

# Mise en place d'un AD sur Windows Server 2016 & d'un serveur DNS



Dans cette documentation nous irons configurer une image server 2016 vierge pour y ajouter AD et un serveur DNS.

Cette documentation est réalisée dans le cadre d'un TP guidé, il peut donc y avoir d'autre méthode plus ou moins simple pour y parvenir. Pour mieux s'y retrouver cette documentation disposera de plusieurs screenshots illustrant les consignes.

Prenez note que lorsque **[SERVER]** apparait c'est que les manipulations sont à faire côté serveur, quand **[CLIENT]** apparait c'est que les manipulations sont à faire côté client.

A vos serveurs !

## Préambule

Nous considérons que vous êtes équipé de cette manière :

1. Une VM sous Windows Serveur 2k16 [SERVER]
2. Une VM sous Windows 10 20H2 [CLIENT]

Les allocations de matériel (CPU/RAM...) sont à allouer selon vos envies, attention à respecter la configuration minimale.

Rappel des IPs pour l'identité Valentin DEROUET :

1. [SERVER] : **172.16.3.131**
2. [CLIENT] : **172.16.3.130**

Mot de passe par défaut : **Not24get**

Rappel des deux commandes essentiels :

1. `ncpa.cpl` (ouverture du panel "Connexion réseau")
2. `sysdm.cpl` (ouverture du panel "Gestion de l'ordinateur")

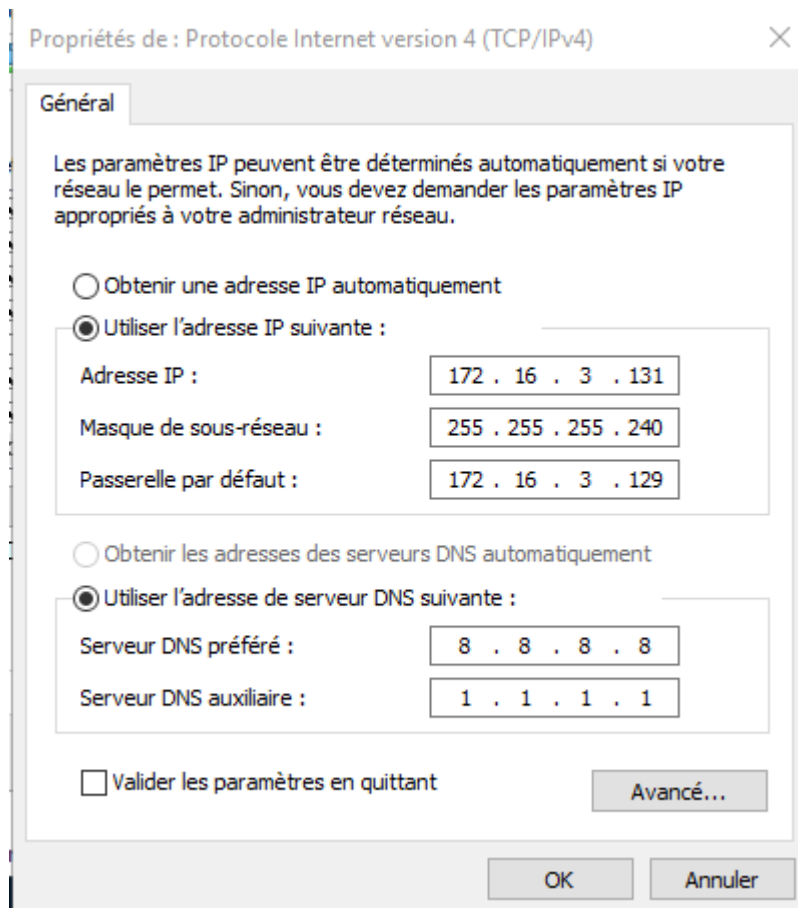
**Conseil :** Ajouter les deux machines dans un logiciel tel que mRemoteNG pour faciliter l'administration.

# Premier démarrage du [SERVER] & du [CLIENT]

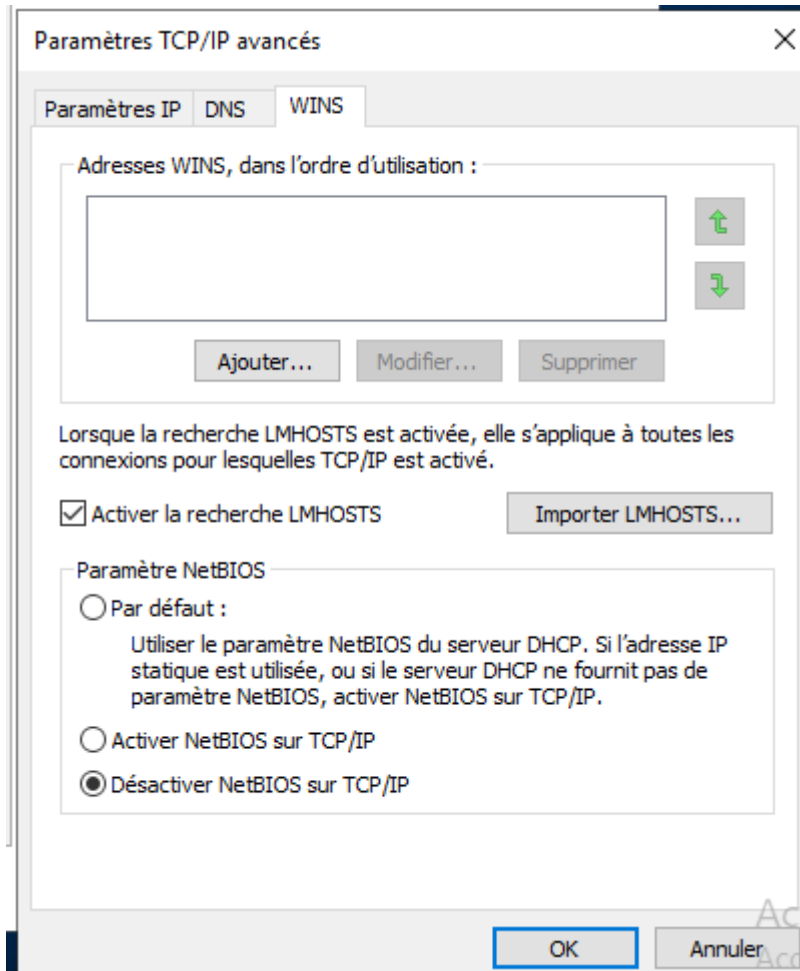
## Configuration des adresses IPs

### ACTIONS A REPRODUIRE SUR LES DEUX MACHINES AVEC L'IP EN N+1.

- exécuter `ncpa.cpl`
- clique droit sur la carte réseau>propriété
- désactiver l'IPv6
- double clique sur "  Protocole Internet version 4 (TCP/IPv4) "
- renseigner les champs suivant :
  - IP, MASK, PASSERELLE
  - Deux DNS (exemple avec ceux de Cloudflare et ceux de Google)



- cliquer sur "Avancé..." puis onglet WINS.
  1. Désactiver le NetBIOS sur TCP/IP.



- Cliquer sur OK, puis sur OK, vérifier que l'ordinateur s'est bien identifié sur le réseau.

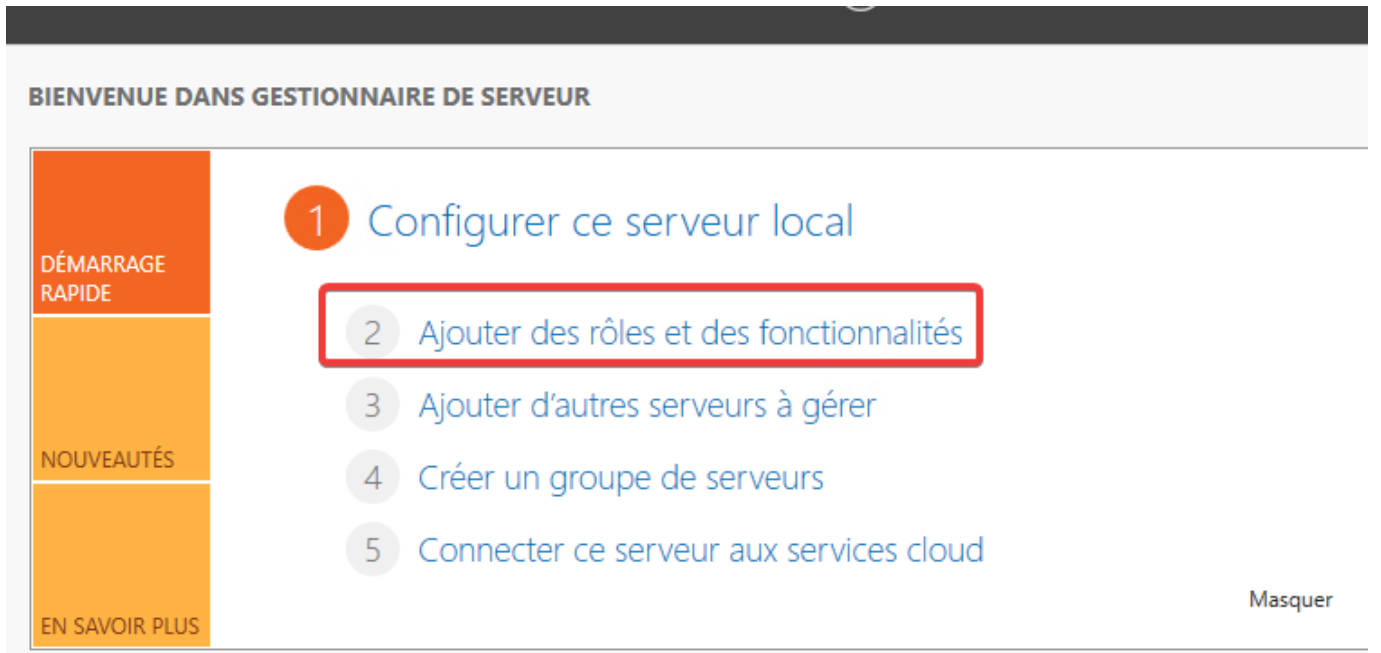
## [SERVER] Début des installations

### Changement du nom du serveur

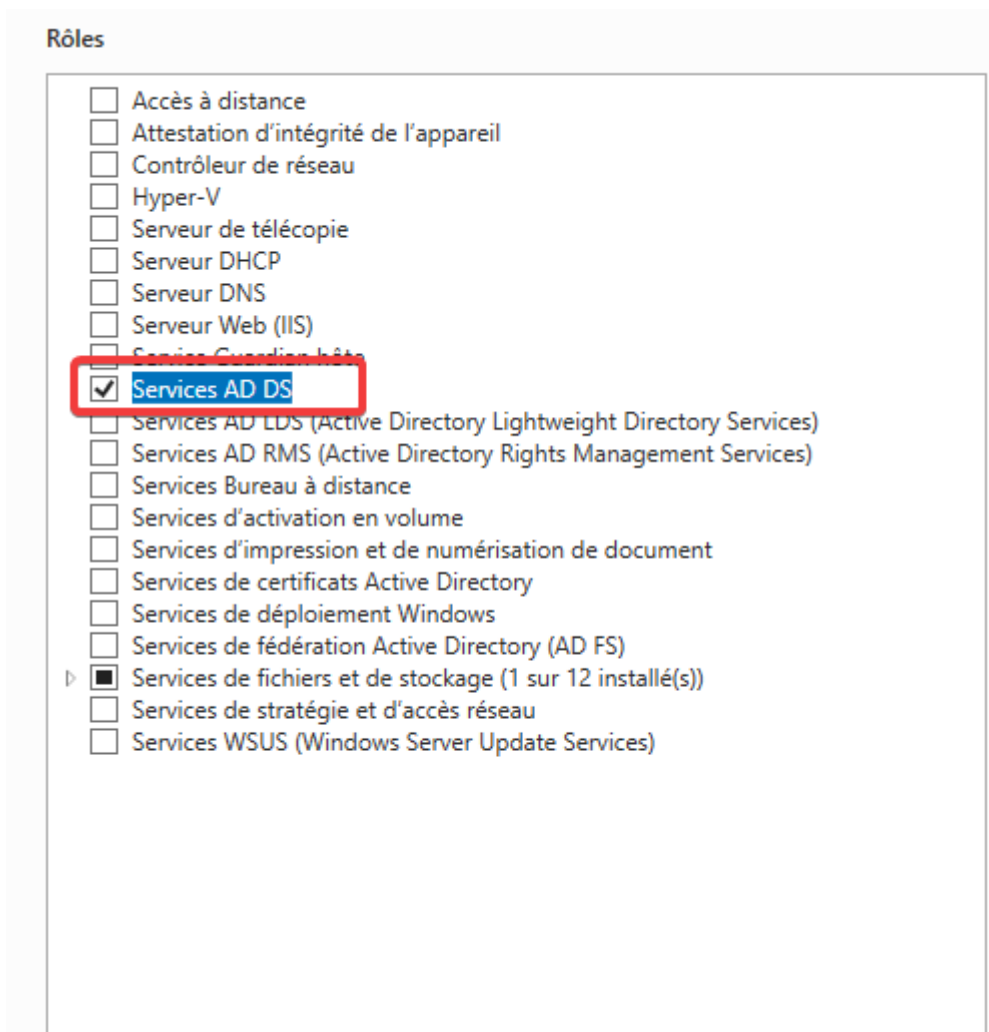
- taper `sysdm.cpl`
- appeler le "DC1"
- fermer les fenêtres puis redémarrer la machine

### Installation du serveur "AD DS"

- ouvrir le gestionnaire de serveur puis ajouter un rôle



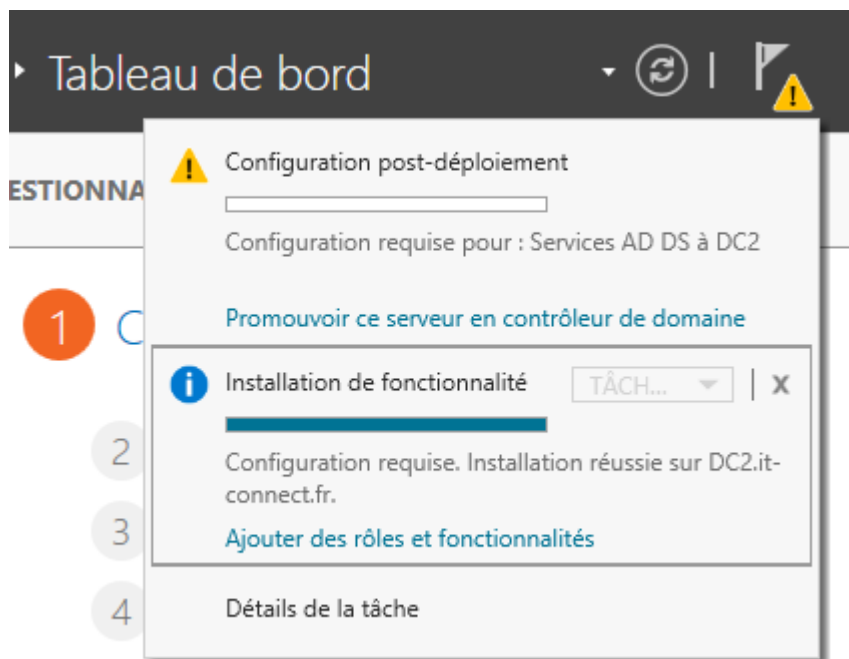
- Faites suivant, "installation basée sur un rôle ou une fonctionnalité", choisir le serveur sur lequel on veut installer la fonctionnalité.
- Cocher "Service AD DS"



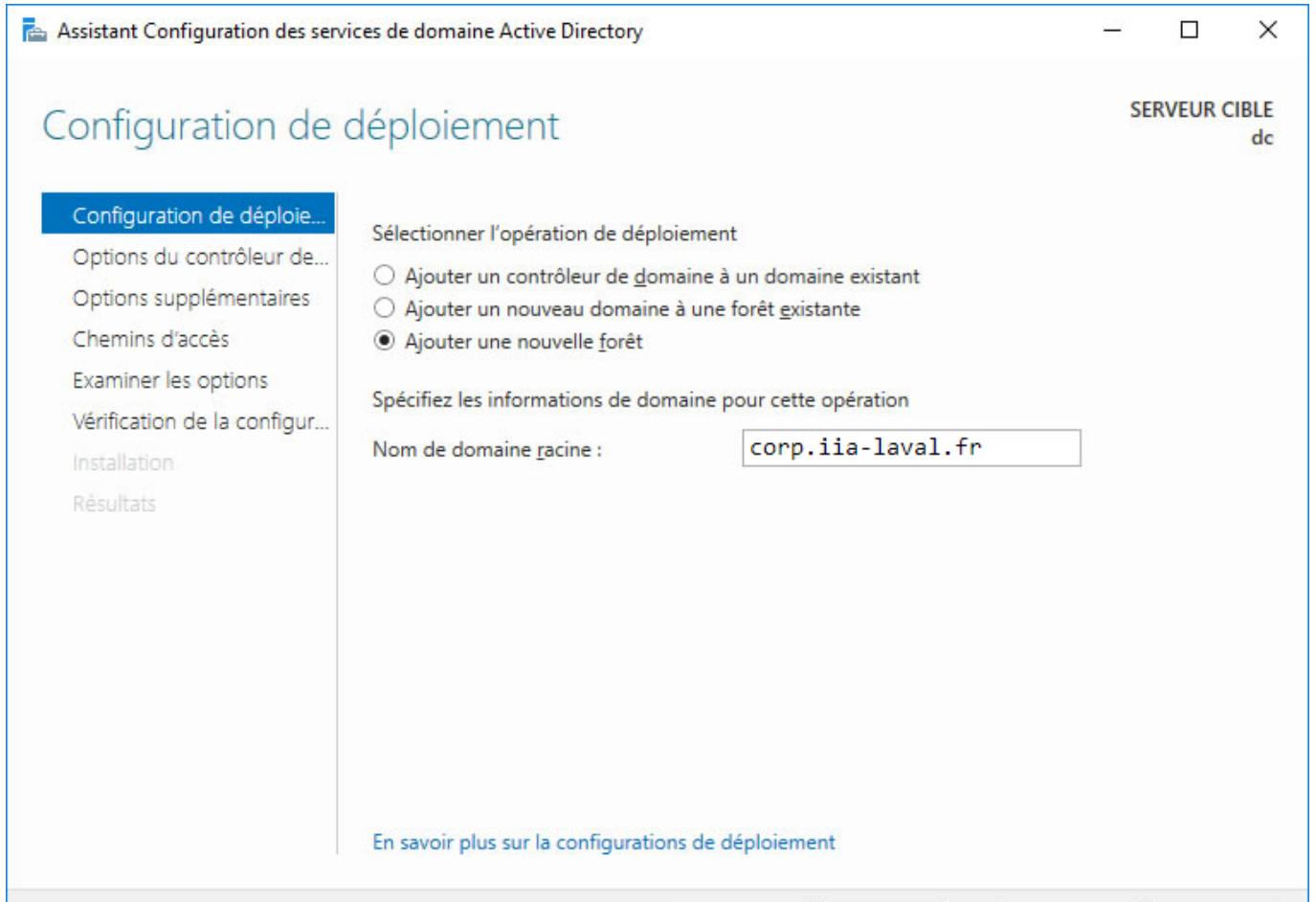
- Choisir les fonctionnalité facultative
- Lancer l'installation puis redémarrer la machine

## Au redémarrage :

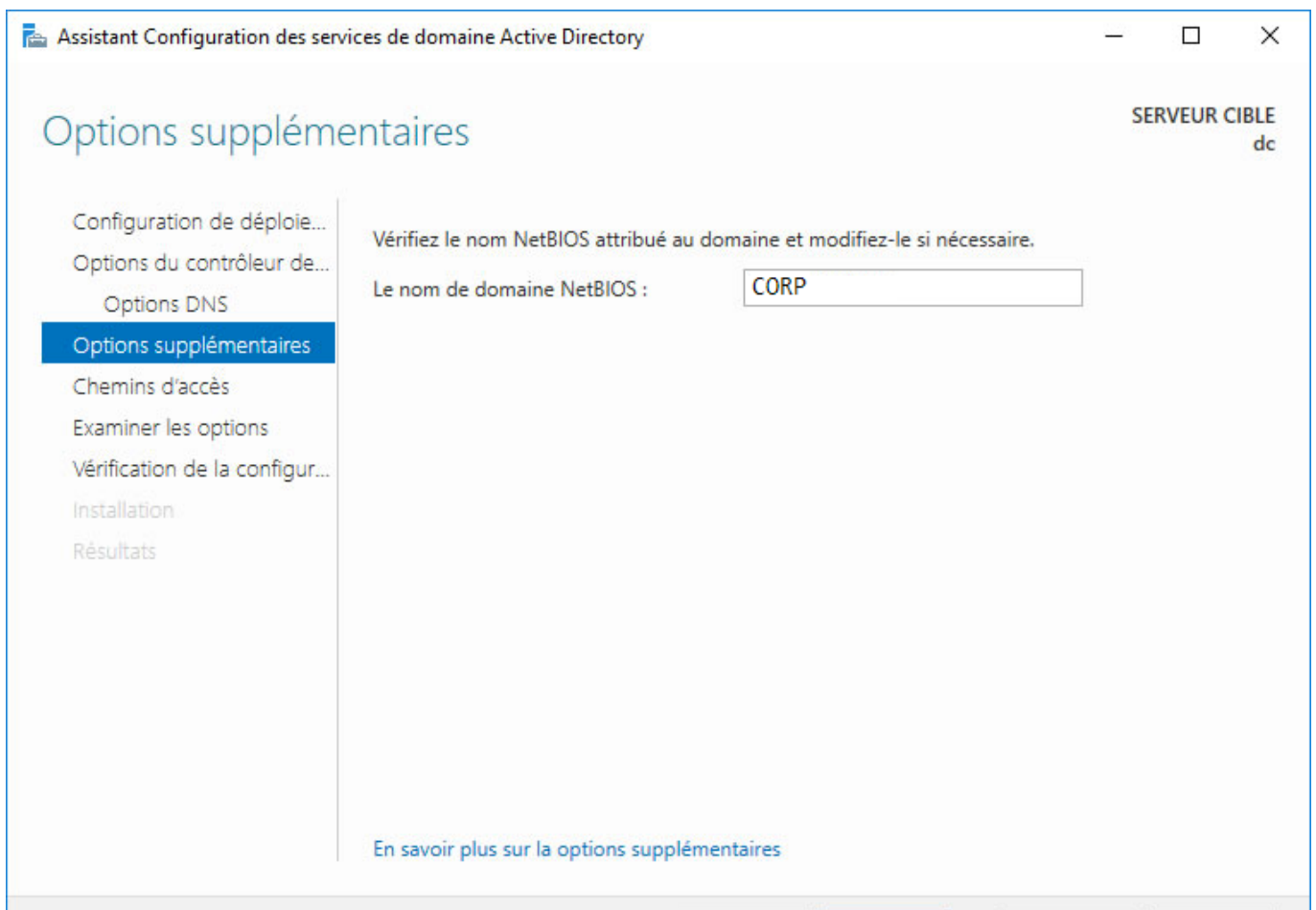
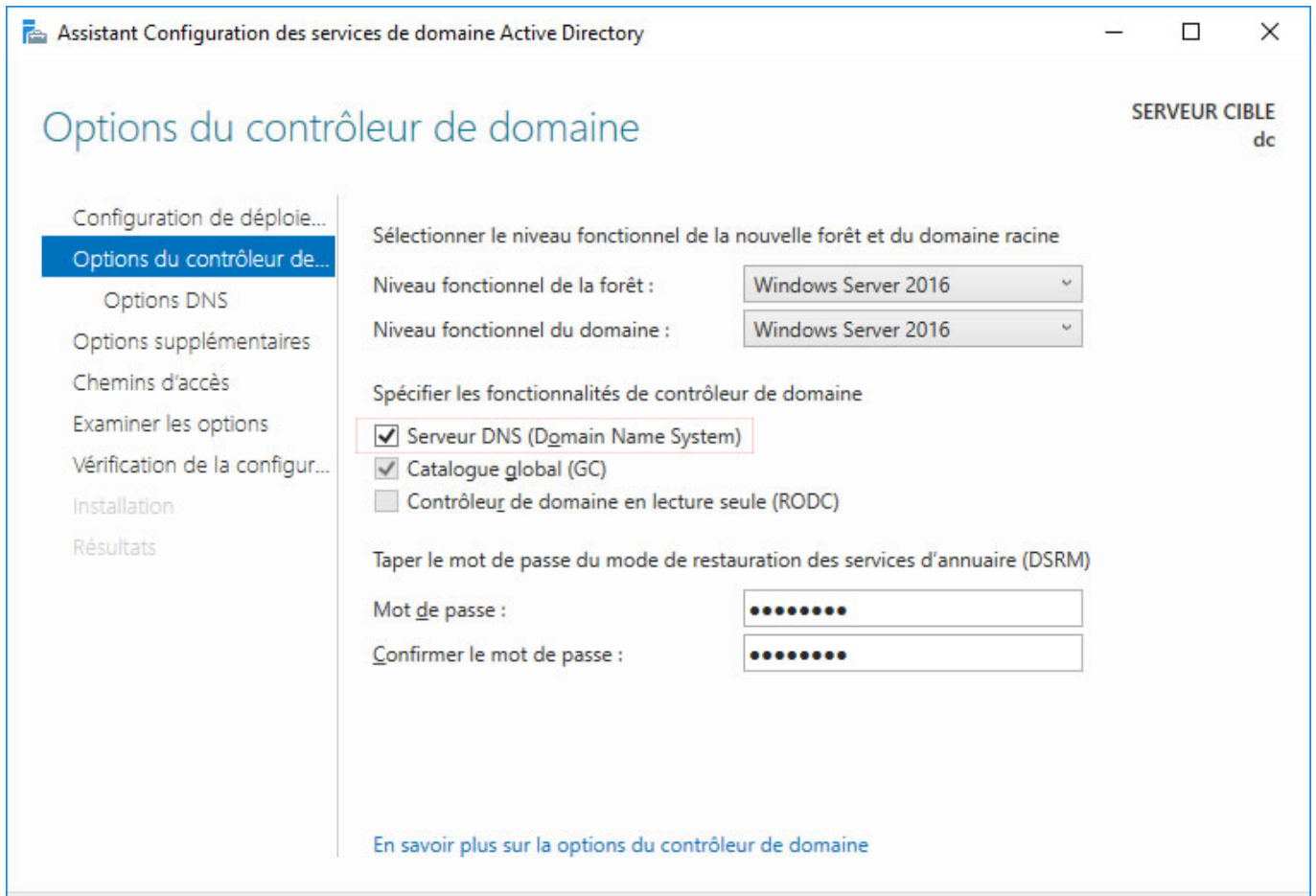
Le serveur vient de redémarrer (cela à pu être long c'est tout à fait normal). Ouvrez le "Gestionnaire de serveur" puis dans le petit drapeau jaune en haut à droite cliquer sur "Promouvoir ce serveur en CDD".



Indiquer ici le nom de la forêt souhaité. Il est souhaitable d'indiqué un domaine dont on est propriétaire.

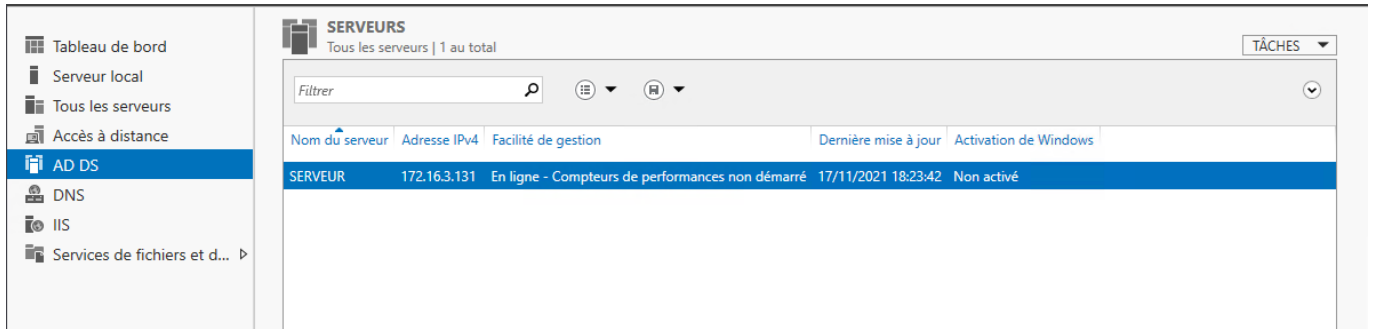


Indiquer ici votre mot de passe maître. N'oubliez pas de cocher "Serveur DNS", cela sera utile plus tard.



Vous pouvez désormais lancer l'installation, cela prendra une dizaines de minutes (au dépend de

votre configuration matérielle). Vous serez invité à redémarrer la machine une fois configuré.

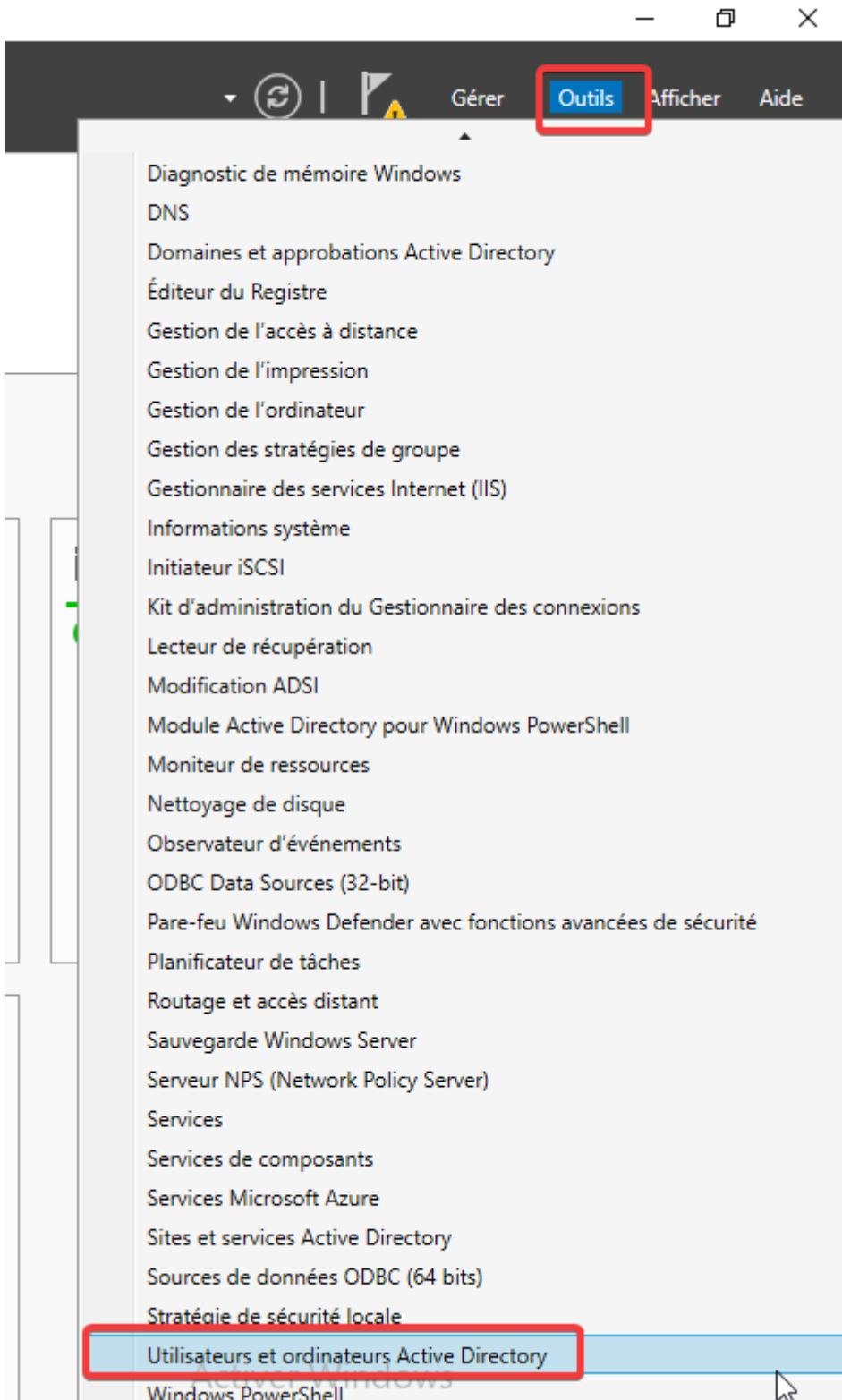


Au redémarrage vous constaterez dans l'onglet "AD DS" que "DC1" est désormais bien en ligne. La configuration de base est désormais terminée.

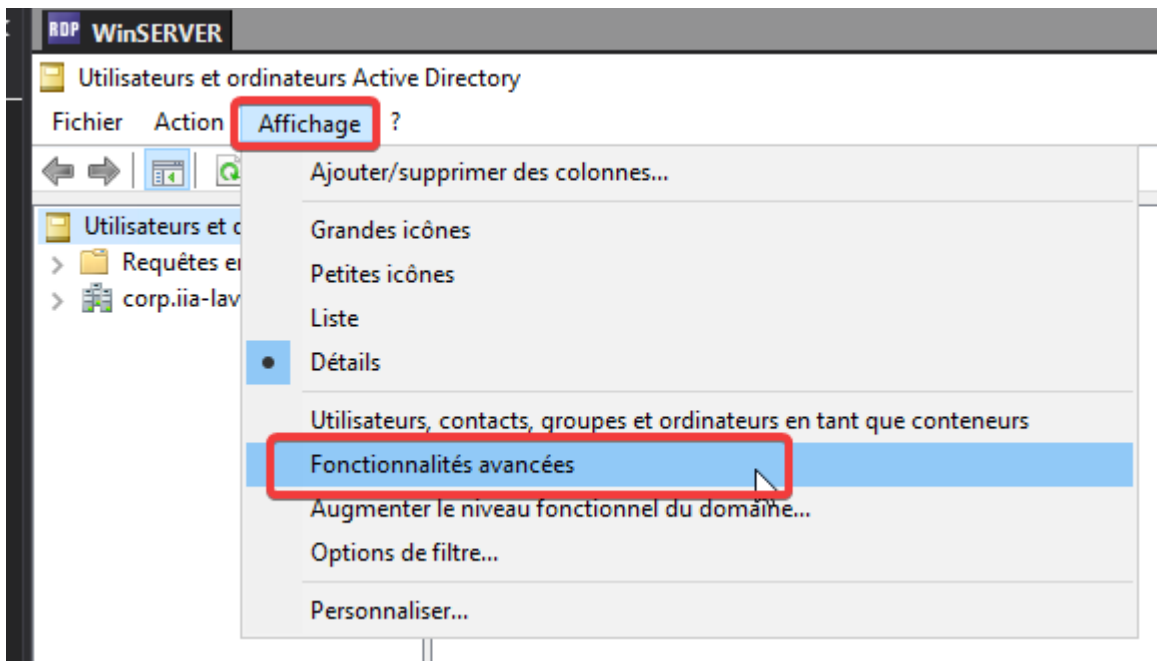
## Créations des objets dans l'AD & d'un utilisateur test

Ouvrez utilitaire de management des users et des machines.

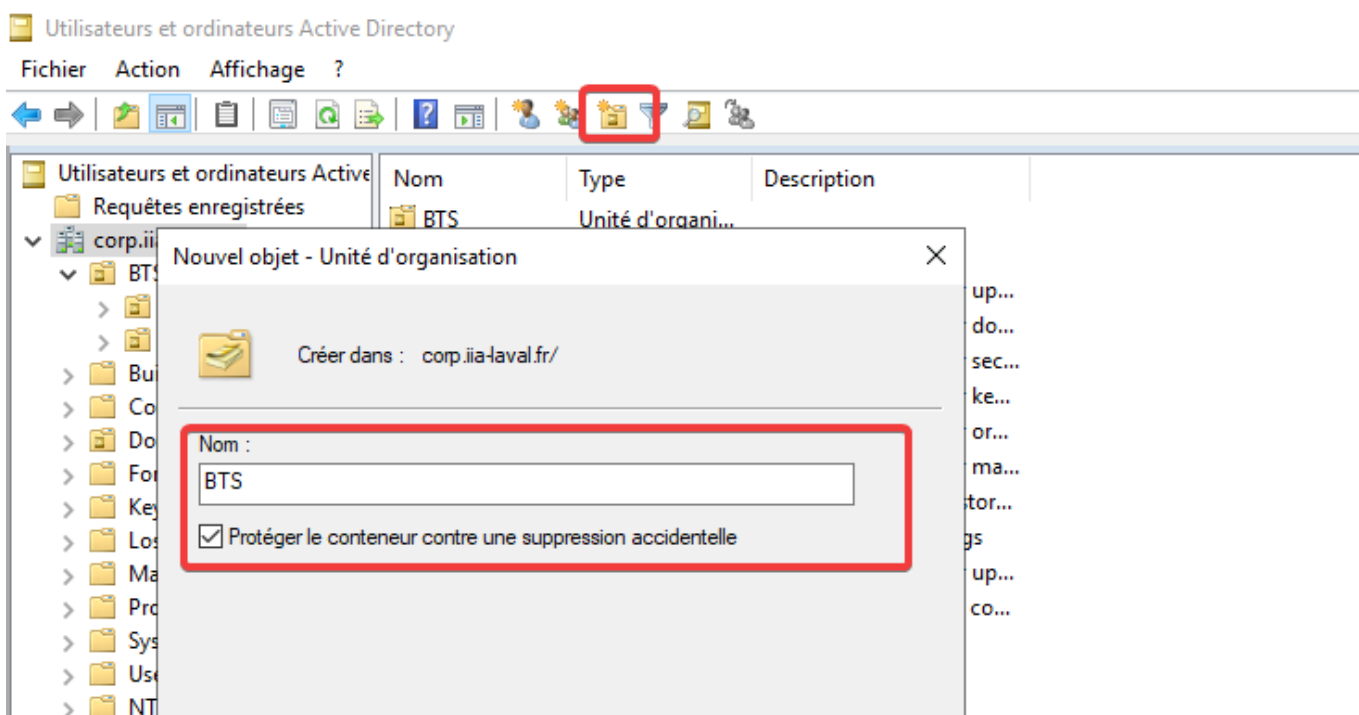




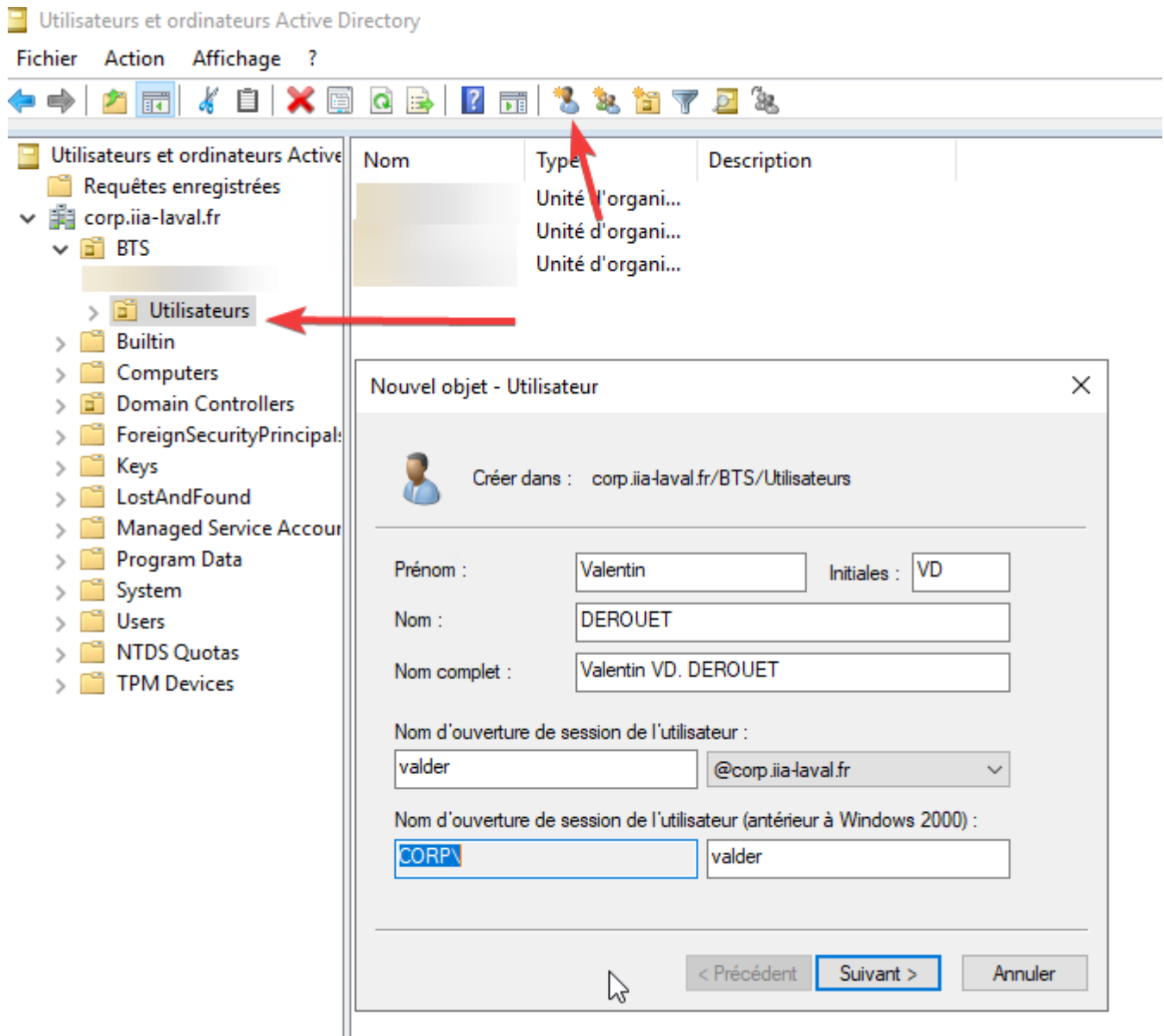
Pour plus de praticité, activer les fonctionnalités avancées :



Créez l'objet BTS à la racine du serveur.

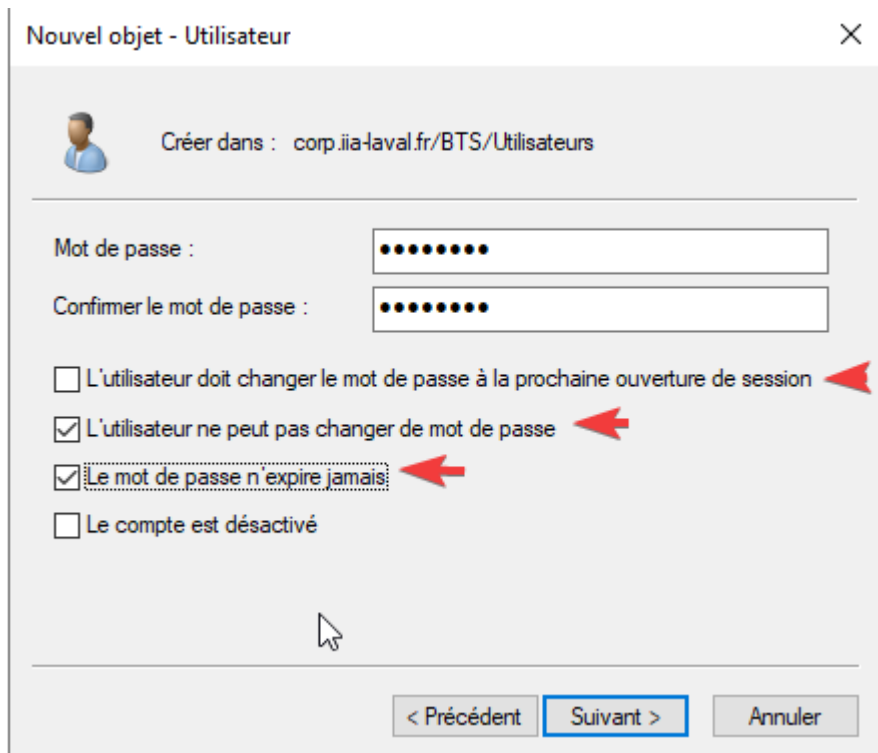


Créer un objet "Utilisateur", dans ce dernier, ajouter un utilisateur de votre choix :



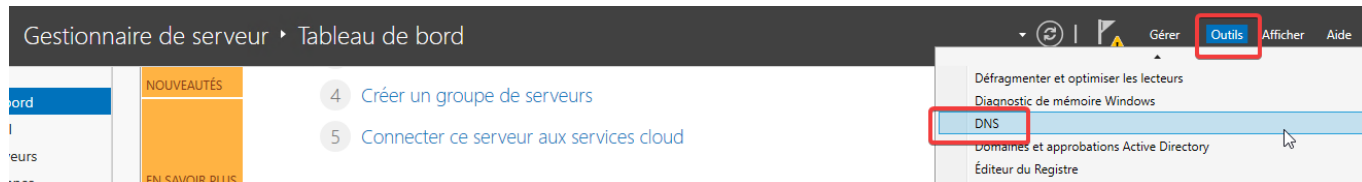
Ajouter un mot de passe (exemple: Not24get) puis :

- Décocher "L'utilisateur doit changer le mot de passe à la prochaine ouverture de session"
- Cocher "L'utilisateur ne peut pas changer de mot de passe"
- Cocher "Le mot de passe n'expire jamais"



## Configuration de règles DNS

Ouvrez l'outil de management DNS dans :

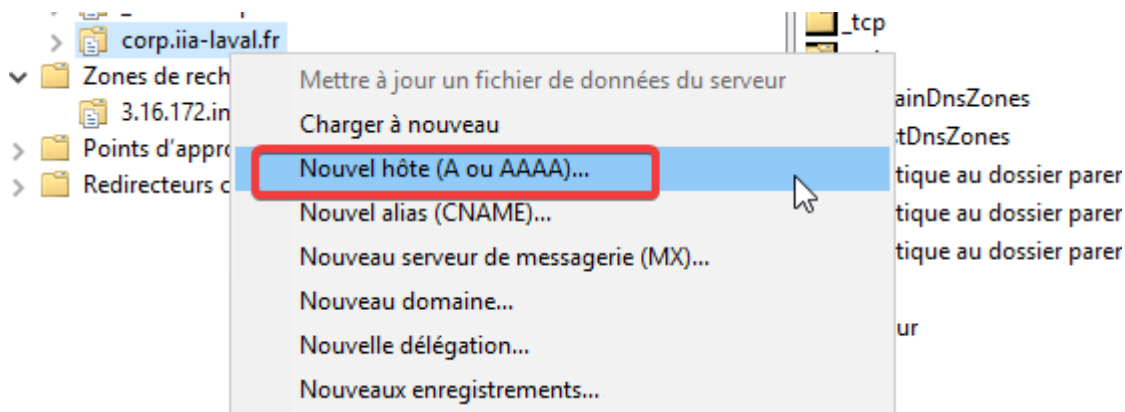


**[MEMO]** Type de record pour les DNS :

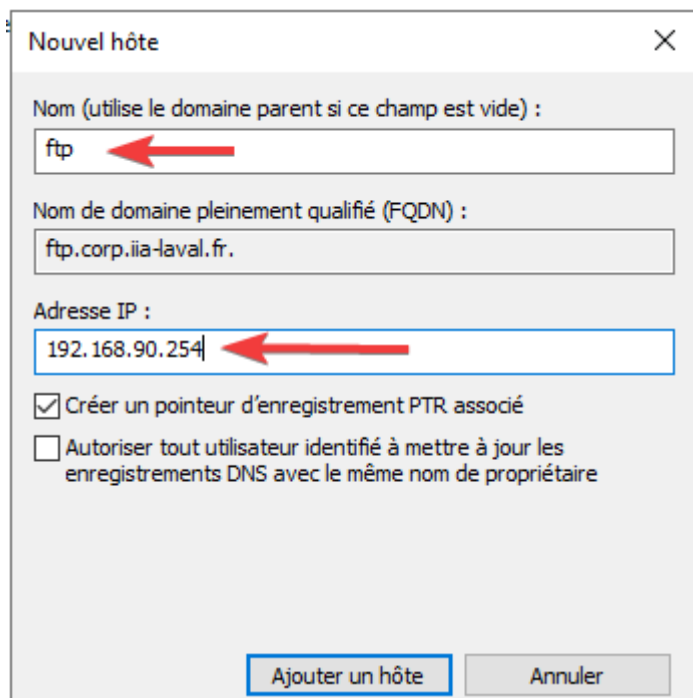
Common DNS Record Types	
Record	Description
A	Address record (IPv4)
AAAA	Address record (IPv6)
CNAME	Canonical Name record
MX	Mail Exchanger record
NS	Nameserver record
PTR	Pointer record
SOA	Start of Authority record
SRV	Service Location record
TXT	Text record

### Création d'une règle de type A

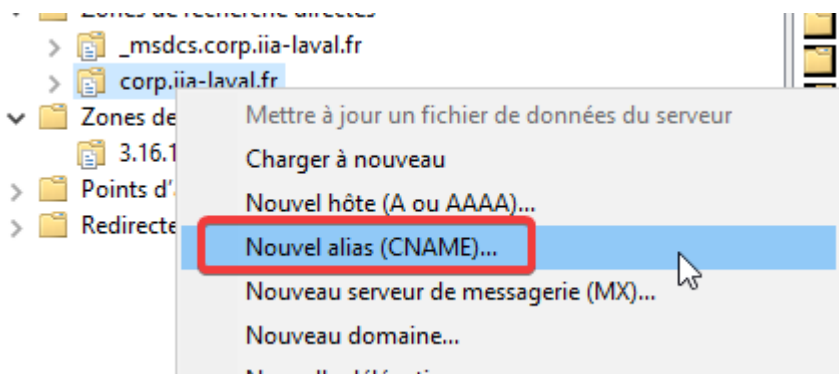
- Cliquez droit dans DC1>zones de recherche directe>corp.iia-laval.fr
- Nouvel hôte (A/AAAA)



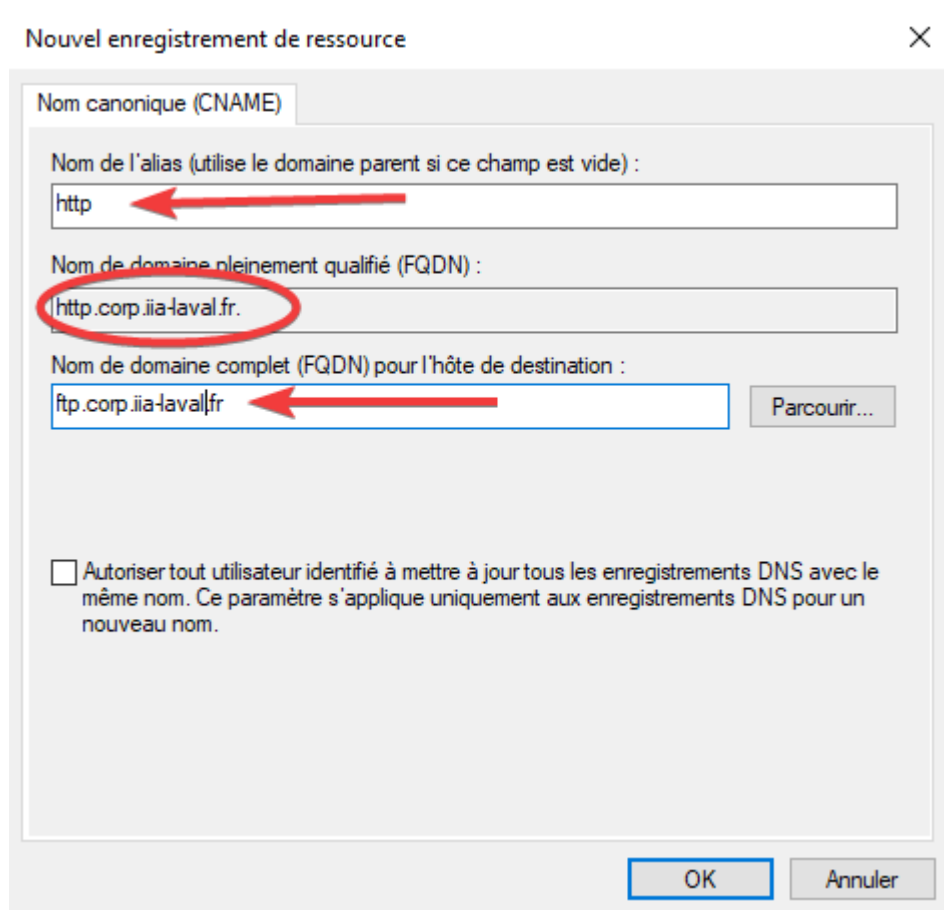
Remplir les champs "Nom" & "Adresse IP". Cocher "Créer un pointeur d'enregistrement PTR associé"



### Création d'une règle de type CNAME



Vous pouvez aller rechercher le FQDN avec le bouton parcourir.



Une fois les deux règles créées :

ftp	Hôte (A)	192.168.90.254
http	Alias (CNAME)	ftp.corp.iia-laval.fr

## Vérifications sur le [CLIENT]

Ouvrez un cmd, puis essayez de ping : - [ftp.corp.iia-laval.fr](http://ftp.corp.iia-laval.fr) - [http.corp.iia-laval.fr](http://http.corp.iia-laval.fr) - [test.corp.iia-laval.fr](http://test.corp.iia-laval.fr)

Dans le premier cas, le DNS répond bien et nous renvoi bien l'adresse IPV4 indiquée.

```
C:\Users\adminlocal>ping ftp.corp.iia-laval.fr
Envoi d'une requête 'ping' sur ftp.corp.iia-laval.fr [192.168.90.254] avec 32 octets de données :
```

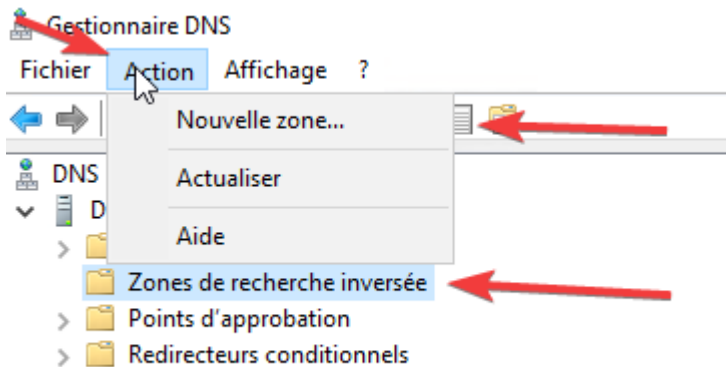
Dans le deuxième cas, le DNS fait bien le lien entre http et [ftp.corp.iia-laval.fr](http://ftp.corp.iia-laval.fr).

```
C:\Users\adminlocal>ping http.corp.iia-laval.fr
Envoi d'une requête 'ping' sur ftp.corp.iia-laval.fr [192.168.90.254] avec 32 octets de données :
```

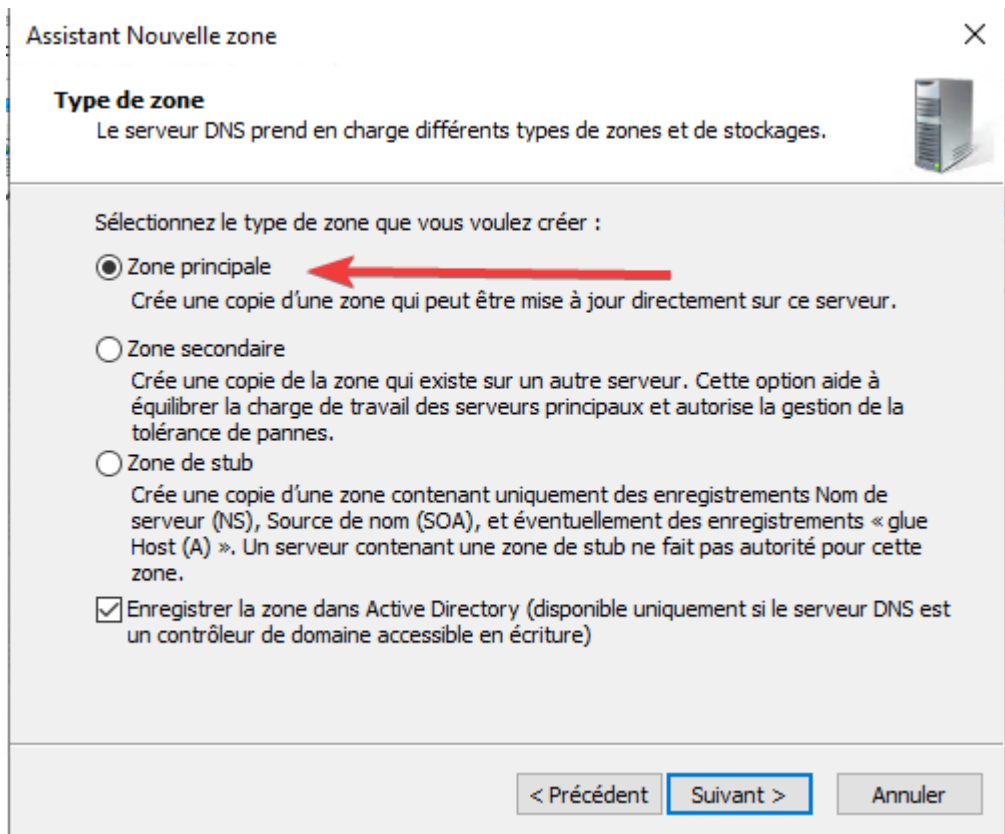
Dans le troisième cas, le DNS ne trouve pas la règle avec comme nom "test", il réponse donc que le nom d'hôte est introuvable. Tout est normal.

```
C:\Users\adminlocal>ping test.corp.iaa-laval.fr  
La requête Ping n'a pas pu trouver l'hôte test.corp.iaa-laval.fr. Vérifiez le nom et essayez à nouveau.
```

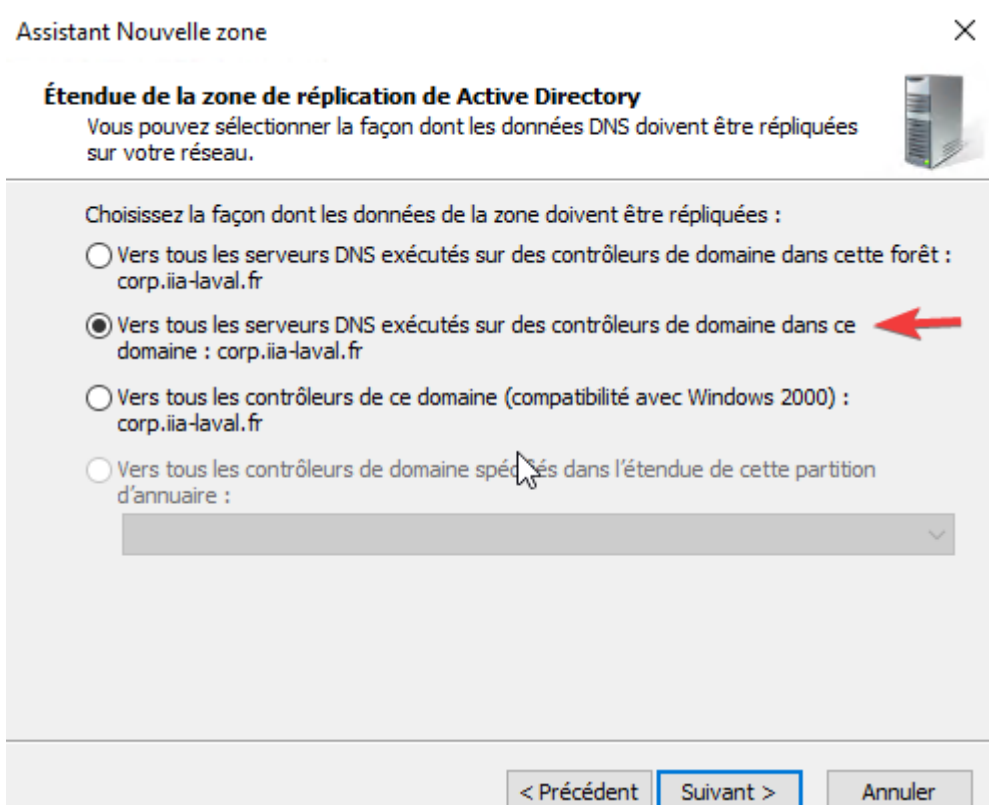
## Création d'une nouvelle zone dans "Zones de recherche inversée"



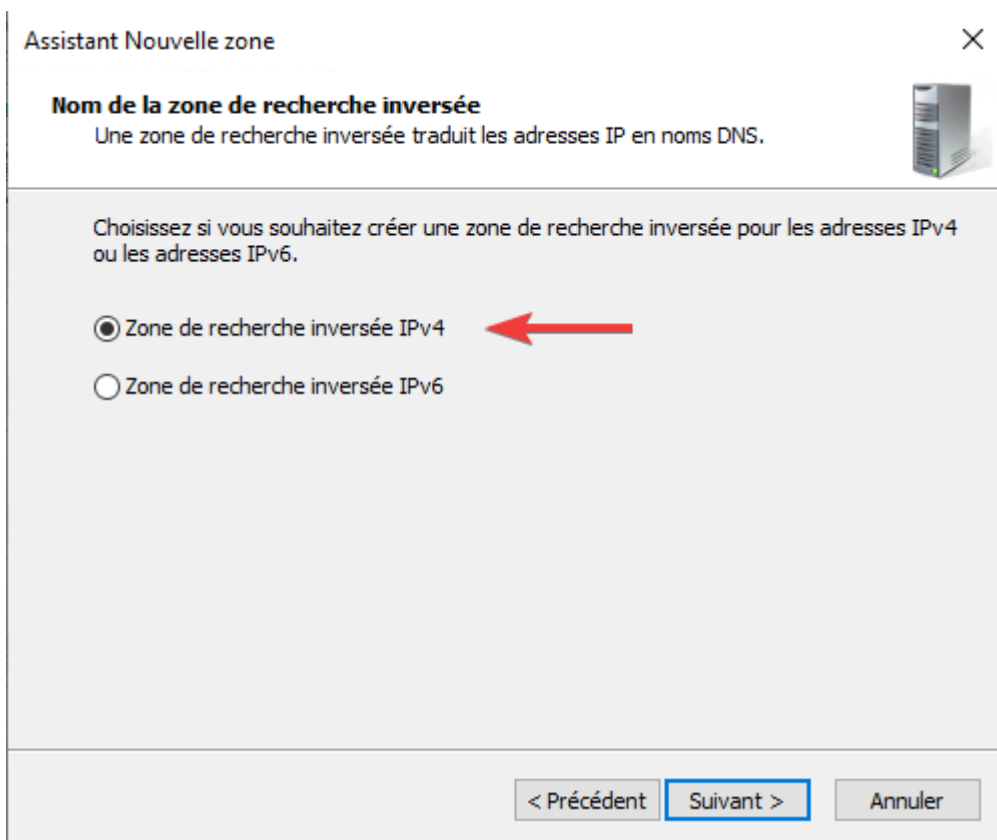
Choisir "Zone principale"



Choisir "Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans ce domaine : corp.iaa.fr"



Choisir en IPV4, l'IPV6 ne nous concerne pas pour le moment.



Compléter l'adresse IPV4 du **serveur** sans le <u>dernier octet</u>.




Assistant Nouvelle zone ✕

**Nom de la zone de recherche inversée**  
Une zone de recherche inversée traduit les adresses IP en noms DNS.

Pour identifier la zone de recherche inversée, entrez l'ID réseau ou le nom de la zone.


ID réseau :



L'ID réseau est la partie des adresses IP qui appartient à cette zone. Entrez l'ID réseau dans son ordre normal (non inversé).

Si vous utilisez un zéro dans l'ID réseau, il va apparaître dans le nom de la zone. Par exemple, l'ID réseau 10 crée la zone 10.in-addr.arpa, l'ID réseau 10.0 crée la zone 0.10.in-addr.arpa.

Nom de la zone de recherche inversée :




Laissez en recommandé.

Assistant Nouvelle zone ✕


**Mise à niveau dynamique**  
Vous pouvez spécifier que cette zone DNS accepte les mises à jour sécurisées, non sécurisées ou non dynamiques.

Les mises à jour dynamiques permettent au client DNS d'enregistrer et de mettre à jour de manière dynamique leurs enregistrements de ressources avec un serveur DNS dès qu'une modification a lieu.  
Sélectionnez le type de mises à jour dynamiques que vous souhaitez autoriser :


N'autoriser que les mises à jour dynamiques sécurisées (recommandé pour Active Directory) 

Cette option n'est disponible que pour les zones intégrées à Active Directory.


Autoriser à la fois les mises à jours dynamiques sécurisées et non sécurisées  
Les mises à jour dynamiques d'enregistrement de ressources sont acceptées à partir de n'importe quel client.


 Cette option peut mettre en danger la sécurité de vos données car les mises à jour risquent d'être acceptées à partir d'une source non approuvée.

Ne pas autoriser les mises à jour dynamiques  
Les mises à jour dynamiques des enregistrements de ressources ne sont pas acceptées par cette zone. Vous devez mettre à jour ces enregistrements manuellement.



Vérification de la création de la règle :

Nom	Type	État	État DNSSEC	Maître des clés
 3.16.172.in-addr.arpa	Serveur principal intégré à Act...	En cours d'ex...	Non signé	

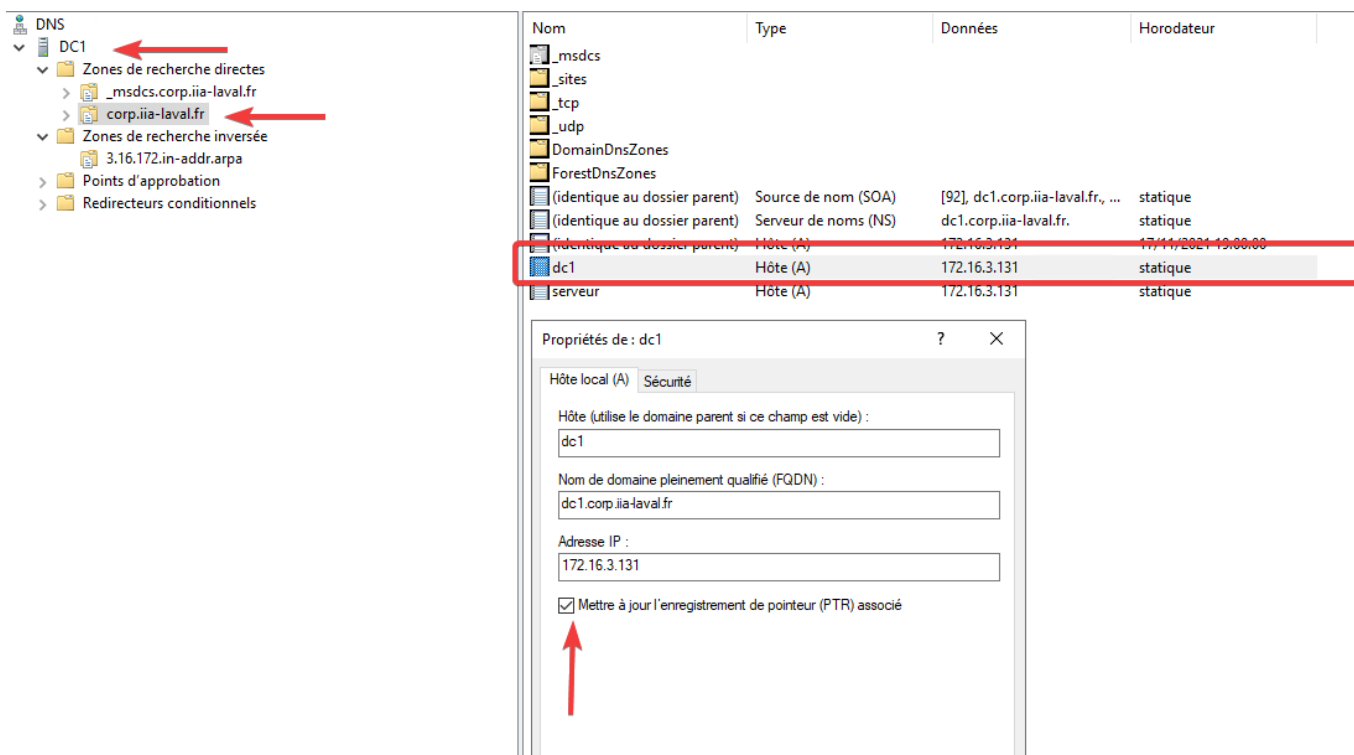


## Création d'un PTR

Création d'un nouveau pointeur dans DC1, deux techniques : - Utiliser l'automation "Mettre à jour l'enregistrement de pointeur (PTR) associé" - Créer manuellement le pointeur dans la zone de recherche inversée

### Création Automatique :

Décochez, puis valider, puis retourner dans la fenêtre pour de nouveau le cocher.



Nom	Type	Données	Horodateur
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(identique au dossier parent)	Source de nom (SOA)	[92], dc1.corp.iia-laval.fr, ...	statique
(identique au dossier parent)	Serveur de noms (NS)	dc1.corp.iia-laval.fr.	statique
(identique au dossier parent)	Hôte (A)	172.16.3.131	17/11/2021 19:00:00
dc1	Hôte (A)	172.16.3.131	statique
serveur	Hôte (A)	172.16.3.131	statique

Propriétés de : dc1

Hôte local (A) Sécurité

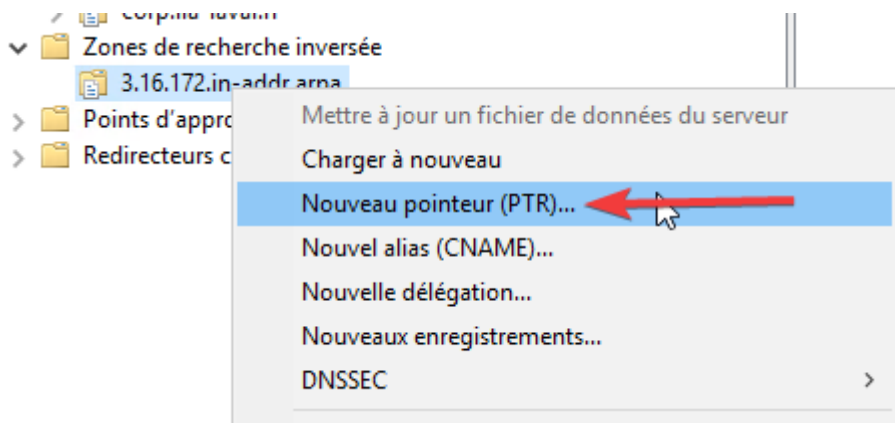
Hôte (utilise le domaine parent si ce champ est vide) :  
dc1

Nom de domaine pleinement qualifié (FQDN) :  
dc1.corp.iia-laval.fr

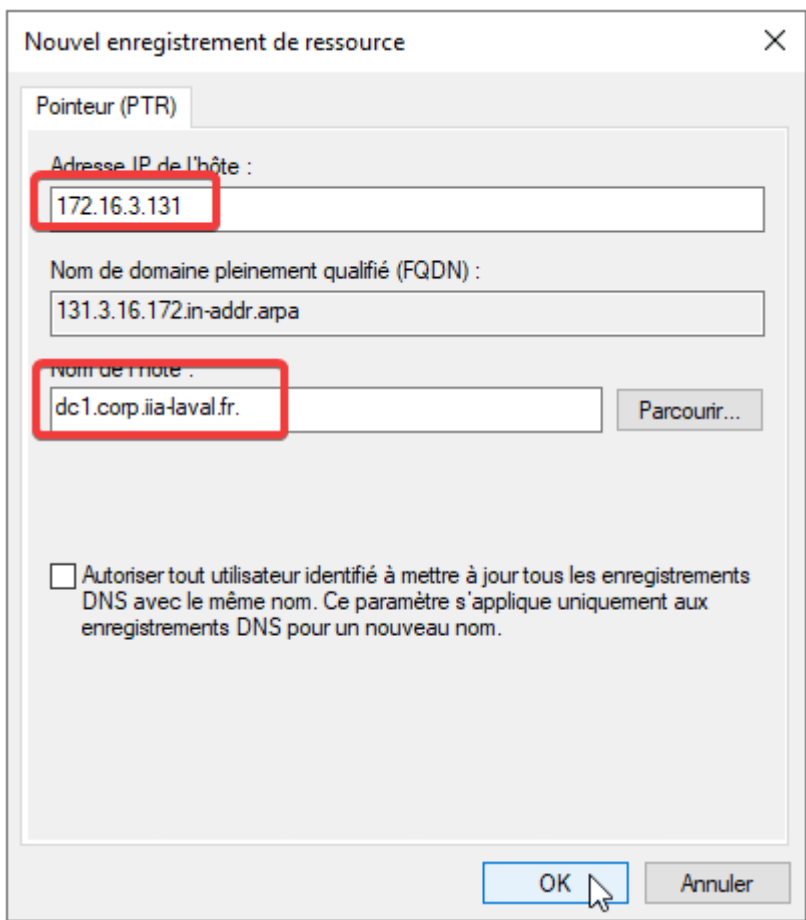
Adresse IP :  
172.16.3.131

Mettre à jour l'enregistrement de pointeur (PTR) associé

### Création manuelle :



Indiquer l'adresse IPV4 du serveur, puis le nom d'hôte correspondant.



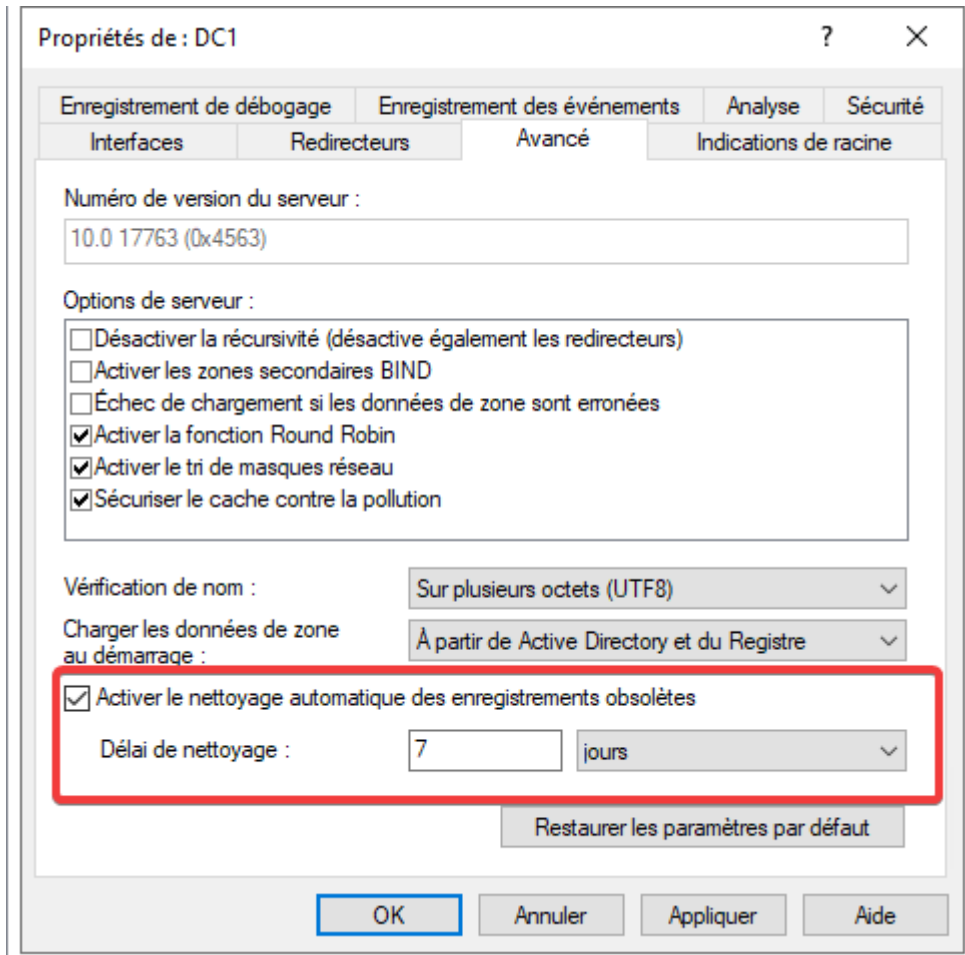
**Tips utile :**

En générale les zones DNS dans un domaine Active Directory acceptent les mises à jour sécurisées des enregistrements directement par les postes clients.

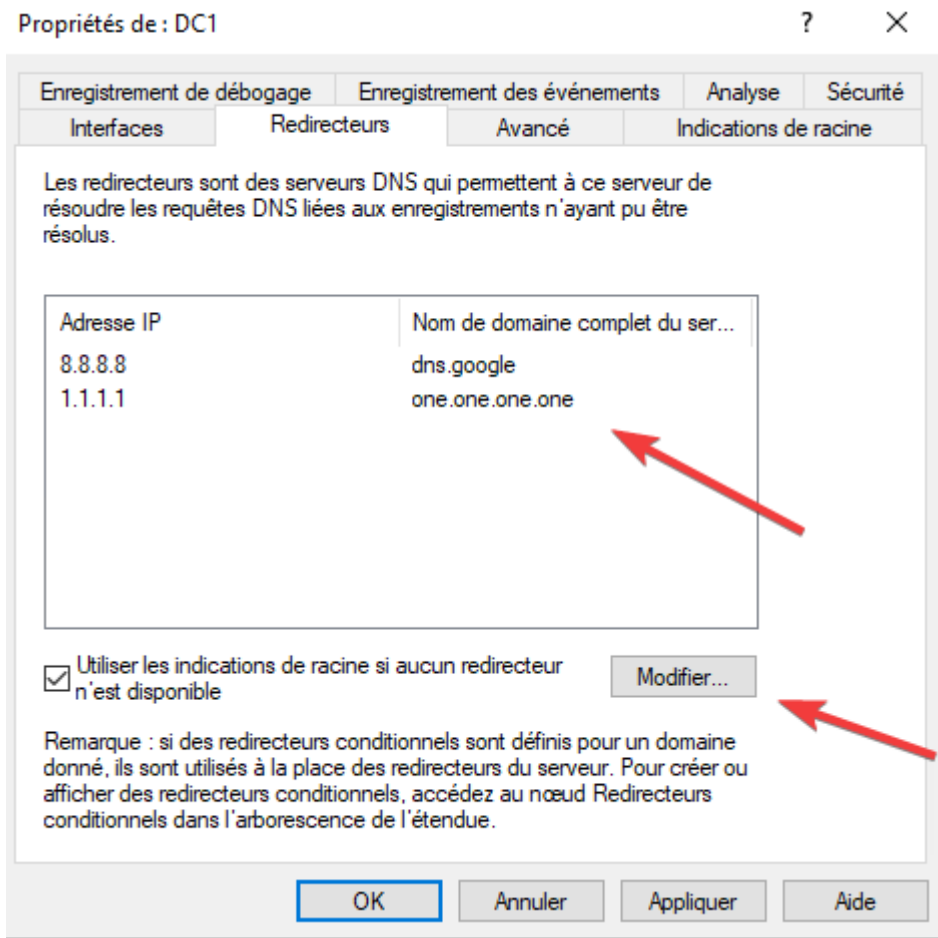
Afin de garder les zones DNS propres il est recommandé lorsqu'on ne gère pas manuellement les enregistrements DNS, de nettoyer les zones.

En effet, selon votre configuration, les postes vont créer automatiquement des enregistrements A, voir les enregistrements PTR (dans la zone de recherche inversé).

Lorsque ces postes sont supprimés ou lorsqu'ils ne sont présents ponctuellement il est possible que votre zone DNS contienne des enregistrements obsolètes.



Dans l'onglet "Redirections", vous pouvez ajouter, si ce n'est déjà fait, des DNS de secours en cas de problème :



Voici quelques exemples de secours :

- **Cisco OpenDNS**: 208.67.222.222
- **Cloudflare**: 1.1.1.1
- **Google Public DNS**: 8.8.8.8
- **Quad9**: 9.9.9.9

# [CLIENT] Connexion d'un client sur Active Directory

## Vérification sur le client si le serveur répond bien

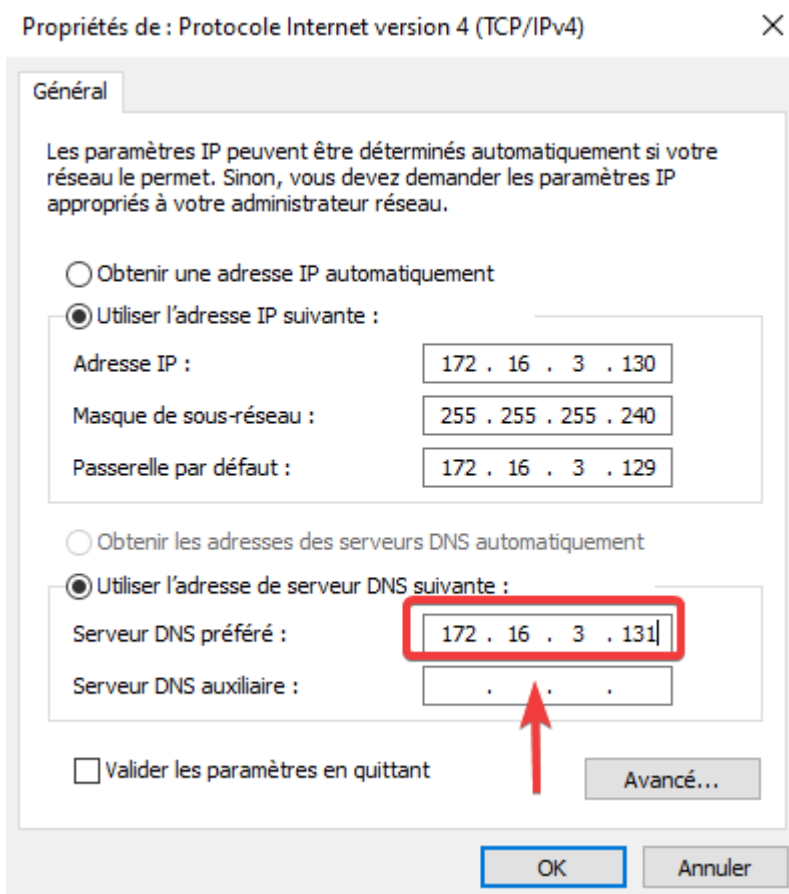
```
C:\Users\adminlocal>ping 172.16.3.131

Envoi d'une requête 'Ping' 172.16.3.131 avec 32 octets de données :
Réponse de 172.16.3.131 : octets=32 temps<1ms TTL=128
Réponse de 172.16.3.131 : octets=32 temps=1 ms TTL=128
Réponse de 172.16.3.131 : octets=32 temps=1 ms TTL=128
Réponse de 172.16.3.131 : octets=32 temps=1 ms TTL=128

Statistiques Ping pour 172.16.3.131:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms

C:\Users\adminlocal>_
```

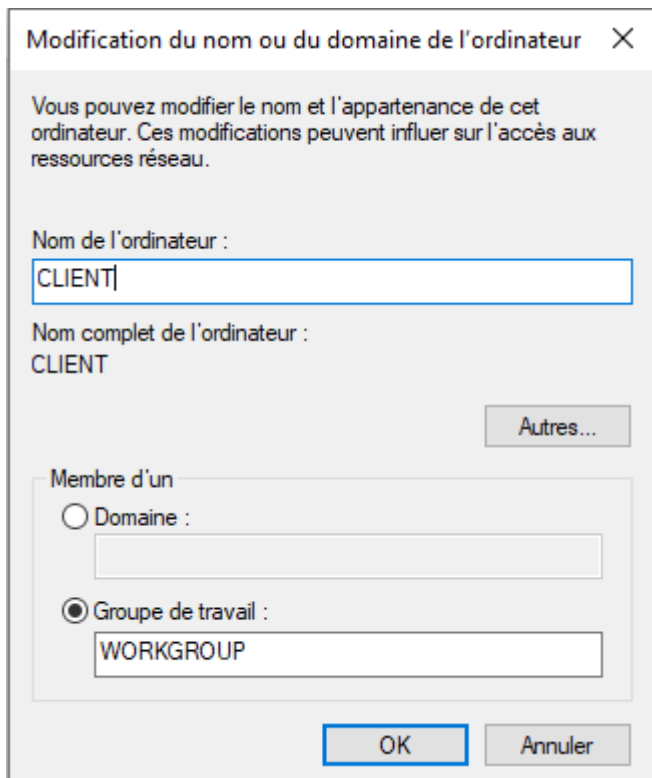
Changer les DNS par l'adresse IPV4 du serveur :



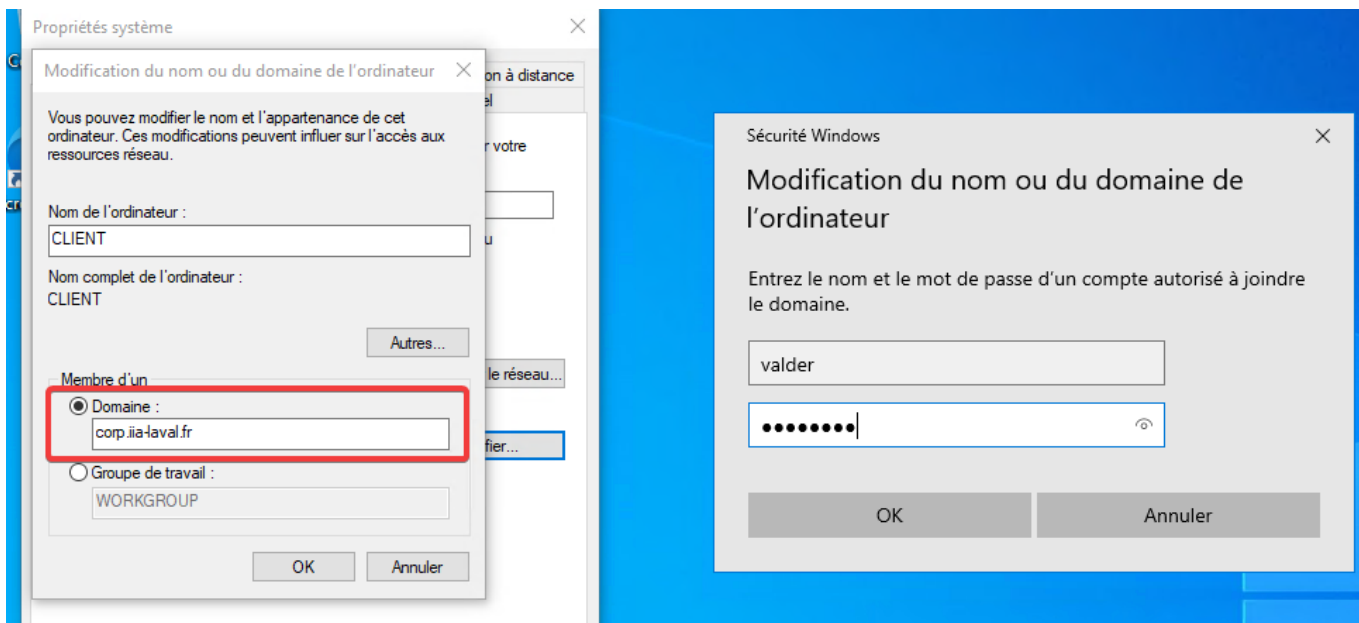
Vous pouvez tester Internet, en faisant une requête sur votre moteur de recherche préféré.

## Changement du nom du PC et du domaine

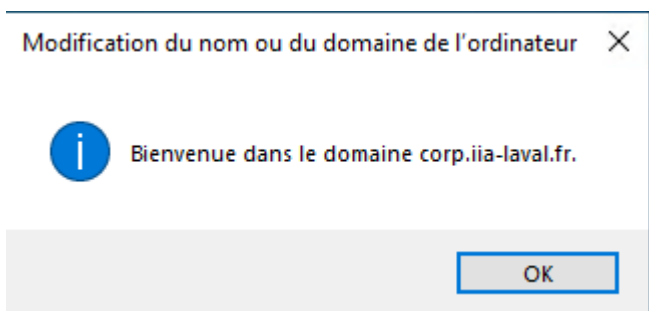
Changer le nom du pc du client avec `sysdm.cpl`, puis redémarrer avant de changer le domaine.



Une fois redémarrer, relancer sysdm.cpl puis changer le domaine par corp.iia-laval.fr. Une authentification vous sera demandez, utilisez le compte que vous avez créé tout à l'heure pour vous connecter.

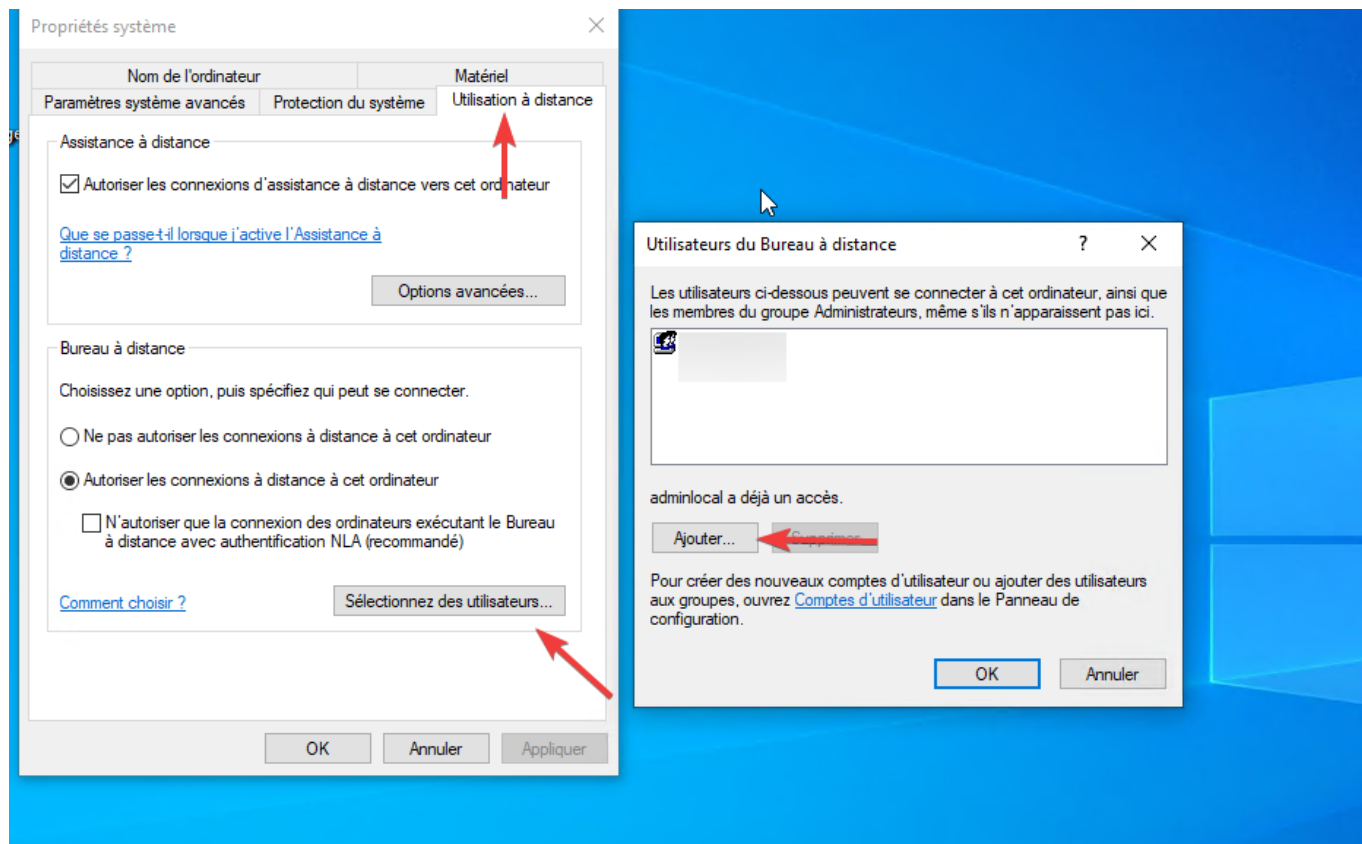


Connexion réussie !

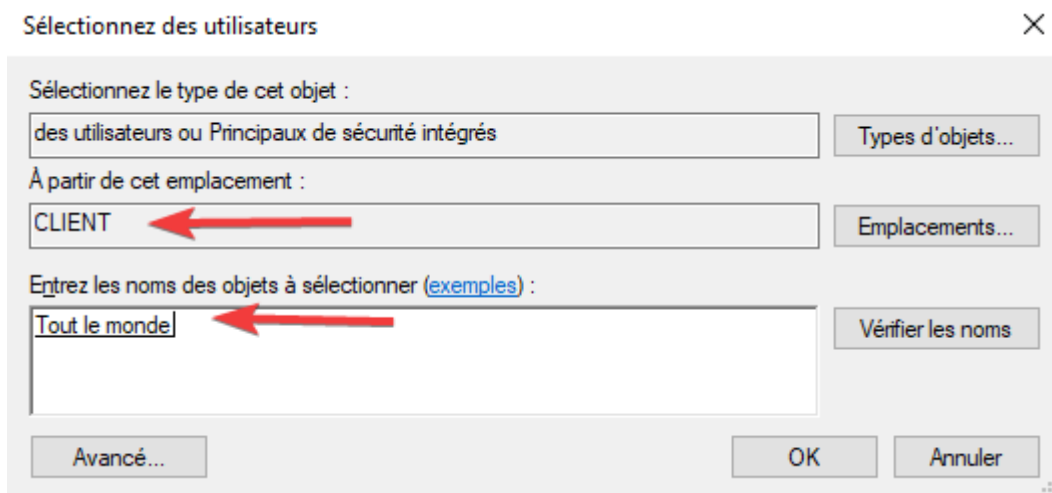


# Activer le RDP dans "sysdm.cpl"

Ouvrez les propriétés système, puis dans "Utilisation à distance", ajoutez des users.



- Sélectionner des users
  - Ajouter > Emplacements > Sélectionner "CLIENT"
  - Taper "Tout le monde"
- > Vérifier les noms





# [SERVER] Mise en situation avec une TPE

## Créations des utilisateurs

Voici le tableau des utilisateurs que nous devons créer.

Nom	Prénom	Nom d'ouverture de session	Profil Service	Description	Autre
AVANT	Nicolas	navant	GP-Direction	Directeur	
TERRE	Marcel	mterre	GP-RH	DRH	
AIMABLE	Lucie	laimable	GP-RH	RH	
BILLE	Daniel	dbille	GP-Technique	Chef op	Accès au dossier RH en lecture
ELEC	Marco	melec	GP-Technique	Ouvrier	Horaire 6H-10H
TELI	Jacques	jteli	GP-Technique	Ouvrier	Horaire 10H-14H
CASSE	Michel	mcasse	GP-Technique	Ouvrier	Horaire 14H-18H

Nous allons séparer ces 7 utilisateurs en 3 catégories : - Une Unité D'organisation "Direction"

1. AVANT Nicolas

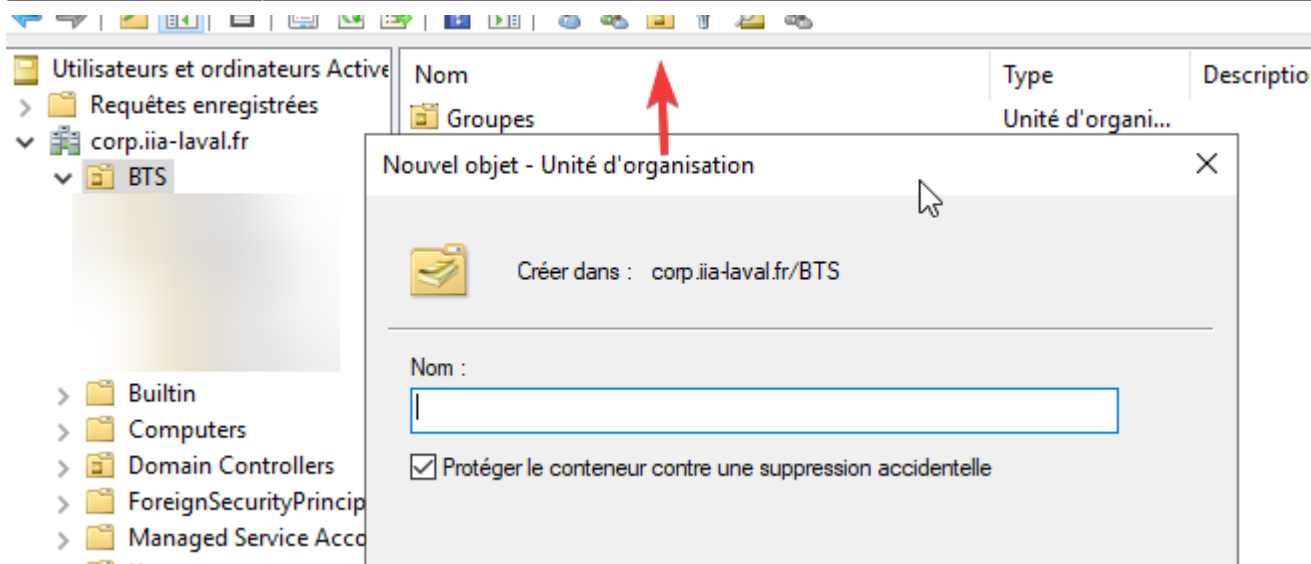
- Une Unité D'organisation "RH"

1. AIMABLE Lucie

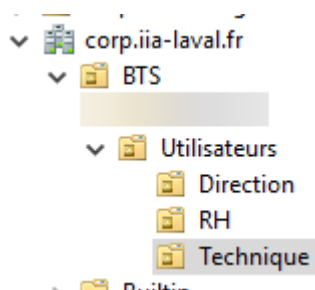
- Une Unité D'organisation "Technique"

1. BILLE Daniel
2. ELEC Marco
3. TELI Jacques
4. CASSE Michel

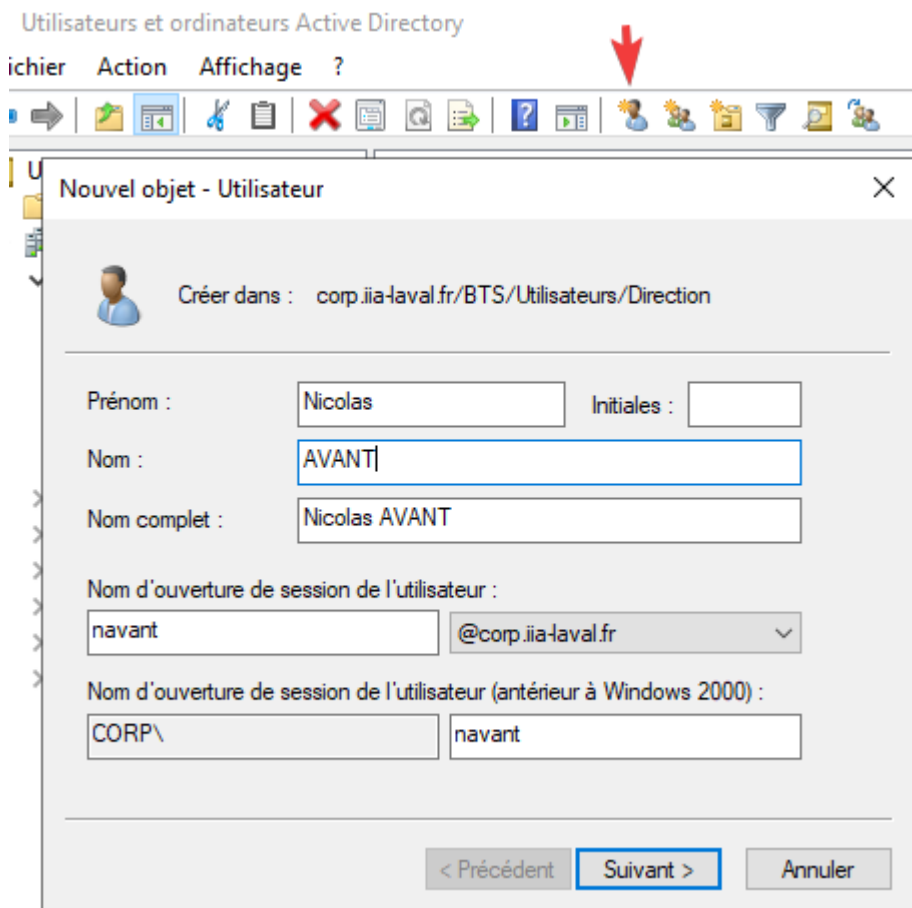
Vous devez donc créer 4 UO comme ceci :

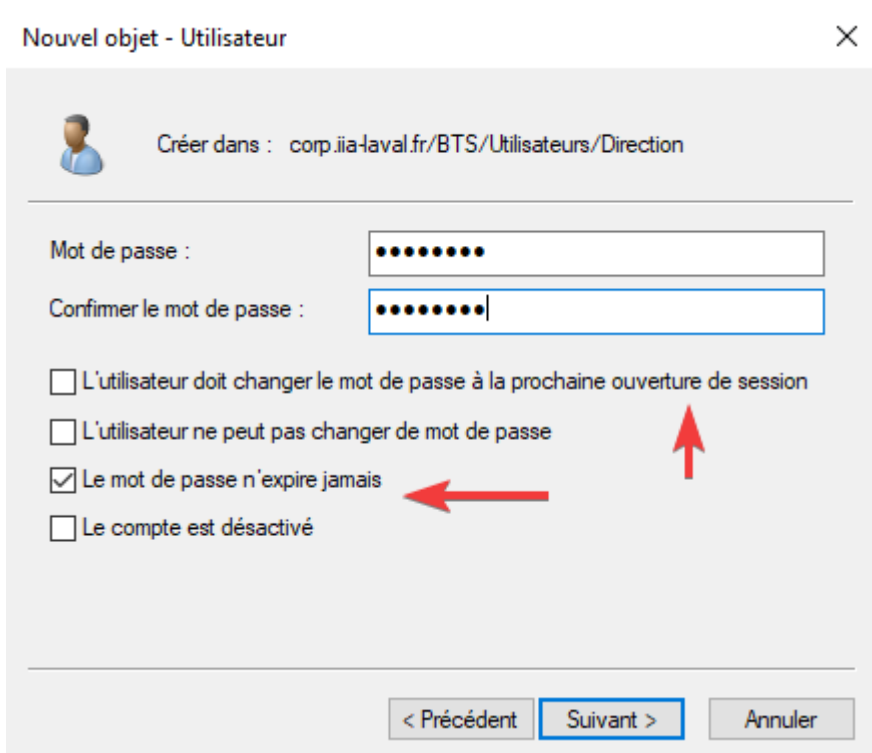


Voici la structure visée :



Exemple avec Nicolas AVANT :





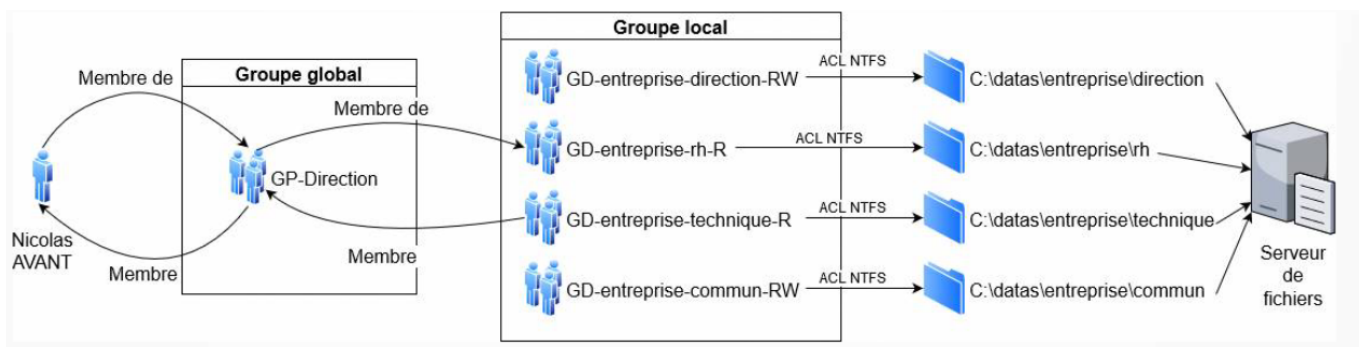
Validez, puis répéter la procédure avec tous les utilisateurs.

Objectif visé avec l'UO "Technique":

Utilisateurs et ordinateurs Active		Nom	Type	Description
>	Requêtes enregistrées			
>	corp.iia-laval.fr			
>	BTS			
>	Groupes			
>	Utilisateurs			
	Direction	Daniel Bille	Utilisateur	Chef op
	RH	Jacques TELI	Utilisateur	Ouvrier
	Technique	Marco ELEC	Utilisateur	Ouvrier
		Michel CASSE	Utilisateur	Ouvrier

## Créations des groupes

Voici notre cas d'étude (avec l'exemple de Nicolas AVANT):



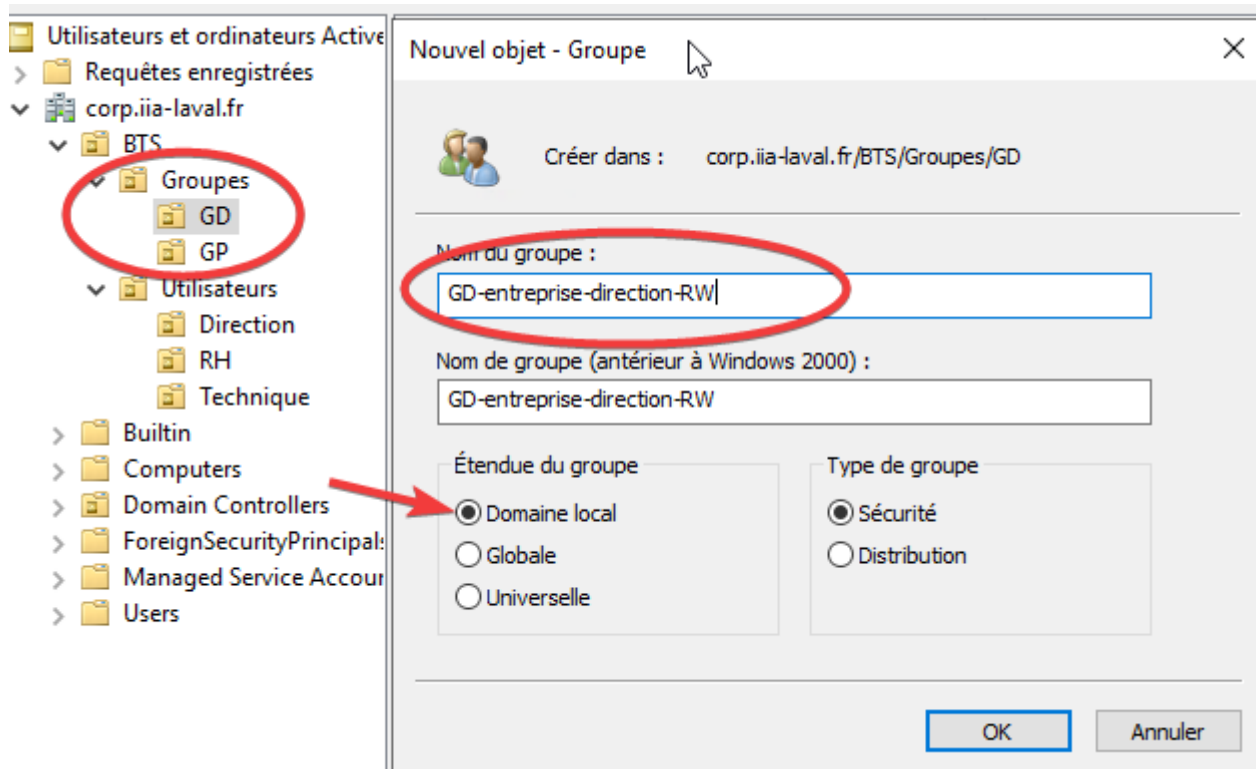
Les permissions des groupes:

Dossier	Groupe	Droits
Direction	GD-entreprise-direction-RW	RW
RH	GD-entreprise-rh-RW	RW
	GD-entreprise-rh-R	R
RH/Paie	GD-entreprise-rh_paie-RW	RW
Technique	GD-entreprise-technique-RW	RW
	GD-entreprise-technique-R	R
Commun	GD-entreprise-commun-RW	RW

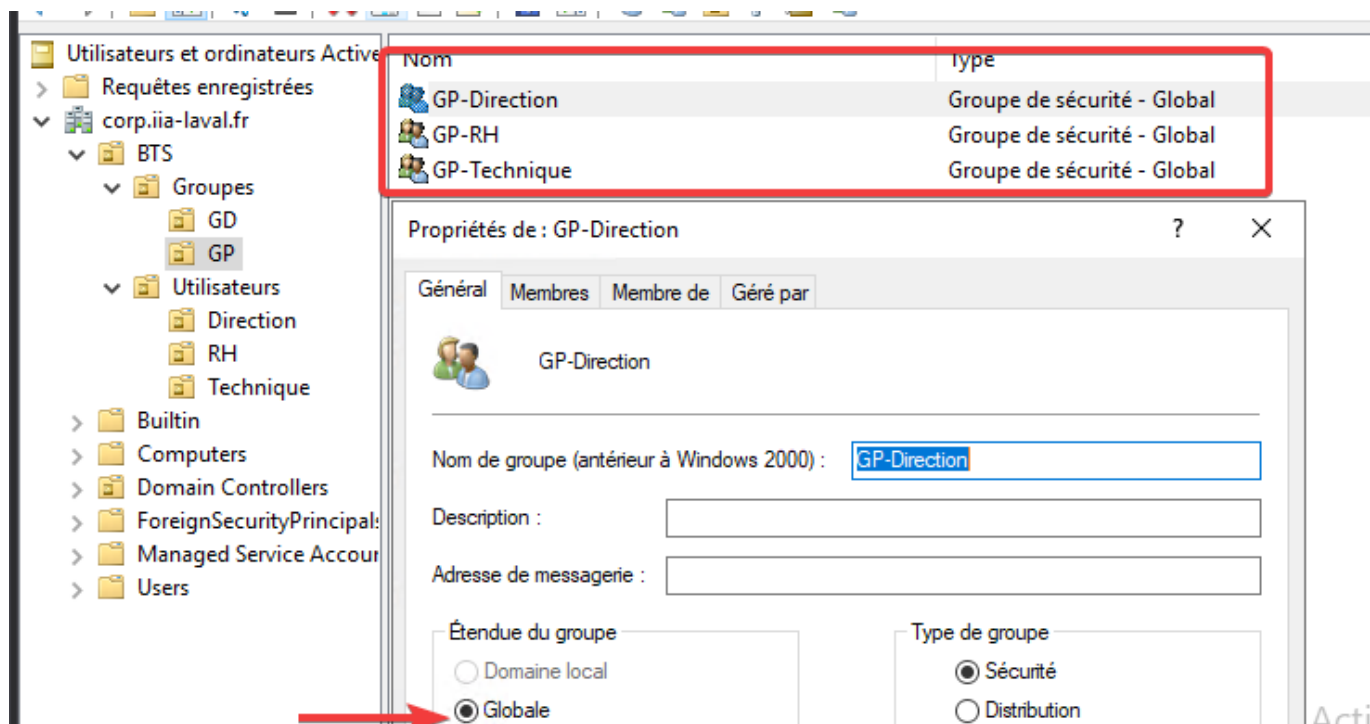
Groupe Profile (Global)	Groupe Dossier (Domaine local)
GP-Direction	GD-entreprise-direction-RW GD-entreprise-rh-R GD-entreprise-technique-R GD-entreprise-commun-RW
GP-RH	GD-entreprise-rh-RW GD-entreprise-rh_paie-RW GD-entreprise-commun-RW
GP-Technique	GD-entreprise-technique-RW GD-entreprise-commun-RW

Créer une UO dans BTS qui s'appel "Groupes". Dans cette dernière, créer une UO "GD" et "GP".

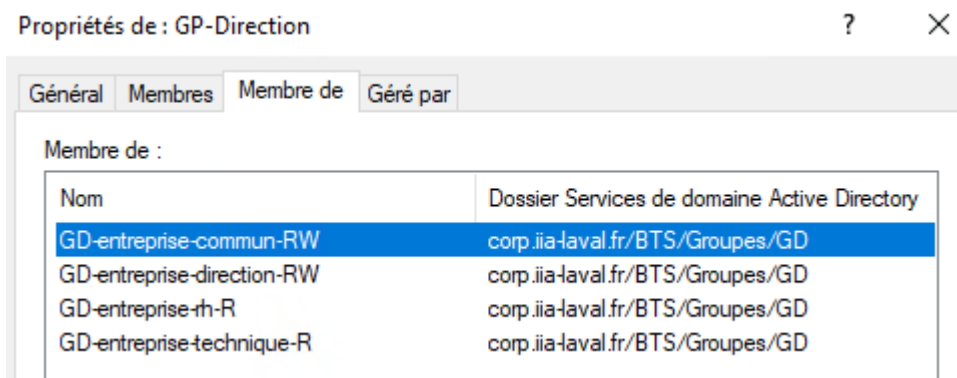
Dans l'UO "GD", créer tous les groupes dans le domaine local.



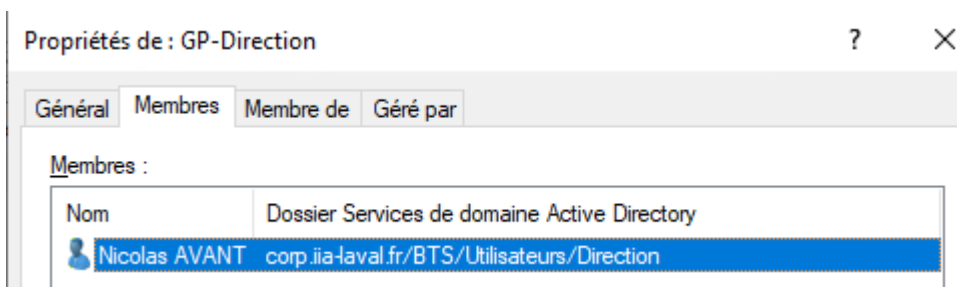
Dans l'UO "GP", créer tous les groupes en mode étendue "Globale".



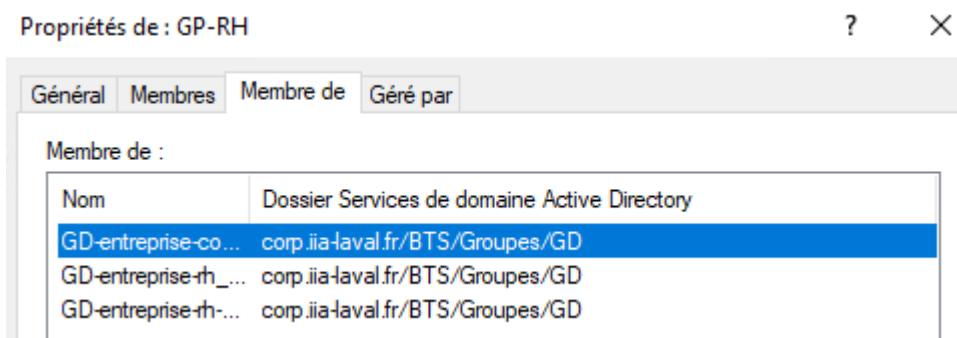
Dans GP-Direction, ouvrez l'onglet "Membre de", puis ajouter comme le tableau indique les groupes suivant :



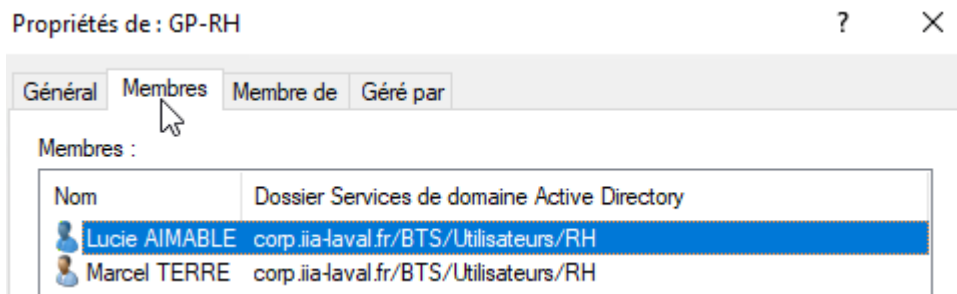
Dans l'onglet "Membres", ajouter "Nicolas AVANT", toujours en correspondance au tableau :



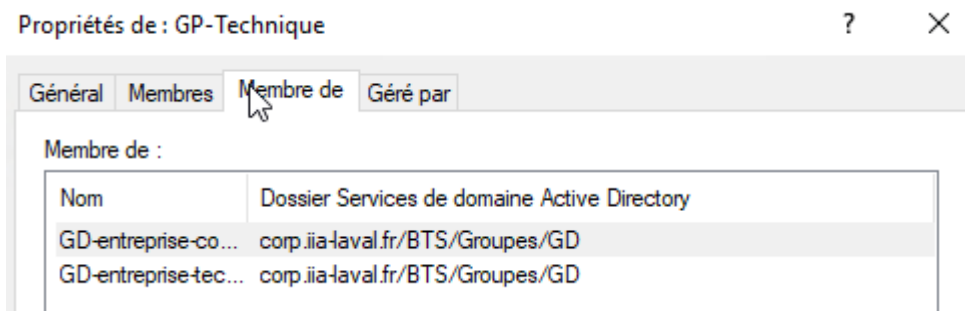
Dans GP-RH, ouvrez l'onglet "Membre de", puis ajouter comme le tableau indique les groupes suivant :



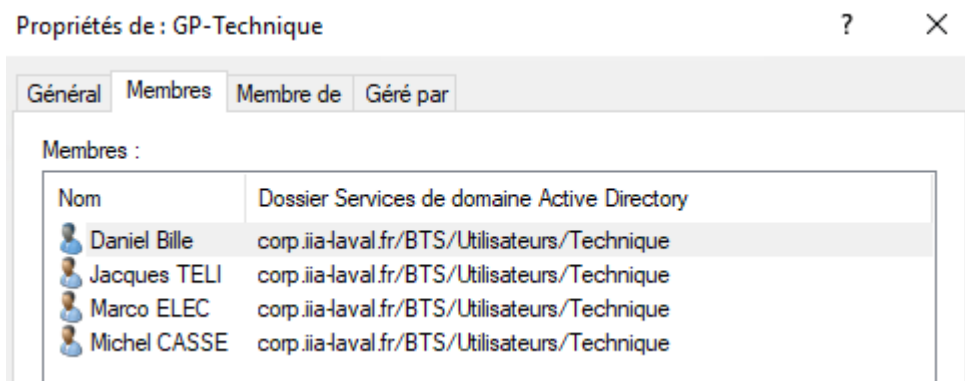
Dans l'onglet "Membres", ajouter "Lucie AIMABLE" & "Marcel TERRE", toujours en correspondance au tableau :



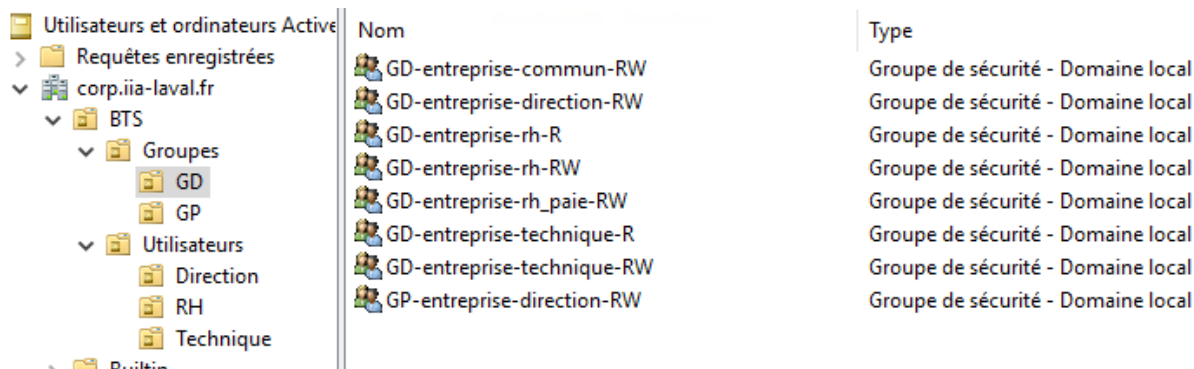
Dans GP-RH, ouvrez l'onglet "Membre de", puis ajouter comme le tableau indique les groupes suivant :



Dans l'onglet "Membres", ajouter "Daniel BILLE" & "Jacques TELI" & "Marco ELEC" & "Michel CASSE", toujours en correspondance au tableau :



Ce qui est visé :



## Créations des espaces de stockages

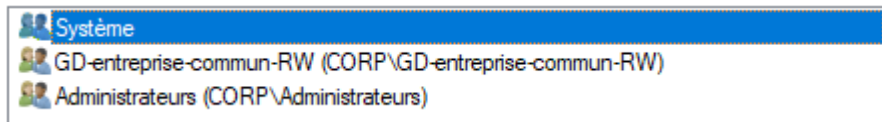
Le but ici est que chaque secteur de l'entreprise dispose d'un stockage. Il faut noter la subtilité avec "PAIE", il faudra créer un espace unique dans le dossier "RH". L'arborescence visée est celle-ci:

```
PS C:\data> tree
Structure du dossier
C:
├── entreprise
│   ├── commun
│   ├── direction
│   ├── rh
│   │   └── paie
│   └── technique
```

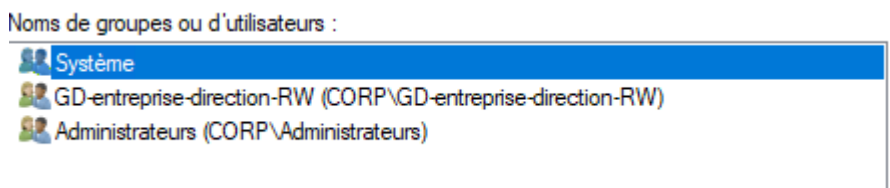
Créer donc les dossiers nécessaires dans le C:\data.

## Attributions des droits aux dossiers

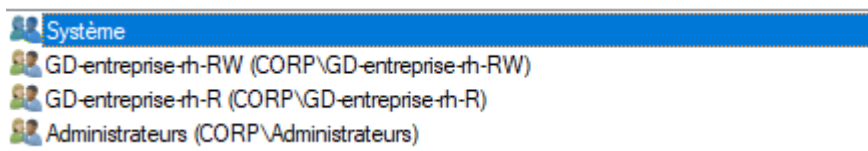
Exemple avec le dossier commun, qui est accessible par tout le monde :



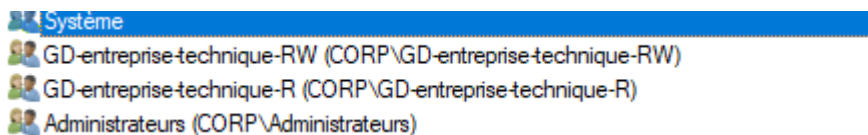
Pour le dossier "direction" :



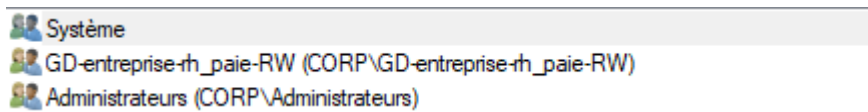
Pour le dossier "rh" :



Pour le dossier "rh/paie" :



Pour le dossier "technique" :



Ajouter selon la correspondance du tableau ci dessus les permissions aux dossiers.

**Tips:** Gestion de permissions. - R = read - W = write - O = only

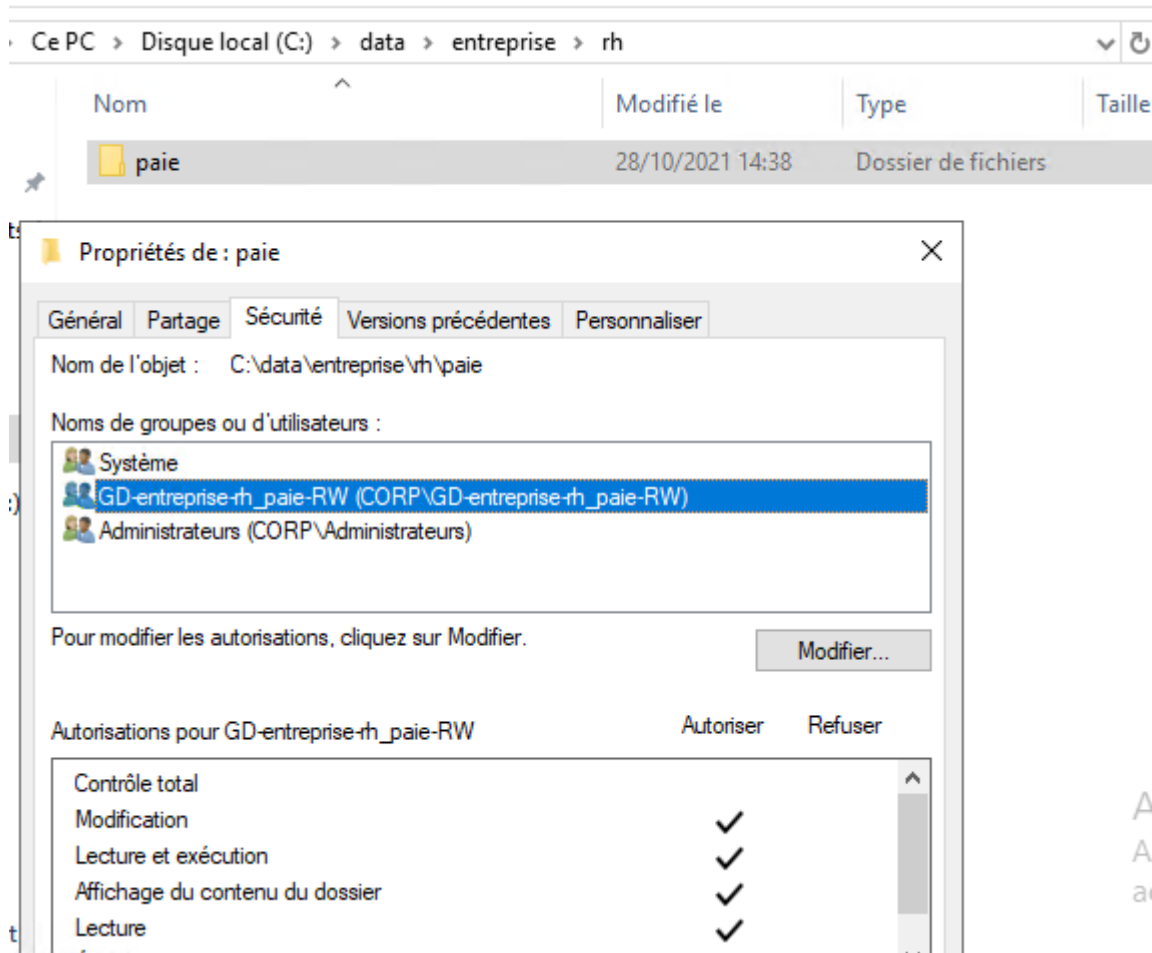
1. exemples :

1. RO : read-only
2. RW : read & write

Sur linux on aura plus tendance à utiliser la commande `chmod`. Voici un site qui permet de calculer les valeurs : <https://chmod-calculator.com/>. Le plus important à retenir est le 777 qui donne toutes les permissions.

Attention à la subtilité avec le dossier `rh/paie` :

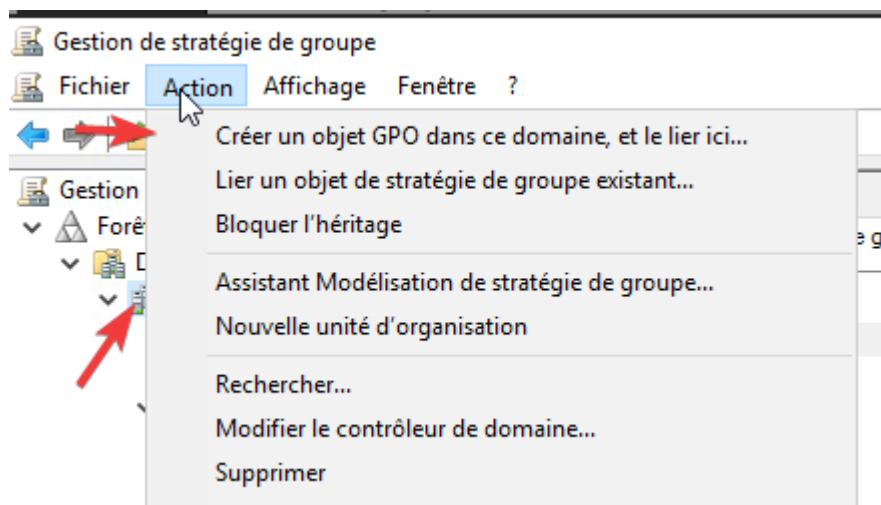




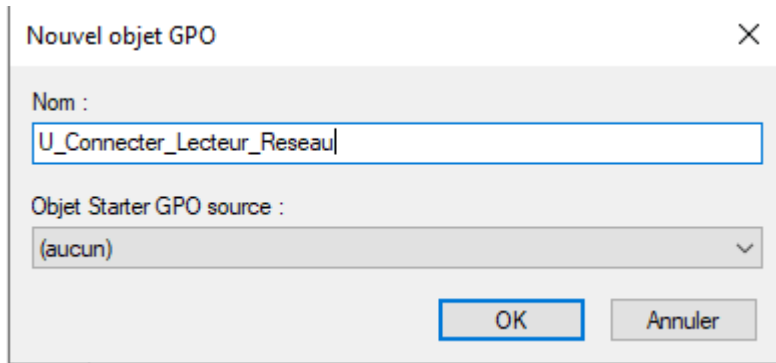
Ajouter le groupe correspondant au groupe "paie".

## Montage du disque automatiquement

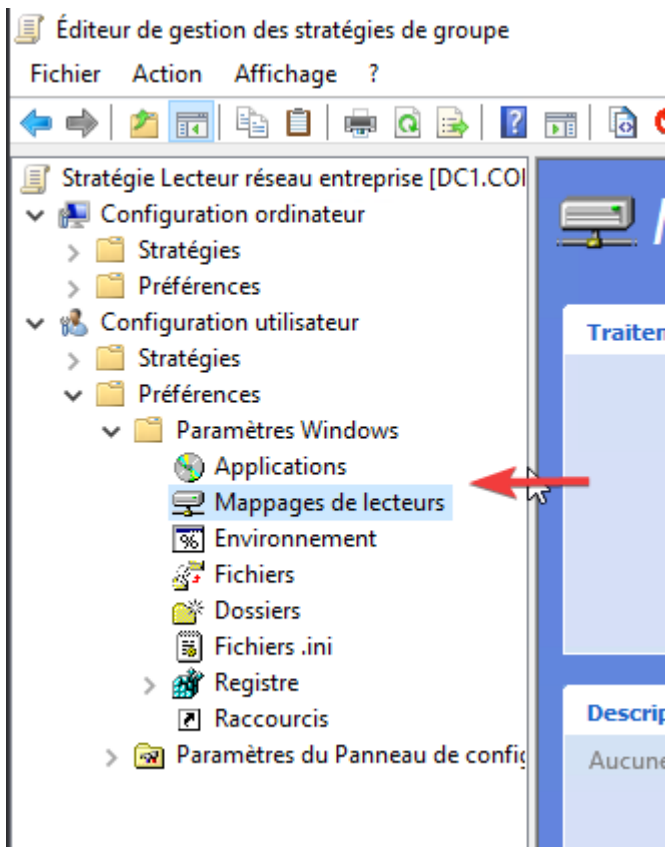
Ouvrez l'outil de "Gestion de stratégie de groupe", sélectionner le domaine corp.iia-laval.fr, puis créer une nouvelle GPO.



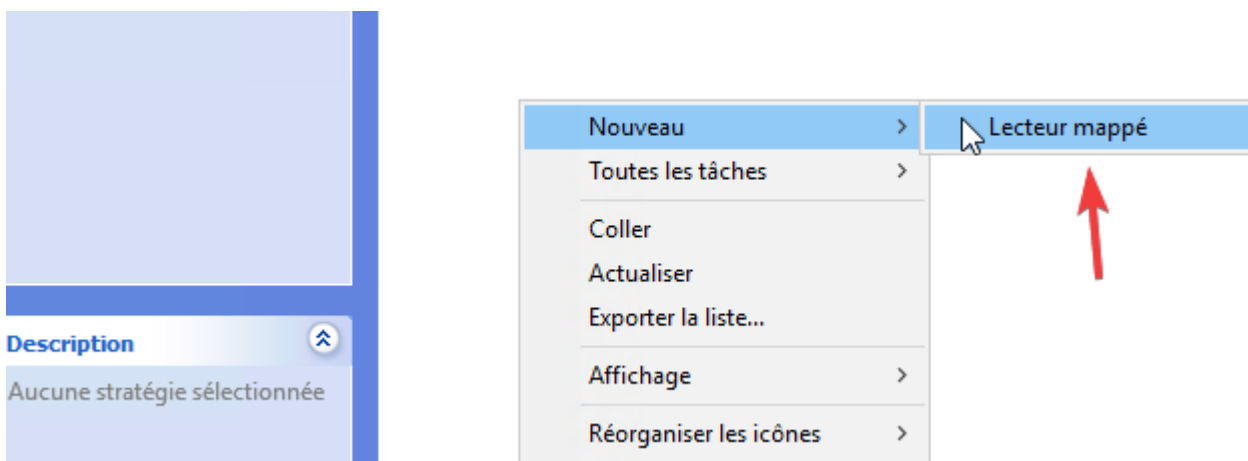
Utiliser un nom explicite pour mieux organiser les GPO.



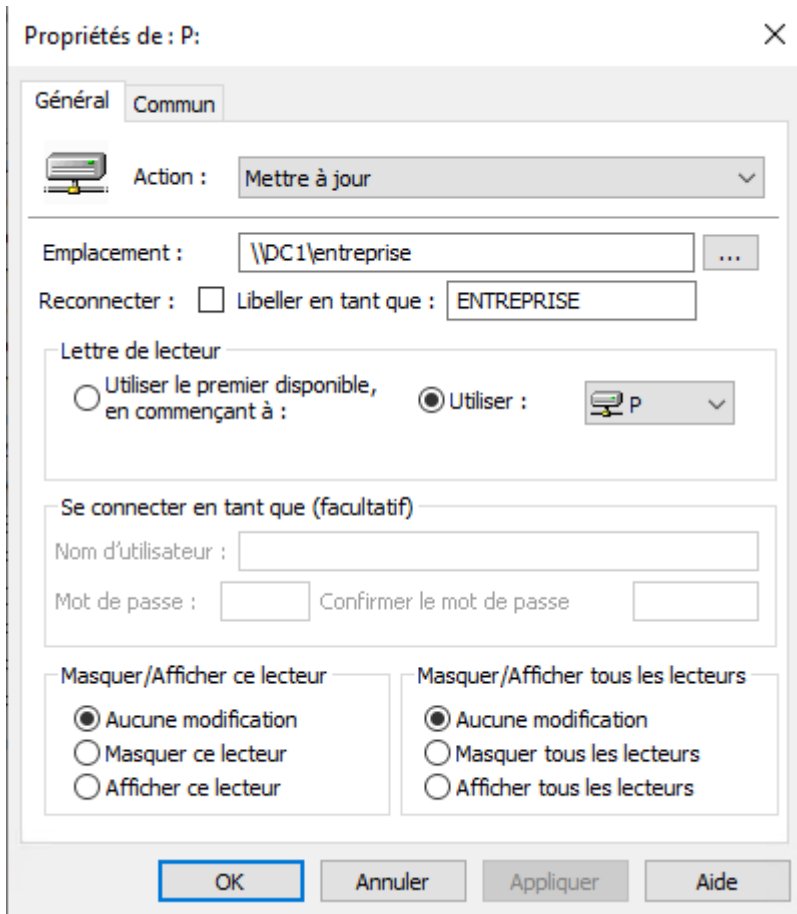
Editer la GPO, en faisant clique droit dessus. Ouvrer l'onglet "Mappages de lecteurs" :



Puis clique droit, Nouveau>Lecteur mappé :



Choisissez la lettre de lecteur P : :



## Essai avec le compte à Michel CASSE

Sur le **[CLIENT]**, essayez de vous connecter avec l'utilisateur mcasse. Lancer une invite de commande puis tapez :

```
gpupdate /force
```

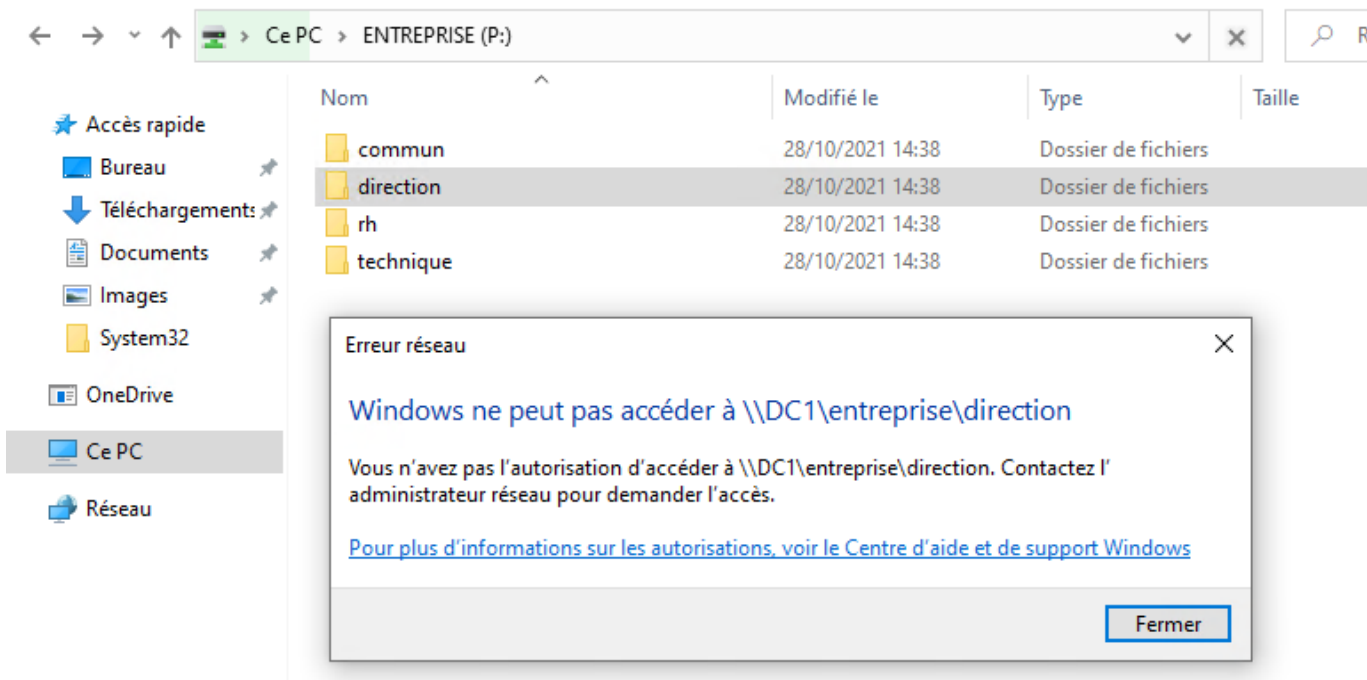
```
C:\Users\mcasse>gpupdate /force
Mise à jour de la stratégie...

La mise à jour de la stratégie d'ordinateur s'est terminée sans erreur.
La mise à jour de la stratégie utilisateur s'est terminée sans erreur.
```

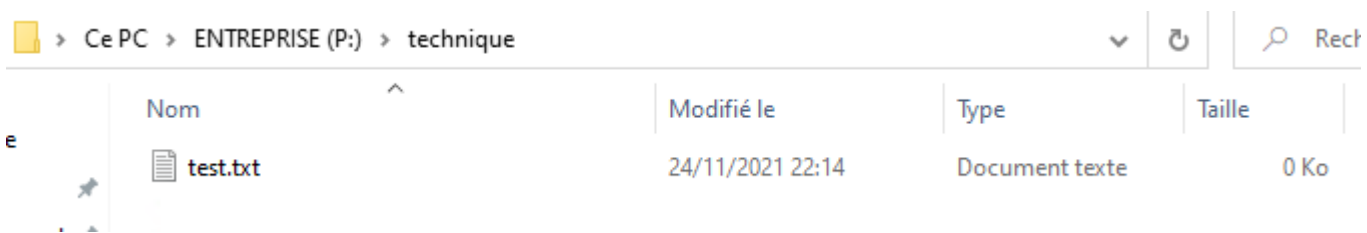
Cela à pour but de actualiser les règles imposer par AD sur le **[CLIENT]**.

Le lecteur réseau "ENTREPRISE" apparait.

Test accès au dossier "Direction" :



Test accès écriture/suppression "technique" :

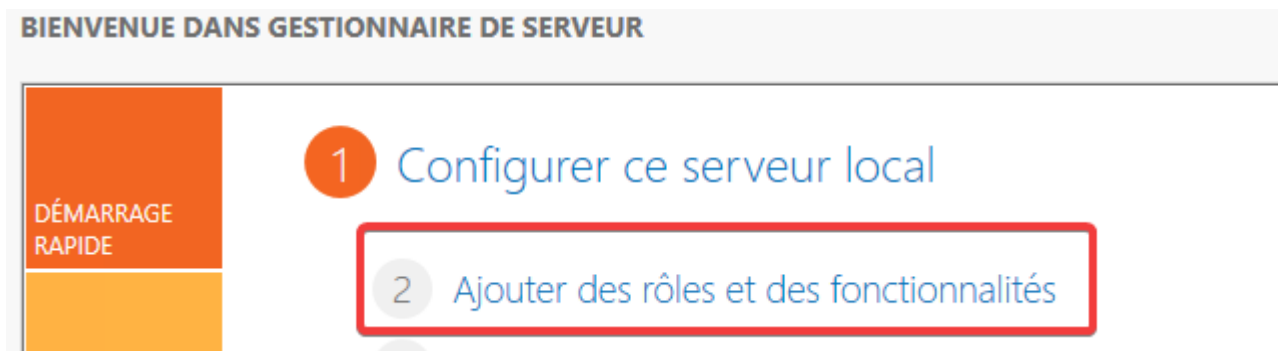


Tout fonctionne parfaitement, les permissions sont fonctionnelles.

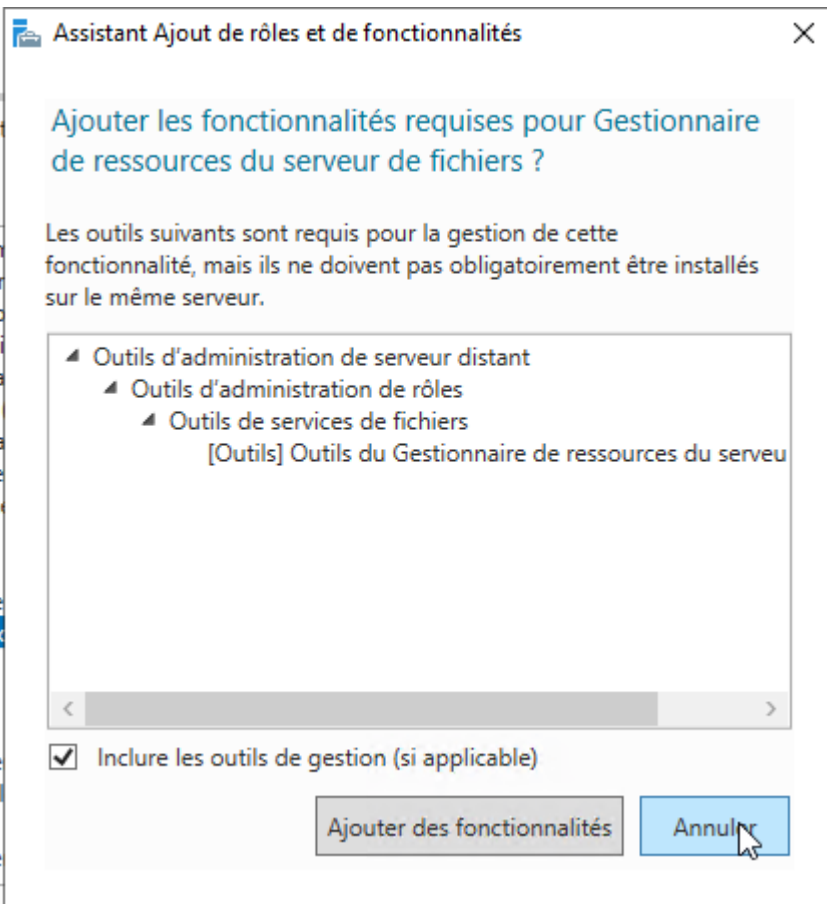
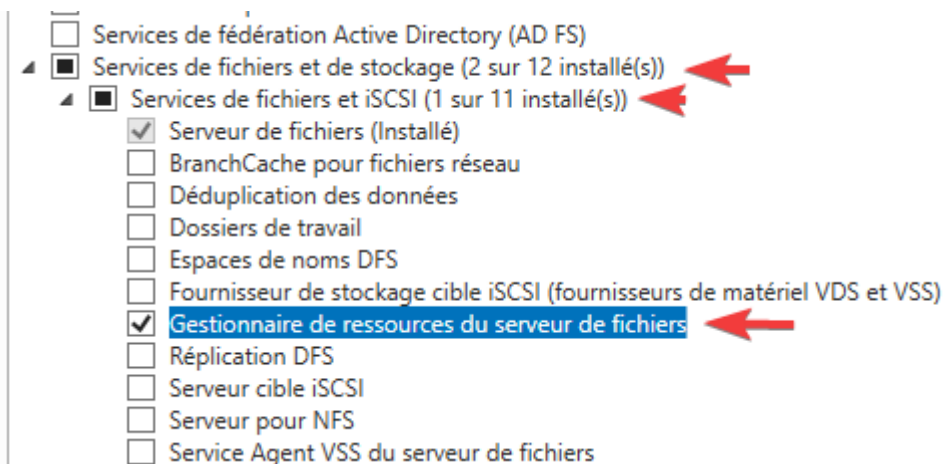
## Filtrage des fichiers .locky

### Installation de la fonctionnalité "Gestionnaire de ressources du serveur de fichiers"

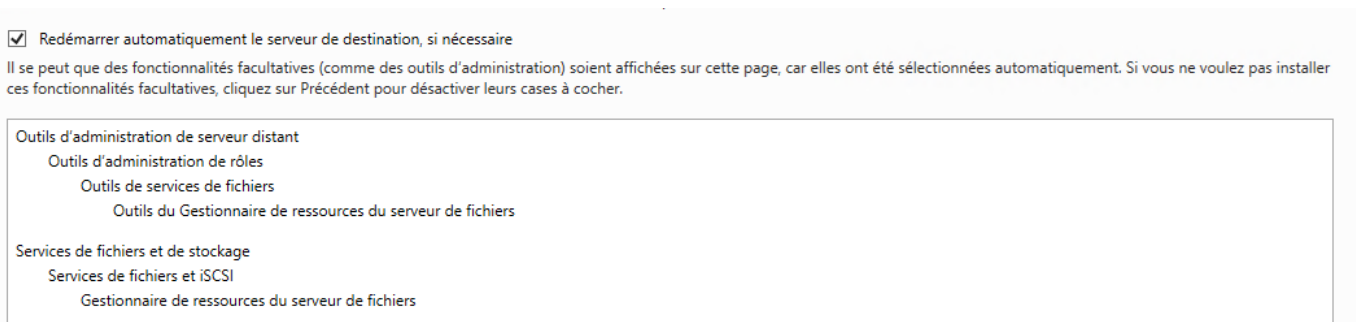
Ouvrez le gestionnaire de serveur.



Installez la fonctionnalité "Gestionnaire de ressources du serveur de fichiers"

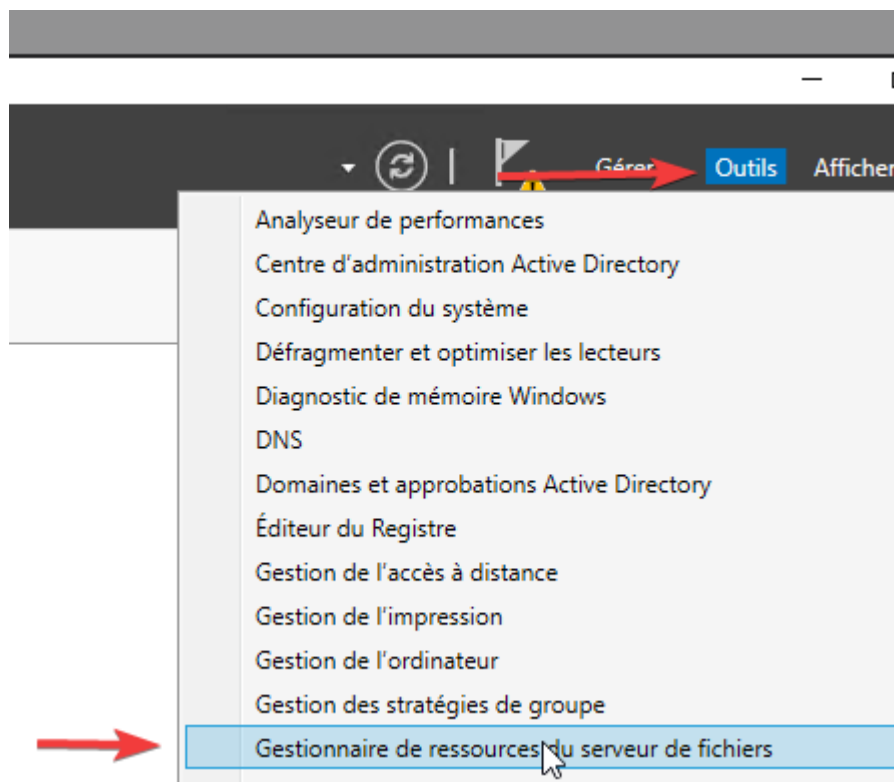


Le redémarrage du serveur n'est pas obligatoire.

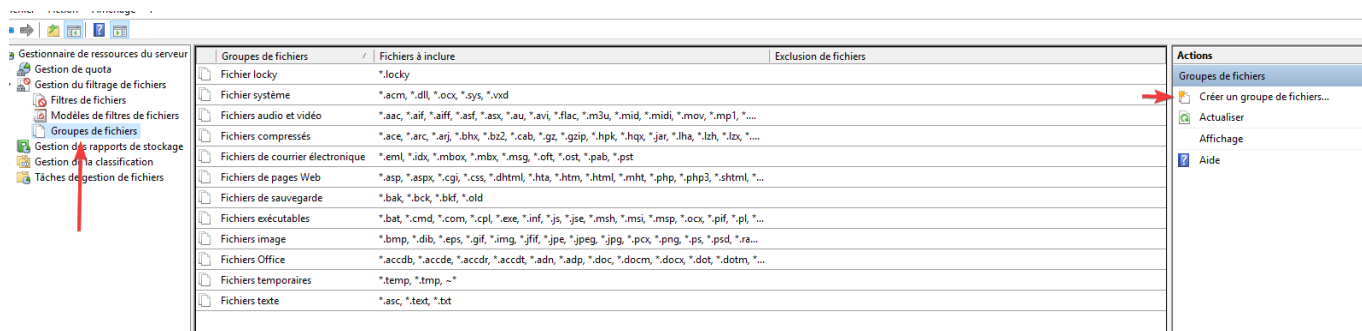


L'installation est désormais terminée, vous pouvez ouvrir le module installé.

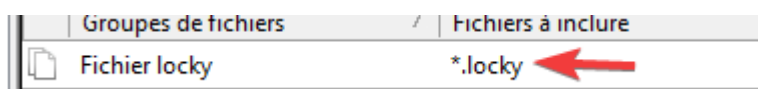
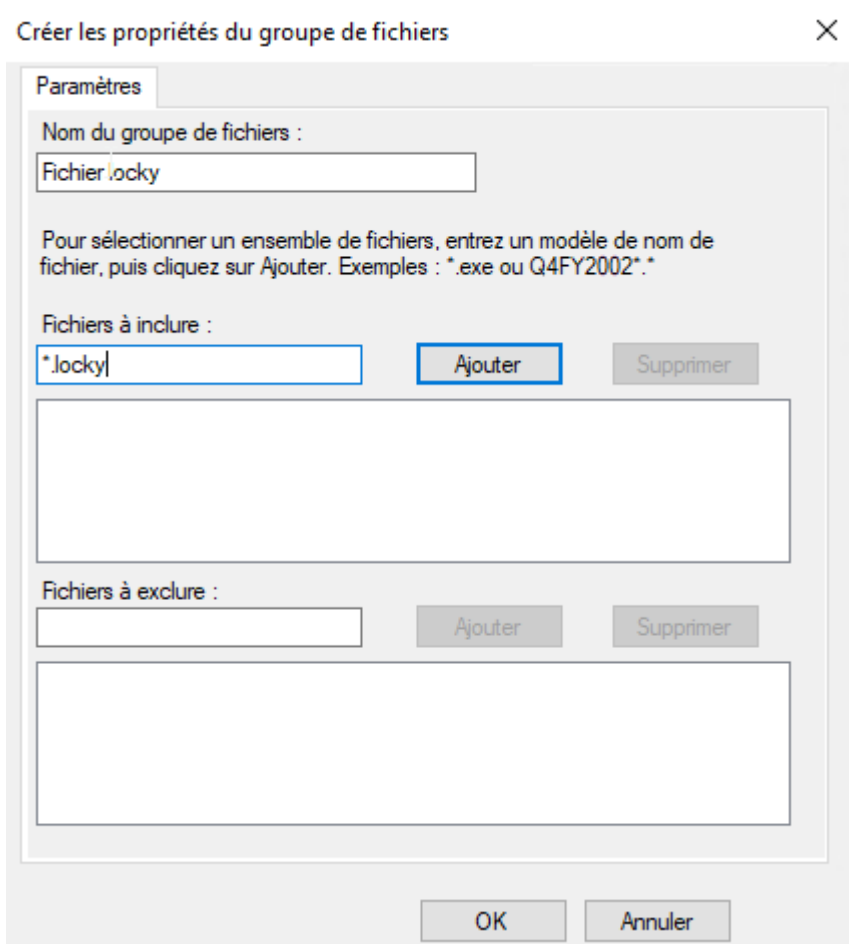
## Création d'un groupe de fichiers



Dans l'onglet à gauche, cliquer sur "Groupes de fichiers". Puis ensuite à droite "Créer un groupe de fichier".



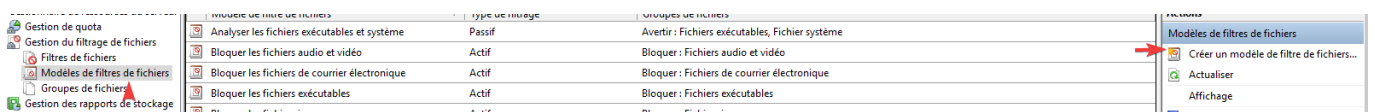
Si vous souhaitez filtrer d'autres extensions, il suffit de les ajouter comme pour \*.locky



Le groupe de fichier locky est bel et bien créé.

## Création du modèle de filtre de fichiers

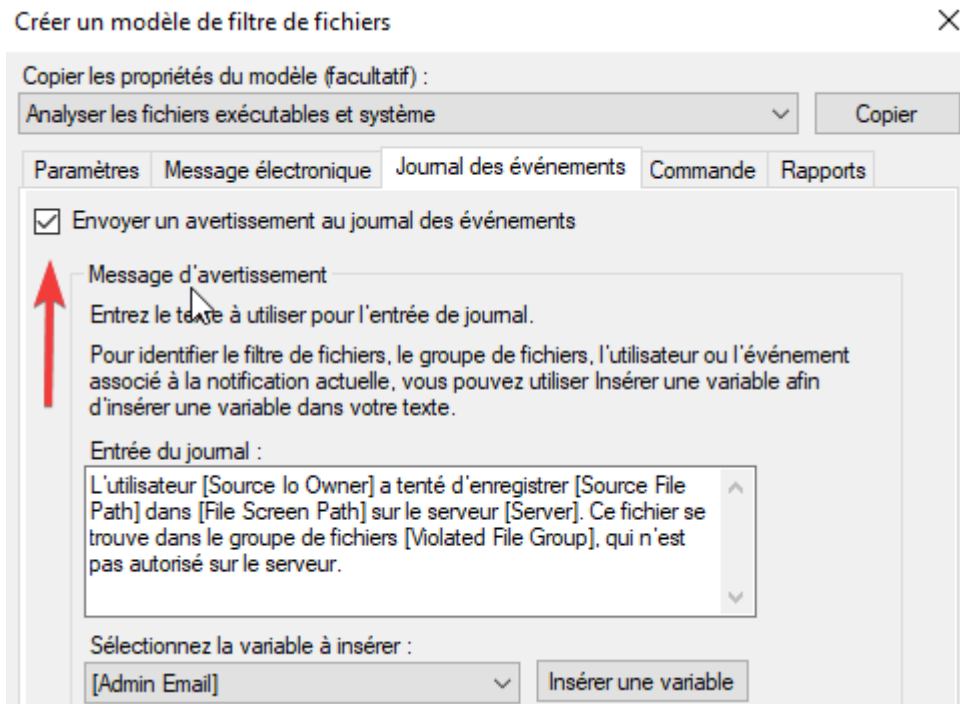
Changer d'onglet pour aller dans le "Modèles de filtres de fichiers".



Attention à bien sélectionner un filtrage actif.

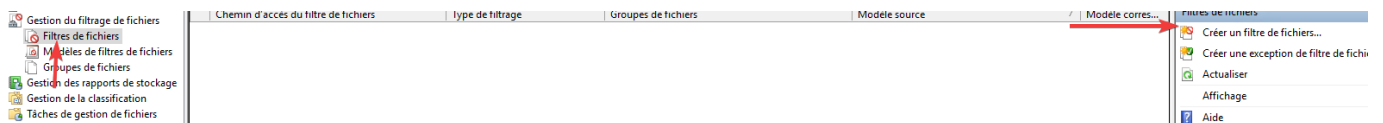




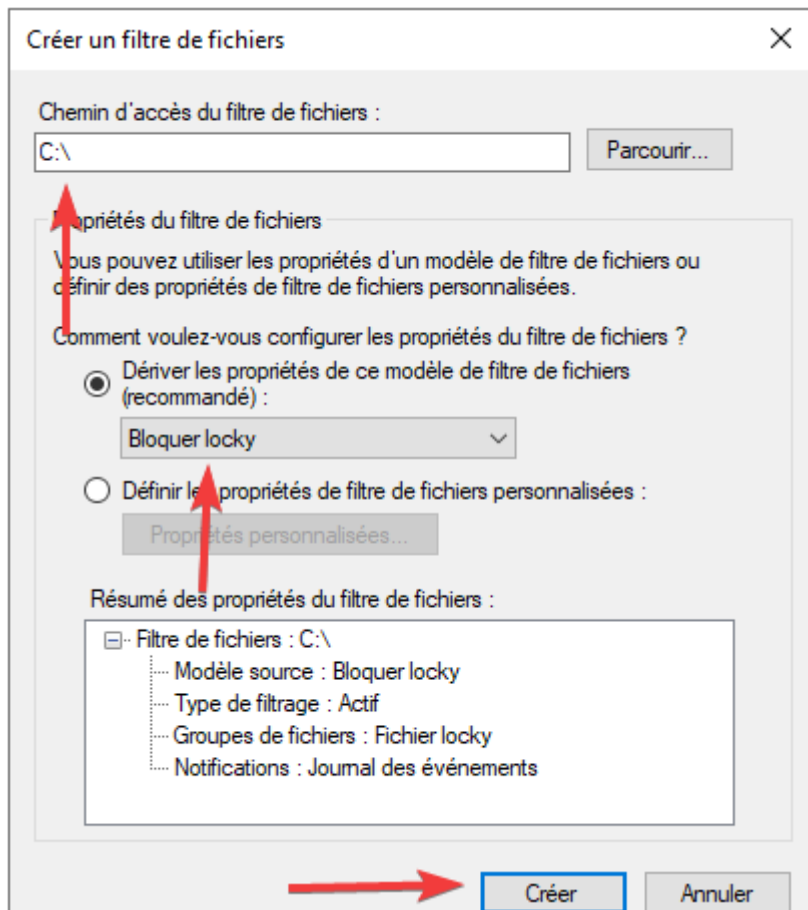


## Appliquer un filtre de fichiers

Pour terminer nous allons appliquer ce filtre au serveur.

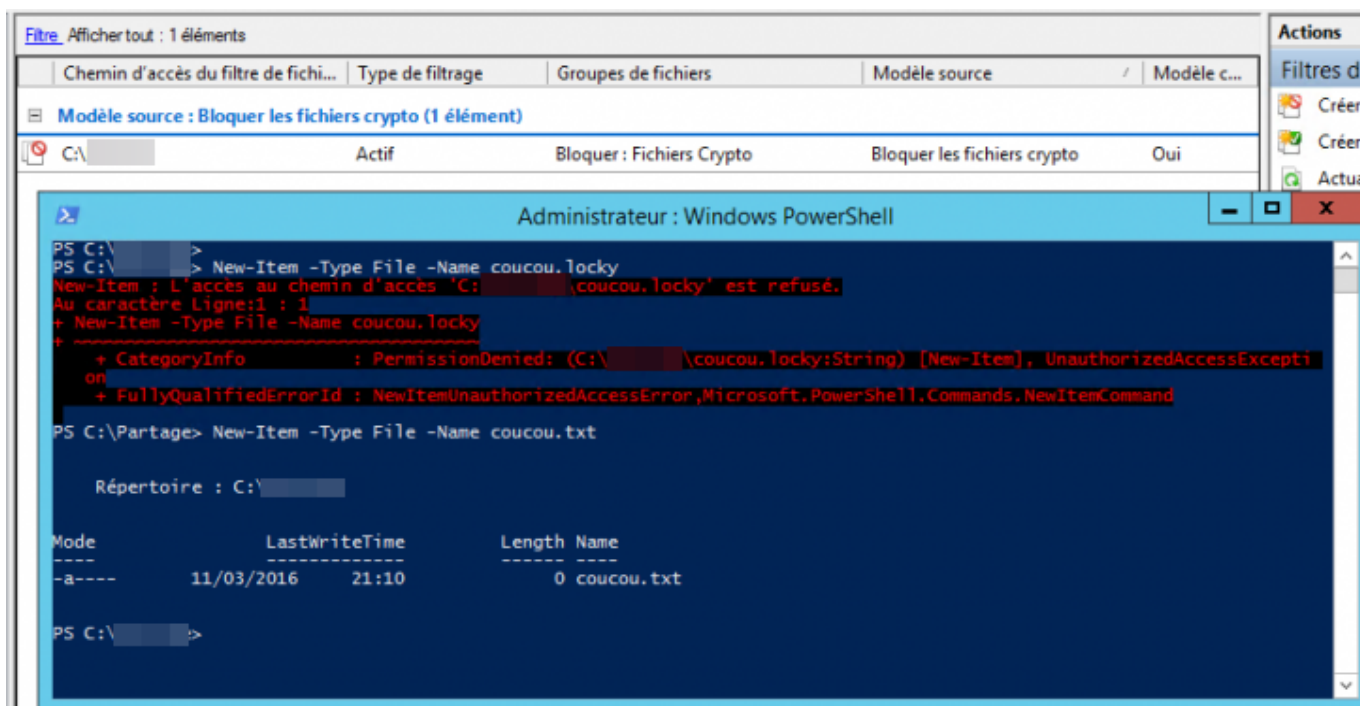


Ici on à carrément tout le C : \ qui est sous watchdog.



## Essai avec le compte à Michel CASSE

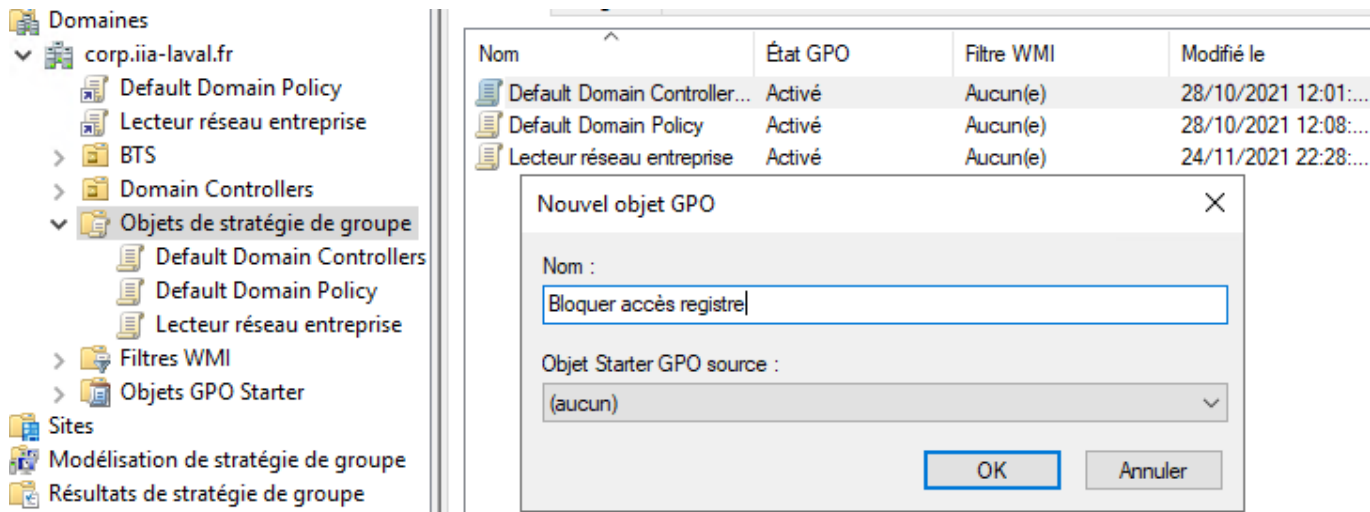
La configuration est validée et active sur le chemin C:\ , si j'ouvre une console PowerShell et que je tente de créer un fichier avec une extension interdite, j'obtiens un accès refusé. À l'inverse, si je crée un fichier avec une extension autorisée, la création s'effectue.



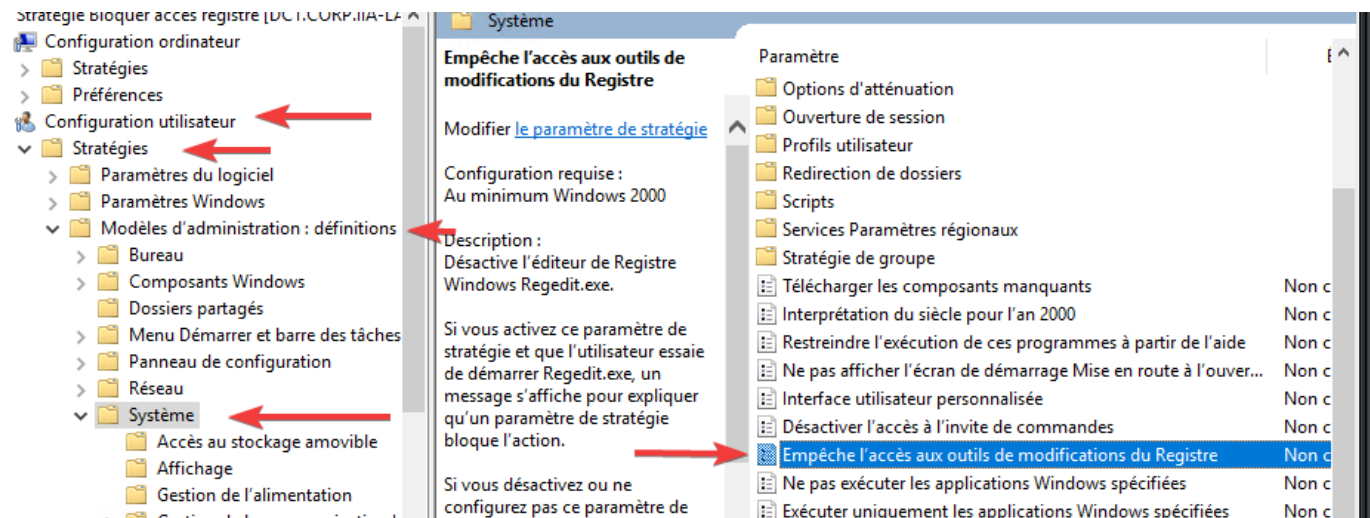
# Bloquer l'accès au registre et au panneau de configuration via GPO

## Accès au registre

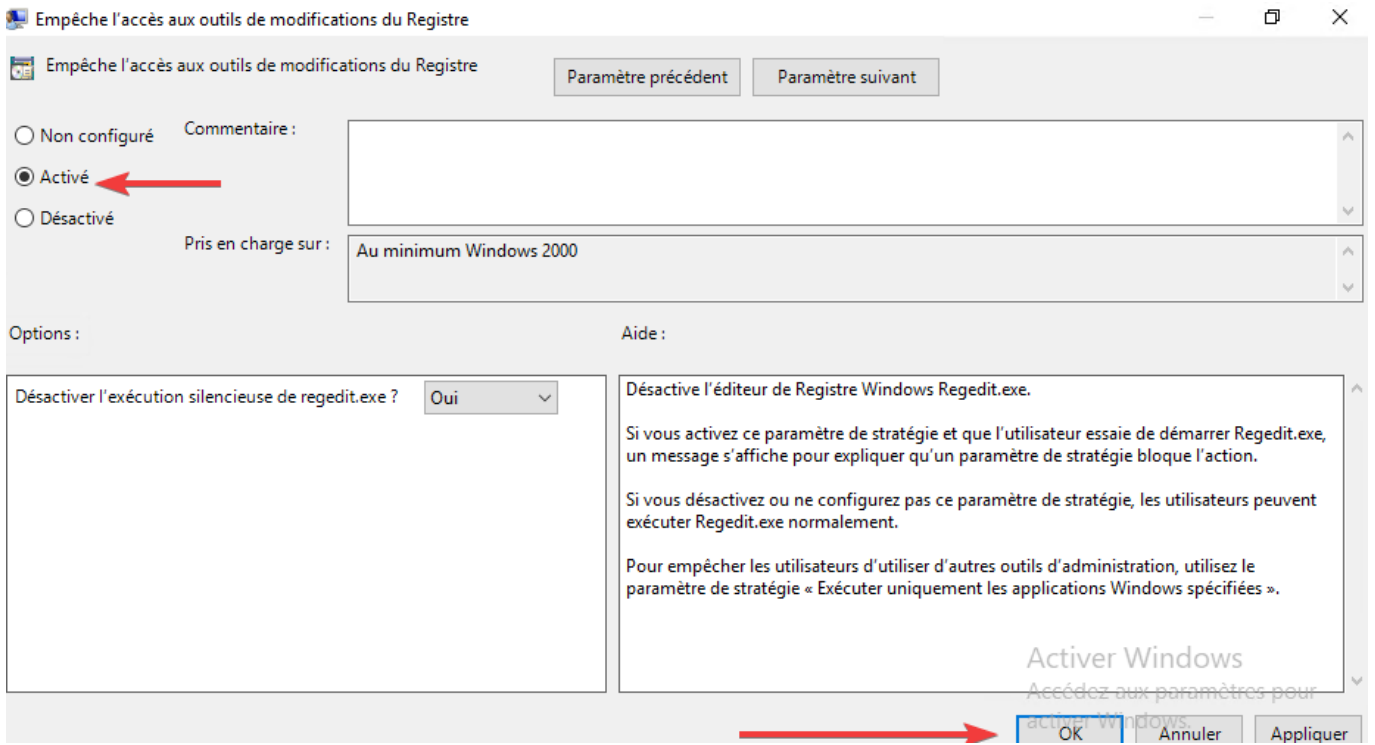
Créer une nouvelle règle dans le gestionnaire de stratégie de groupe :



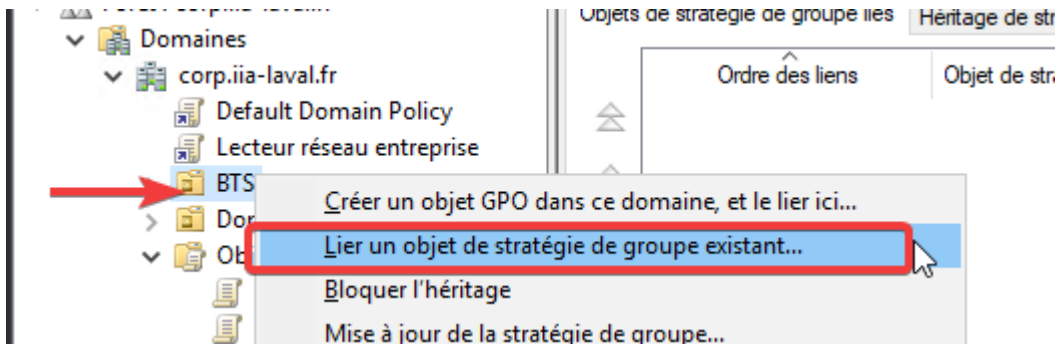
Naviguer pour trouver "Empêche l'accès aux outils de modifications du Registre" :

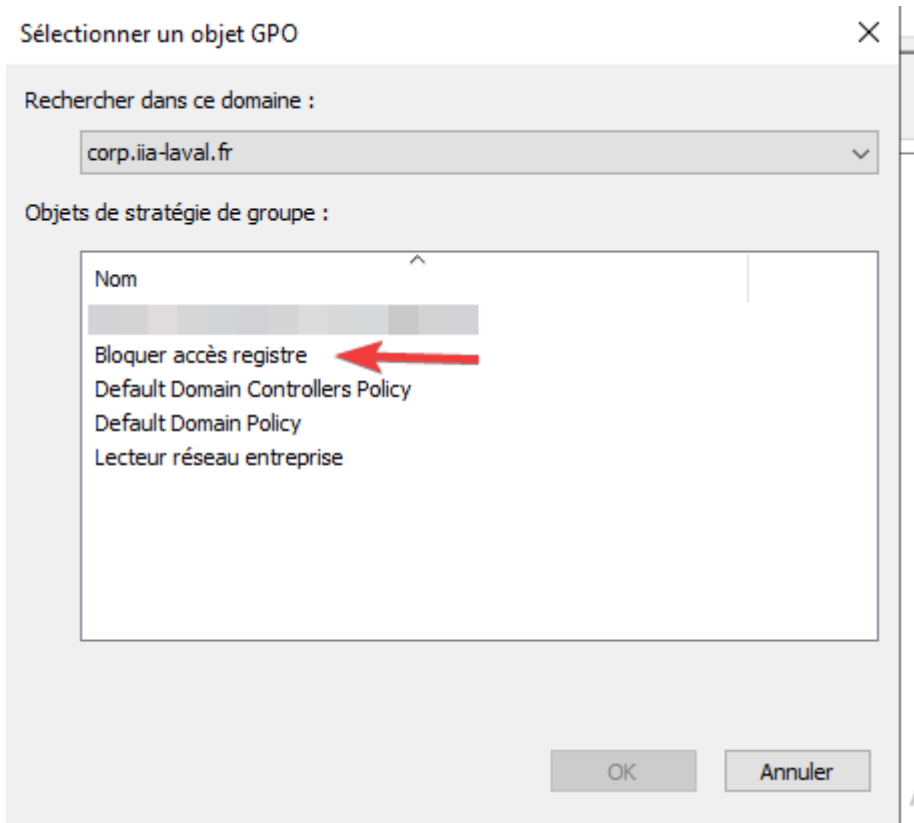


Passer la règle en "Oui" :



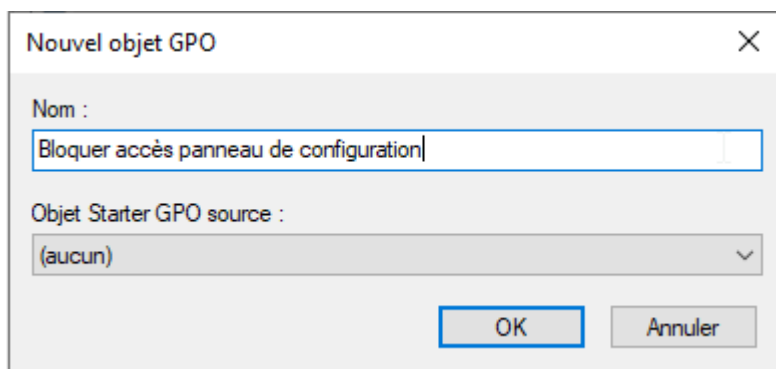
**Important !** Lier la règle aux groupes "BTS" :



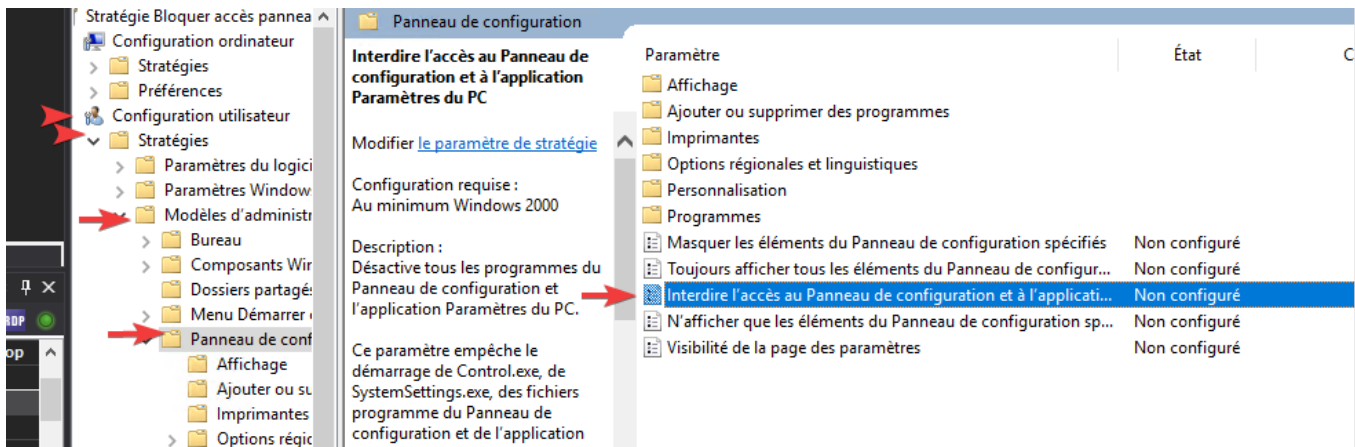


## Accès au panneau de configuration

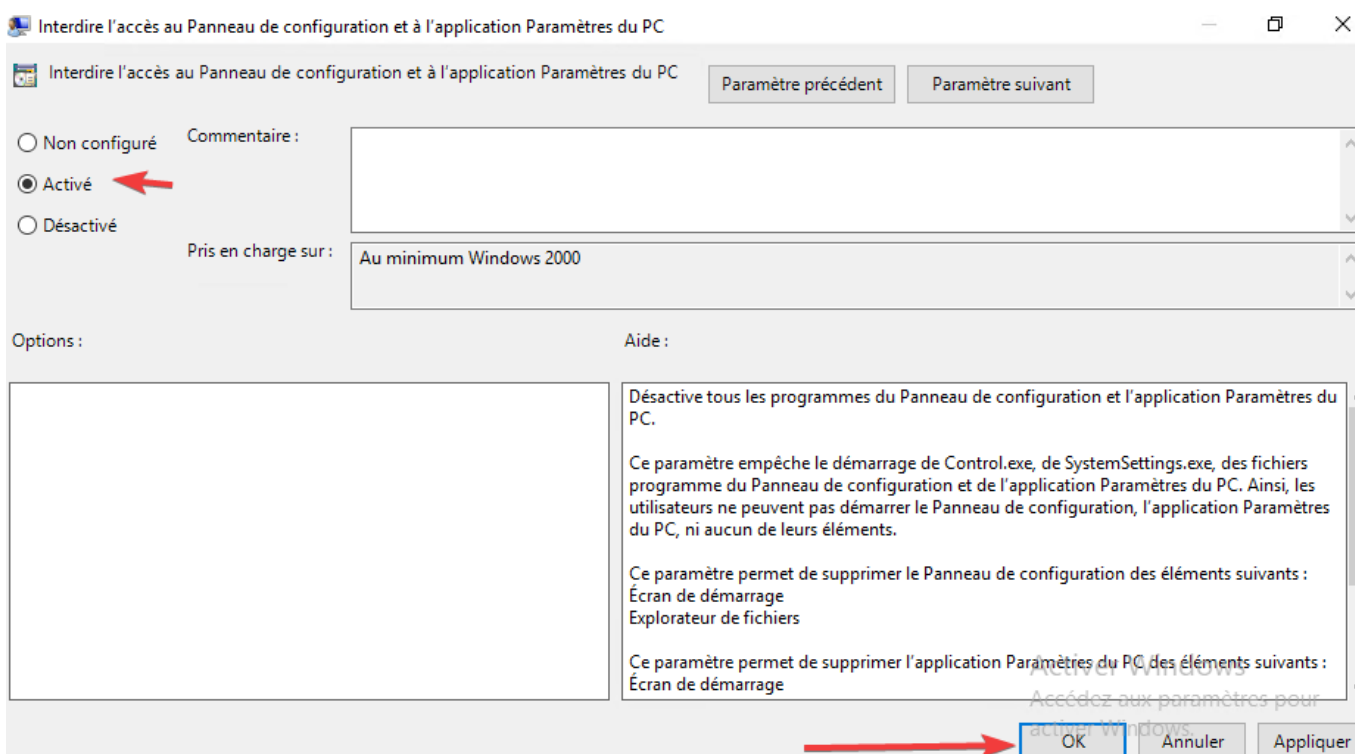
Créer une nouvelle règle dans le gestionnaire de stratégie de groupe :



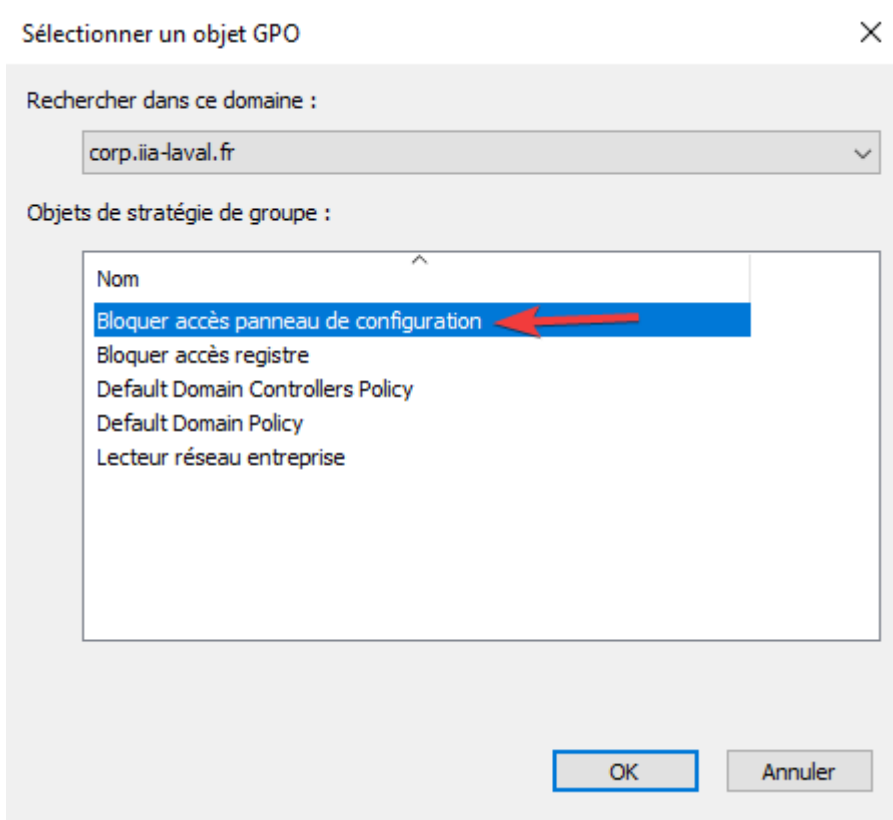
Naviguer pour trouver "Interdire l'accès au Panneau de configuration et à l'application Paramètres du PC" :



Passer la règle en "Oui" :



Pour terminer, lier la règle :



## Essais avec le compte à Michel CASSE

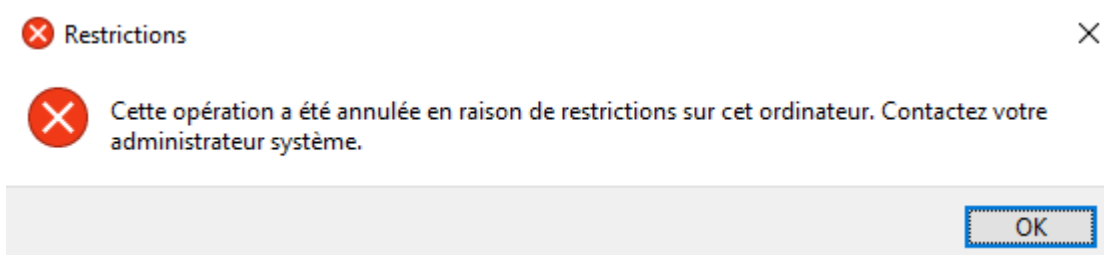
Sur le **[CLIENT]**, essayez de vous connecter avec l'utilisateur mcasse (comme déjà vu précédemment). Lancer une invite de commande puis tapez :

gpupdate /force

```
C:\Users\mcasse>gpupdate /force
Mise à jour de la stratégie...

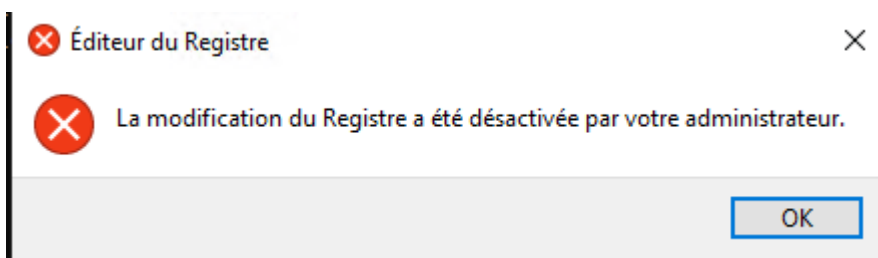
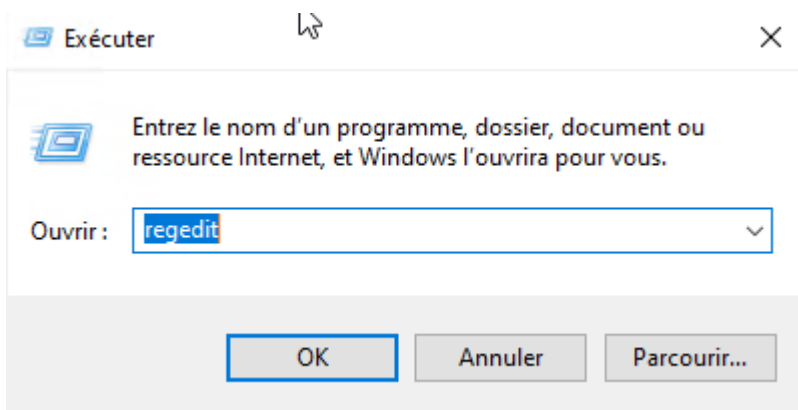
La mise à jour de la stratégie d'ordinateur s'est terminée sans erreur.
La mise à jour de la stratégie utilisateur s'est terminée sans erreur.
```

## Test avec le panneau de configuration



L'accès est refusé.

## Test avec regedit



L'accès est refusé.

Les règles sont belles et bien appliquées.

## Créations d'un dossier personnel pour tous les users de 100 Mo

### Création des dossiers users manuellement

A partir de cette arborescence, recréer le dossier "users".

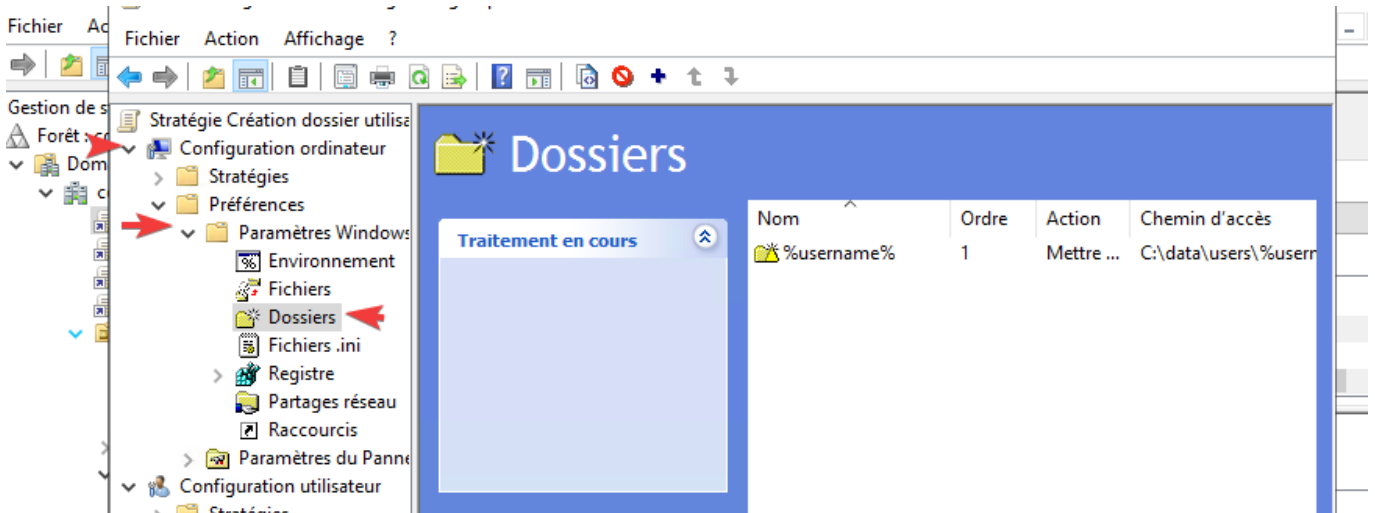
```
PS C:\data> tree
structure du dossier
le numéro de série du volume est F813-0D8D
.:
- entreprise
  - commun
  - direction
  - rh
    - paie
  - technique
- users
  - dbille
  - jteli
  - laimable
  - mcasse
  - melec
  - mterre
  - navant
```



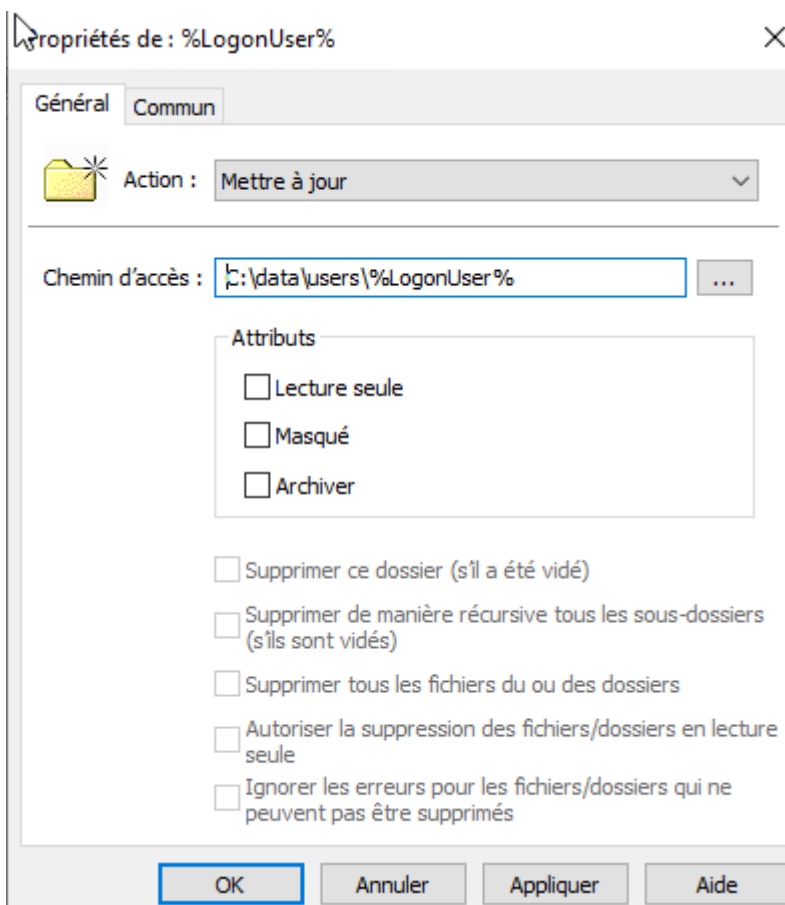
## Création du dossier "user" automatiquement

Lorsque l'entreprise possède plusieurs centaines d'utilisateurs, il est plus simple que la création soit faite automatiquement. Pour cela nous allons créer une GPO qui créera un dossier dans C:\data\users\ avec comme nom le nom de la session.

Ouvrir le Gestionnaire de stratégie de groupe, créer une nouvelle GPO, nommer la "Création dossier utilisateur".



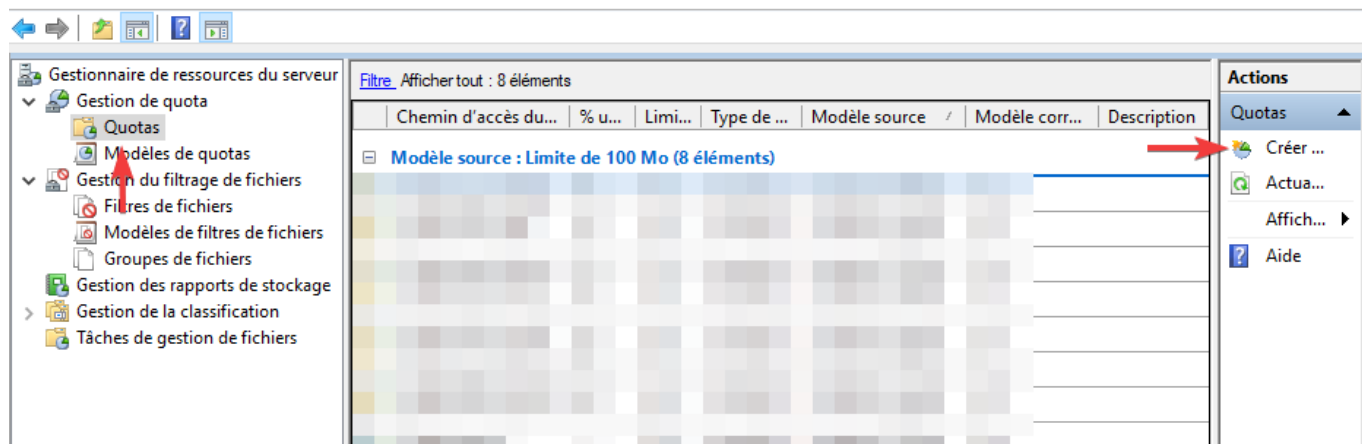
Indiquer le path où les dossiers seront créés.



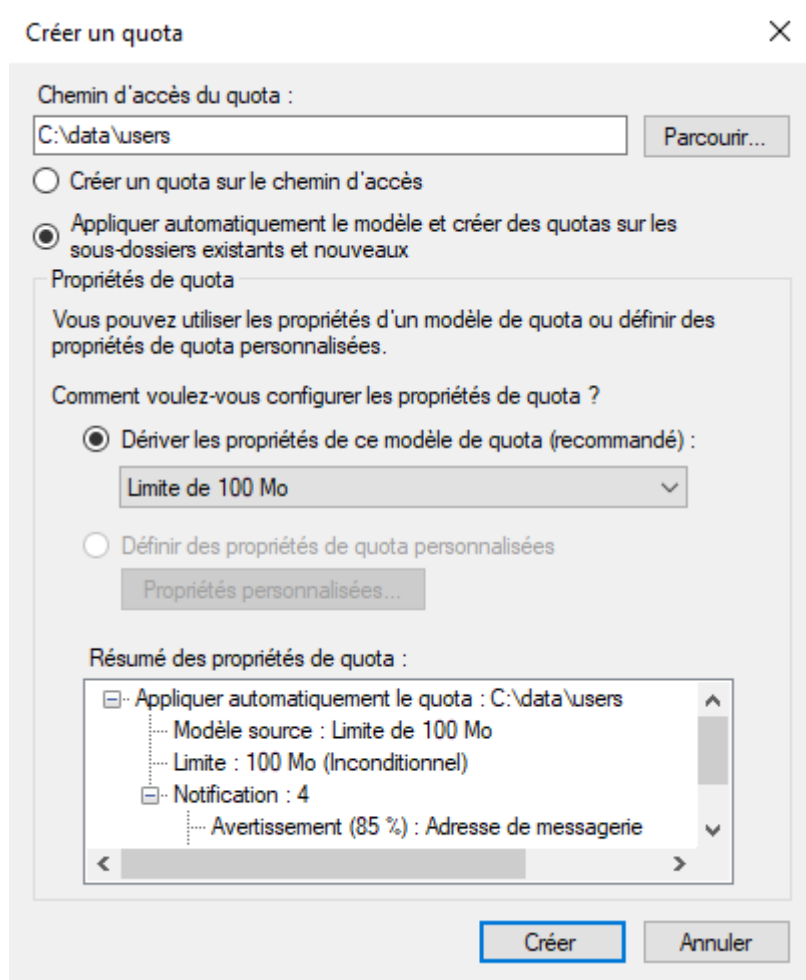
A chaque nouvelle connexion, le dossier sera, si il existe déjà rien ne sera fait.

## Appliquer le quota sur les sous-dossiers de "users"

Ouvrez le Gestionnaire de ressources du serveur de fichiers précédemment installé.



Créer un quota en utilisant le modèles de quota de 100 Mo. Spécifier le path avec C:\data\users.

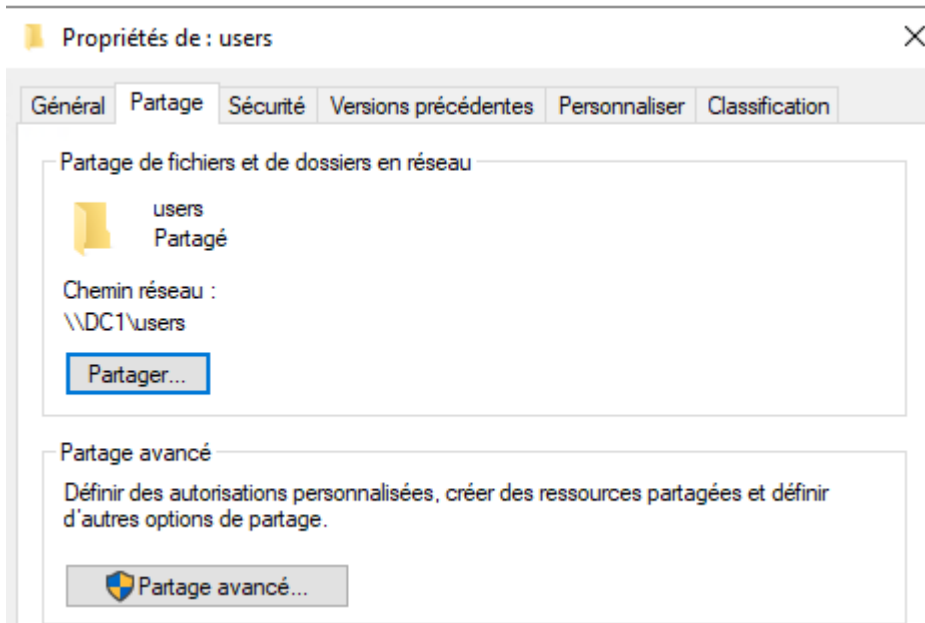


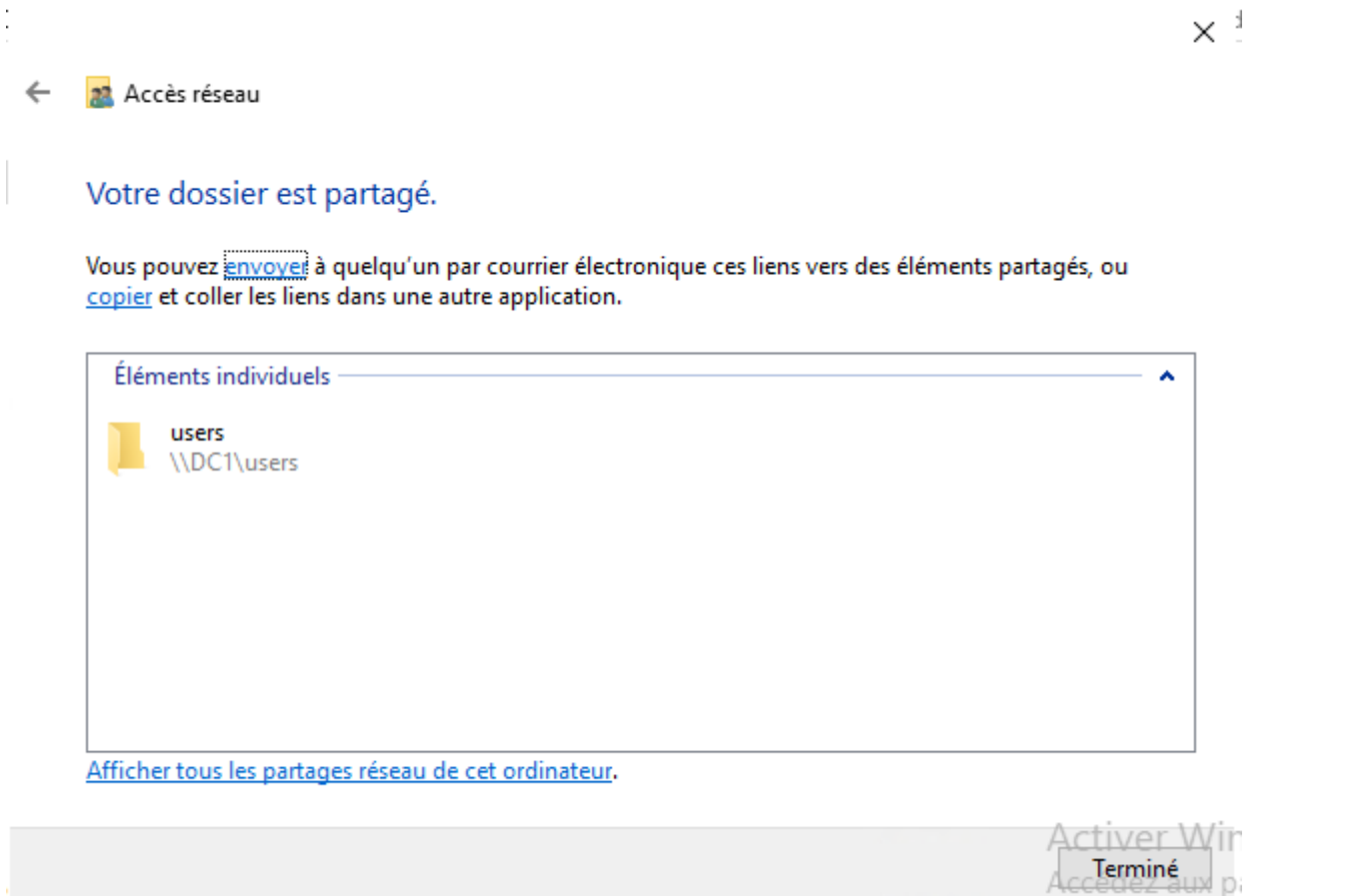
Vous retrouvez ici tous les quotas pour les dossiers existants.

Chemin d'accès du...	% u...	Limi...	Type de ...	Modèle source /	Modèle c
[-] <b>Modèle source : Limite de 100 Mo (8 éléments)</b>					
C:\data\users\dbille	0%	100 ...	Inconditi...	Limite de 100 Mo	Oui
C:\data\users\jteli	0%	100 ...	Inconditi...	Limite de 100 Mo	Oui
C:\data\users\laima...	0%	100 ...	Inconditi...	Limite de 100 Mo	Oui
C:\data\users\mcas...	0%	100 ...	Inconditi...	Limite de 100 Mo	Oui
C:\data\users\melec	0%	100 ...	Inconditi...	Limite de 100 Mo	Oui
C:\data\users\mterre	0%	100 ...	Inconditi...	Limite de 100 Mo	Oui
C:\data\users\navant	0%	100 ...	Inconditi...	Limite de 100 Mo	Oui
C:\data\users\*	---	100 ...	Inconditi...	Limite de 100 Mo	Oui

## Partage du dossier "users"

Pour rendre accessible l'ensemble des dossiers dans "users", il faut partager publiquement le dossier "users".

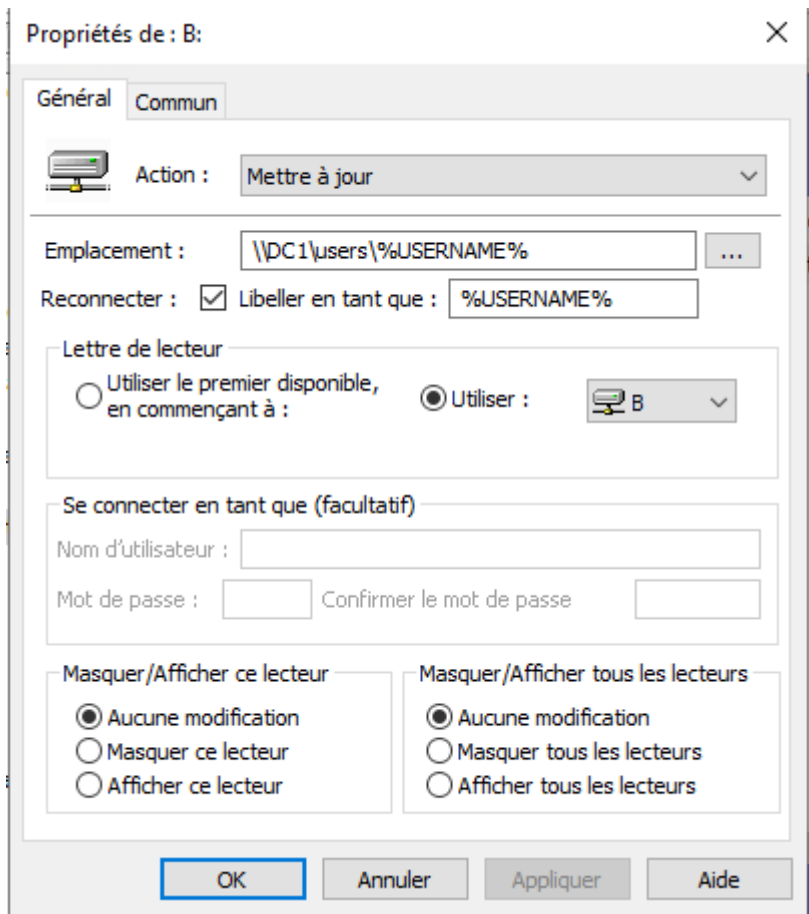




Le partage est existant sous le nom de `\\DC1\users`.

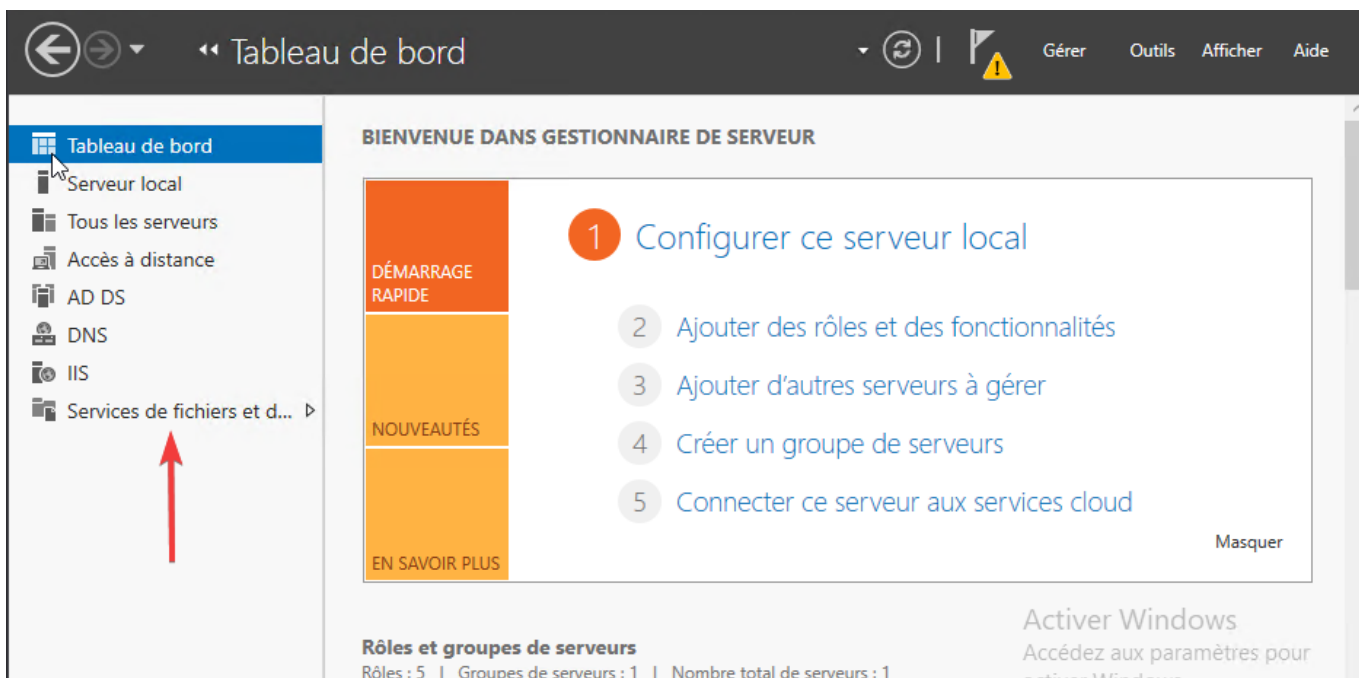
## Montage du lecteur "Users"

Comme déjà fait précédemment, créer une GPO pour monter un lecteur. Ici le lecteur B: , spécifier le path et ajouter la variable %USERNAME%.

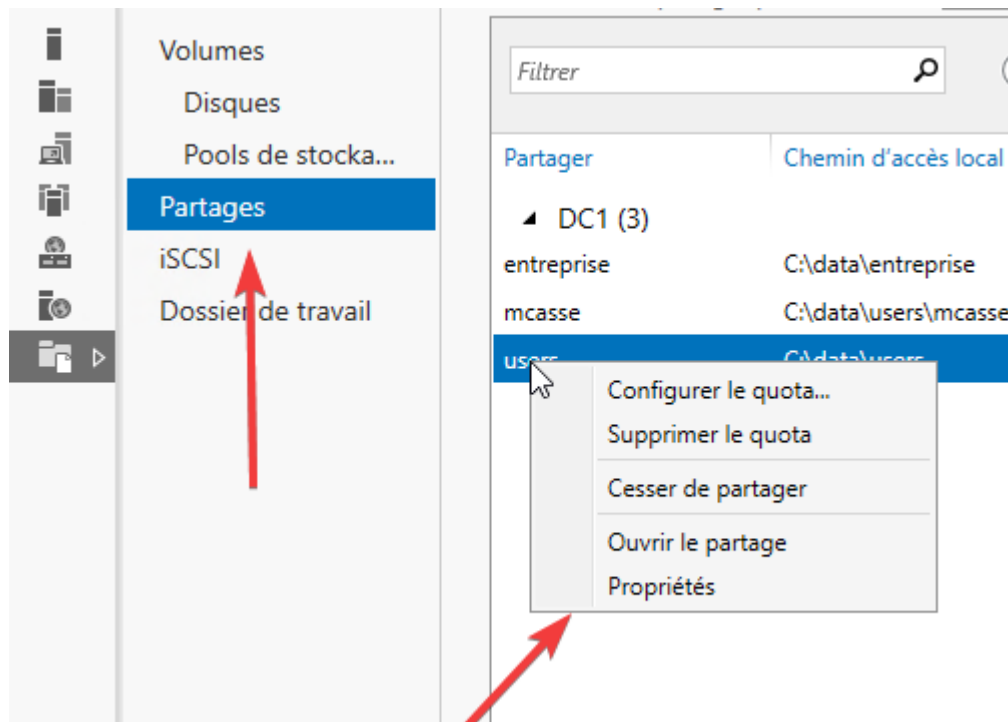


## Cacher les dossiers non accessible

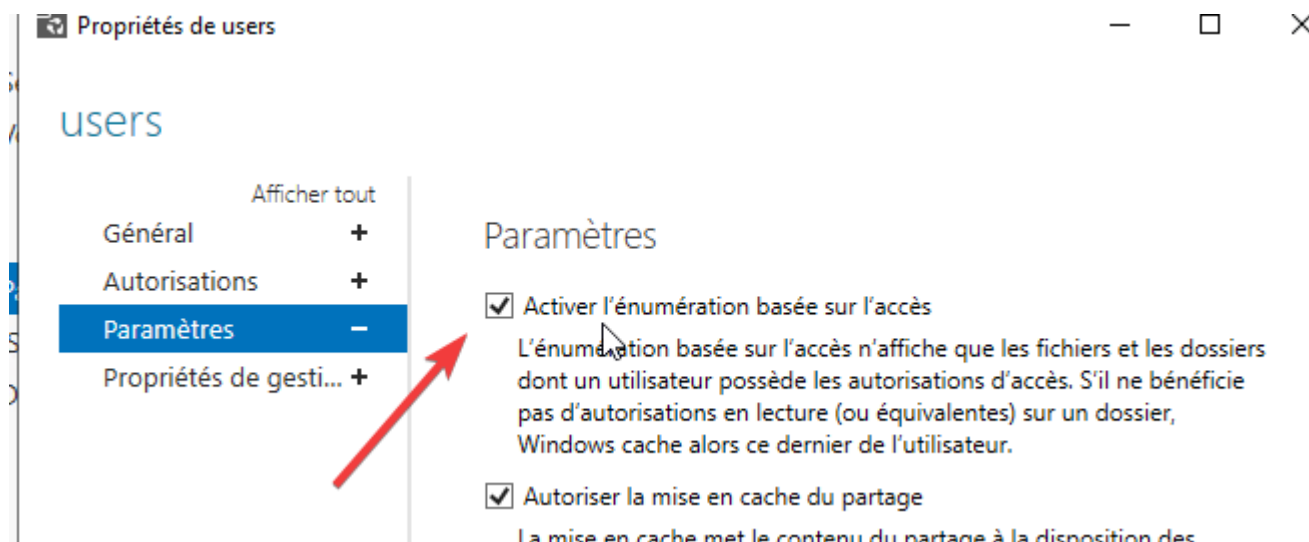
Par mesure de sécurité, cacher les dossiers non accessibles aux utilisateurs.



Clique droit sur le partage de fichier "users".

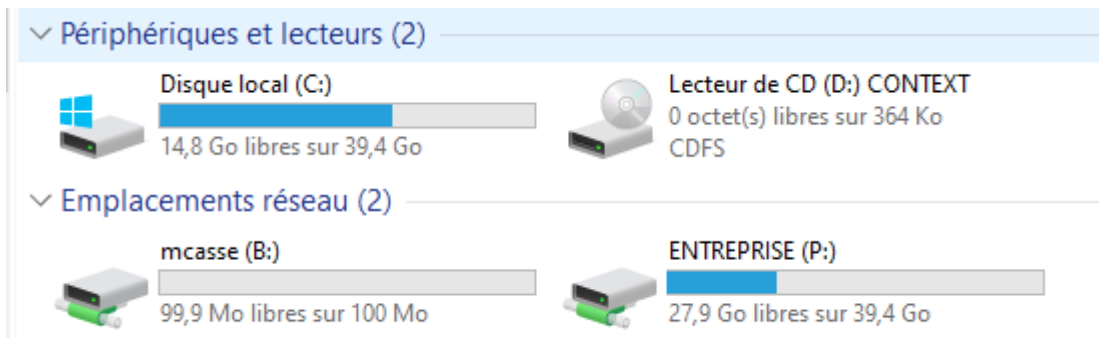


Cocher "Activer l'énumération basée sur l'accès".

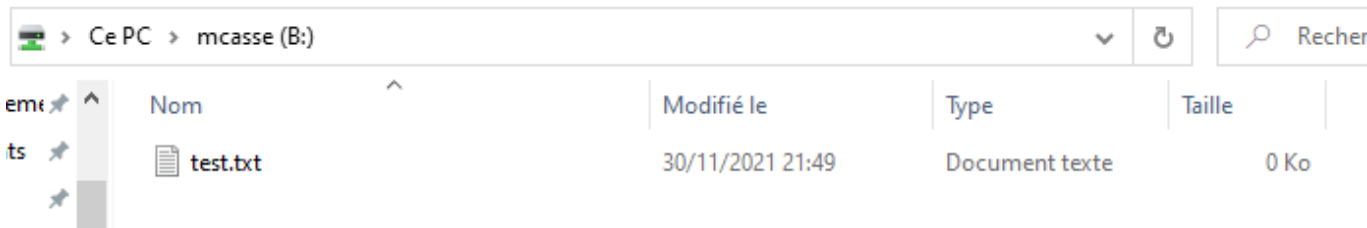


## Essai avec le compte à Michel CASSE

Pour terminer, tester avec un compte. Ici mcasse, une fois connecté on remarque que le lecteur est bien monté que le quota est bel et bien de 100 Mo.



Il dispose par ailleurs les droits d'écritures et de suppressions.



## Mes sources

1. Tous les screens en raw : [http://files.stoneset.fr/stoneset/images/doc\\_ad/?C=M;O=D](http://files.stoneset.fr/stoneset/images/doc_ad/?C=M;O=D)
2. <https://chmod-calculator.com/>
3. <https://rdr-it.com/windows-serveur-appliquer-des-quotas-sur-des-dossiers/>
4. <https://rdr-it.com/mappage-lecteur-reseau-gpo-et-script/>
5. <https://techexpert.tips/fr/windows-fr/gpo-empêcher-l'accès-au-registre-windows/>
6. <https://www.it-connect.fr/gpo-empêcher-l'accès-au-panneau-de-configuration-paramètres/>
7. <https://computerz.solutions/windows-server-quota-sur-dossiers/>
8. <https://www.tutos-informatique.com/cacher-dossier-windows-arborescence/>

From: <https://wiki.stoneset.fr/> - **StoneSet - Documentations**

Permanent link: <https://wiki.stoneset.fr/doku.php?id=wiki:windows:howtoconfiguresimplead>

Last update: **2022/11/08 09:28**

