 april 2021
```

```
switch#
```

```
switch#show clock
```

```
15:19:05.609 CEST Mon Apr 4 2021
```

```
switch(config)#clock timezone cet 1
```

```
switch(config)#clock summer-time cest recurring last Sun Mar  
3:00 last Sun Oct 3:00
```

```
switch#
```

VLAN

Accéder au mode de configuration

Sur un switch Cisco (par exemple), une fois connecté en mode privilégié (`enable`), vous entrez en mode de configuration globale :

```
enable
```

```
configure terminal
```

3. Définir ou vérifier les VLANs

Si le VLAN n'existe pas encore, vous devez le créer. Sinon, vous pouvez directement l'utiliser. Par exemple :

Créer un VLAN 10 :

```
vlan 10
```

```
name VLAN_10
```

4. Assigner un port à un VLAN

Ensuite, vous assignez un port spécifique à un VLAN. Voici comment procéder :

Accédez au mode de configuration du port spécifique. Par exemple, pour assigner le port **Fa0/1** au VLAN 10 :

```
interface fa0/1
```

```
switchport mode access
```

```
switchport access vlan 10
```

- Ce port sera maintenant associé au VLAN 10.

Pour un autre port, comme **Fa0/2**, assigné au VLAN 20 :

```
interface fa0/2 switchport mode access switchport access vlan 20
```

5. Vérification de la configuration

Pour vérifier que les ports sont bien assignés, vous pouvez utiliser la commande suivante :

```
show vlan
```

Cela vous montre la liste des VLANs et des ports associés.

6. Configurer un Trunk si nécessaire

Si vous devez faire passer plusieurs VLANs sur un lien entre des switches (c'est ce qu'on appelle un "trunk"), vous devrez configurer le port en mode "trunk". Par exemple, pour le port **Fa0/24** :

```
interface fa0/24
```

```
switchport mode trunk
```

```
switchport trunk allowed vlan 10,20
```

Cela permettra au port **Fa0/24** de transporter les VLANs 10 et 20.

SERVEUR

pour changer l'adres ip du serveur-> aller sur le serveur HyperV

#nano /etc/network/interfaces

apres avoir modifier

ifdown -a

ifup -a

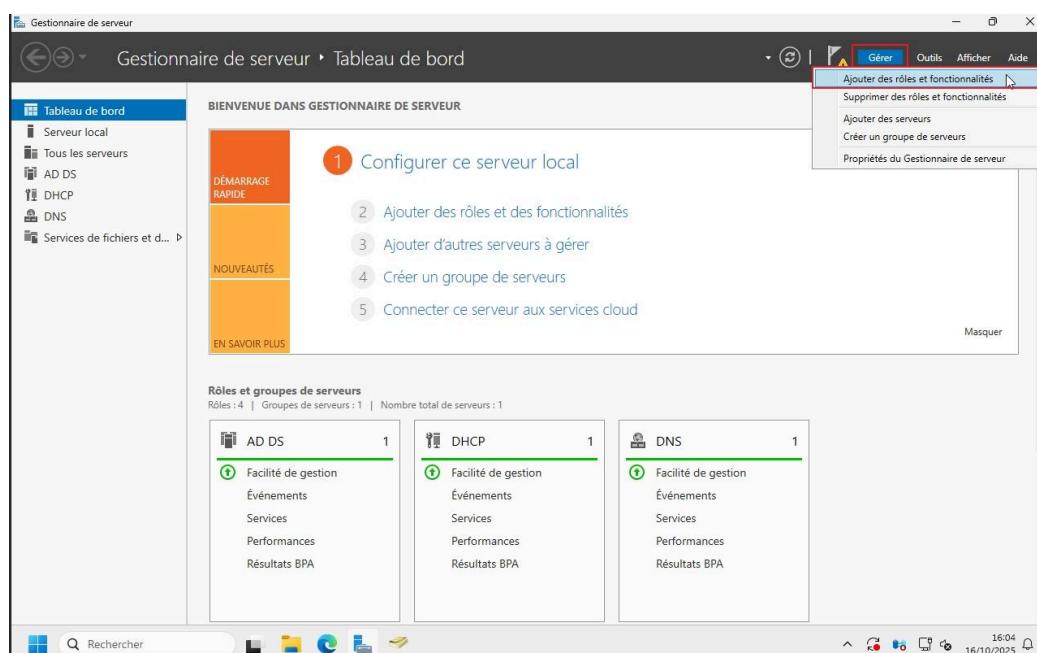
PROMOUVOIR CE SERVEUR EN CONTRÔLEUR DE DOMAINE

Changer le nom du serveur

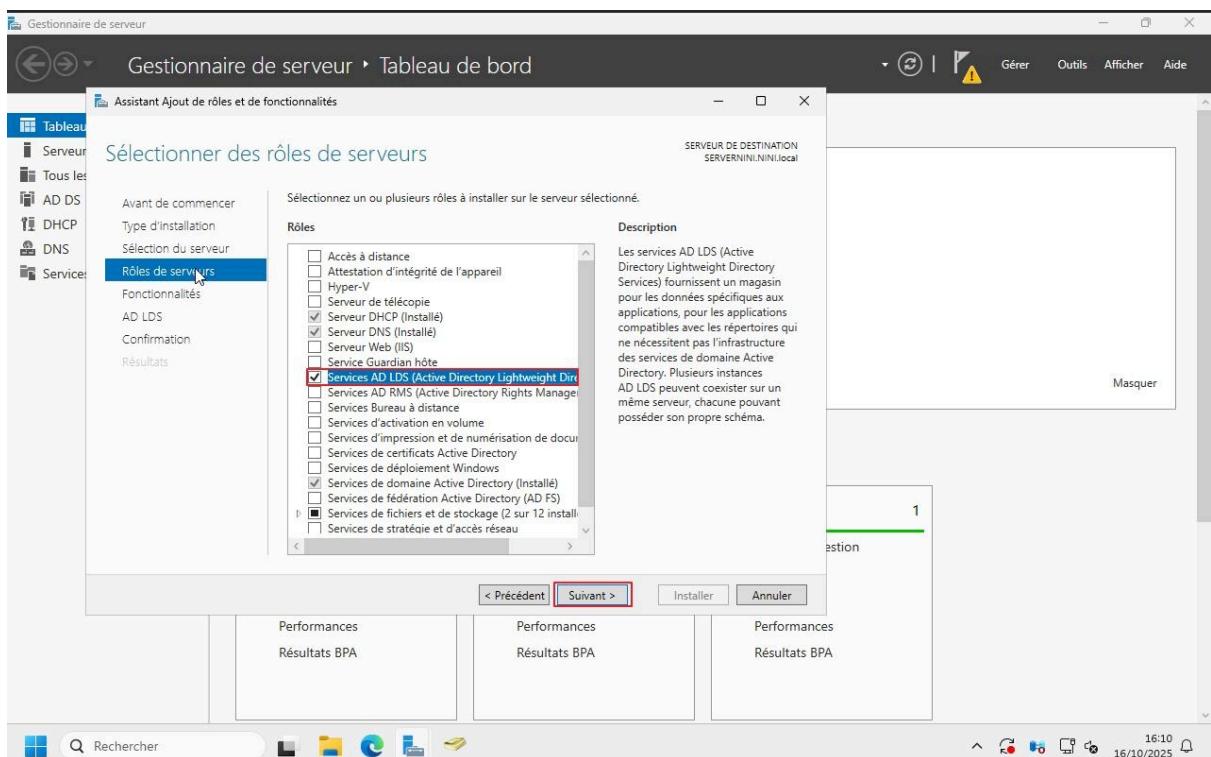
Redémarrer

Ouvrir le gestionnaire de serveur

Chercher puis cliquer sur “Ajouter des rôles et des fonctionnalités”



Sélectionner “ Installation basée sur un rôle ou sur une fonctionnalité”



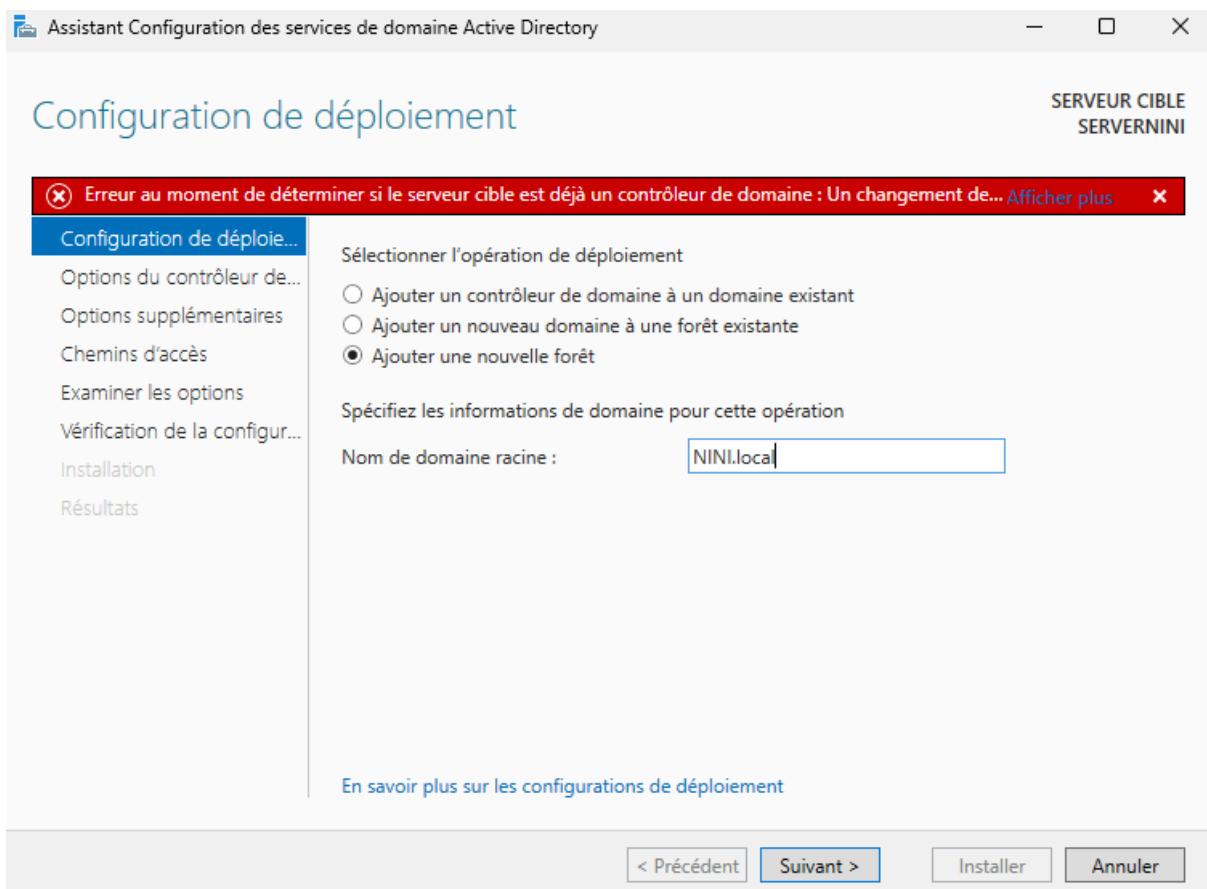
Cocher les services déjà présents sur le screen précédent.

Puis faire suivant jusqu'à avoir le bouton “Installer”, puis cliquez dessus.

Lorsque tout est installé, cliquer sur le petit drapeau puis sur “Promouvoir en contrôleur de domaine”

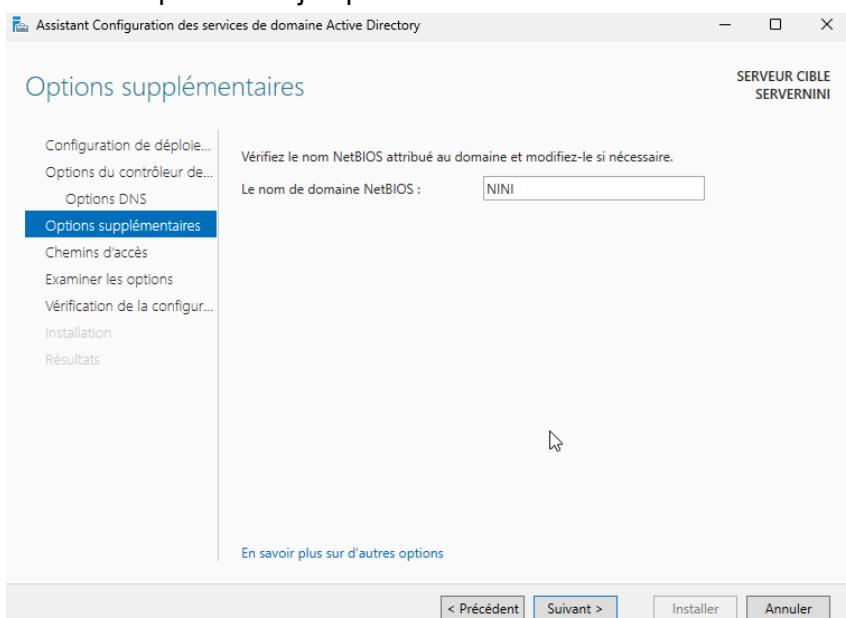
Choisir l'option “ajouter une nouvelle forêt” et la nommer “nom de l'entreprise”.local, pour nous c'est NINI

ex : NINI.local



Le mdp demandé est le mdp admin de la machine

Tout laisser par défaut jusqu'à avoir cette fenêtre :

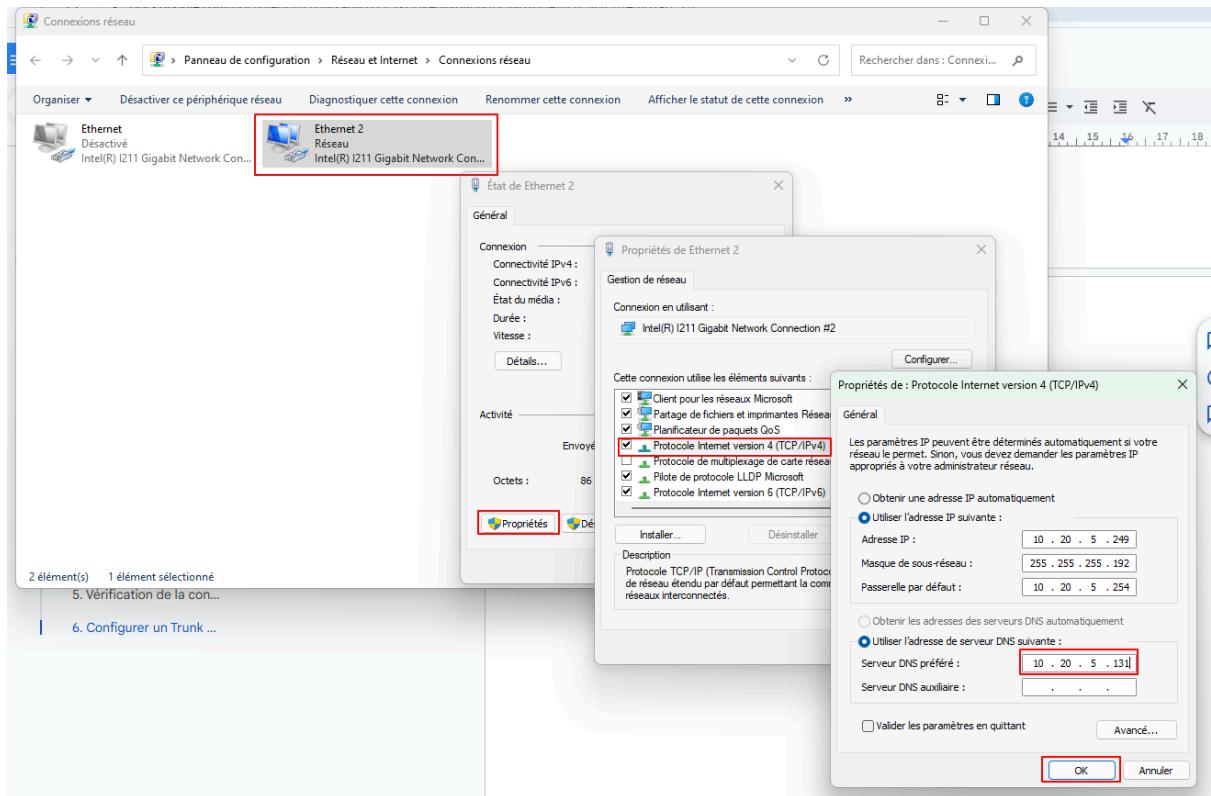


Tout laisser par défaut jusqu'au bouton "installer", puis lorsque le téléchargement est fini, redémarrer la machine.

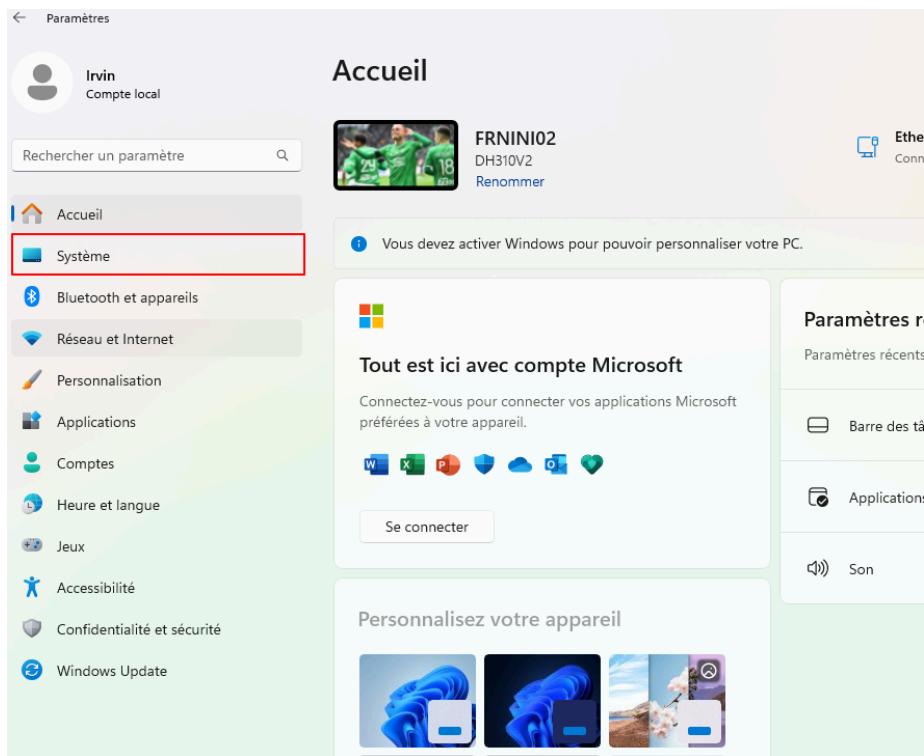
Faire rentrer un pc dans son domaine :

Regarder sa config réseau :

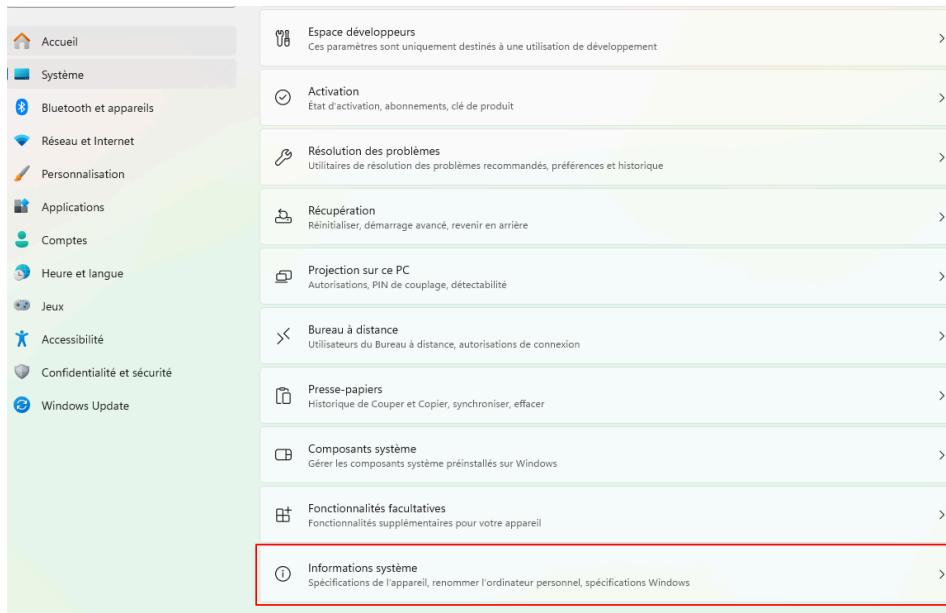
menu démarrer -> clic droit exécuter -> ncpa.cpl -> prendre la carte réseau qui est activée -> ipv4 -> mettre l'adresse de son contrôleur de domaine (pour nous le serveur AD) dans la case DNS



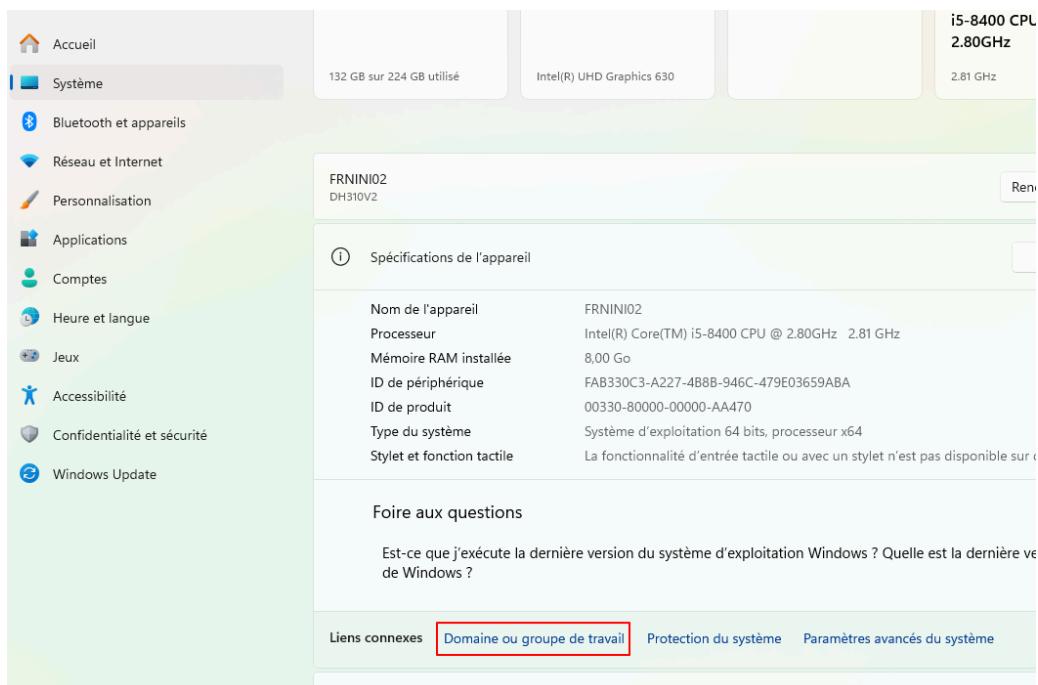
puis aller dans les paramètres de windows puis dans système :



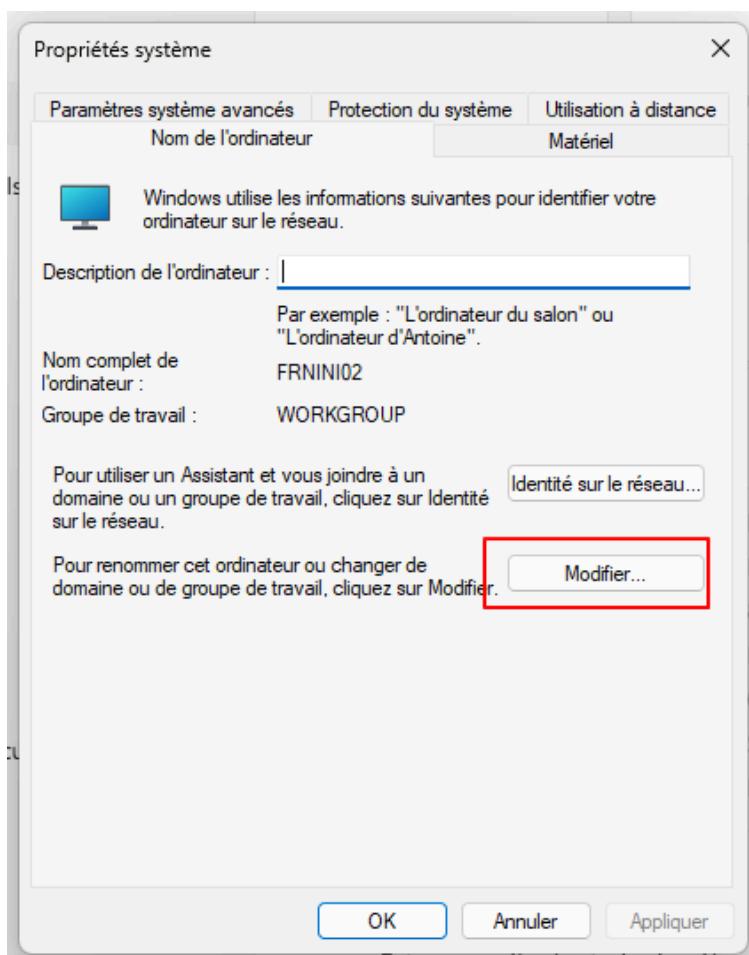
Puis aller dans “ Informations système ” (tout en bas de la page) :



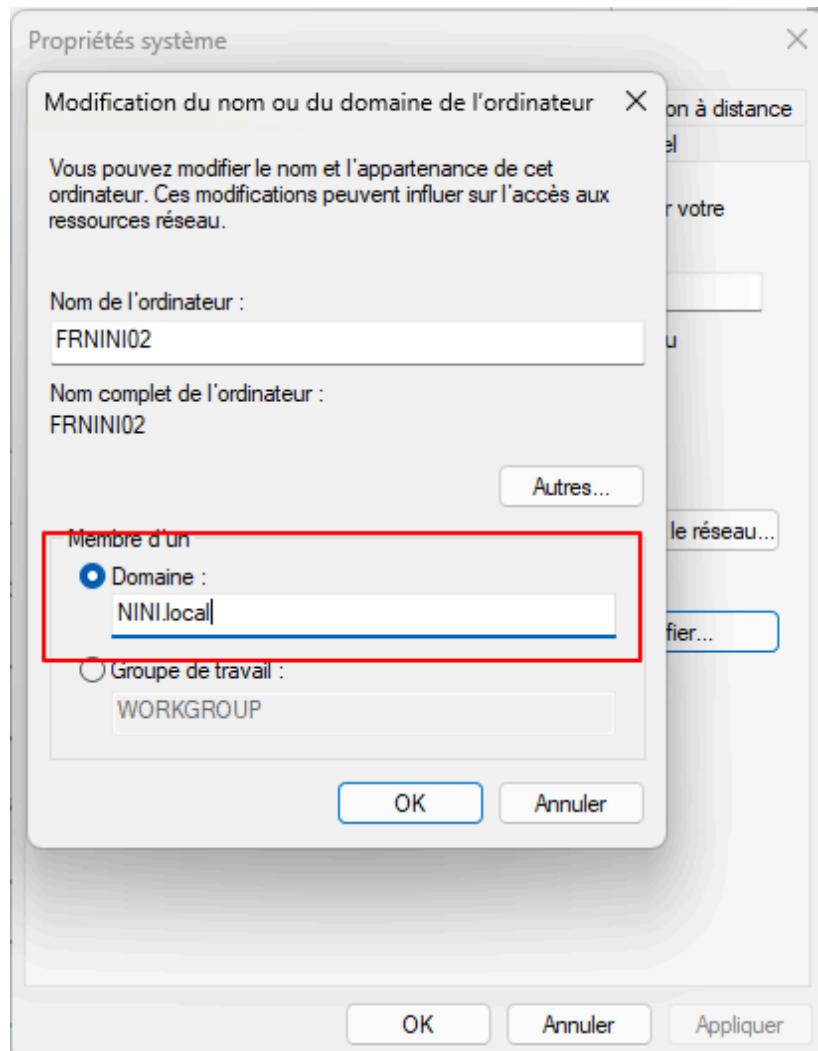
Cliquer sur “Domaine ou groupe de travail” :



Cliquer sur “Modifier” :

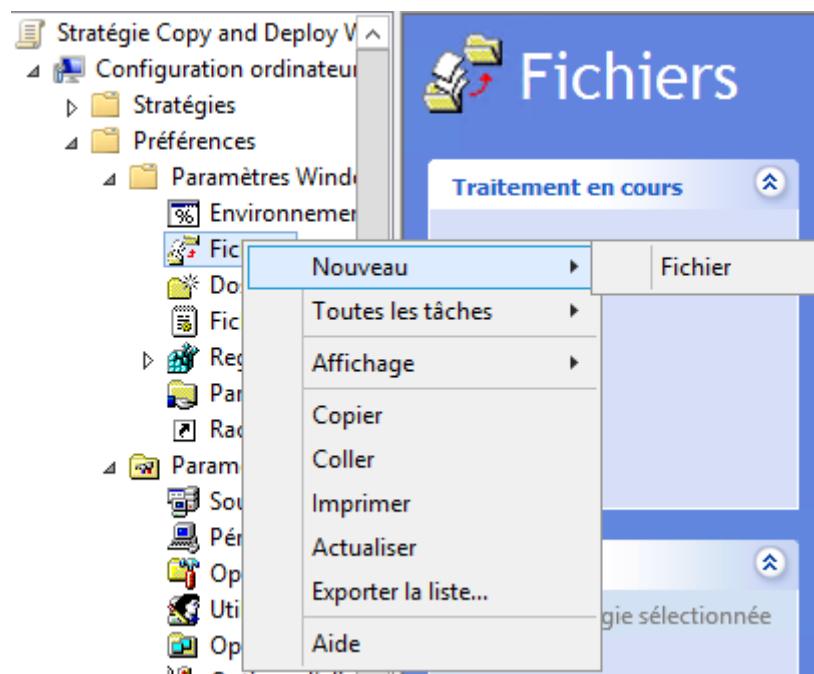


Puis cliquer sur "Domaine" puis rentrer son nom de domaine, après il y aura une fenêtre pour rentrer le login admin du serveur.



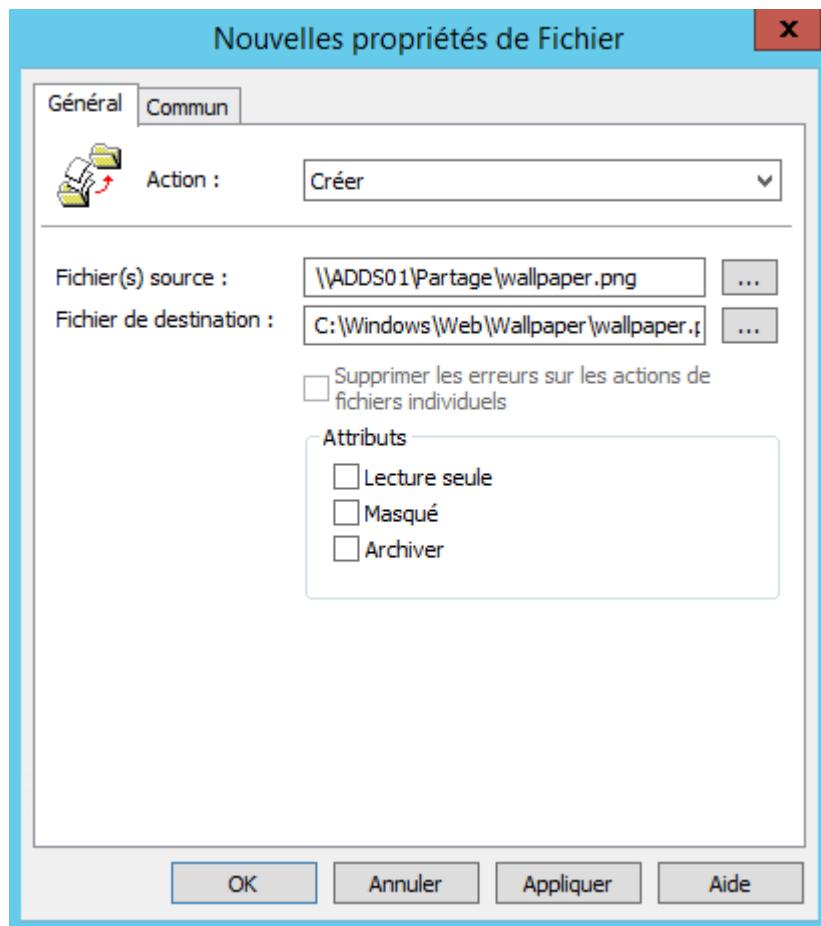
Créer une GPO (ici celle pour changer le fond d'écran)

Pour commencer, on va créer un paramètre de préférence pour que le fichier image du fond d'écran soit copié sur les ordinateurs distants. On va créer un nouveau fichier, sous « Configuration ordinateur », « Préférences », « Paramètres Windows » et « Fichiers ».

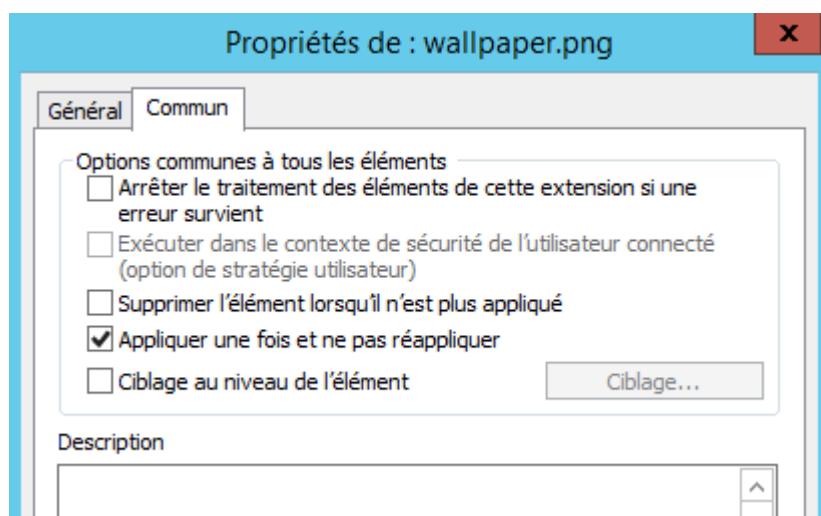


Sélectionnez l'action « Créer » puisque ce fichier n'existe pas, et pour le fichier source indiquez le chemin vers le fichier image qui est sur votre partage. Pour le fichier de destination, indiquez où vous souhaitez copier le fichier sur l'ordinateur, en local.

Pour le chemin vers le fichier source, préférez l'utilisation du nom complet de votre serveur.

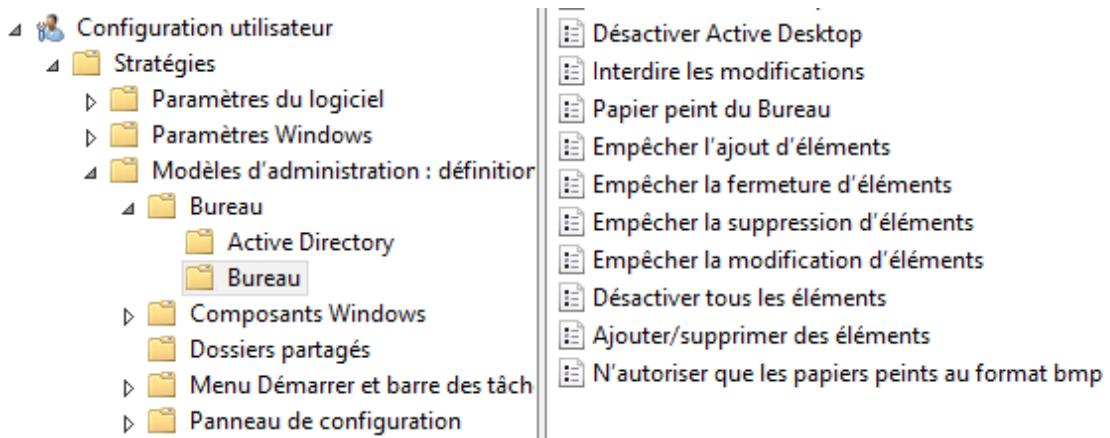


Dans l'onglet « Commun », vous devez cocher « Appliquer une fois et ne pas réappliquer » pour ne pas que le fond d'écran soit copié à chaque fois.



Un paramètre nommé « Papier peint du Bureau » doit être activé au sein de la stratégie de groupe. Il se situe à l'emplacement suivant :

- Configuration utilisateur, Modèles d'administration, Bureau, Bureau



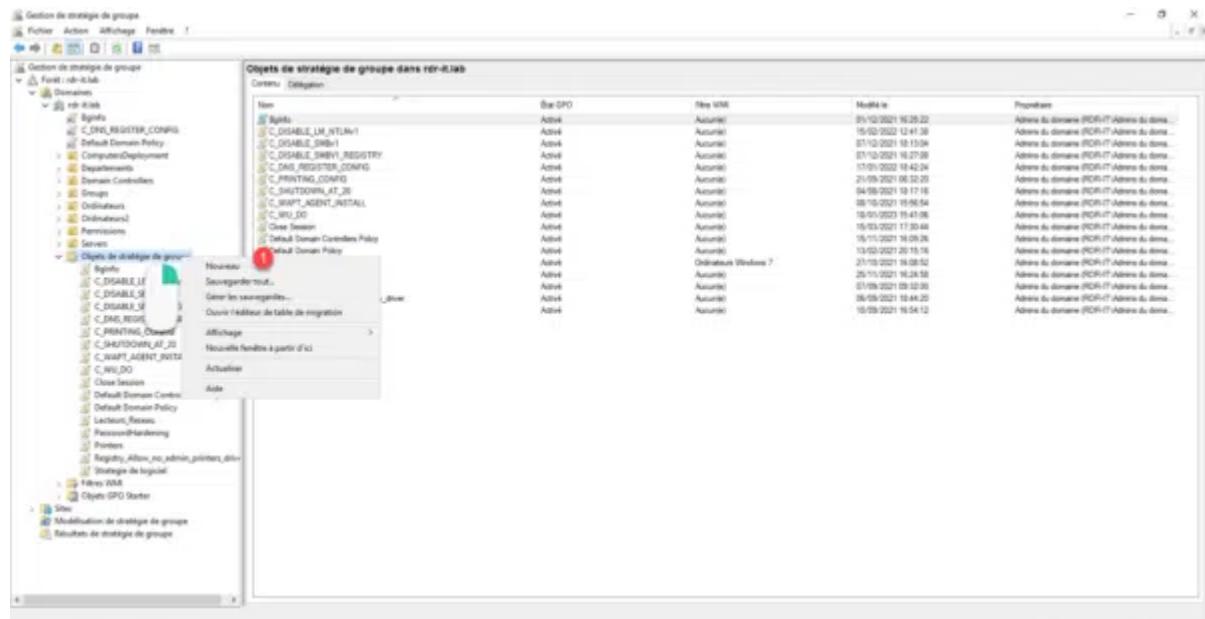
Se connecter à un autre pc.

Pensez à récupérer les dernières stratégies de groupe avec un cmd, puis redemarrer le pc :

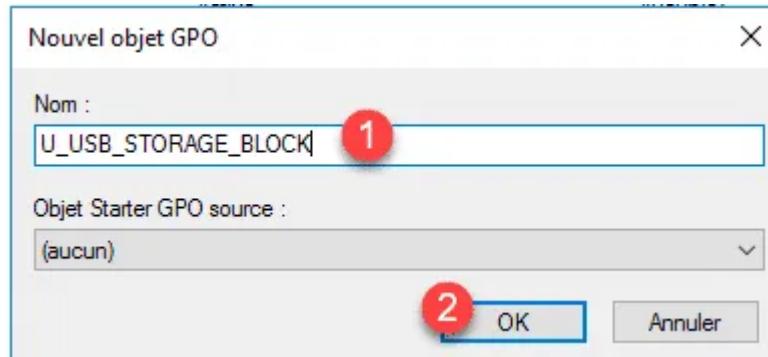
```
gpupdate /force
```

Créer une GPO (ici celle pour bloquer l'accès aux USB)

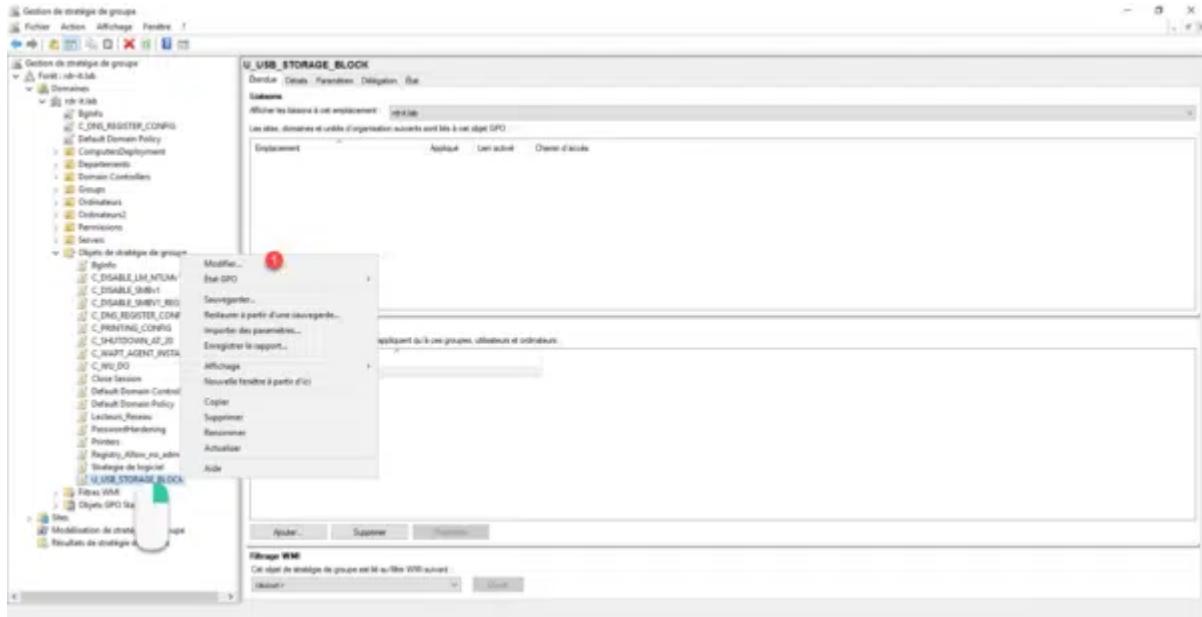
Ouvrir la console Gestion de stratégie de groupe, depuis la console, faire un clic sur Objets de stratégie de groupe et cliquer sur Nouveau 1.



Nommer 1 la stratégie de groupe et cliquer sur OK 2 pour créer l'objet.



Faire un clic droit sur l'objet stratégie de groupe que l'on vient de créer et cliquer sur Modifier 1.



Dans le tutoriel, je vais appliquer les paramètres au niveau de la configuration Utilisateur, pour accéder aux paramètres voici les emplacements :

- Configuration ordinateur : Stratégies / Modèles d'administration / Système / Accès au stockage amovible
- Configuration utilisateur : Stratégies / Modèles d'administration / Système / Accès au stockage amovible

| Paramètre | Etat | Commentaire |
|---|---------------|-------------|
| Définir la taille des records; avant de lancer le redémarrage | Non configuré | Non |
| CD et DVD : refuser l'accès en écriture | Non configuré | Non |
| CD et DVD : refuser l'accès en lecture | Non configuré | Non |
| CD et DVD : refuser l'accès en écriture | Non configuré | Non |
| Classe préinstallée : refuser l'accès en lecture | Non configuré | Non |
| Classe préinstallée : refuser l'accès en écriture | Non configuré | Non |
| Lecteur de disquette : refuser l'accès en écriture | Non configuré | Non |
| Lecteur de disquette : refuser l'accès en lecture | Non configuré | Non |
| Lecteur de disquette : refuser l'accès en lecture | Non configuré | Non |
| Disques amovibles : refuser l'accès en écriture | Non configuré | Non |
| Disques amovibles : refuser l'accès en lecture | Non configuré | Non |
| Disques amovibles : refuser l'accès en écriture | Non configuré | Non |
| Tous les clés de stockage amovible : refuser tous les accès | Non configuré | Non |
| Tous stockage amovible : permet l'accès direct pendant des | Non configuré | Non |
| Lecteurs de bandes : refuser l'accès en écriture | Non configuré | Non |
| Lecteurs de bandes : refuser l'accès en lecture | Non configuré | Non |
| Péphériques NWD : refuser l'accès en lecture | Non configuré | Non |
| Péphériques NWD : refuser l'accès en écriture | Non configuré | Non |

Ordinateur

| Paramètre | État | Commentaire |
|--|---------------|-------------|
| [x] Définir le délai (en secondes) avant de forcer le redémarrage | Non configuré | Non |
| [x] CD et DVD : refuser l'accès en lecture | Non configuré | Non |
| [x] CD et DVD : refuser l'accès en écriture | Non configuré | Non |
| [x] Classes personnalisées : refuser l'accès en écriture | Non configuré | Non |
| [x] Classes personnalisées : refuser l'accès en écriture | Non configuré | Non |
| [x] Lecteurs de disquettes : refuser l'accès en lecture | Non configuré | Non |
| [x] Lecteurs de disquettes : refuser l'accès en écriture | Non configuré | Non |
| [x] Disques amovibles : refuser l'accès en lecture | Non configuré | Non |
| [x] Disques amovibles : refuser l'accès en écriture | Non configuré | Non |
| [x] Toutes les classes de stockage amovible : refuser tous les accès | Non configuré | Non |
| [x] Lecteurs de bandes : refuser l'accès en lecture | Non configuré | Non |
| [x] Lecteurs de bandes : refuser l'accès en écriture | Non configuré | Non |
| [x] Périphériques WPD : refuser l'accès en lecture | Non configuré | Non |
| [x] Périphériques WPD : refuser l'accès en écriture | Non configuré | Non |

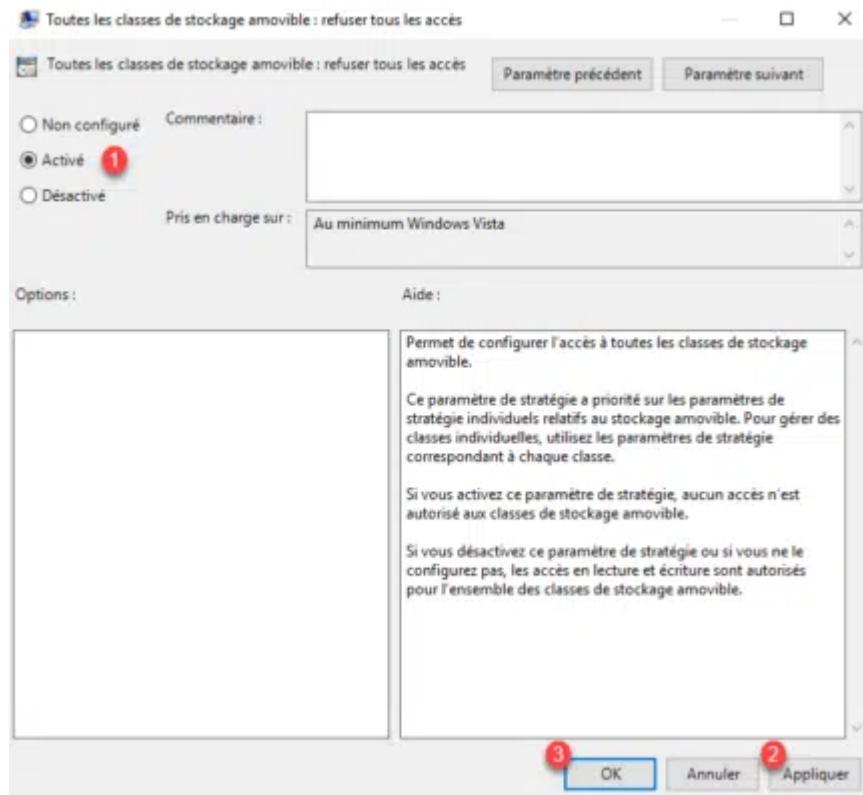
Utilisateur

Aller à l'emplacement en fonction de comment vous souhaitez appliquer la stratégie de groupe (GPO).

Faire un double clic sur le paramètres : Toutes les classes de stockage amovible : refuser tous les accès 1.

| Paramètre | État | Commentaire |
|--|-----------------|-------------|
| [x] Définir le délai (en secondes) avant de forcer le redémarrage | Non configuré | Non |
| [x] CD et DVD : refuser l'accès en lecture | Non configuré | Non |
| [x] CD et DVD : refuser l'accès en écriture | Non configuré | Non |
| [x] Classes personnalisées : refuser l'accès en écriture | Non configuré | Non |
| [x] Classes personnalisées : refuser l'accès en écriture | Non configuré | Non |
| [x] Lecteurs de disquettes : refuser l'accès en lecture | Non configuré | Non |
| [x] Lecteurs de disquettes : refuser l'accès en écriture | Non configuré | Non |
| [x] Disques amovibles : refuser l'accès en écriture | Non configuré | Non |
| [x] Toutes les classes de stockage amovible : refuser tous les accès | 1 Non configuré | Non |
| [x] Lecteurs de bandes : refuser l'accès en lecture | Non configuré | Non |
| [x] Lecteurs de bandes : refuser l'accès en écriture | Non configuré | Non |
| [x] Périphériques WPD : refuser l'accès en lecture | Non configuré | Non |
| [x] Périphériques WPD : refuser l'accès en écriture | Non configuré | Non |

Activer 1 la paramètre puis cliquer sur Appliquer 2 et OK 3.

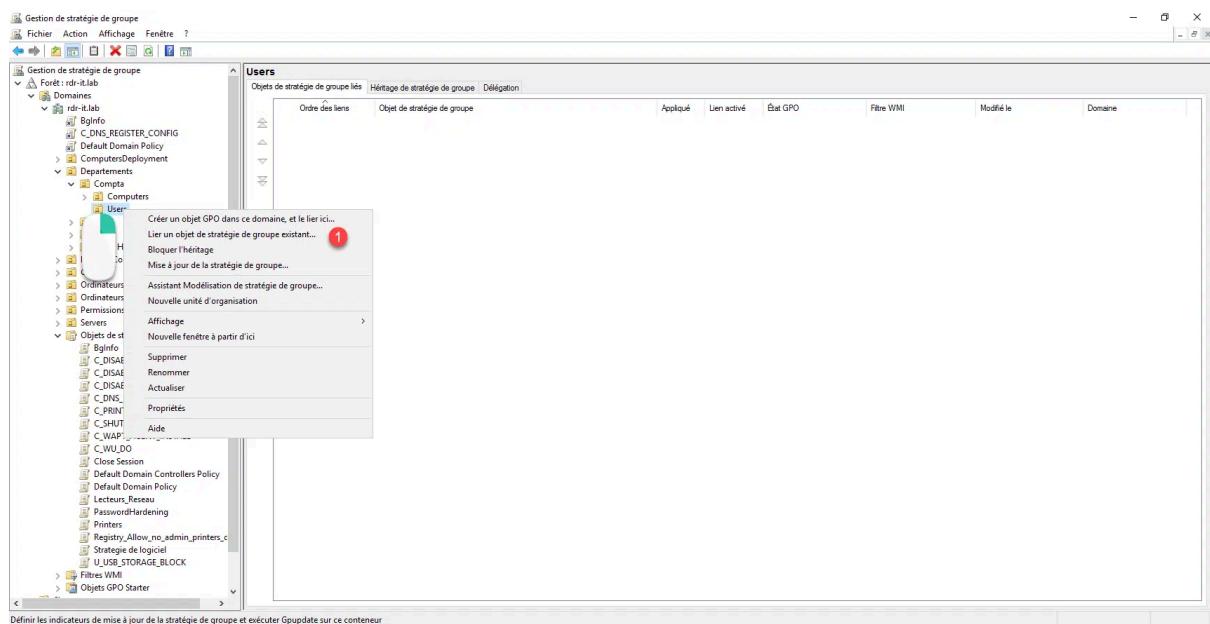


La stratégie de groupe est configurée, fermer l'éditeur de gestion des stratégies de groupe.

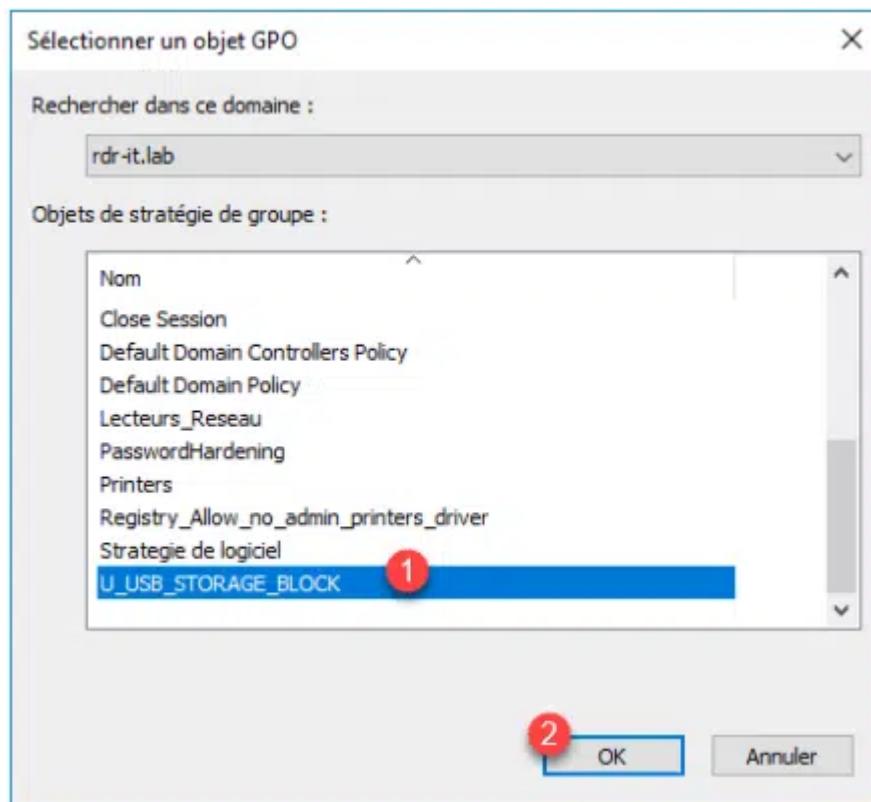
Pour appliquer notre GPO, nous allons maintenant lier l'objet pour qu'elle soit appliquée.

Dans l'exemple, je vais appliquer à l'OU Departements / Compta / Users afin que les utilisateurs qui se trouvent dedans ne puissent pas utiliser de stockage amovible.

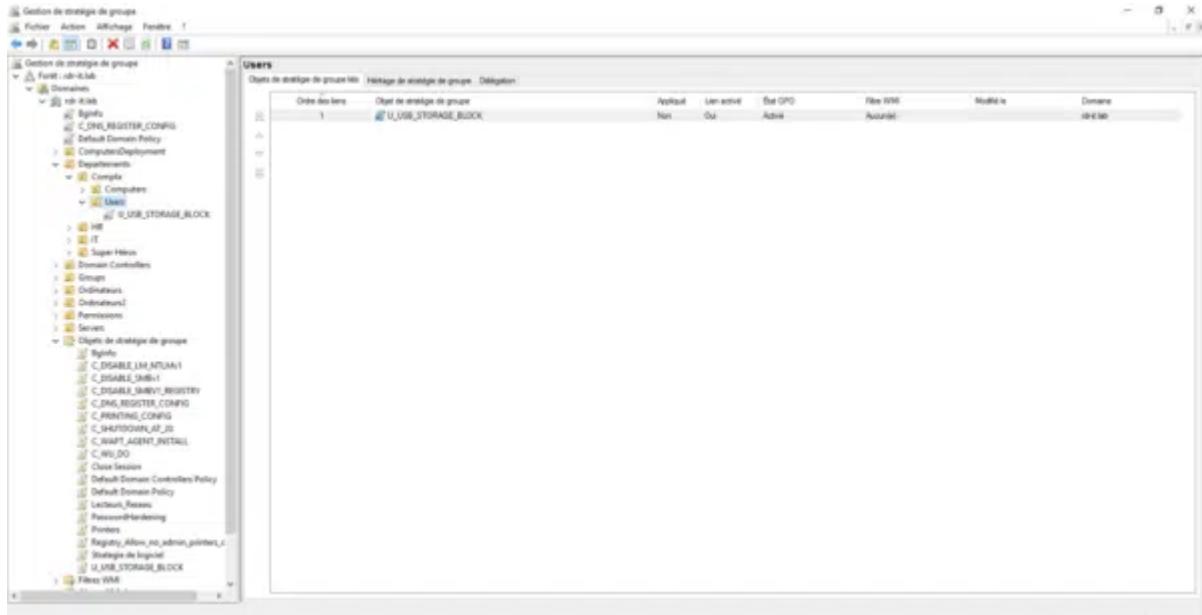
Faire un clic droit à l'emplacement souhaité et cliquer sur Lier un objet de stratégie de groupe existant 1.



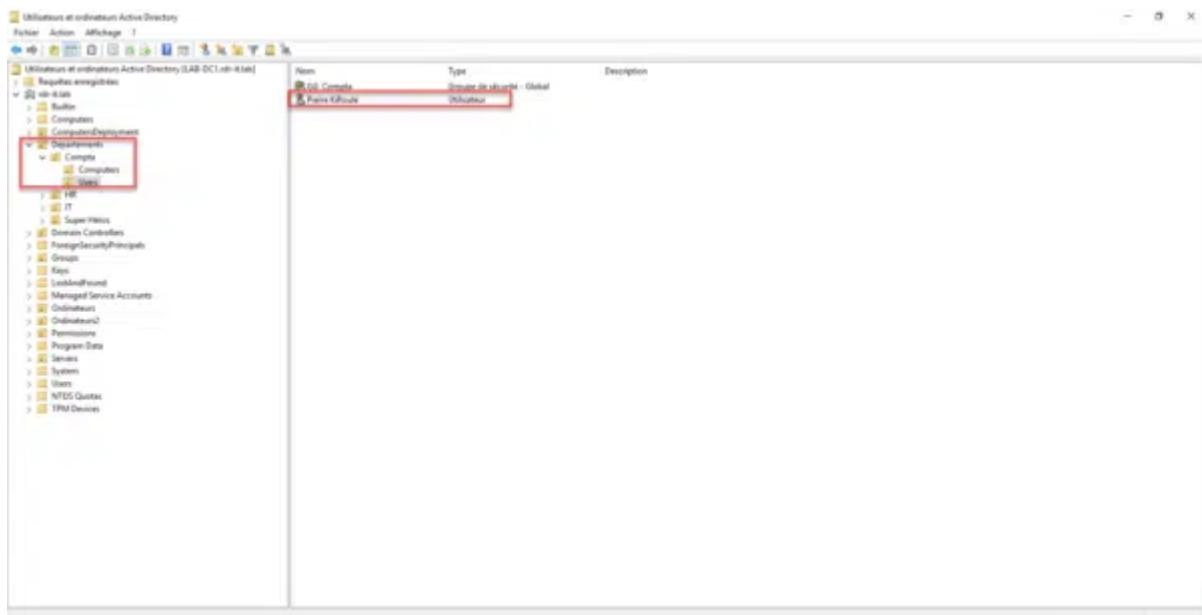
Sélectionner l'objet 1 et cliquer sur OK 2.



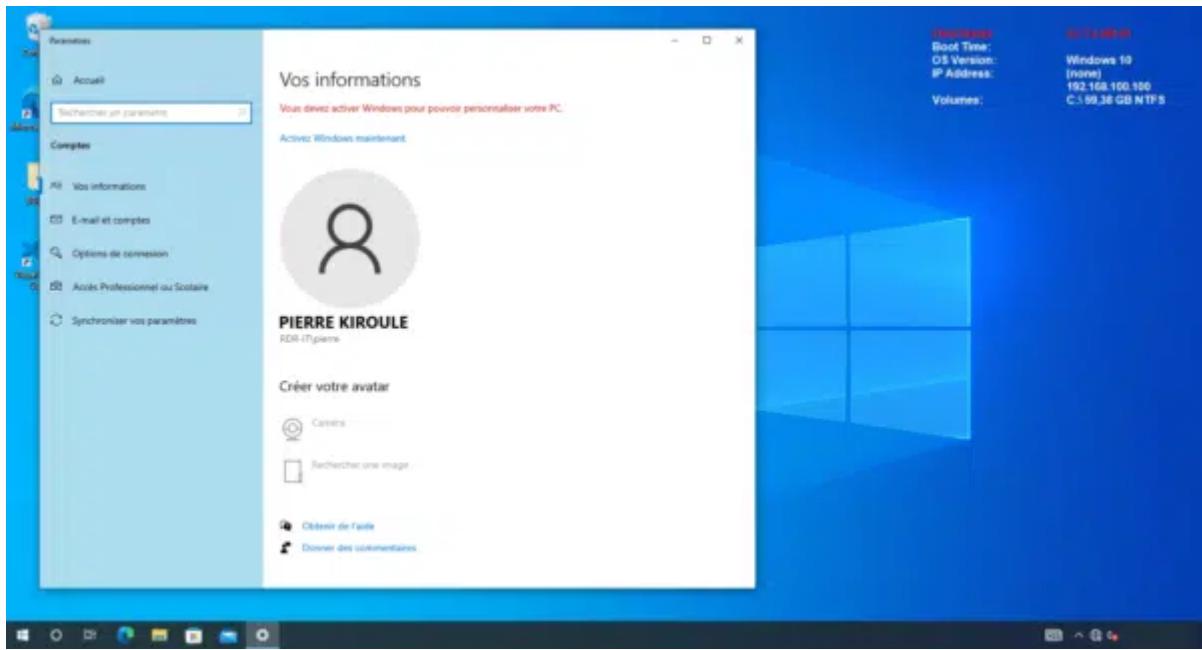
La GPO pour bloquer l'accès aux clés USB est lié à l'unité d'organisation.



Maintenant, on va tester la stratégie, pour cela je vais me connecter sur un ordinateur avec l'utilisateur Pierre KiRoule, qui se trouve dans l'OU Departements / Compta / Users.



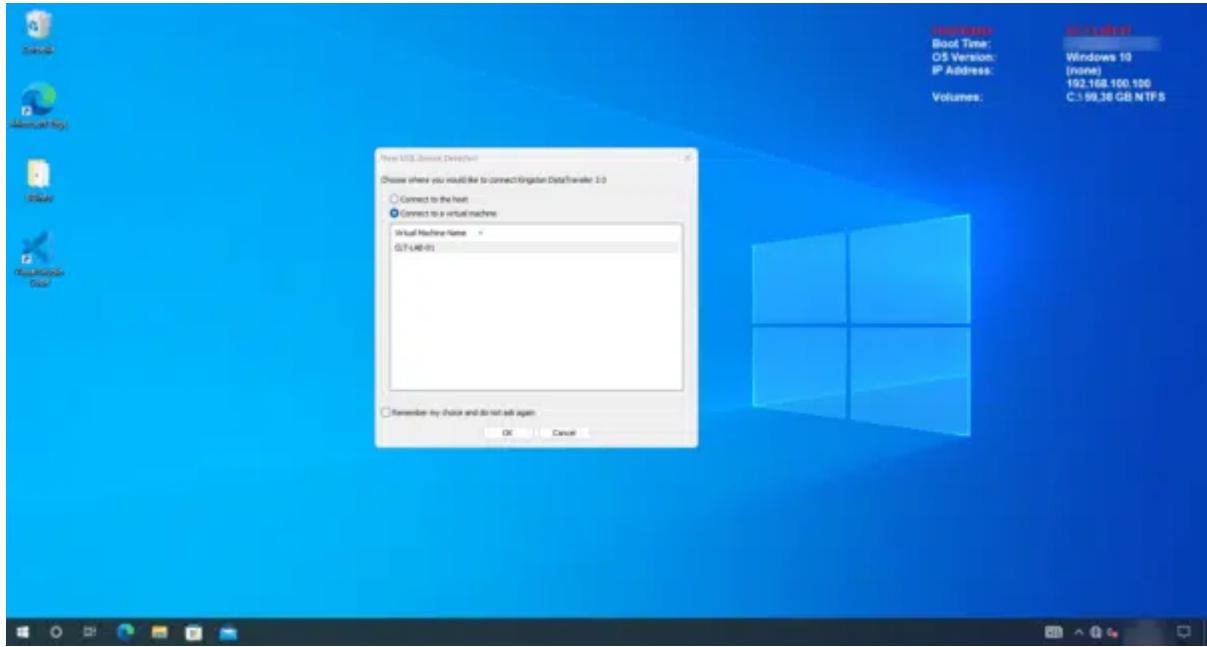
Comme vous pouvez le voir sur la capture ci-dessous, j'ai ouvert la session de Pierre KiRoule sur un ordinateur Windows 10.



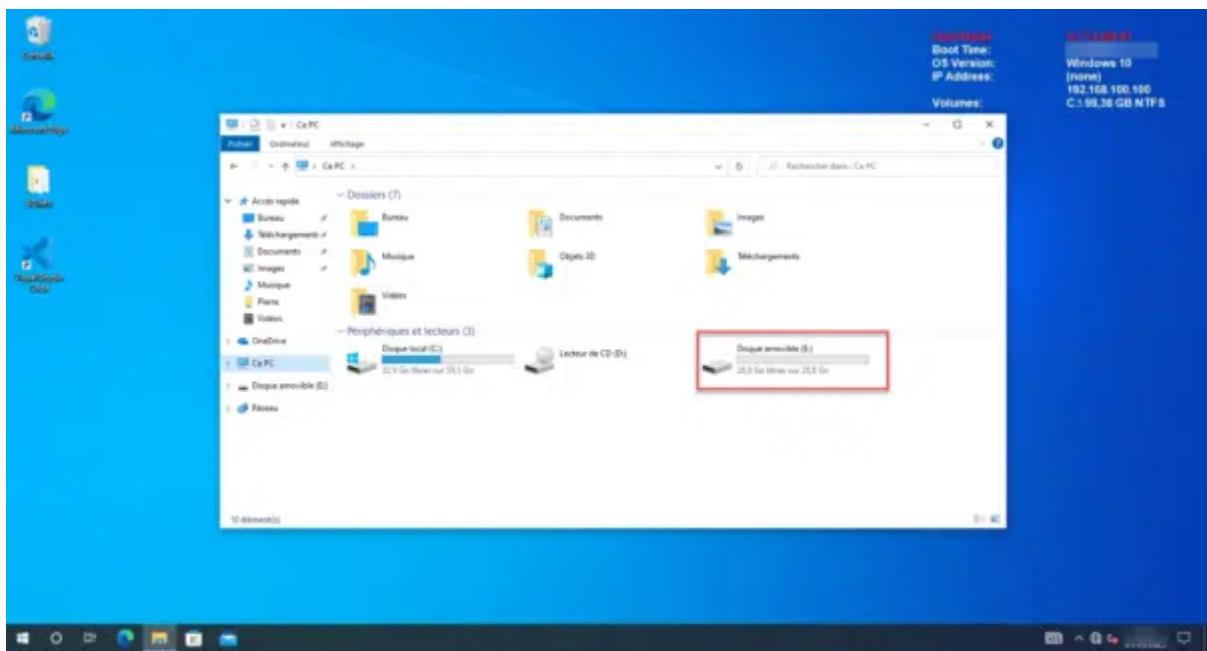
Pour m'assurer de la prise en compte de la stratégie de groupe, je vérifie avec la commande gprestult /r.

Comme on peut le voir sur la capture, la stratégie est bien appliquée.

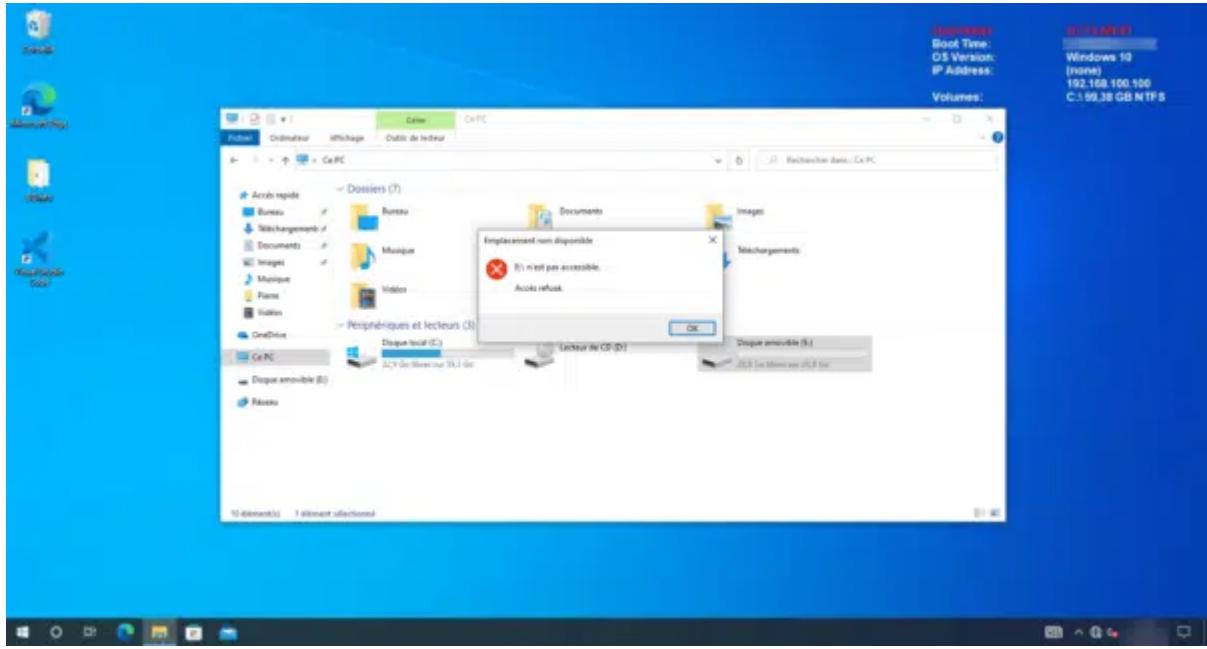
Je connecte une clé USB à ma machine.



Maintenant, on ouvre l'explorateur et on peut voir la clé USB.



Si on essaie de l'ouvrir, un message d'erreur s'affiche, indiquant : Accès refusé, la stratégie de groupe fonctionne.



Vous savez maintenant bloquer l'accès aux clés USB à l'aide d'une stratégie groupe.

GPO POUR MESSAGE DEBUT DE SESSION

Tutoriel GPO - Message pour les utilisateurs après connexion

Sur le contrôleur de domaine, ouvrez l'outil de gestion des stratégies de groupe.

Start



Search

Everywhere ▾

group Policy Management



Group Policy Management



Edit group policy



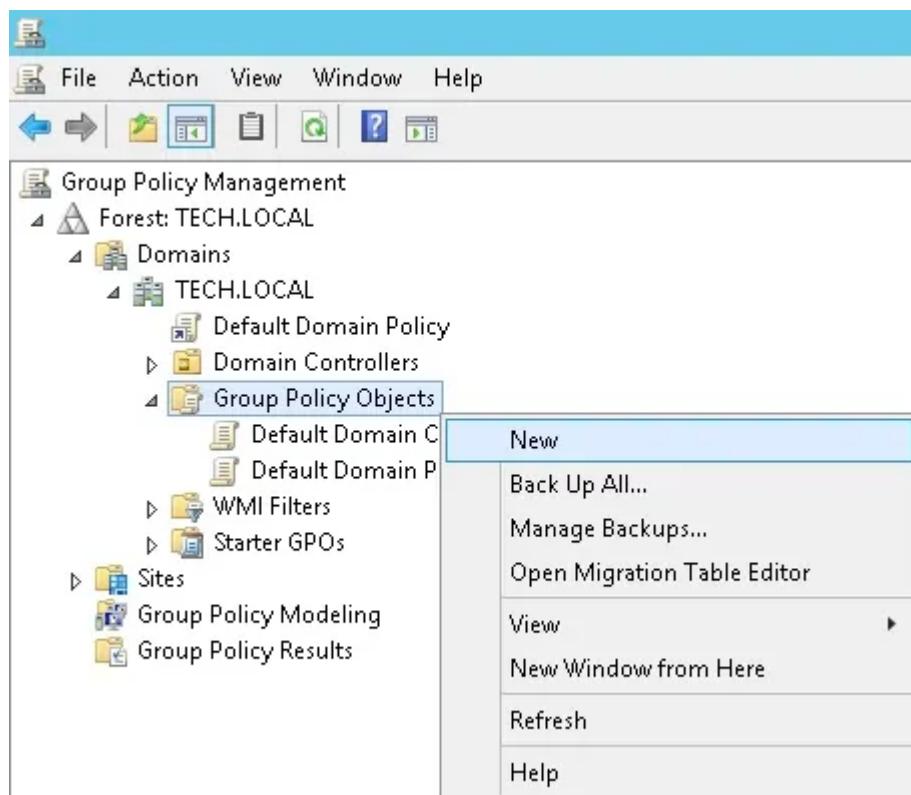
Edit local users and groups



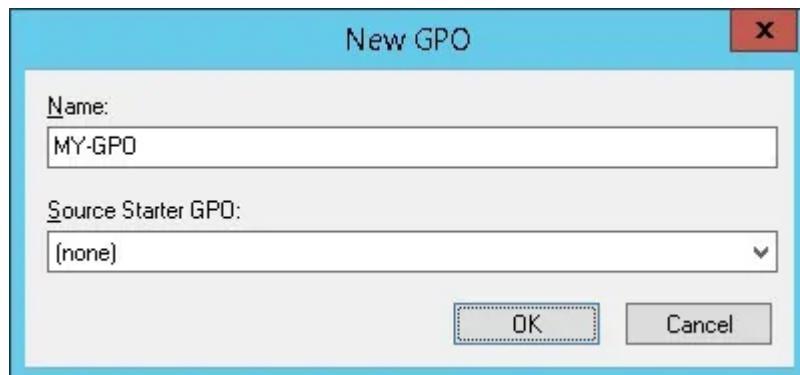
Group similar windows on the taskbar

group

Créez une stratégie de groupe.



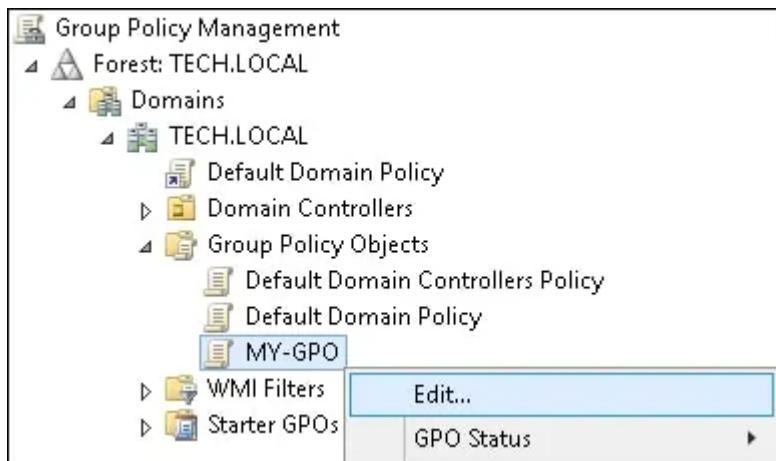
Entrez un nom pour la nouvelle stratégie de groupe.



Dans notre exemple, le nouveau GPO a été nommé : MY-GPO.

Dans l'écran Gestion des stratégies de groupe, développez le dossier nommé Objets de stratégie de groupe.

Cliquez avec le bouton droit sur votre nouvel objet stratégie de groupe et sélectionnez l'option Modifier.



Dans l'écran de l'éditeur de stratégies de groupe, développez le dossier de configuration de l'ordinateur et recherchez l'élément suivant.

Syntax Highlighter

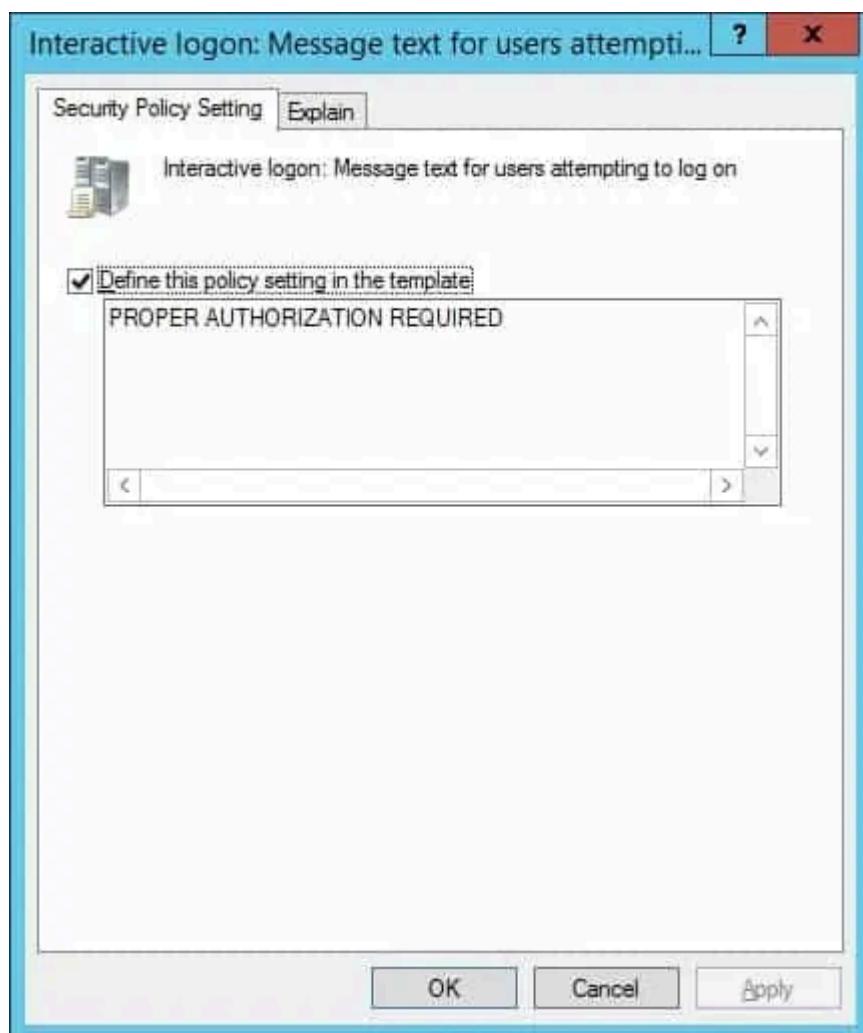
```
Computer Configuration > Policies > Windows Settings > Security Settings >  
Local Policies > Security Options
```

Accédez au dossier nommé Options de sécurité.



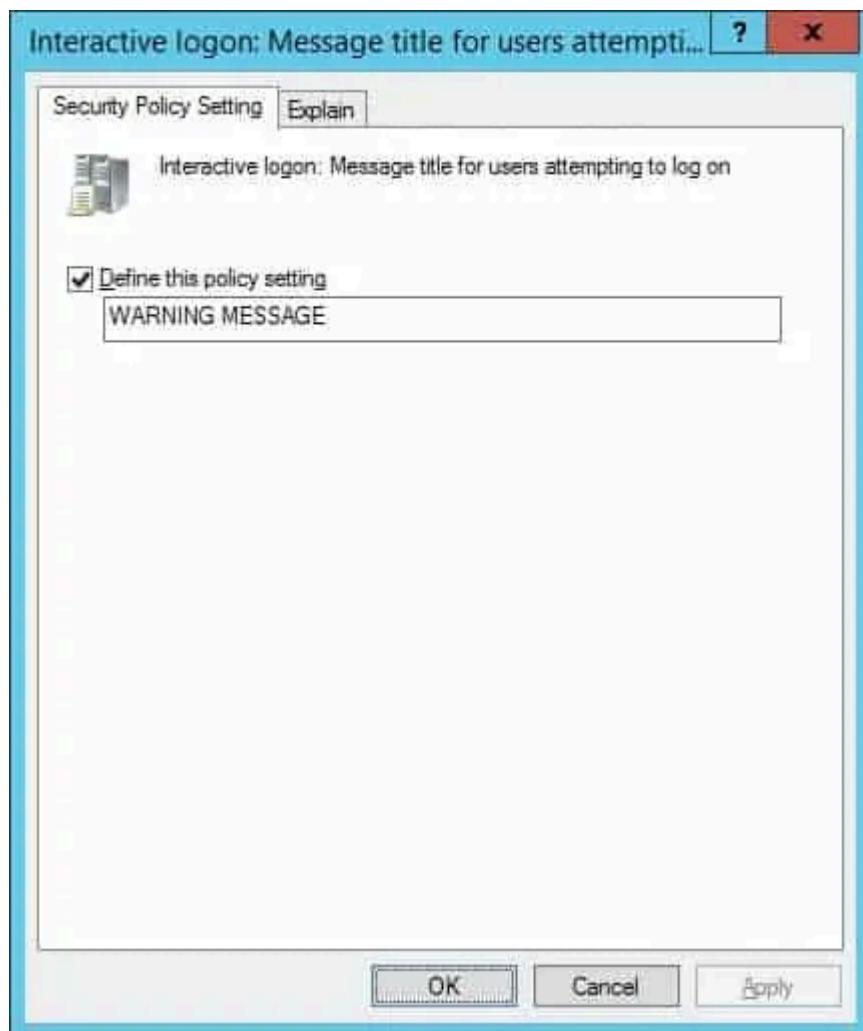
Activez l'élément suivant et configurez le texte du message souhaité.

- Ouverture de session interactive : texte de message pour les utilisateurs qui tentent de se connecter.



Activez l'élément suivant et configurez le titre du message souhaité.

- Ouverture de session interactive : titre du message pour les utilisateurs qui tentent de se connecter.

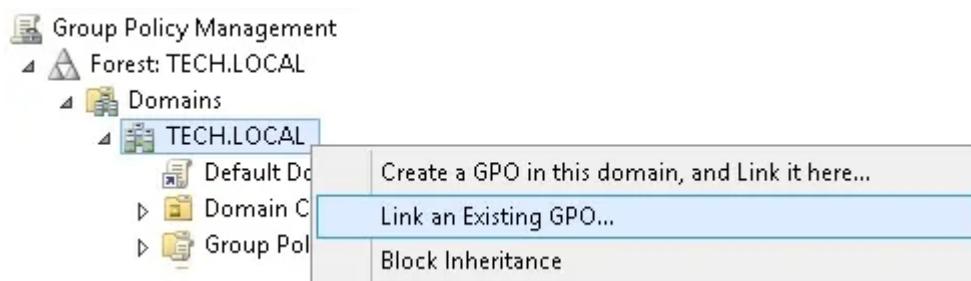


Pour enregistrer la configuration de stratégie de groupe, vous devez fermer l'éditeur de stratégie de groupe.

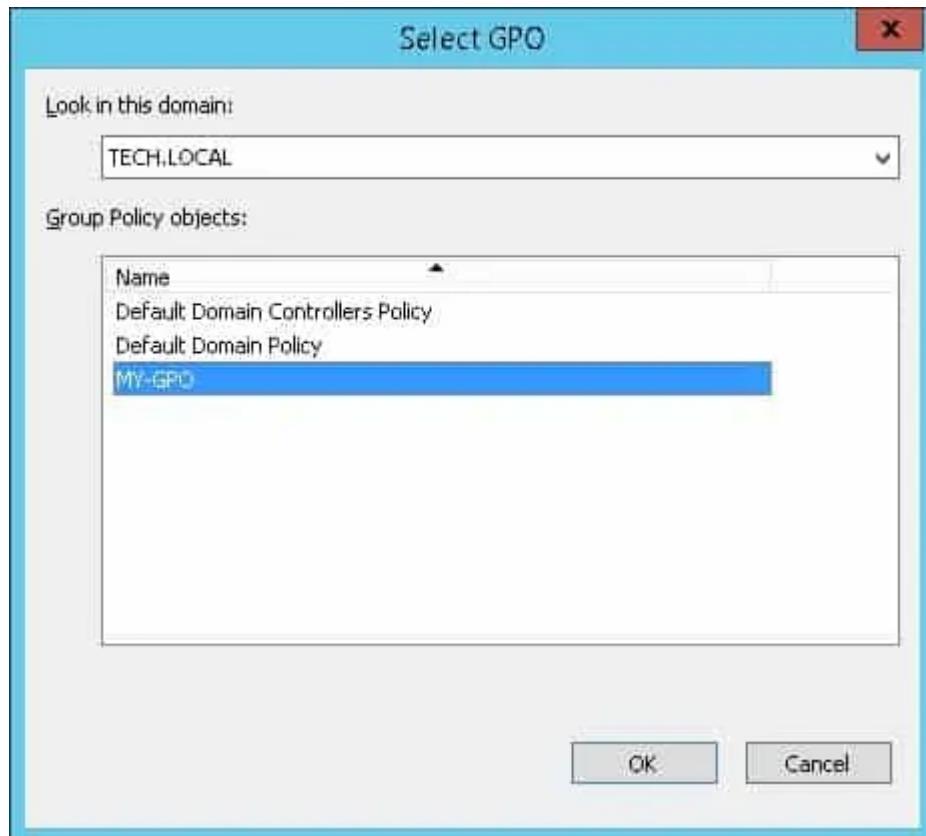
Félicitations! Vous avez terminé la création de GPO.

Tutoriel GPO - Afficher un message texte pour les utilisateurs après la connexion

Dans l'écran Gestion des stratégies de groupe, vous devez cliquer avec le bouton droit sur l'unité organisationnelle souhaitée et sélectionner l'option pour lier un objet de stratégie de groupe existant.



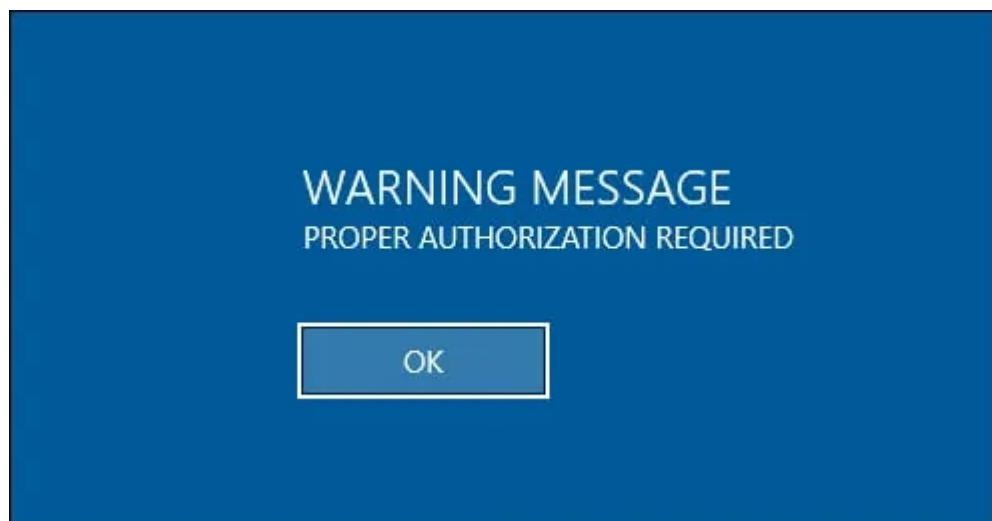
Dans notre exemple, nous allons lier la stratégie de groupe nommée MY-GPO à la racine du domaine.



Après l'application de l'objet, vous devez attendre 10 ou 20 minutes.

Pendant ce temps, le GPO sera répliqué à d'autres contrôleurs de domaine.

Sur un ordinateur distant, connectez-vous et vérifiez le message d'alerte affiché.



Dans notre exemple, nous ajoutons une bannière d'ouverture de session à l'aide de GPO.

DFS

Installer sur le serveur

gerer -> roles de serveurs -> services de fichiers et de stockage -> espaces de noms DFS

II. Les types de racines DFS

Il existe deux types de racines DFS : "Racine autonome" et "Racine de noms de domaine". Une racine DFS est également appelée un espace de noms. Voici des explications pour bien comprendre la différence.

- Racine autonome (Espace de noms autonome)

Une racine autonome est associée à un seul serveur d'espace de noms. Cela signifie qu'il ne peut pas y avoir plusieurs serveurs d'espace de noms pour assurer l'accès à son contenu, et donc il n'y a pas de haute disponibilité. Néanmoins, il est tout à fait possible d'avoir plusieurs serveurs de fichiers pour chaque cible.



Voici un exemple de chemin d'accès vers une racine autonome :

\\\srv-adds-01.it-connect.local\Partages

- Racine de noms de domaine (Espace de noms de domaine)

Une racine de noms de domaine s'appuie sur le nom de domaine Active Directory et la résolution DNS pour fonctionner. Ainsi, le nom du serveur DFS n'est pas repris dans le chemin UNC puisqu'il est remplacé par le nom de domaine. Ainsi, il est possible d'avoir plusieurs serveurs d'espace de noms (serveurs DFS) pour une même racine de noms de domaine.

Voici un exemple de chemin d'accès vers une racine de noms de domaine :

\\\it-connect.local\Partages

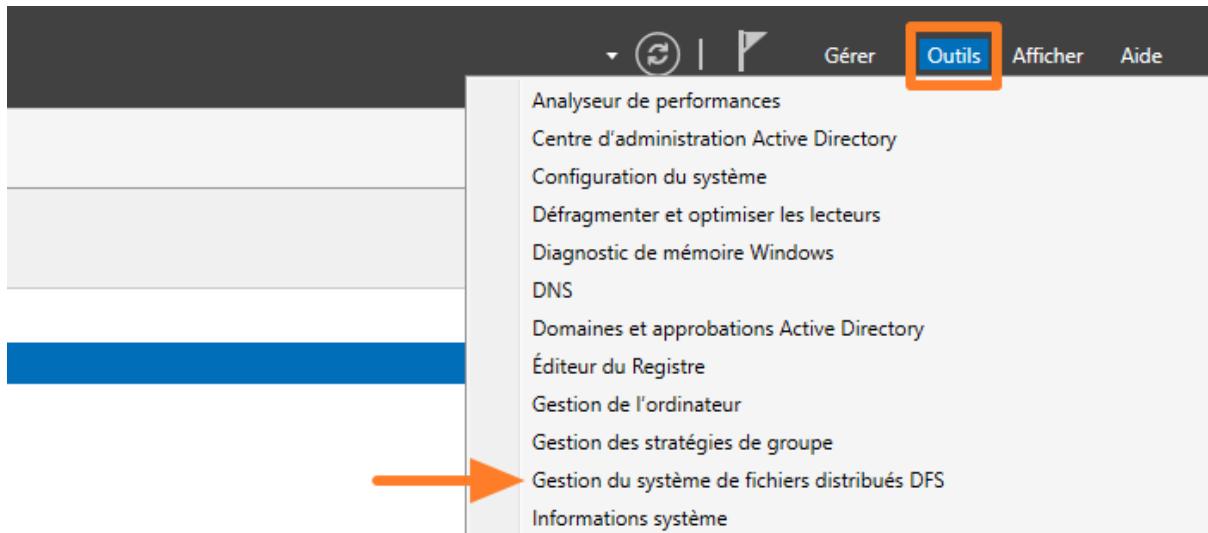
Dans la suite de ce tutoriel, nous mettrons en œuvre une racine DFS de noms de domaine. Entre les deux types de racines, la configuration est identique. C'est uniquement un choix différent qui est effectué lors de la création de la racine DFS.

III. Créer une racine DFS : espace de noms de domaine

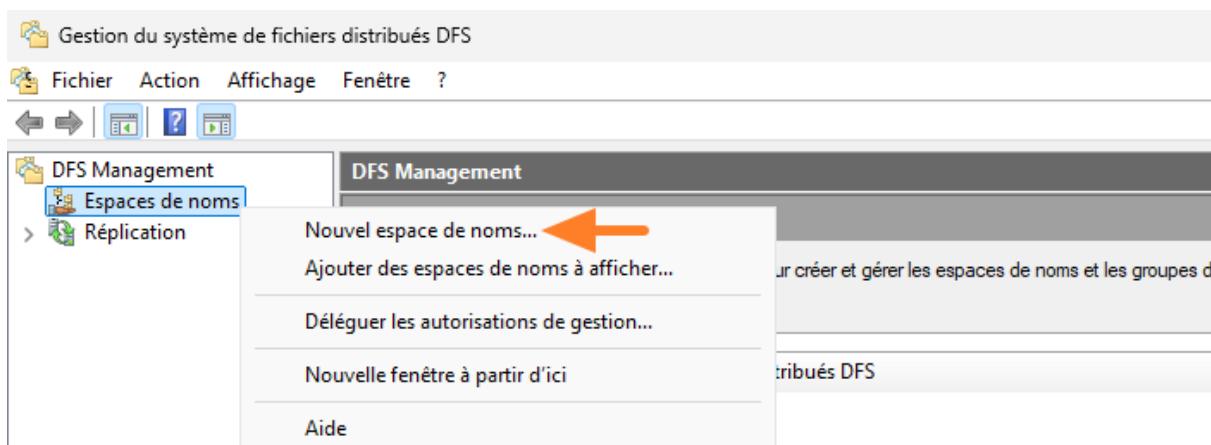


Désormais, nous allons créer notre racine DFS en prenant le soin de choisir le type "Espace de noms de domaine". Il est à noter que les racines de ce type sont inscrites dans l'annuaire Active Directory.

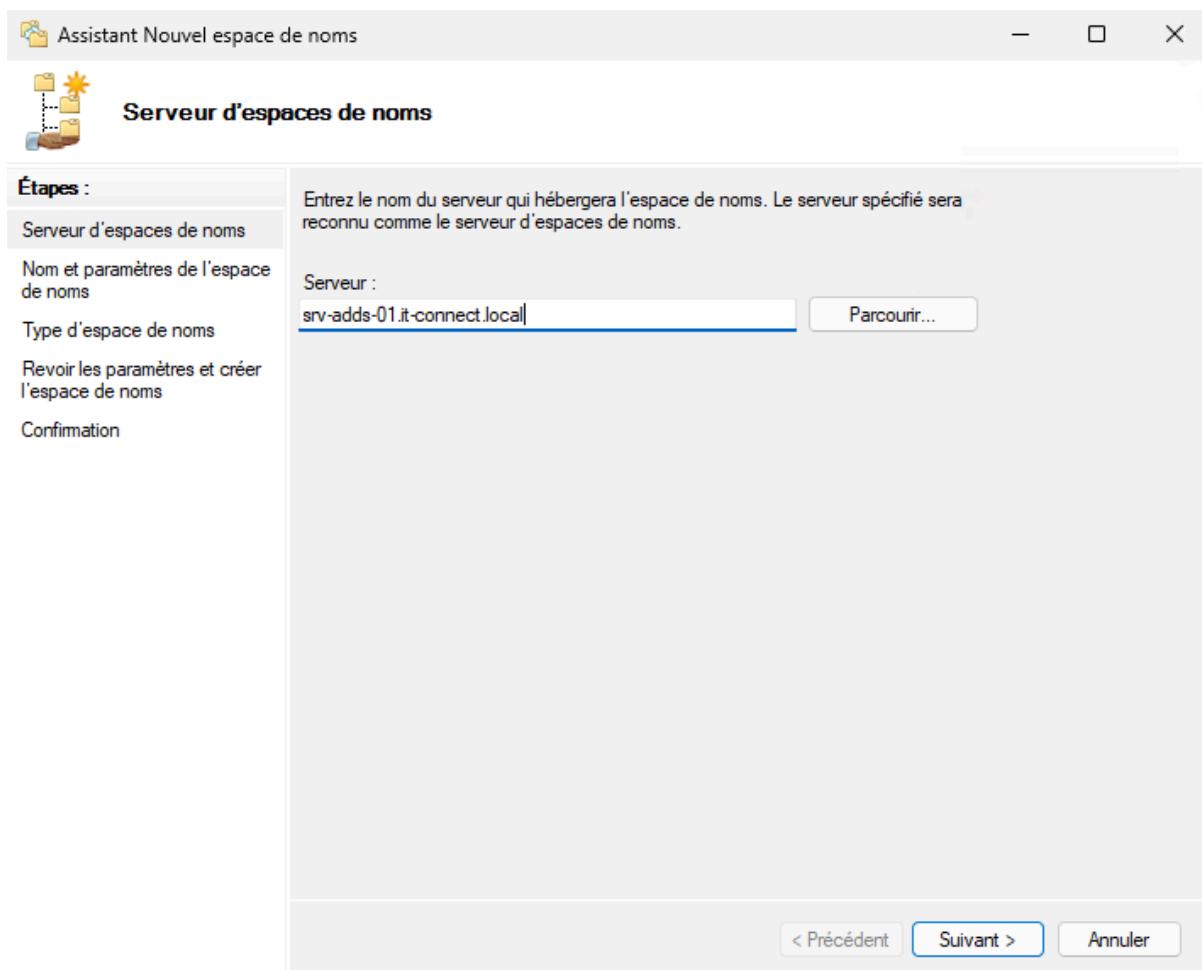
Ouvrez le Gestionnaire de serveur, cliquez sur « Outils » puis ouvrez la console « Gestion du système de fichiers distribués DFS ».



Effectuez un clic droit sur « Espaces de noms » et « Nouvel espace de noms... ».

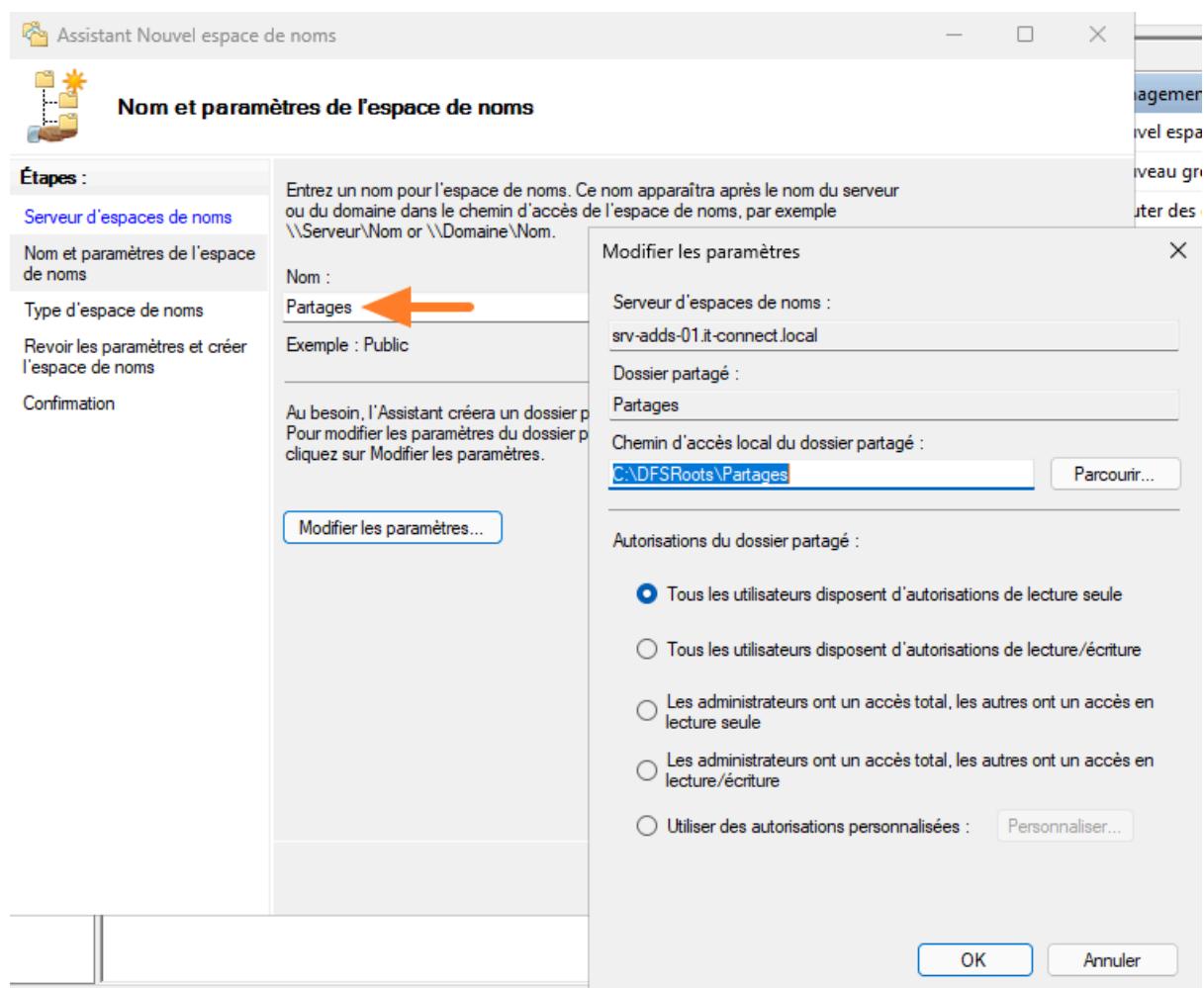


Commencez par indiquer le serveur d'espaces de noms qui hébergera cette nouvelle racine DFS. Vous devez spécifier le nom du serveur où le rôle DFS a été installé, donc "SRV-ADDS-01.it-connect.local". Vous pouvez écrire le nom manuellement ou cliquer sur le bouton « Parcourir... » pour rechercher le serveur. Ensuite, cliquez sur « Suivant » une fois la sélection effectuée.



Indiquez "Partages" comme nom de racine. Ensuite, cliquez sur le bouton « Modifier les paramètres » afin de voir quels sont les paramètres disponibles. Ici, vous avez la possibilité de définir les droits d'accès sur cette racine. Par défaut, tous les utilisateurs (comprenez utilisateurs lambdas et administrateurs) ont un accès en lecture seule.

Vous pouvez adapter ce comportement si besoin, ce qui ne vous empêchera pas de gérer les droits pour les sous-répertoires de cette racine. Enfin, validez en cliquant sur « OK » puis sur « Suivant ».



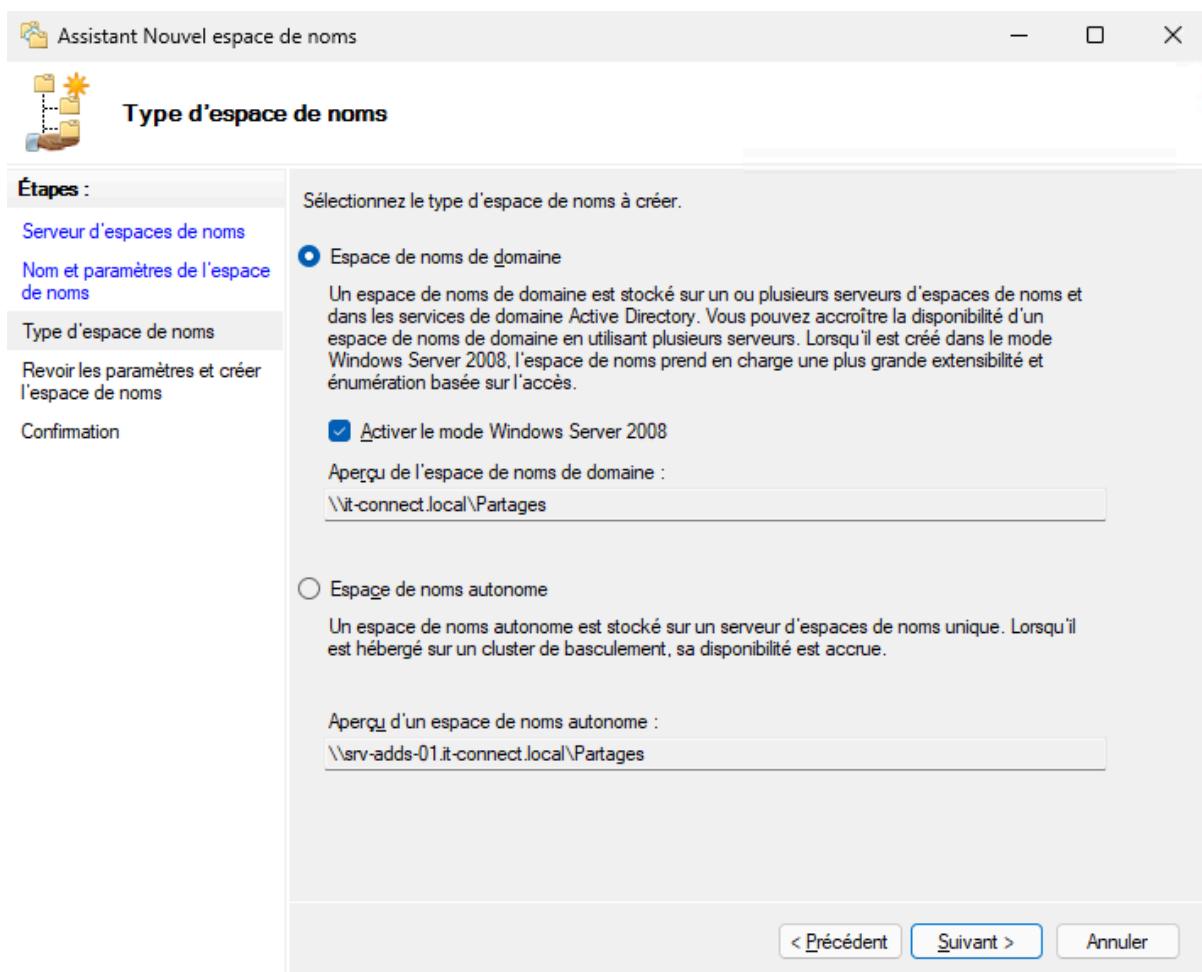
Cette fois-ci, sélectionnez la valeur « Espace de noms de domaine ». Il est recommandé de conserver cochée l'option "Activer le mode Windows Server 2008". Il permet de bénéficier de quelques fonctions supplémentaires, dont l'énumération basée sur l'accès (ABE – Access Based Enumeration).

Les prérequis pour utiliser ce mode, bien qu'existant, sont légers :

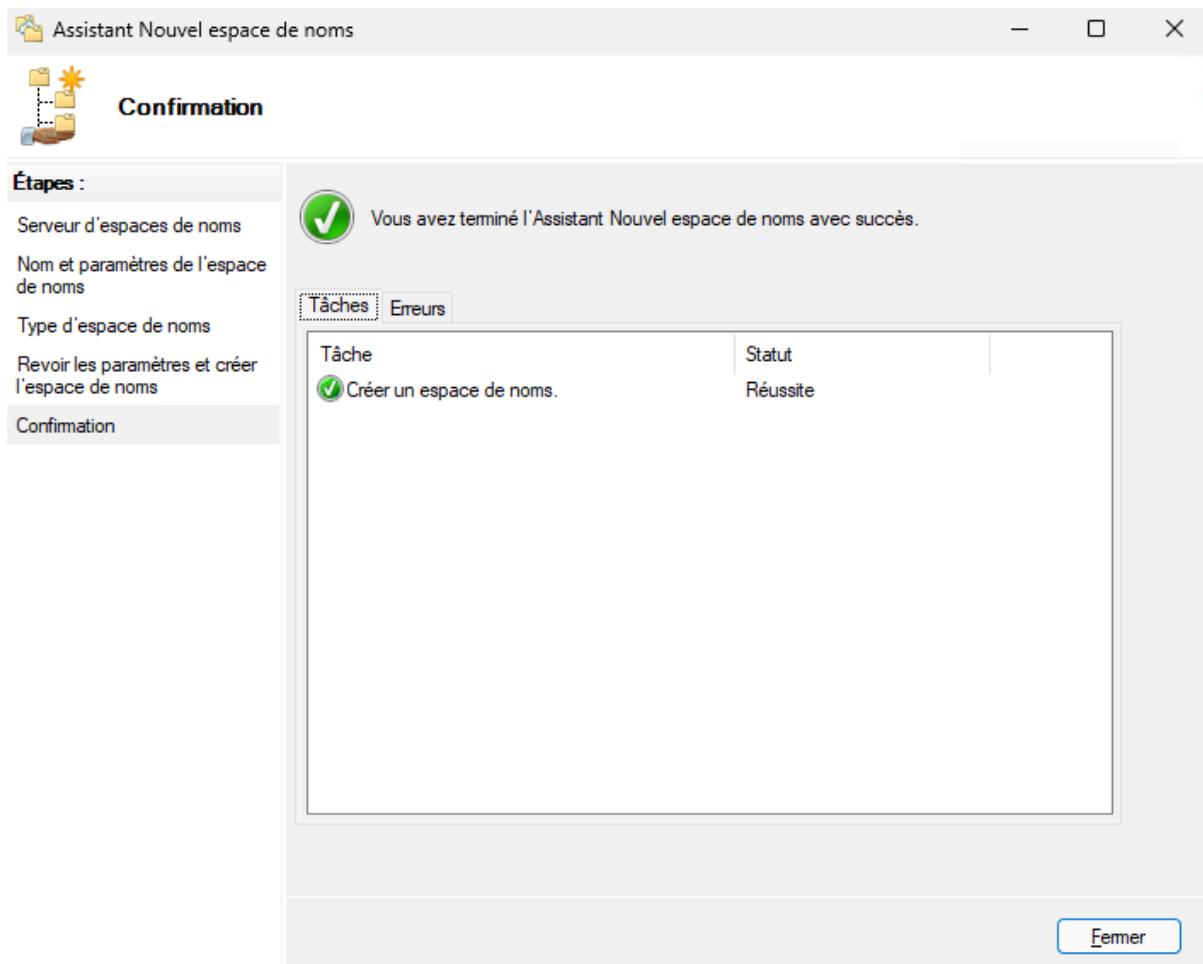
- Niveau fonctionnel de la forêt en Windows Server 2003 (minimum)
- Niveau fonctionnel du domaine en Windows Server 2008 (minimum)
- Les serveurs DFS exécutent Windows Server 2008 (minimum)

Si ces prérequis ne sont pas valables dans votre cas, l'option sera grisée et ne pourra pas être activée.

Cliquez sur « Suivant » pour continuer.



La fenêtre de résumé apparaît, cliquez sur « Créer » pour créer la racine DFS. Patientez un instant, jusqu'à obtenir le message de validation de la création. Cliquez sur « Fermer ».



Étant donné que notre racine DFS s'appuie sur la résolution DNS pour fonctionner, nous utiliserons le nom de domaine dans le chemin UNC. Ainsi, pour accéder à la racine de l'espace de noms DFS, le chemin réseau sera :

\\\it-connect.local\Partages

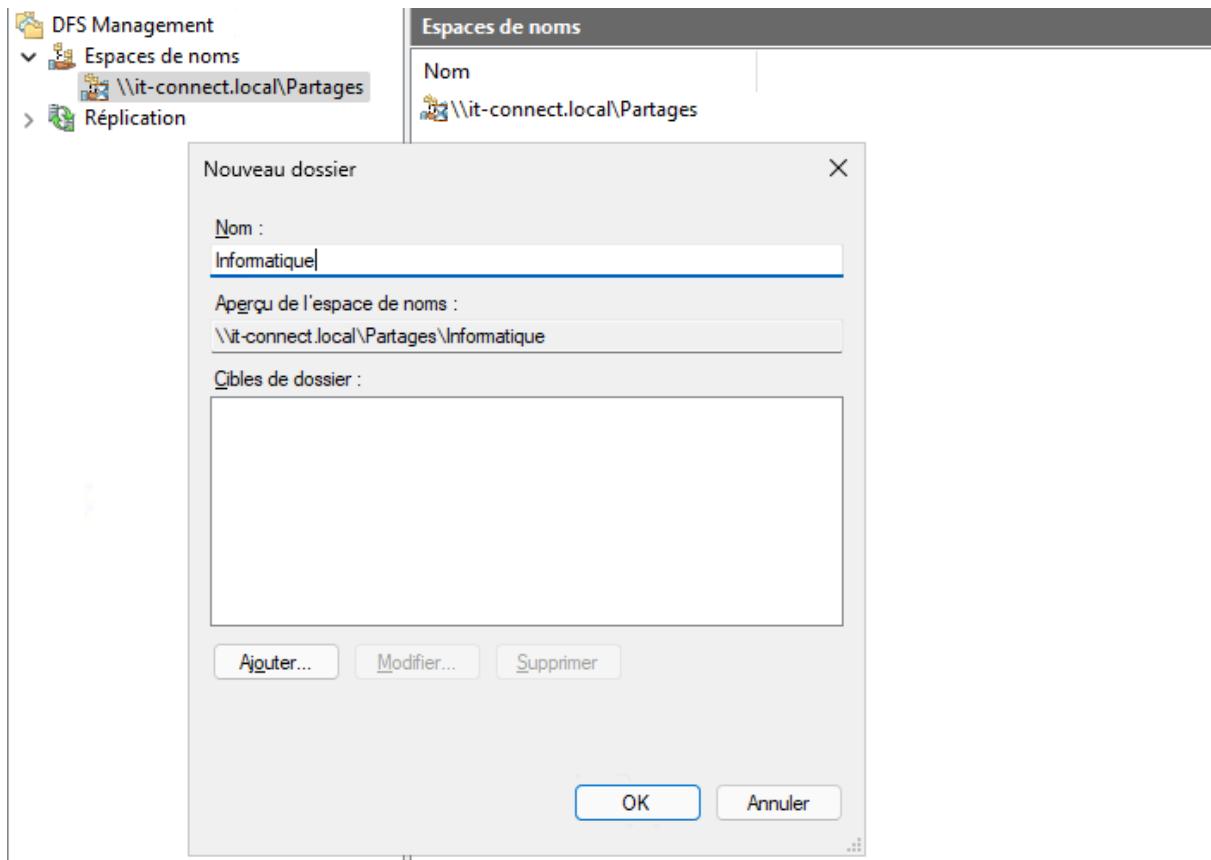
IV. Crée l'arborescence de dossiers DFS



Afin de créer un dossier – également appelé « liaison DFS », suivez la procédure suivante. Pour information, la création d'une liaison DFS est identique que ce soit pour une racine autonome ou une racine espace de noms de domaine.

Dans la console « Gestion du système de fichiers distribués DFS », effectuez un clic droit sur la racine DFS que nous avons créé précédemment. Cliquez sur « Nouveau

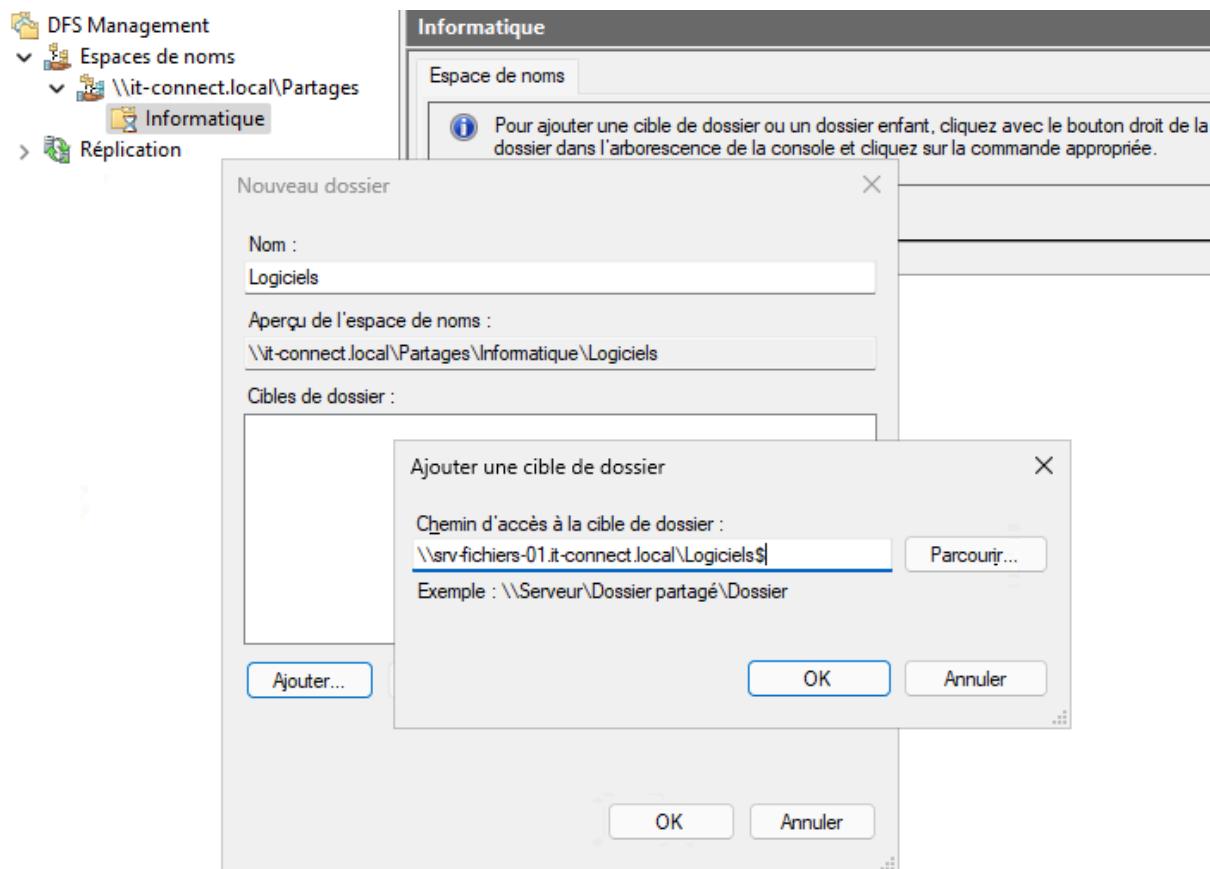
dossier ». Nommez ce dossier "Informatique" puis validez avec le bouton "OK". Ce dossier, d'après notre schéma initial, sert uniquement à organiser l'espace de noms, donc il n'a pas de cible.



Répétez l'opération, via un clic droit sur "Informatique", puis "Nouveau dossier". Cette fois-ci, nommez le dossier "Logiciels" et cliquez sur le bouton "Ajouter" car vous allez devoir déclarer une nouvelle cible.

Dans cet exemple, le partage est hébergé sur le serveur "SRV-FICHIERS-01.it-connect.local" et il se nomme "Logiciels\$". Si vous avez besoin d'aide pour la mise en place de ce partage, consultez ces articles :

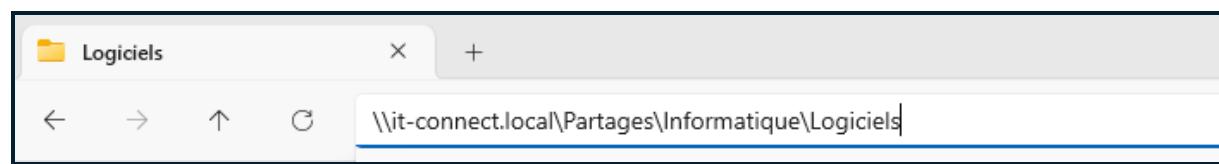
- [Comment créer son premier partage SMB sur Windows Server ?](#)
- [Comment configurer les permissions NTFS et de partage ?](#)



Remarque : Il est préférable de créer auparavant le dossier partagé sur le serveur cible auparavant, même si la création est possible depuis le serveur DFS (si vous cliquez sur le bouton "Parcourir").

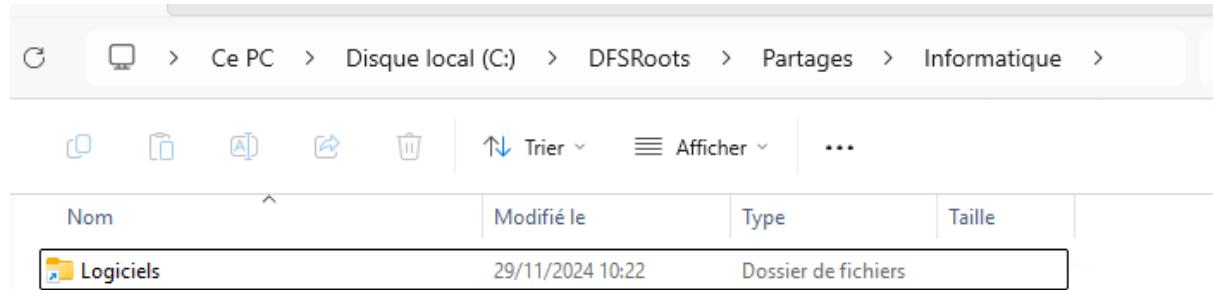
Validez. Désormais, vous pouvez accéder à votre cible "Logiciels" via ce chemin UNC :

`\\\it-connect.local\Partages\Informatique\Logiciels\`



Quand vous accédez au contenu de "Logiciels" et que vous déposez ou consultez des fichiers, vous travaillez en réalité sur l'espace de stockage "\\\it-connect.local\Logiciels\$", de façon transparente.

Il est à noter que sur un serveur DNS, l'arborescence est créée sur le volume "C" dans un répertoire nommé "DFSRoots". Il ne contient aucune donnée, mais il sert à créer l'arborescence de dossiers telle qu'elle est créée dans la console DFS.



V. L'énumération basée sur l'accès avec DFS

L'énumération basée sur l'accès (ABE) est une fonctionnalité très intéressante, car elle permet de montrer à l'utilisateur uniquement les dossiers auxquels il a le droit d'accéder, à minima en lecture seule. Autrement dit, si un utilisateur n'a pas les permissions sur un dossier, il ne le verra pas dans son Explorateur de fichiers.

Dans le cadre de l'utilisation de DFS, vous pouvez activer l'énumération basée sur l'accès dans les propriétés du partage étant référencé comme cible.

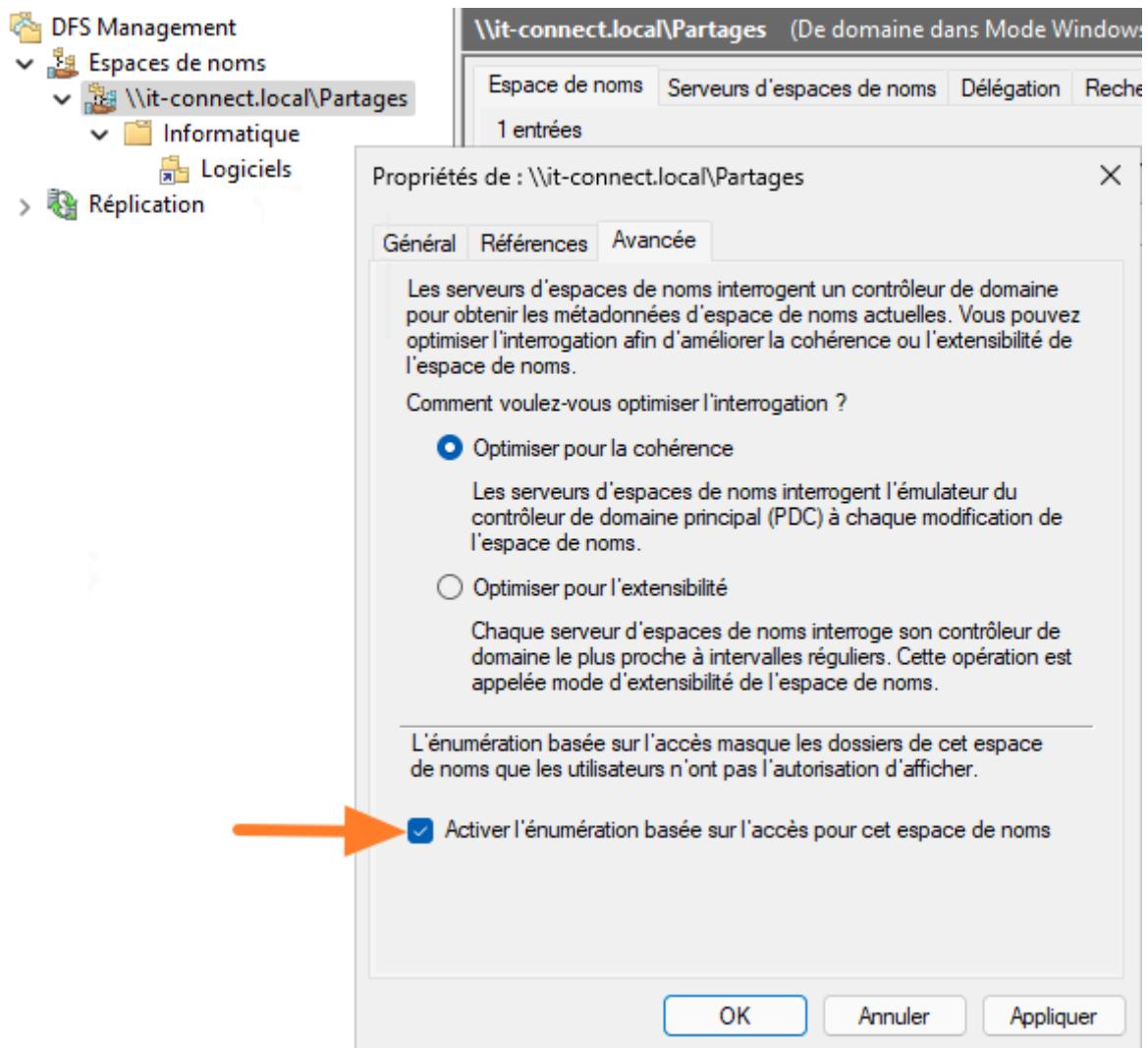
The screenshot shows the Windows File Explorer Properties dialog for a share named "Logiciels\$". The top navigation bar includes tabs for "Partager", "Chemin d'accès local", "Protocole", and "Type de disponibilité". The "Protocole" tab is selected, showing "SMB" and "Non-cluster". The main content area displays the share name "Logiciels\$" and its path "P:\Logiciels\$". A sub-dialog titled "Logiciels\$" is open, showing the "Paramètres" (Parameters) section. The "Paramètres" tab is selected in the left sidebar. The right pane contains several checkboxes:

- Activer l'énumération basée sur l'accès
- Autoriser la mise en cache du partage
- Activer le cache de filiale (BranchCache) sur le partage de fichiers
- Chiffrer l'accès aux données

Below the checkboxes, descriptive text explains each option.



De plus, vous pouvez accéder aux propriétés de l'espace de noms pour activer cette option dans les paramètres. Effectuez un clic droit sur "\it-connect.local\Partages", puis cliquez sur "Propriétés". Ensuite, cliquez sur l'onglet "Avancée" et activez l'option "Activer l'énumération basée sur l'accès pour cet espace de noms".

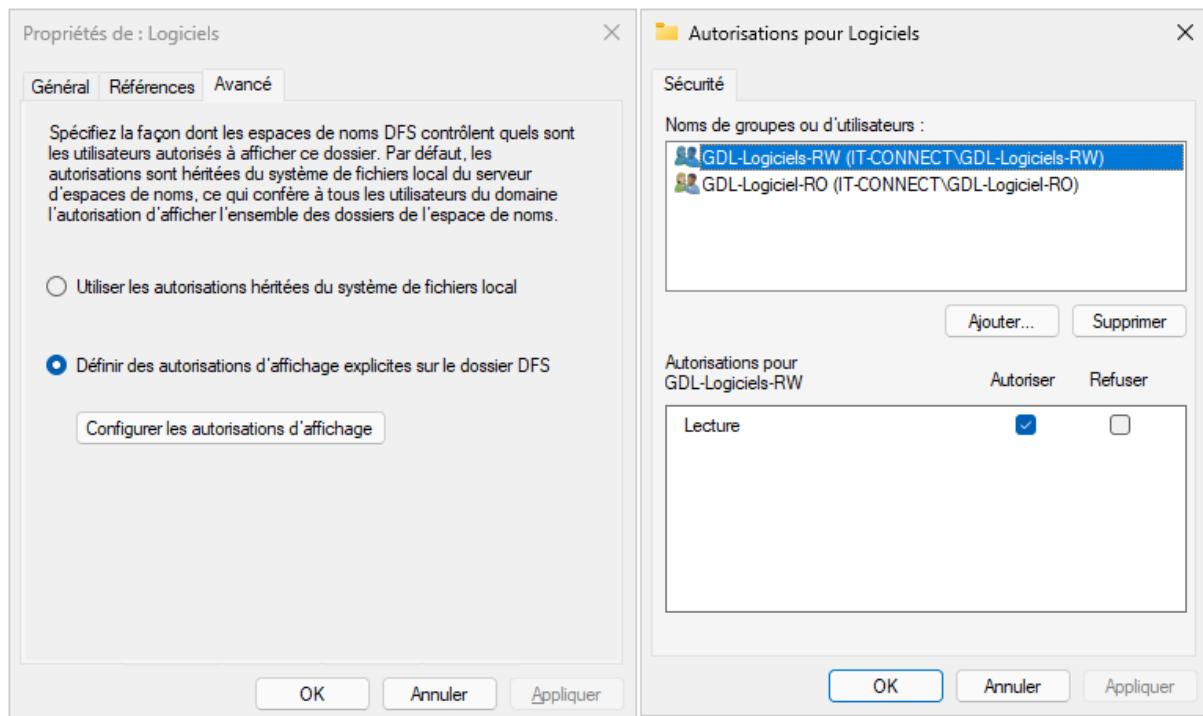


Validez.

Désormais, nous allons évoquer les permissions d'affichage du dossier "Logiciels" présent dans notre racine DFS. Ceci est une notion importante pour gérer l'afficher des dossiers (en lien avec l'ABE), sans être dépendant des permissions sur le système de fichiers local.

Effectuez un clic droit sur "Logiciels" puis choisissez "Propriétés" et basculez sur l'onglet "Avancé". Ici, vous pouvez cocher l'option "Définir des autorisations d'affichage explicites sur le dossier DFS" et cliquer sur le bouton juste en dessous. Vous n'avez plus qu'à ajouter les groupes d'utilisateurs qui ont accès à ce dossier dans votre racine DFS : il n'y a qu'eux qui pourront le voir.

Ici, j'ajoute les deux groupes de sécurité créés conformément à la bonne pratique de gestion des permissions AGDLP. Il conviendra également de définir les permissions NTFS et de partage au niveau du partage "Logiciels\$" situé sur le serveur de fichiers (cible).



Vous pouvez valider.

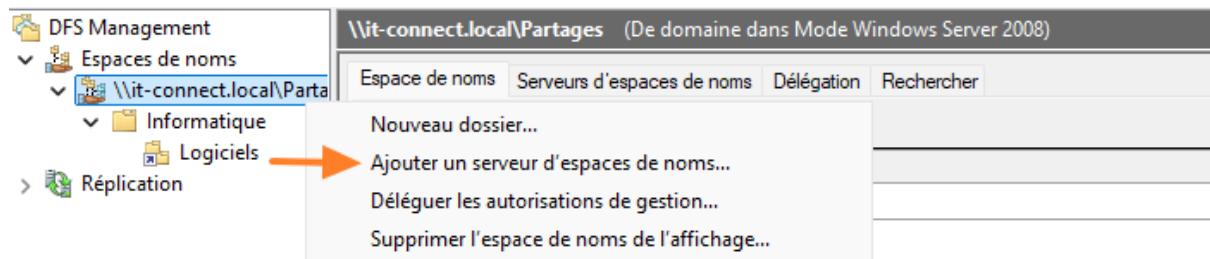
VI. Ajouter un serveur d'espaces de noms supplémentaire

Dans le cadre d'une racine d'espace de noms, il est possible d'ajouter plusieurs serveurs DFS. Cela permettra, pour une même racine DFS, d'utiliser plusieurs serveurs, et ainsi d'assurer la redondance et la haute disponibilité du service. C'est un bon moyen de pérenniser la mise en place du DFS.

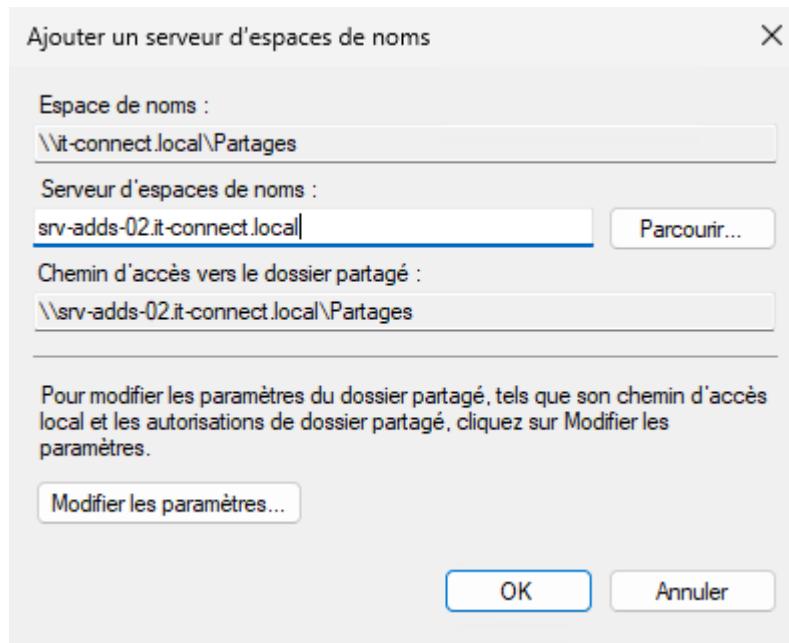
Vous devez commencer par installer le rôle « Espaces de nom DFS » sur le second serveur. Dans cet exemple, il s'agira du serveur "SRV-ADDS-02.it-connect.local". Pour rappel, l'installation peut être effectuée via PowerShell, sinon utilisez l'interface graphique.

Install-WindowsFeature FS-DFS-Namespace -IncludeManagementTools

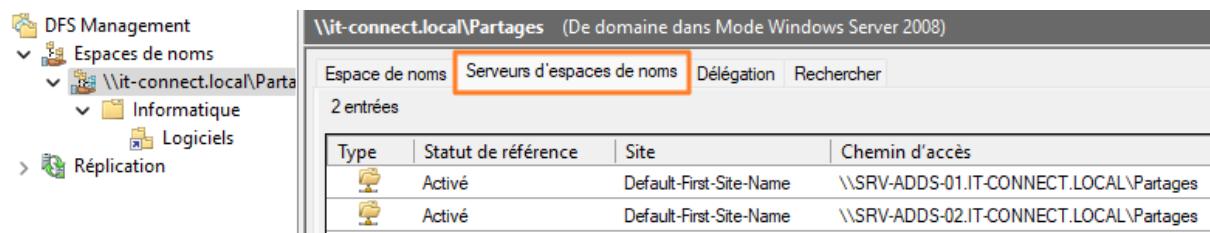
Quand c'est fait, ouvrez la console DFS. Effectuez un clic droit sur la racine DFS créée précédemment et cliquez sur « Ajouter un serveur d'espaces de noms ».



Une fenêtre s'ouvre à l'écran. Saisissez le nom du second serveur DFS ou cliquez sur « Parcourir » afin de rechercher le serveur dans l'annuaire Active Directory. Validez.



Vous trouverez ce serveur supplémentaire dans l'onglet « Serveurs d'espaces de noms » en sélectionnant la racine DFS dans l'arborescence sur la gauche. Désormais, la racine DFS "Partages" est hébergée par 2 serveurs d'espaces de noms.



Si un serveur est hors service, le second permettra toujours d'accéder à la racine DFS.
De plus, si vous avez une infrastructure répartie sur plusieurs sites, vous pouvez faire en sorte que le client Windows sollicite le serveur DFS de son site pour accéder aux ressources (cela s'appuie sur les sites Active Directory).

Serveur web

II. Comment installer Netplan sur Debian ?

Sur Ubuntu, Netplan est installé par défaut puisqu'il sert à gérer le réseau. Sur Debian, notamment Debian 12, ce n'est pas le cas. Pour installer Netplan, voici les commandes à exécuter :

```
sudo apt-get update
```

```
sudo apt-get install netplan.io
```

Pour mettre en place des configurations réseau complexes avec Netplan, Open vSwitch doit être installé sur la machine. Il n'est pas utile pour configurer une adresse IP statique sur une ou plusieurs interfaces, ou simplement pour configurer une interface en DHCP.

III. Configuration réseau avec Netplan

Sur Ubuntu, la configuration réseau se fait principalement via Netplan pour les versions récentes. Nous allons modifier le fichier de configuration Netplan pour définir notre adresse IP statique.

Ouvrez un terminal et exéutez la commande suivante pour éditer le fichier de configuration (sous Debian, ce fichier doit être créé) :

```
sudo nano /etc/netplan/01-network-manager-all.yaml
```

Ajoutez les lignes indiquées ci-dessous dans le fichier pour configurer votre adresse IP statique.

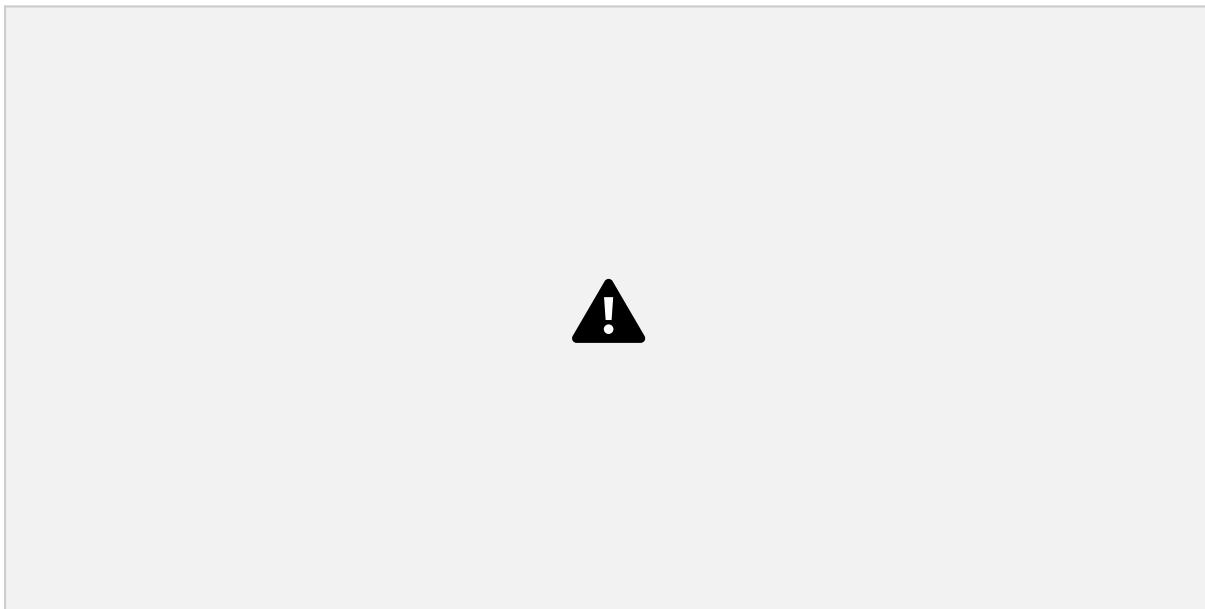
Ceci va permettre de configurer l'interface réseau "ens33" avec l'adresse IP statique "192.168.14.130/24", la passerelle par défaut "192.168.14.2", les serveurs DNS "1.1.1.1" et "9.9.9.9" et le domaine de recherche "it-connect.local". Nous voyons bien que ce fichier de configuration utilise le format YAML.

L'instruction "renderer" sert à indiquer le nom du backend à utiliser pour configurer le réseau, soit NetworkManager, soit "networkd" de Systemclt.

```
network:  
    version: 2  
    renderer: NetworkManager  
  
    ethernets:  
        ens33:  
            dhcp4: no  
            addresses:  
                - 192.168.14.130/24  
            routes:  
                - to: default  
                  via: 192.168.14.2  
            nameservers:  
                addresses:  
                    - 1.1.1.1  
                    - 9.9.9.9  
            search:
```

- it-connect.local

Voici un aperçu en image :



Quand c'est fait, enregistrez et fermez ce fichier.

Note : sur Debian, continuez d'utiliser le fichier "/etc/resolv.conf" pour gérer le DNS, car Netplan semble récupérer les informations dans ce fichier, malgré la déclaration des DNS dans le fichier YAML. Si vous savez comment déléguer la gestion du DNS à Netplan, je suis preneur de l'information.

Puis, nous allons modifier les permissions sur ce fichier de configuration. Sinon, Netplan renverra l'avertissement "Permissions for /etc/netplan/01-network-manager-all.yaml are too open. Netplan configuration should NOT be accessible by others." au moment d'appliquer la configuration (ceci n'empêche pas la configuration de s'appliquer).

Voici la commande à exécuter :

`sudo chmod 600 /etc/netplan/01-network-manager-all.yaml`

IV. Appliquer la configuration Netplan

Désormais, nous devons appliquer les changements pour qu'ils prennent effet. Utilisez les commandes suivantes pour générer la configuration et l'appliquer auprès du gestionnaire de réseau du système :

`sudo netplan generate`

`sudo netplan apply`

Cette commande reconfigure toutes les interfaces réseau mentionnées dans le fichier de configuration. Si tout est correct, votre interface réseau utilisera maintenant l'adresse IP statique que vous avez définie. Sinon, un message d'erreur est susceptible d'être retourné dans la console.

Sachez que vous pouvez tester la configuration avant de l'appliquer :

`sudo netplan try`

V. Comment vérifier la configuration ?

Pour afficher et vérifier votre nouvelle configuration réseau, vous pouvez utiliser les options spécifiques de Netplan, à la place de la traditionnelle commande "ip a". Voici plusieurs commandes pour afficher la configuration complète ou celle d'une carte réseau spécifique.

`sudo netplan get`

`sudo netplan status ens33`

`sudo netplan status --all`

Voici un aperçu du résultat obtenu. Nous pouvons constater que l'interface "ens33" est bien gérée par Netplan par l'intermédiaire de NetworkManager.



L'alternative, ce serait d'utiliser "*ip address*" comme ceci :

`ip a show ens33`

Si la configuration n'est pas correcte, essayez le mode debug lors de l'application de la nouvelle configuration :

`sudo netplan --debug apply`