

Mission 14 – Création d'un annuaire
Active Directory - WS2019/22
Authentification centralisée
Redirection des répertoires utilisateur
GPO



Un annuaire est une structure hiérarchique stockant des informations sur les objets du réseau. Un service d'annuaire, comme Active Directory Domain Services (AD DS), propose des méthodes pour stocker des données d'annuaire et rendre ces données disponibles aux utilisateurs et administrateurs du réseau. Par exemple, les services de domaine Active Directory stockent des informations sur les comptes d'utilisateurs, comme les noms, les mots de passe, les numéros de téléphone et permet aux utilisateurs autorisés du même réseau d'accéder à ces informations.

Active Directory stocke des informations relatives aux objets d'un réseau et les met à la disposition des utilisateurs et des administrateurs réseau afin qu'ils puissent les trouver et les utiliser rapidement. Active Directory utilise un magasin de données structuré comme la base de son organisation hiérarchique et logique des informations de répertoire.

Ce magasin de données, également appelé annuaire, contient des informations sur les objets Active Directory. Ces objets incluent généralement des ressources partagées telles que des serveurs, des volumes, des imprimantes et des comptes d'utilisateur et d'ordinateur réseau. Pour plus d'informations sur le magasin de données Active Directory, consultez Magasin de données Directory.

La sécurité est intégrée avec Active Directory par le biais de l'authentification de connexion et du contrôle d'accès aux objets du répertoire. Avec une simple ouverture de session réseau, les administrateurs peuvent gérer les données et l'organisation de l'annuaire au sein de leur réseau, et les utilisateurs du réseau autorisés peuvent accéder aux ressources n'importe où sur le réseau. L'administration basée sur des stratégies facilite même la gestion des réseaux les plus complexes. Pour plus d'informations sur la sécurité Active Directory, consultez Vue d'ensemble de la sécurité.

Active Directory inclut également les éléments suivants :

- Un ensemble de règles, le schéma, qui définit les classes d'objets et les attributs contenus dans l'annuaire, les contraintes et les limites qui s'appliquent aux instances de ces objets, ainsi que le format de leurs noms. Pour plus d'informations sur le schéma, consultez Schéma.

- Un catalogue global qui contient des informations sur chaque objet de l'annuaire. Les utilisateurs et les administrateurs peuvent ainsi rechercher des informations dans l'annuaire, quel que soit le domaine de l'annuaire qui contient les données. Pour plus d'informations sur le catalogue global, consultez Catalogue global.

- Un mécanisme de requête et d'index, de sorte que les objets et leurs propriétés puissent être publiés et recherchés par les utilisateurs du réseau ou des applications. Pour plus d'informations sur l'interrogation du répertoire, consultez Recherche dans Active Directory Domain Services.

- Un service de répllication qui distribue les données d'annuaire sur l'ensemble du réseau. Tous les contrôleurs de domaine dans un domaine participent à la répllication et contiennent une copie complète de toutes les informations d'annuaire liées à leur domaine. Toute modification des données d'annuaire est répliquée sur tous les contrôleurs de domaine inclus dans le domaine. Pour plus d'informations sur la répllication Active Directory, consultez Concepts de répllication Active Directory.

Adressage des machines

Liste des serveurs (Windows 2019/22 Server)

Groupe	Domaine	IP du serveur
Asie	asie.lan	10.31.176.200
Europe	europe.lan	10.31.192.200
Océanie	oceanie.lan	10.31.208.200
Afrique	afrique.lan	10.31.224.200
USA	usa.lan	10.31.240.200

Liste des clients (Windows 10/11 Professionnel)

Groupe	Domaine	IP du serveur
Asie	asie.lan	10.31.176.201 10.31.184.201
Europe	europe.lan	10.31.192.201 10.31.200.201
Océanie	oceanie.lan	10.31.208.201 10.31.216.201
Afrique	afrique.lan	10.31.224.201 10.31.232.201
USA	usa.lan	10.31.240.201 10.31.248.201

Ces serveurs sont hébergés sur le système de virtualisation ProxMox .

Vous accéderez à vos systèmes windows server et windows clients via le protocole RDP (Bureau à distance)

Si vous n'êtes pas sous Windows, vous pouvez installer : <https://remmina.org/>

En cas de problème d'accès au Bureau à Distance, vous pouvez vous connecter sur le serveur ProxMox afin d'accéder directement à votre serveur.

Pour l'installation des machines virtuelles vous devez obligatoirement lire la documentation :

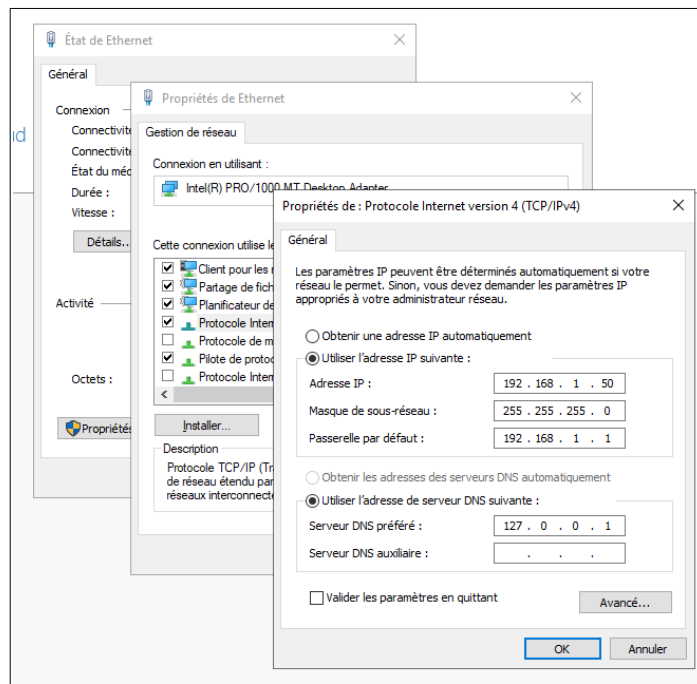
- Windows 10/11 : https://pve.proxmox.com/wiki/Windows_10_guest_best_practices
- Windows 2019/22 : https://pve.proxmox.com/wiki/Windows_2022_guest_best_practices
- Drivers VirtIO : https://pve.proxmox.com/wiki/Windows_VirtIO_Drivers

Configuration de Windows 2019 Server

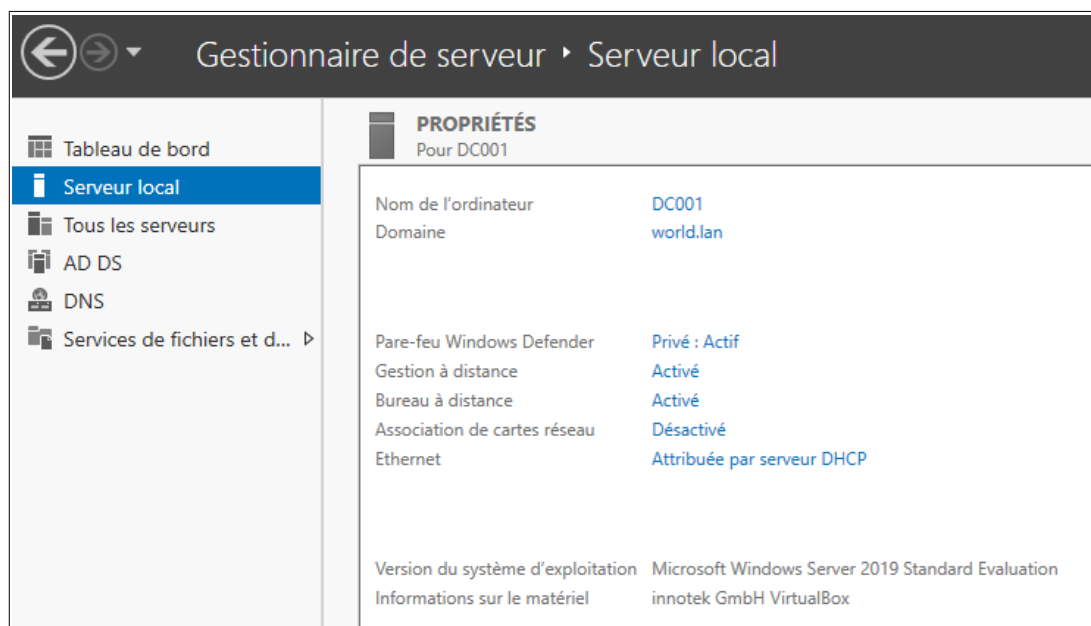
Afin de pouvoir promouvoir le serveur comme contrôleur de domaines il faut le basculer en IP Fixe. Il assurera également le rôle de serveur DNS sur le domaine et donc sera son propre serveur DNS.

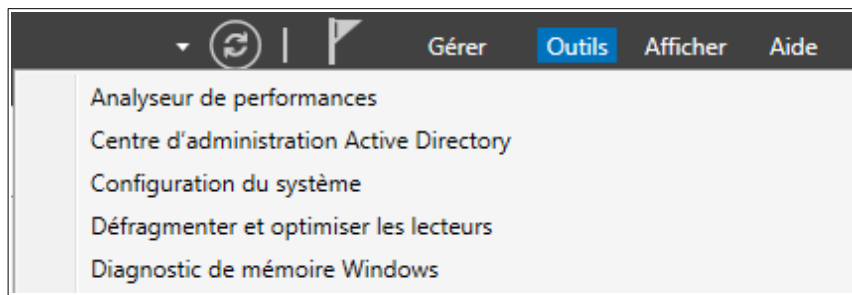
Paramètres réseau et internet

- Modifier les options d'adaptateur
 - Ethernet
 - Propriétés
 - Double clic sur ipv4



Le programme **Gestionnaire de Serveur** permet d'ajouter, gérer les différents services et rôles offerts par Windows Server 2019. Il permet également de visualiser les différents événements (logs) et les services qui sont en cours d'exécution grâce à différents tableaux de bords.



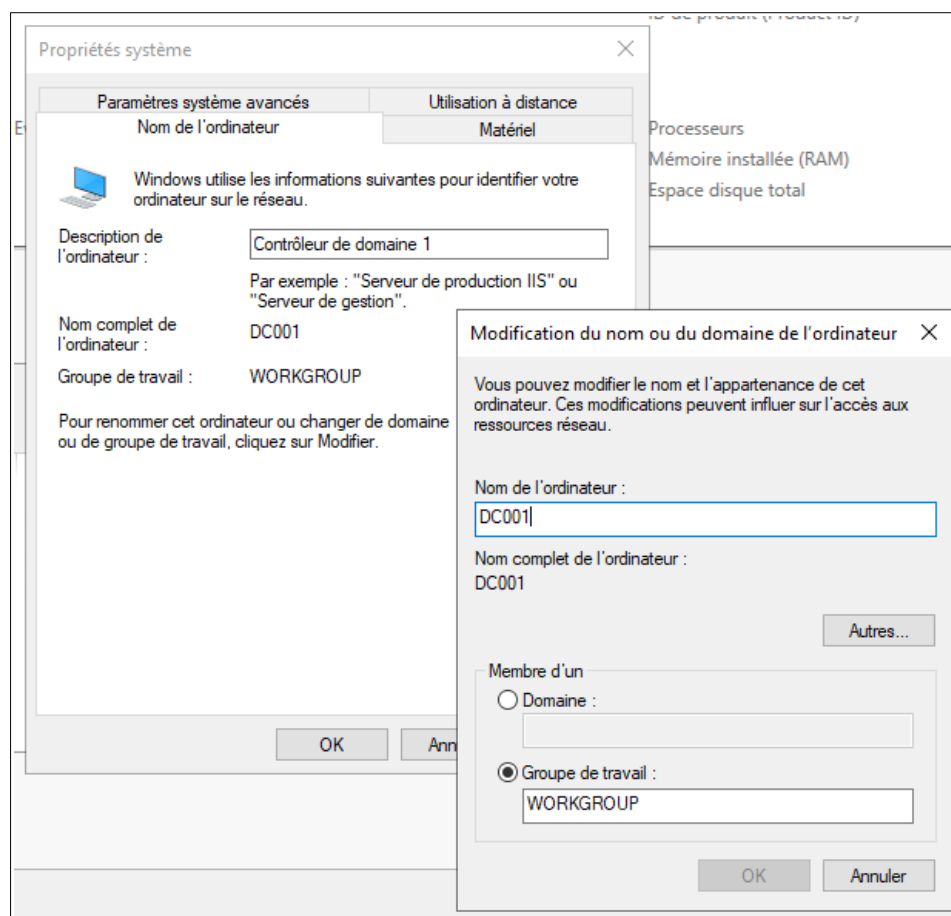


En haut à droite figure une liste d'outils d'administration du serveur, notamment :

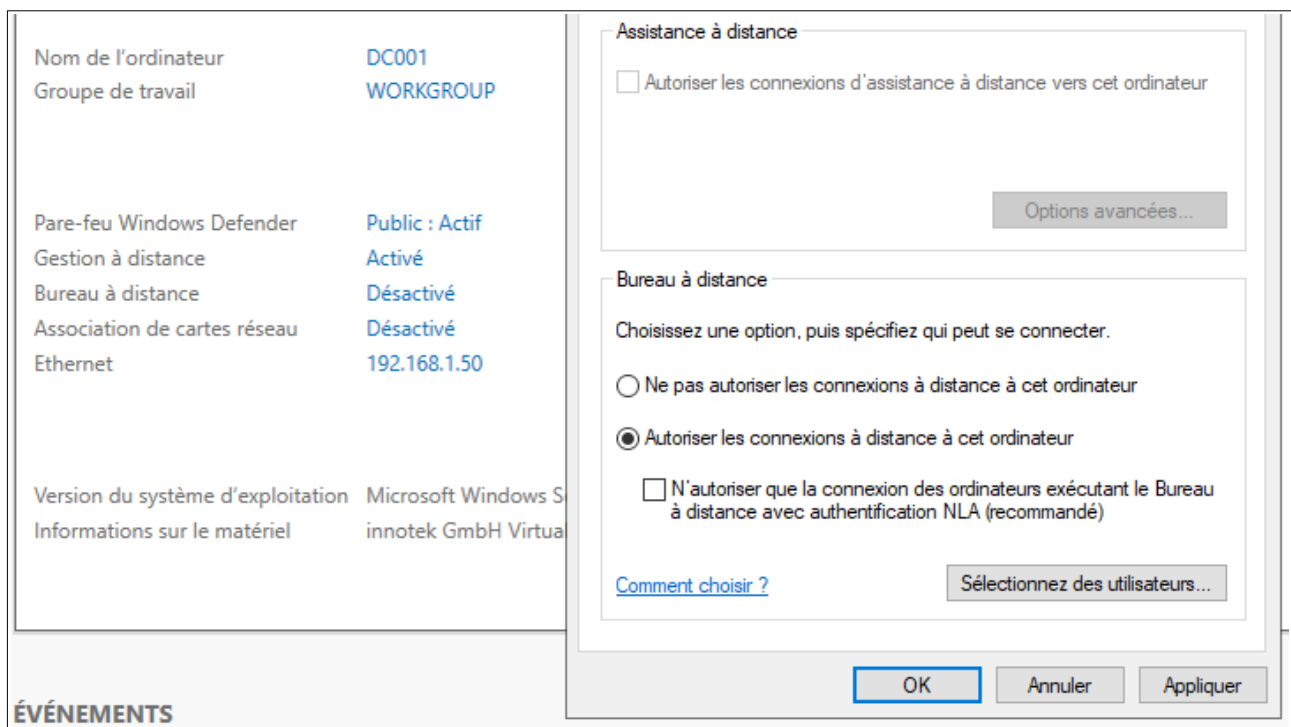
- L'administration de l'AD,
- La gestion des utilisateurs/groupes/ordinateurs de l'AD,
- L'interface de gestion sur service DNS,
- La configuration du Pare-feu,
- La gestion des stratégies de groupe,
- Le planificateur de tâches,
- etc.

Modification du nom de l'ordinateur

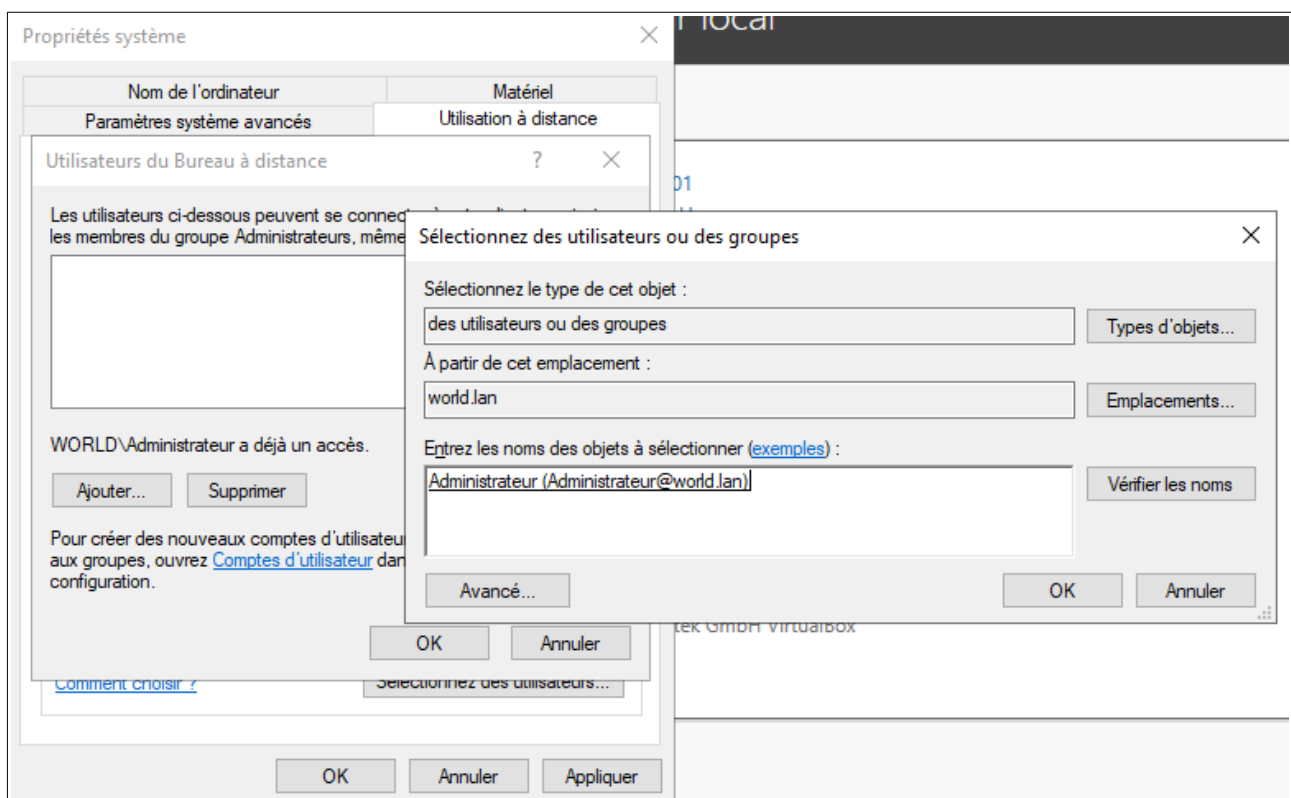
Dans le gestionnaire de serveur, cliquer sur Serveur local, changez son nom puis activez le bureau à distance pour l'administrateur uniquement.



Changement du nom de l'ordinateur

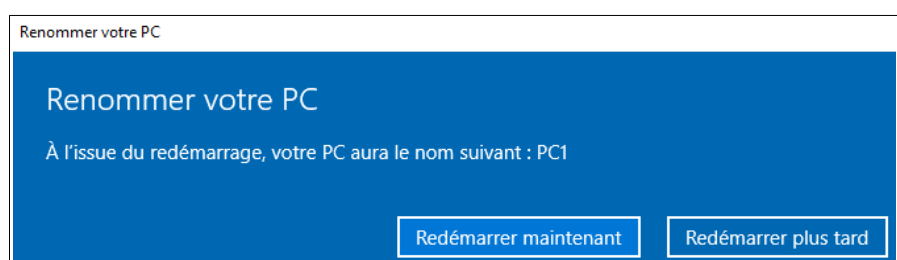


Activer le bureau à distance



Configurer les utilisateurs autorisés à se connecter à distance (après configuration de l'AD)

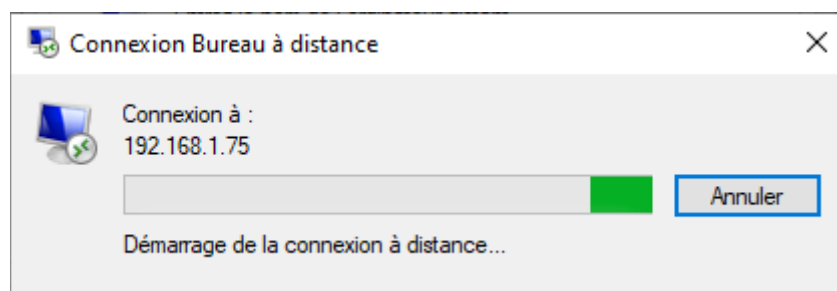
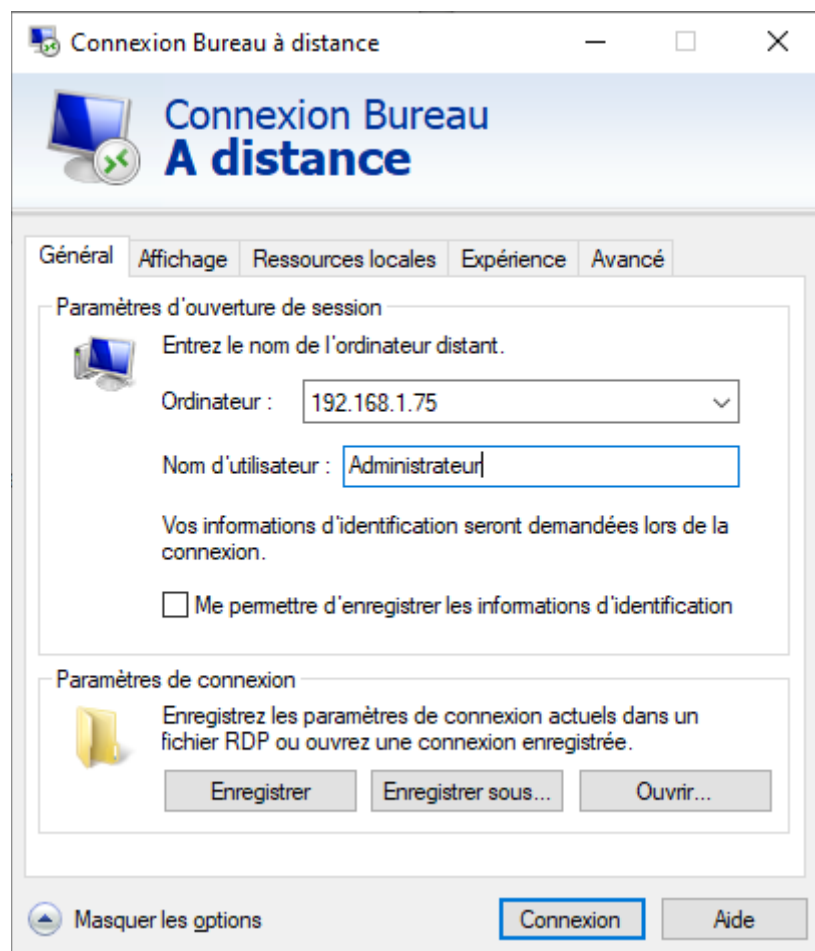
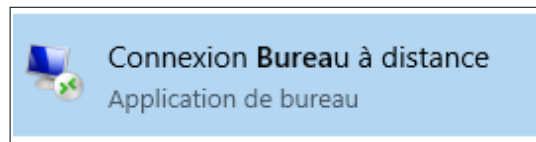
Après toute modification majeure (comme un changement de nom d'hôte o_o), il convient de redémarrer le serveur !
Time for Beer !



Connexion à distance

Après avoir autorisé l'accès à distance sur une machine windows il est possible d'utiliser un logiciel utilisant le protocole RDP pour se connecter en mode graphique à sa machine.

Sous Windows, on utilise l'outil prévu à cet effet.



Sous Linux, on peut utiliser plusieurs logiciels comme Remmina par exemple : <https://remmina.org/>

Installation de l'AD et du DNS.

Dans le gestionnaire de serveur, sur le tableau de bord, cliquez sur « Ajouter des rôles et des fonctionnalités »

Un assistant s'ouvre, cliquez Suivant

Sélectionner le type d'installation

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

Confirmation

Résultats

Sélectionnez le type d'installation. Vous pouvez installer des rôles et des fonctionnalités sur un ordinateur physique ou virtuel en fonctionnement, ou sur un disque dur virtuel hors connexion.
☒ **Installation basée sur un rôle ou une fonctionnalité**
Configurez un serveur unique en ajoutant des rôles, des services de rôle et des fonctionnalités.
☐ **Installation des services Bureau à distance**
Installez les services de rôle nécessaires à l'infrastructure VDI (Virtual Desktop Infrastructure) pour déployer des bureaux basés sur des ordinateurs virtuels ou sur des sessions.

Choisir « installation basée sur un rôle ou une fonctionnalité » puis suivant.

Dans l'écran suivant, vous devrez voir apparaître votre serveur avec son nom, son adresse IP et son OS.

Sélectionner le serveur de destination

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

Confirmation

Résultats

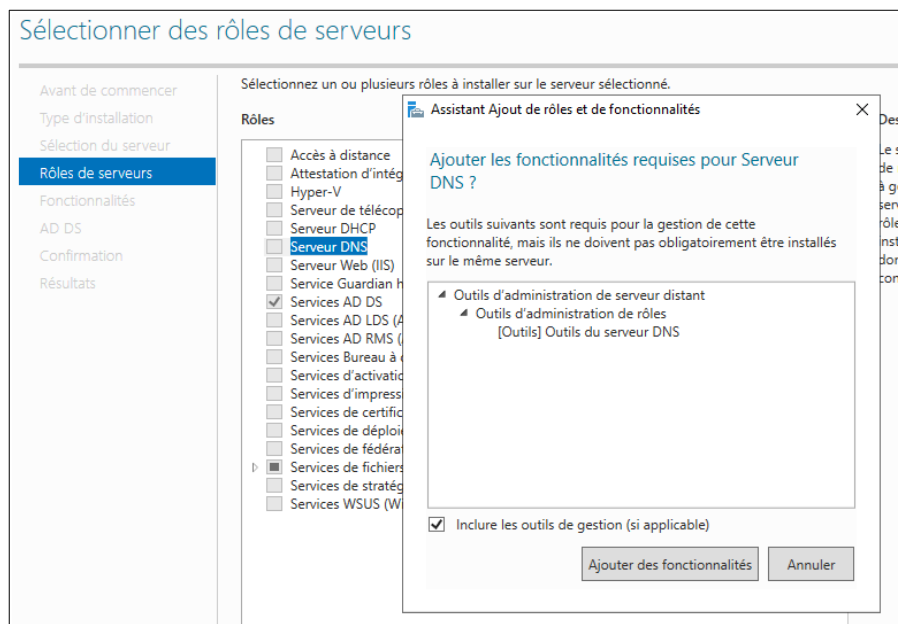
Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et des fonctionnalités.
☒ Sélectionner un serveur du pool de serveurs
☐ Sélectionner un disque dur virtuel
Pool de serveurs
Filtre :

Nom	Adresse IP	Système d'exploitation
DC001	192.168.1.60	Microsoft Windows Server 2019 Standard Evaluation

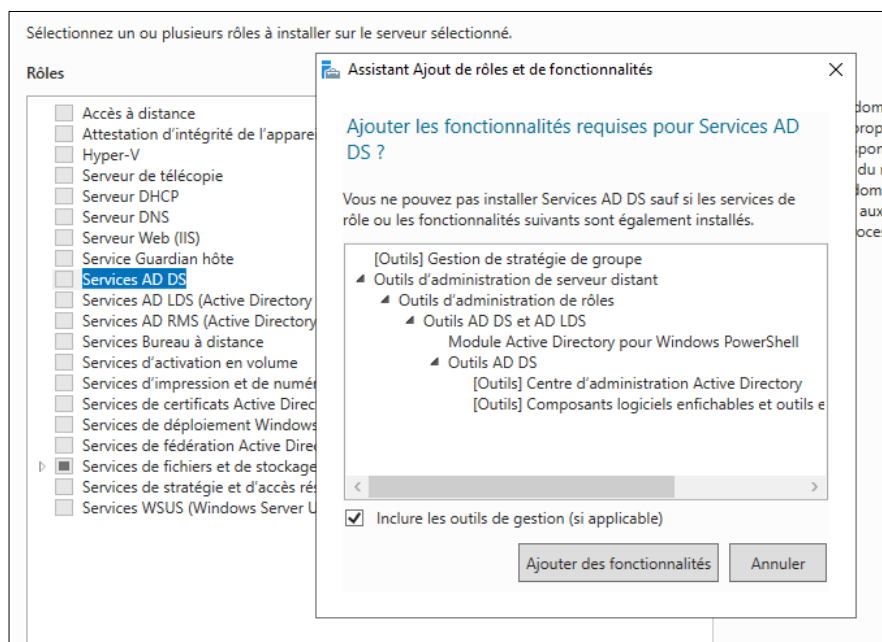
Sélectionnez votre serveur afin d'installer l'Active Directory dessus.

L'écran suivant concerne les différents rôle que vous souhaitez installer sur votre serveur. Vous devez installer les rôles AD DS et DNS.

Cocher le rôle DNS, suivant, suivant, etc...

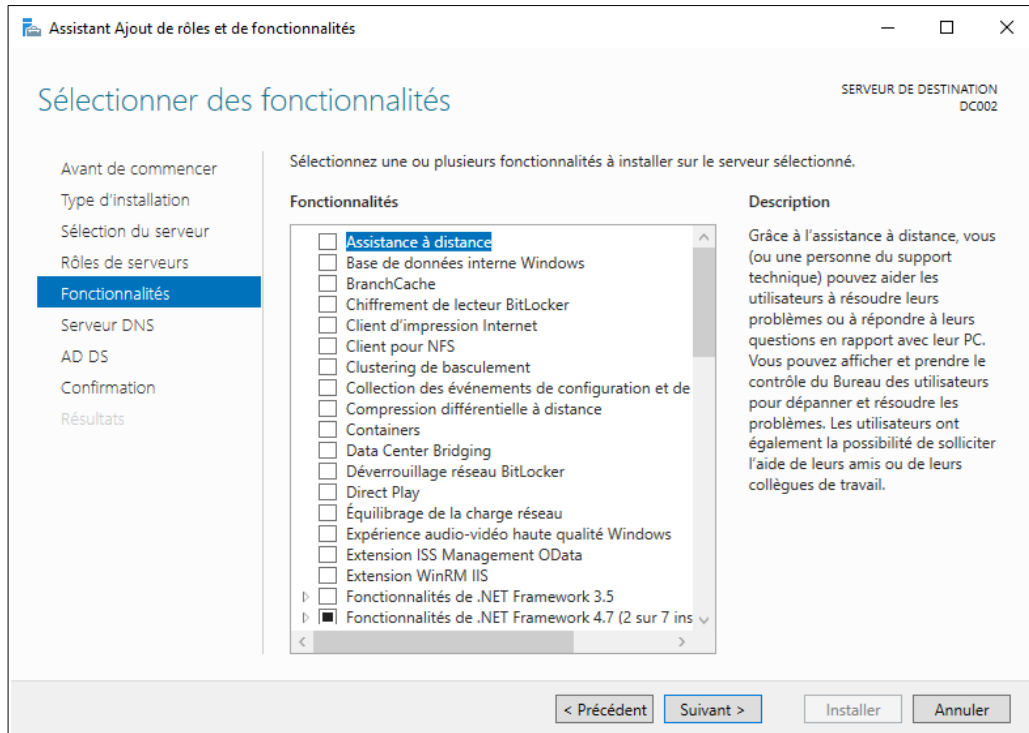


De retour à l'écran de sélection des rôles, cocher le rôle Services AD DS.



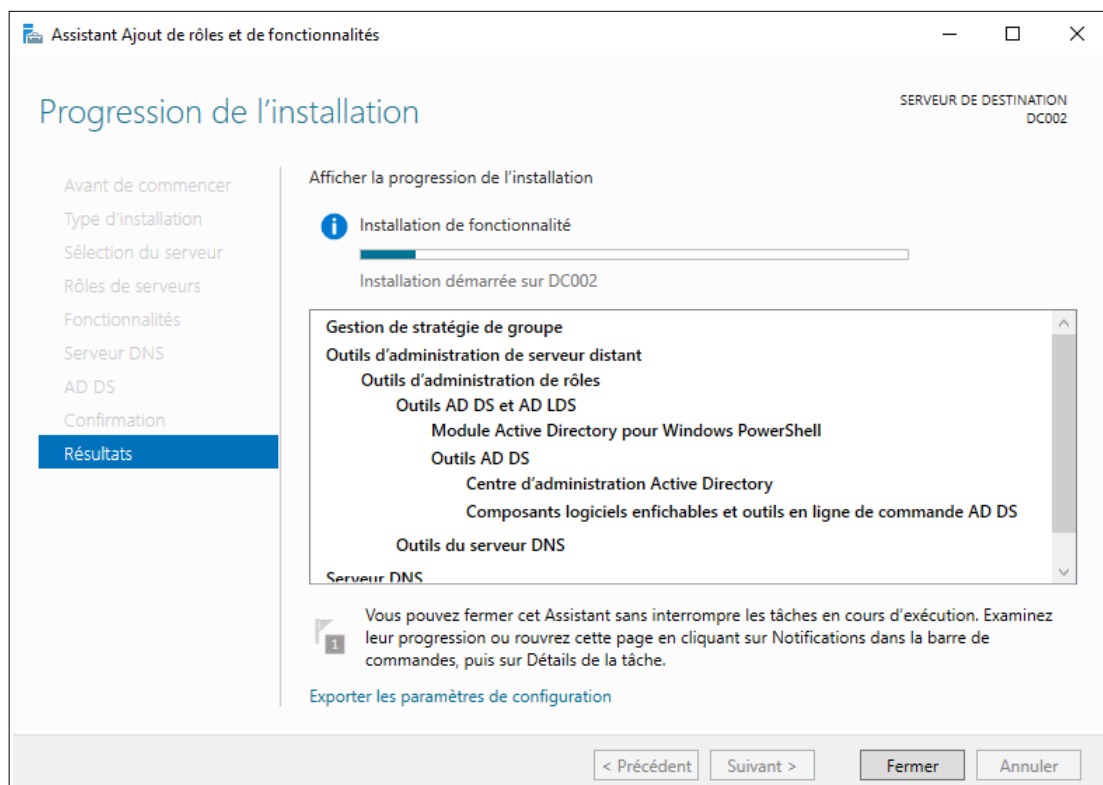
Pour les deux écrans de sélection de rôles précédents, installez les fonctionnalités nécessaires au service afin que le rôle puisse être déployé.

Le service Active Directory a besoin du rôle DNS pour fonctionner, c'est pour cela qu'il est installé et que lors de la configuration IP fixe du serveur, vous avez choisi 127.0.0.1 comme serveur DNS.



Ici, laissez les fonctionnalités par défaut et cliquez sur suivant.

Après avoir sélectionné les deux rôles AD DS et DNS et les fonctionnalités par défaut, cliquez encore sur ... « suivant » et encore « suivant » et encore... ah non « installer » pour commencer l'installation des rôles. Cochez la case « Redémarrer automatiquement le serveur de destination si nécessaire »



On a bien travaillé : Bière !

Rebootez si jamais le reboot nécessaire n'a pas été automatique.

Bière !

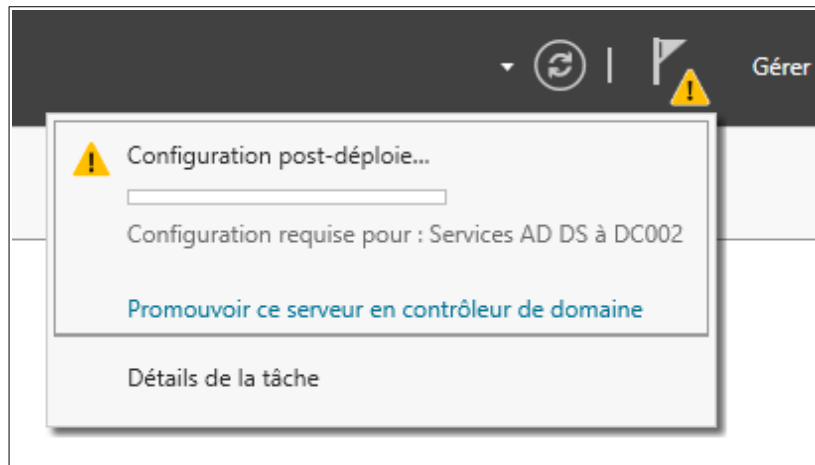
Une fois redémarré, il va falloir promouvoir le serveur en tant que **contrôleur de domaine**.

Si l'option n'est pas proposée,

Contrôleur de domaine

Après installation des rôles AD DS et DNS puis un reboot, il est temps de promulguer le serveur en contrôleur de domaine.

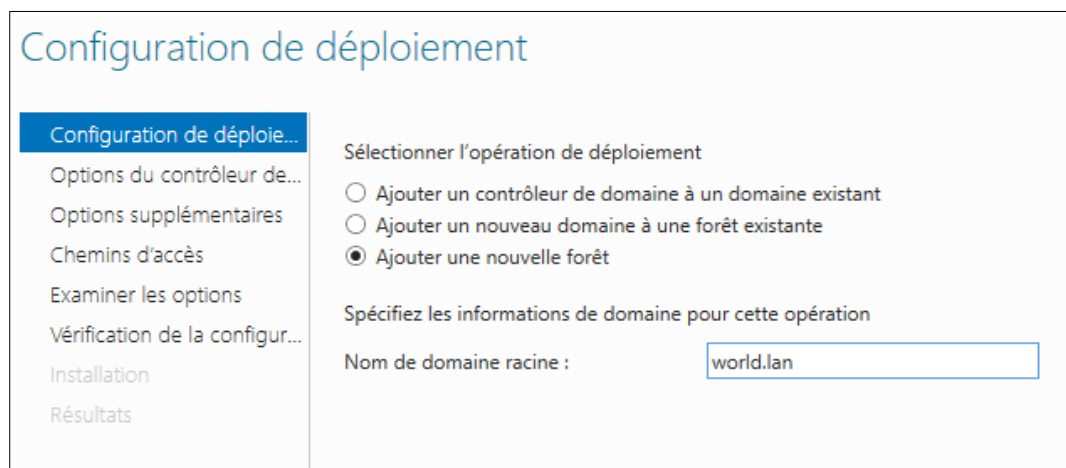
Cliquez en haut à droite sur le flag jaune



Cliquez sur « Promouvoir ce serveur en contrôleur de domaine ».

Cliquez sur « Ajouter une nouvelle forêt », c'est le 1^{er} contrôleur de domaine.

Nom de domaine racine : **votre_zone.lan** (ex : asie.lan)



Suivant

On choisit un mot de passe de restauration. Password87 semble être un candidat robuste (ou pas...).

À l'écran suivant, un warning apparaît. Il semble impossible de créer une délégation de zone DNS car la zone parente faisant autorité est introuvable. Étant donné que c'est le premier contrôleur de domaine, ça paraît assez logique, ce sera lui la zone parente !

Suivant.

On définit le nom NETBIOS (système de nommage des ordinateurs Windows sur un réseau) du domaine. On garde le nom par défaut (c'est à dire le nom du domaine sans l'extension en majuscule)

Suivant

La fenêtre suivant permet de définir certains répertoires intéressants ; Laissez les valeurs par défaut, mais notez que :

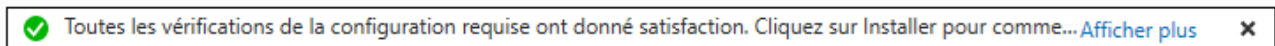
SYSVOL est un répertoire partagé (entre les différents contrôleurs de domaine) qui va contenir différents éléments comme les GPO sur le domaine, des scripts utilisateurs, etc.

NTDS contiendra quand à lui les logs et la base de donnée de l'Active Directory.

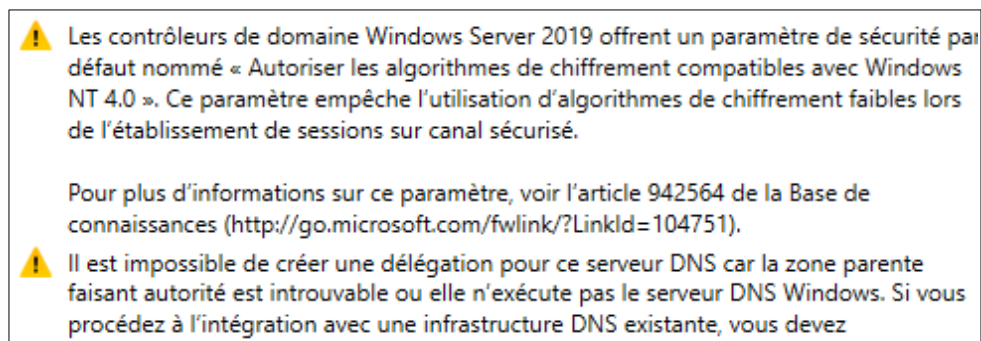
Suivant

Suivant

Le serveur vérifie la configuration requise et donne son verdict.



On obtient quelques warnings sans conséquence :



- Empêcher les algorithmes de chiffrement faible : Super !
- Encore cette histoire normale de zone parente DNS : OK

On installe.

Bière !

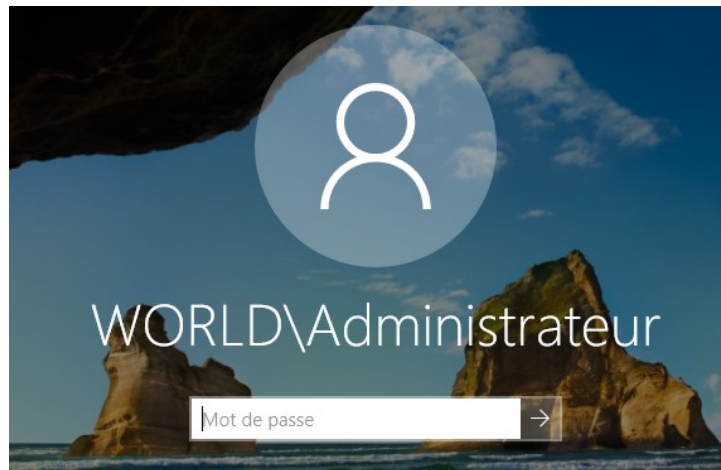
Installation terminée !

Ah bin ça reboot.

Bière !



Bière x2 !



Après reboot, on voit le nom NETBIOS du domaine de tout à l'heure qui s'est incrusté devant le nom d'utilisateur.

Le compte Administrateur du serveur, est devenu automatiquement le compte Administrateur de votre domaine **zone.lan**.

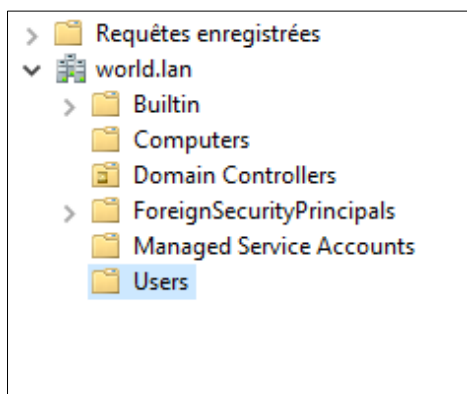
On peut vérifier ça de suite, dans l'outil « *Utilisateurs et ordinateurs Active Directory* »

Utilisateurs et ordinateurs Active Directory			
Fichier Action Affichage ?			
	Nom	Type	Description
Utilisateurs et ordinateurs Active Directory	Administrateur	Utilisateur	Compte d'utilisateur d'administration
Requêtes enregistrées	Administrateurs clés	Groupe de sécurité - Global	Les membres de ce groupe peuvent effectu...
world.lan	Administrateurs clés Entreprise	Groupe de sécurité - Universel	Les membres de ce groupe peuvent effectu...
Builtin	Administrateurs de l'entreprise	Groupe de sécurité - Universel	Administrateurs désignés de l'entreprise
Computers	Administrateurs du schéma	Groupe de sécurité - Universel	Administrateurs désignés du schéma
Domain Controllers	Admins du domaine	Groupe de sécurité - Global	Administrateurs désignés du domaine
ForeignSecurityPrincipals			
Managed Service Accounts			

Création d'utilisateurs

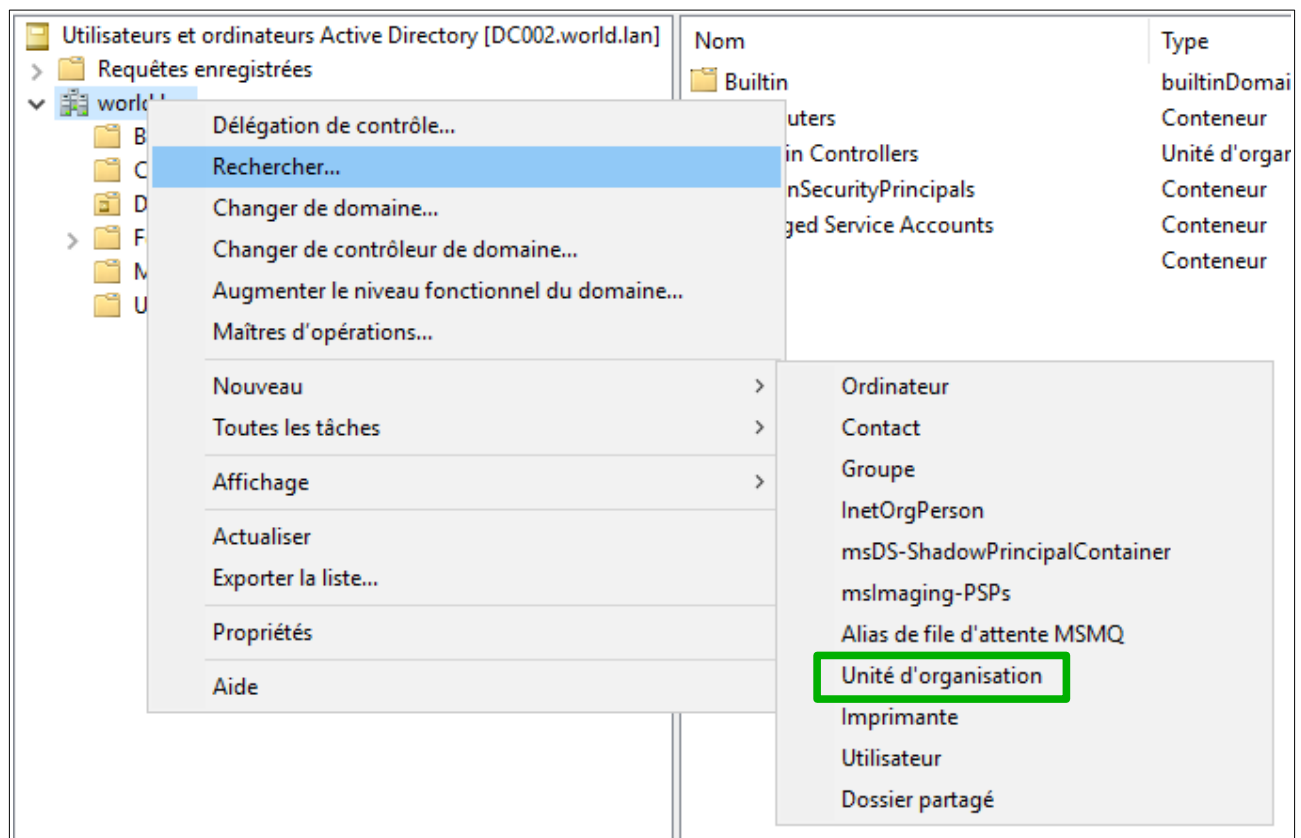
Pour créer des utilisateurs (et plus généralement des ressources) dans l'Active Directory, vous pouvez passer par les outils :

- Centre d'administration Active directory (pour les jeunes)
- Utilisateurs et ordinateurs Active Directory (pour les anciens)




Dans la partie gauche on retrouve les unités d'organisation (OU) créées par défaut lors de l'installation de l'Active Directory.

Commençons par en créer une pour nous utilisateurs. On pourrait utiliser le dossier Users par défaut, mais pour une question d'organisation, on ne le fera pas.



Nouvel objet - Unité d'organisation

 Créer dans : world.lan/

Nom :

☒ Protéger le conteneur contre une suppression accidentelle

Au passage, on peut utiliser un terminal et la commande dsquery pour interroger notre annuaire.

```
dsquery OU domainroot -name Emp*  
"OU=Employés,DC=world,DC=lan"  
  
dsquery OU dc=world,dc=lan -name Emp*  
"OU=Employés,DC=world,DC=lan"
```

Cela permet de visualiser le DN (Distinguished Name) de notre objet. On pourrait d'ailleurs créer les éléments de l'annuaire en ligne de commande, mais bon.

Création d'un utilisateur

Clic droit sur l'OU **Employés** fraîchement créée → Nouveau → Utilisateur

Nouvel objet - Utilisateur

Créer dans : world.lan/Employés

Prénom : Florent Initiales :

Nom : Sautour

Nom complet : Florent Sautour

Nom d'ouverture de session de l'utilisateur : fls@world.lan

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

< Précédent Suivant > Annuler

On remplit les informations.

On note au passage que l'on pourra se connecter avec l'identifiant « **WORLD\fls** » comme les vieux, ou alors **fls@world.lan** comme les jeunes.

On définit le mot de passe : Password87 semble toujours aussi solide.

Créer dans : world.lan/Employés

Mot de passe :

Confirmer le mot de passe :

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

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

☐ Le mot de passe n'expire jamais

☐ Le compte est désactivé

On peut ici :

- Forcer l'utilisateur à changer son mot de passe lors de la 1ère connexion
- Empêcher l'utilisateur de changer son mot de passe.
- Utiliser un mot de passe Ad Vitam Eternam.
- Désactiver le compte (le créer mais le rendre inactif – en attente d'activation)

/!\ Si vous cochez les 2 premières en même temps, le serveur implose.

Cochez à votre guise.

Créez quelques utilisateurs pour les tests.

Utilisateurs et ordinateurs Active Directory [DC002.world.lan]		
> Requetes enregistrees		
v world.lan		
Builtin		
Computers		
Domain Controllers		
> ForeignSecurityPrincipals		
Managed Service Accounts		
Users		
Employes		
Nom	Type	
Albert Einstein	Utilisateur	
Florent Sautour	Utilisateur	
Galileo Galilei	Utilisateur	
Isaac Newton	Utilisateur	
Nicolas Copernic	Utilisateur	

Bière !

Visualisons tous les utilisateurs !

```
dsquery user -name *
"CN=Administrateur,CN=Users,DC=world,DC=lan"
"CN=Invité,CN=Users,DC=world,DC=lan"
"CN=krbtgt,CN=Users,DC=world,DC=lan"
"CN=Florent Sautour,OU=Employes,DC=world,DC=lan"
"CN=Albert Einstein,OU=Employes,DC=world,DC=lan"
"CN=Galileo Galilei,OU=Employes,DC=world,DC=lan"
"CN=Nicolas Copernic,OU=Employes,DC=world,DC=lan"
"CN=Isaac Newton,OU=Employes,DC=world,DC=lan"
```

Phase de tests !

Avant de tester : regardez dans le dossier computers, il doit être vide.

En ligne de commandes

```
dsquery computer -name *
"CN=DC002,OU=Domain Controllers,DC=world,DC=lan"
```

Il s'agit du serveur lui même qui est situé dans l'OU **Domain Controllers**.

On allume un Windows 10 professionnel fraîchement installé (sans comptes locaux autre que le compte admin)

Note : on ne peut pas connecter un Windows 10 familial à un domaine, pas la peine d'essayer.

On se connecte avec le compte admin créé lors de l'installation.

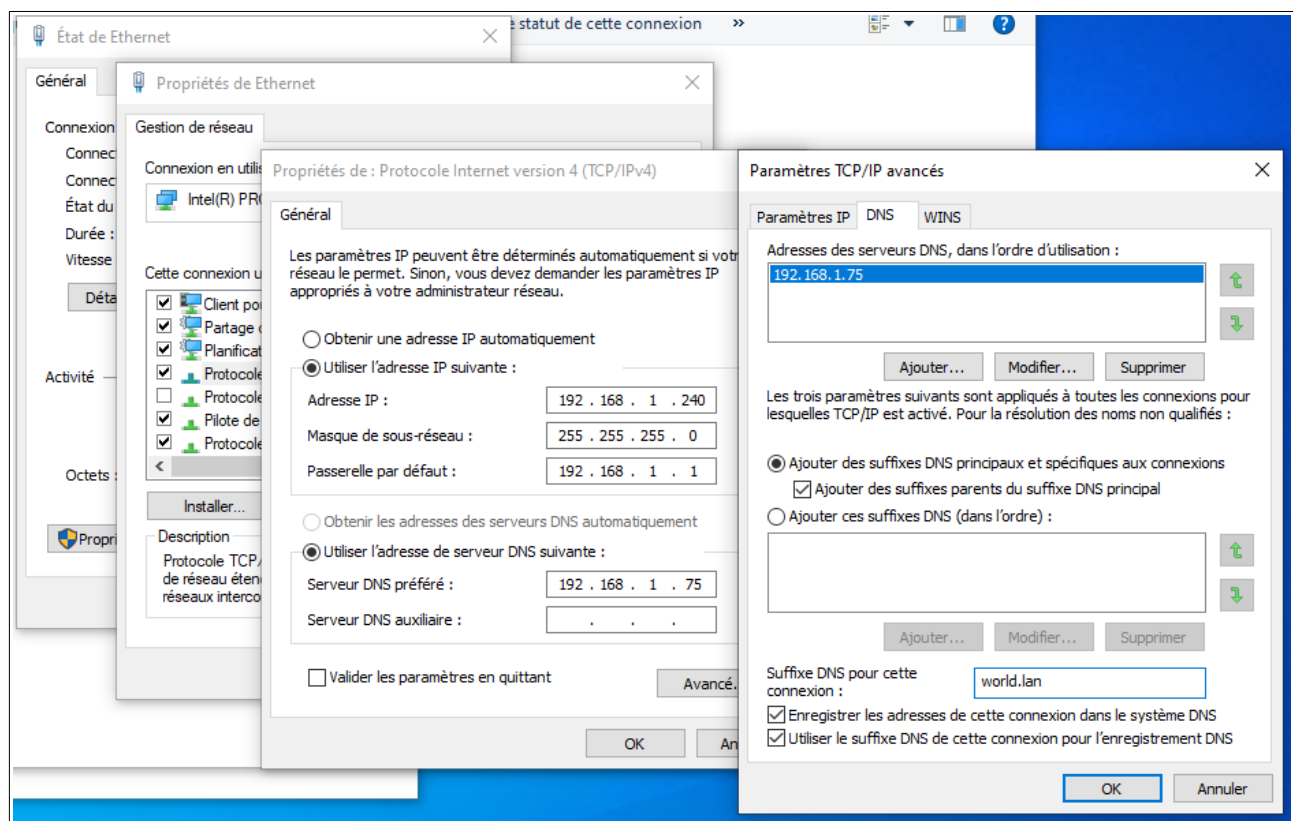
- Login : admin
- Password : password

Note : password is not a secure password

On vérifie les paramètres IP pour s'assurer que la machine puisse bien communiquer avec le serveur Active Directory

On met le serveur Active Directory comme DNS principal, on clique sur « Avancé » puis on définit le suffixe DNS pour cette connexion : **zone.lan**

On coche les 2 cases en bas.



On valide.

```
PS C:\Users\admin> ping 192.168.1.75

Envoi d'une requête 'Ping' 192.168.1.75 avec 32 octets de données :
Réponse de 192.168.1.75 : octets=32 temps<1ms TTL=128
Réponse de 192.168.1.75 : octets=32 temps<1ms TTL=128
Réponse de 192.168.1.75 : octets=32 temps<1ms TTL=128
Réponse de 192.168.1.75 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 192.168.1.75:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
PS C:\Users\admin>
```

```
PS C:\Users\admin> ping DC002.world.lan

Envoi d'une requête 'ping' sur DC002.world.lan [192.168.1.75] avec 32 octets de données :
Réponse de 192.168.1.75 : octets=32 temps<1ms TTL=128
Réponse de 192.168.1.75 : octets=32 temps<1ms TTL=128
Réponse de 192.168.1.75 : octets=32 temps<1ms TTL=128
Réponse de 192.168.1.75 : octets=32 temps<1ms TTL=128

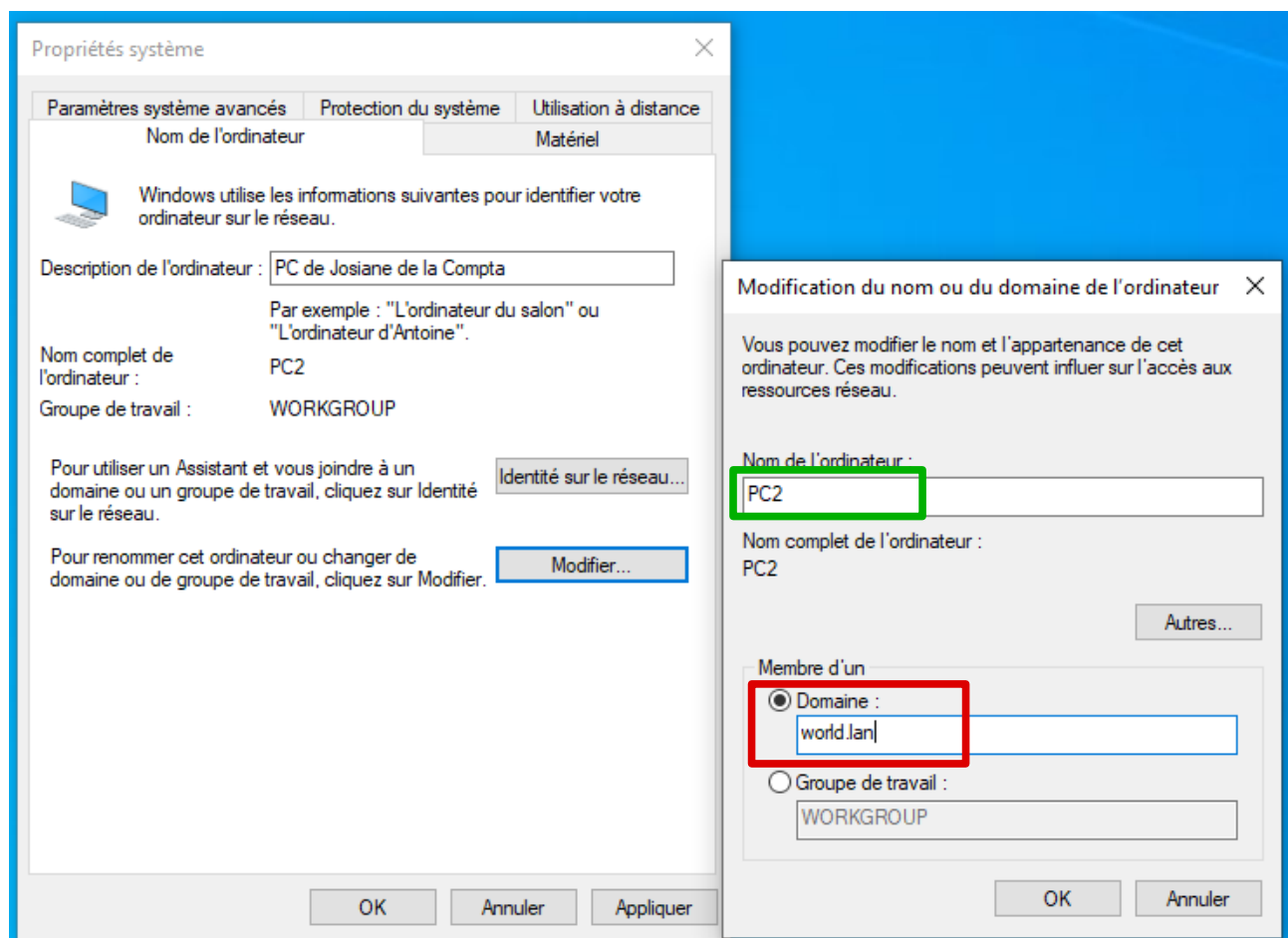
Statistiques Ping pour 192.168.1.75:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

Tout va bien !

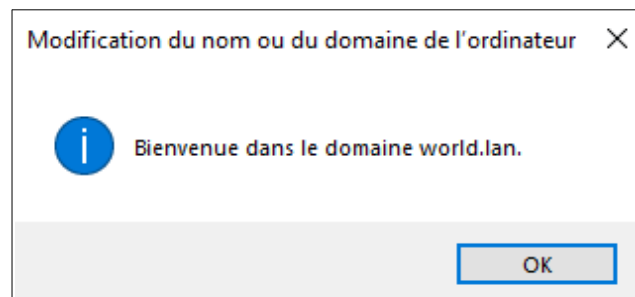
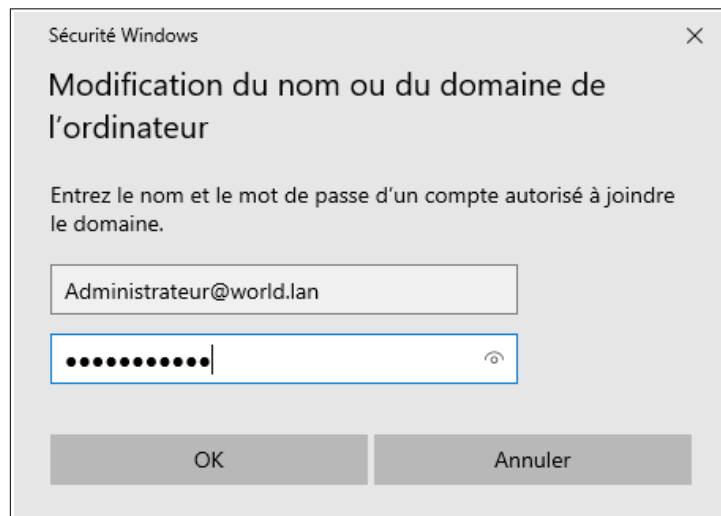
On continue...

On renomme notre PC : clic droit sur le menu « Démarrer » → système → renommer ce PC (Avancé)

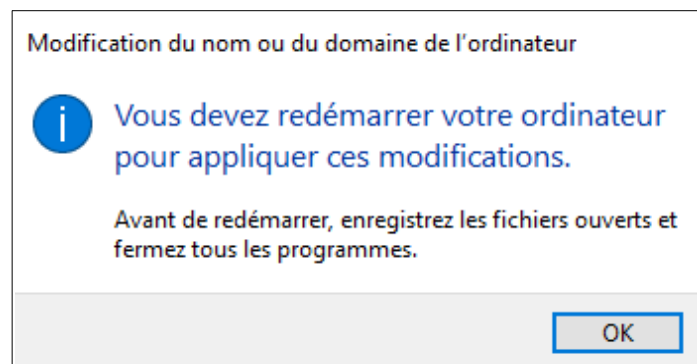
Et on le switch dans notre domaine par la même occasion, on évite un reboot en plus !



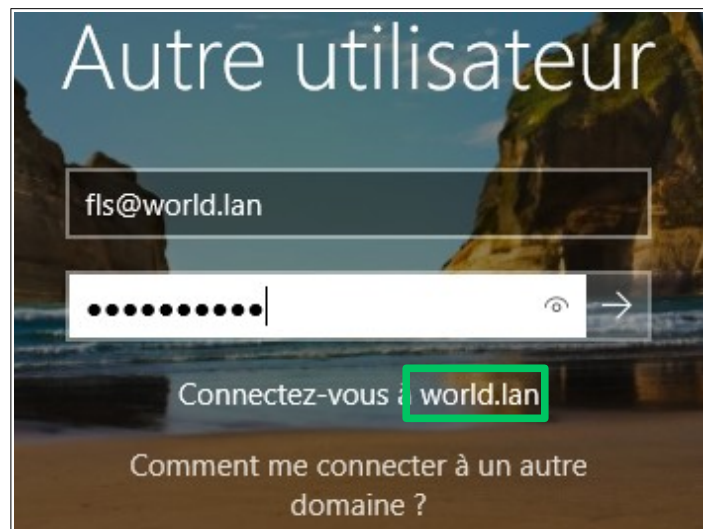
On utilise le compte Administrateur de l'Active Directory pour autoriser l'ordinateur à se connecter au domaine.



Ça faisait longtemps.



Après le reboot on est près à se connecter à notre Windows 10. Pour rappel, sur la machine, seul le compte local admin existe.

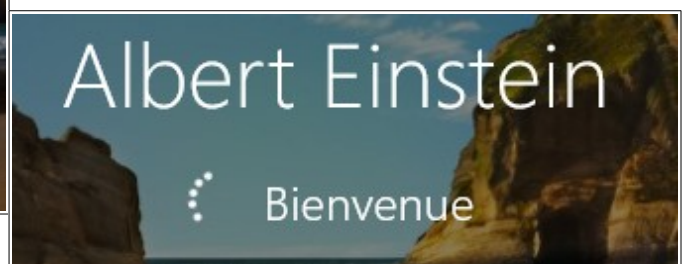


Bonjour

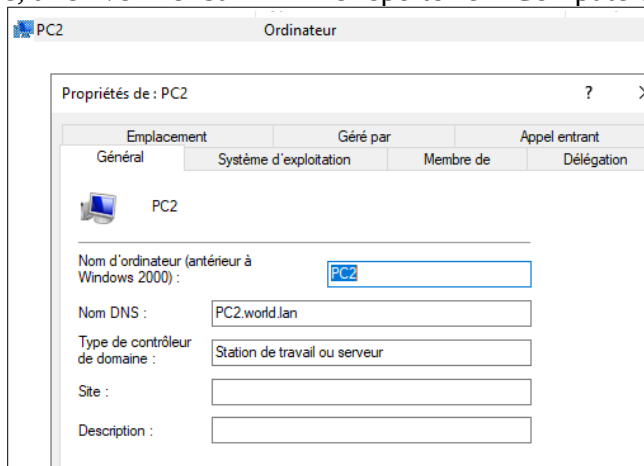
Cette opération peut durer plusieurs minutes

Bière !

Et voilà ! On peut essayer avec les autres utilisateurs de l'AD créés précédemment, ça marche aussi.



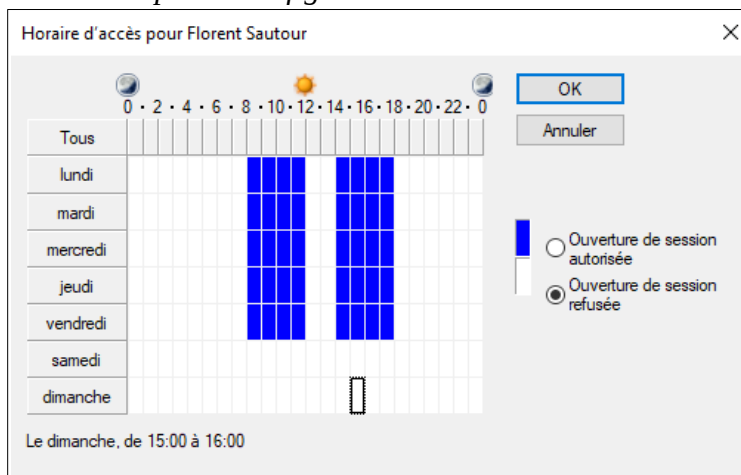
Avant de finir cette partie, allez vérifier sur l'AD le répertoire « Computers »



Le PC sur lequel on vient de se connecter a été enregistré dans l'AD, plutôt pas mal.

En double-cliquant sur un utilisateur dans l'Active Directory, il est possible de configurer un certain nombre de paramètres pour cet utilisateur, n'hésitez pas à y jeter un coup d'œil.

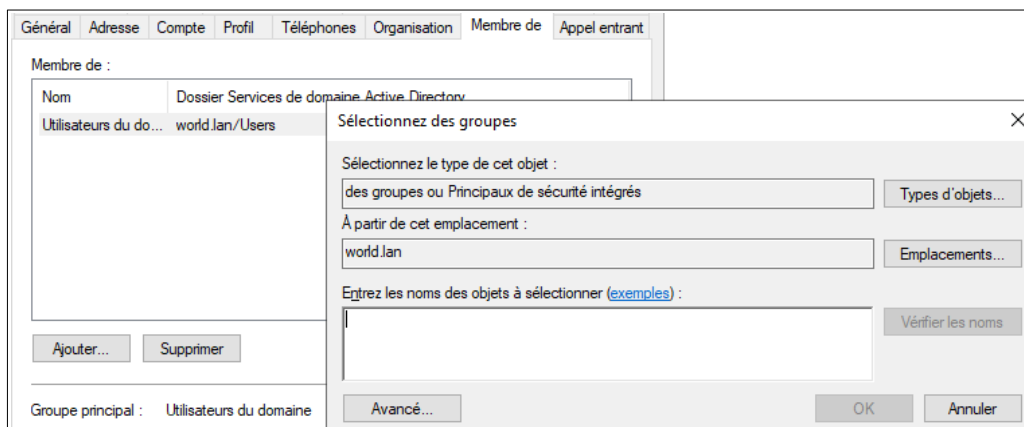
Exemple de configuration d'horaires d'accès.



Testez différents horaires d'accès pour plusieurs de vos utilisateurs et notez les résultats.



Il est possible de créer des groupes et d'associer des utilisateurs à ces groupes dans l'Active Directory, mais on y revient plus tard.



Redirection des répertoires utilisateur et GPO

Nous possédons désormais un système d'authentification centralisé, qui permet à n'importe quel utilisateur enregistré dans l'AD de se connecter sur des machines reliées au domaine de l'AD.

Cependant, les répertoires, fichiers et autres documents créés par ces utilisateurs sur une machine ne seront disponibles que sur cette machine et pas sur une autre.

Dans certains cas, il est possible que des utilisateurs souhaitent accéder à leurs données depuis n'importe quel poste.

Plusieurs solutions sont envisageables :




- Mettre à disposition un espace de stockage réseau aux utilisateurs
- Mettre en place une redirection des répertoires utilisateur afin que les documents d'un utilisateur -(qu'ils soient sur le Bureau, dans le dossier Téléchargements, dans le dossier images, etc.) soient directement stockés sur un espace de stockage accessible en réseau.

Nous allons mettre en place cette seconde solution grâce à une GPO.

Création d'un groupe de sécurité (Recommandations de microsoft)

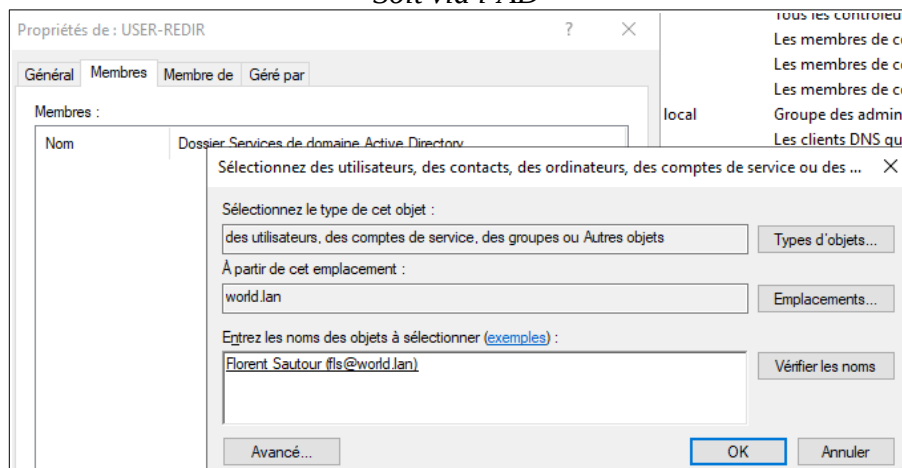
```
New-ADGroup -Name "USER-REDIR" `
-SamAccountName "USER-REDIR" `
-GroupCategory Security -GroupScope DomainLocal `
-Description "Groupe de sécurité pour la redirection de
répertoires"
```

Note : les ` sont l'équivalent des \ sous Linux pour spécifier qu'une commande est écrite sur plusieurs lignes.

 Serveurs RAS et IAS	Groupe de sécurité - Domaine local	Les serveurs de ce groupe peuvent accéder aux propriétés d'ac...
 USER-REDIR	Groupe de sécurité - Domaine local	Groupe de sécurité pour la redirection de répertoires
 Utilisateurs du domaine	Groupe de sécurité - Global	Tous les utilisateurs du domaine

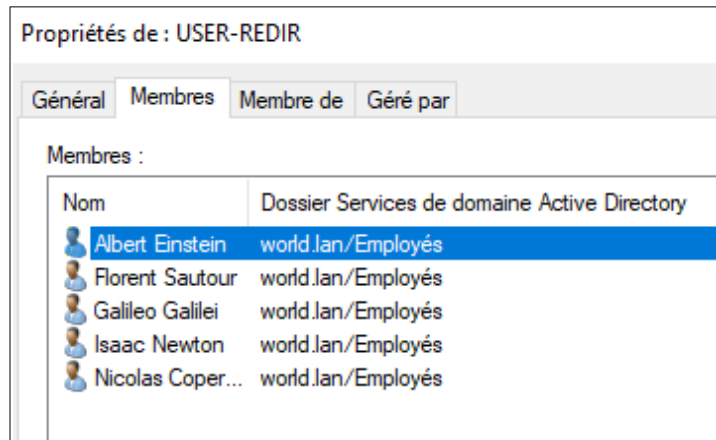
On ajoute les utilisateurs à ce groupe :

Soit via l'AD

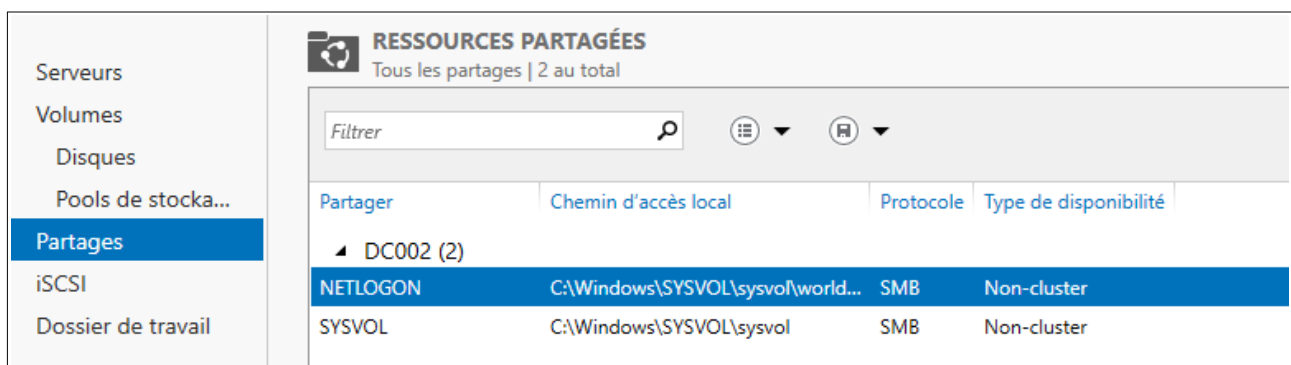


Soit en ligne de commande

```
Add-ADGroupMember -Identity "USER-REDIR" -Members fls, ale, gag, nic, isn
```



Bon, maintenant, il va falloir configurer un espace de stockage pour les répertoires des utilisateurs. On va faire ça directement sur le serveur AD grâce au service de fichiers et de stockage (menu de gauche).

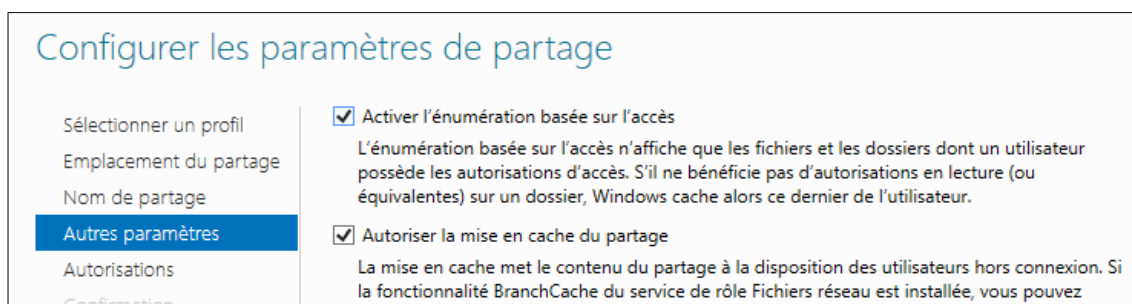


Cliquez sur tâches (en haut au milieu) puis **Nouveau Partage**.

SMB – Rapide (Samba ça vous parle ?)
Choisir votre serveur puis suivant

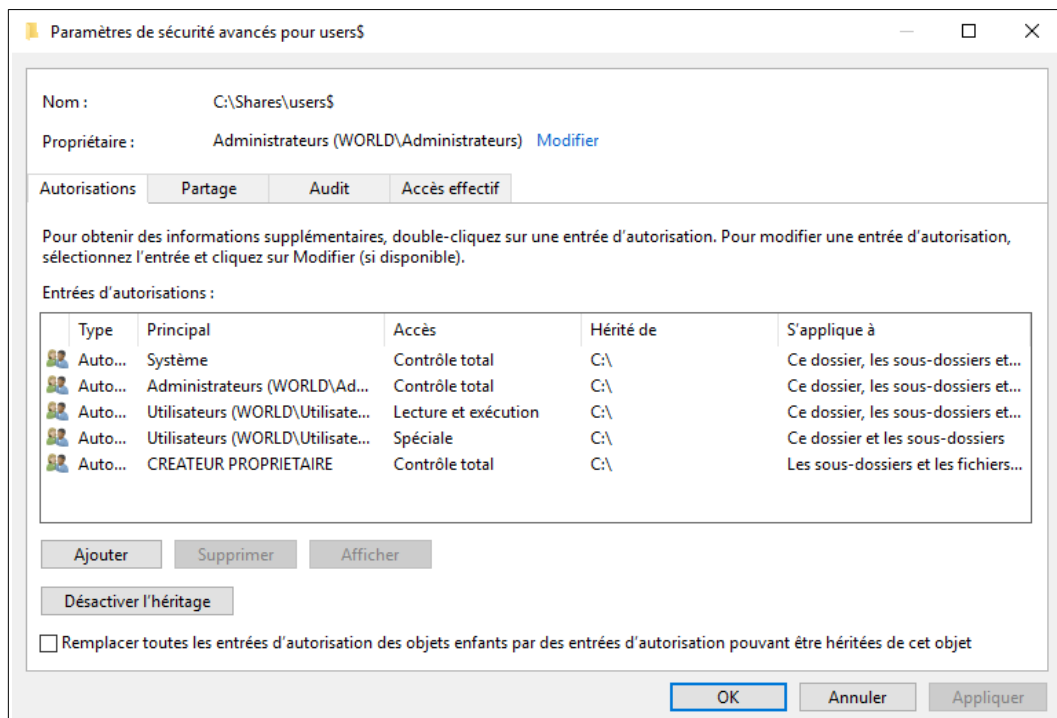
- Nom du partage : users\$
- Chemin local : C:\Shares\users\$
- Chemin distant : \\DC002\users\$

Cochez Activer l'énumération basée sur l'accès, pour masquer les dossiers pour lesquels l'utilisateur n'a aucune permission.



Les permissions

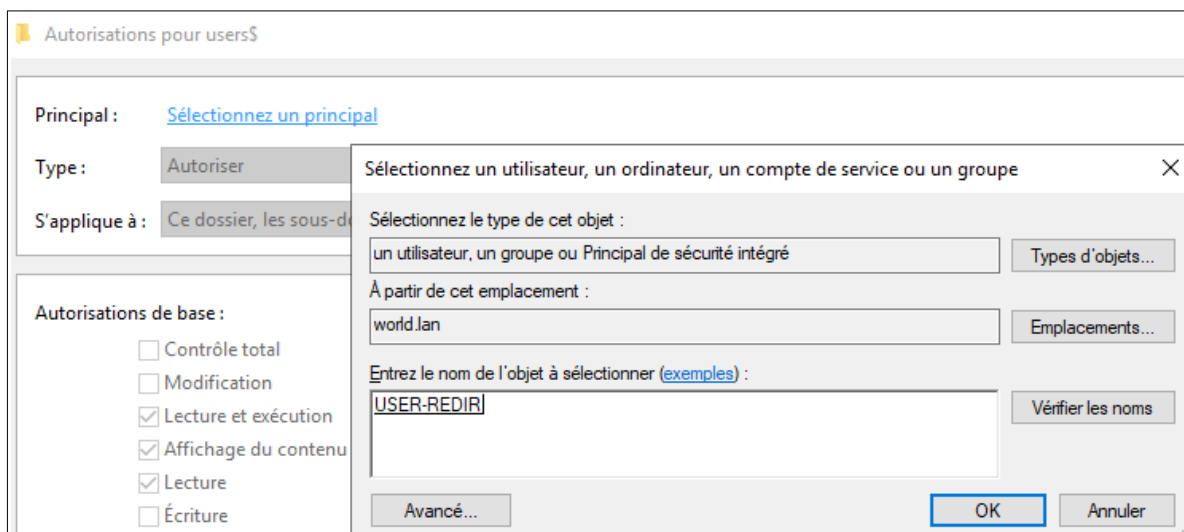
Cliquez sur personnaliser les autorisations...



Désactiver l'héritage → Convertir les autorisations héritées en autorisations explicites sur cet objet.

Ajouter

Sélectionner un principal : aller chercher le groupe USER-REDIR



Principal : USER-REDIR (WORLD\USER-REDIR) [Sélectionnez un principal](#)

Type : Autoriser

S'applique à : Ce dossier seulement

Autorisations avancées :

<input type="checkbox"/> Contrôle total	<input type="checkbox"/> Attributs d'écriture
<input type="checkbox"/> Parcours du dossier/exécuter le fichier	<input type="checkbox"/> Écriture d'attributs étendus
<input checked="" type="checkbox"/> Liste du dossier/lecture de données	<input type="checkbox"/> Suppression de sous-dossier et fichier
<input checked="" type="checkbox"/> Attributs de lecture	<input type="checkbox"/> Suppression
<input checked="" type="checkbox"/> Lecture des attributs étendus	<input checked="" type="checkbox"/> Autorisations de lecture
<input type="checkbox"/> Création de fichier/écriture de données	<input type="checkbox"/> Modifier les autorisations
<input checked="" type="checkbox"/> Création de dossier/ajout de données	<input type="checkbox"/> Appropriation

☐ Appliquer ces autorisations uniquement aux objets et/ou aux conteneurs faisant partie de ce conteneur

[Afficher les autorisations de base](#)

[Effacer tout](#)

Ajoutez une condition pour limiter l'accès. Les autorisations spécifiées ne seront accordées au principal que si les conditions sont remplies.

On supprime les permissions pour tous les utilisateurs afin d'obtenir le résultat suivant

Nom : C:\Shares\users\$

Propriétaire : Administrateurs (WORLD\Administrateurs) [Modifier](#)

Autorisations **Partage** Audit Accès effectif

Pour obtenir des informations supplémentaires, double-cliquez sur une entrée d'autorisation. Pour modifier une entrée d'autorisation, sélectionnez l'entrée et cliquez sur Modifier (si disponible).

Entrées d'autorisations :

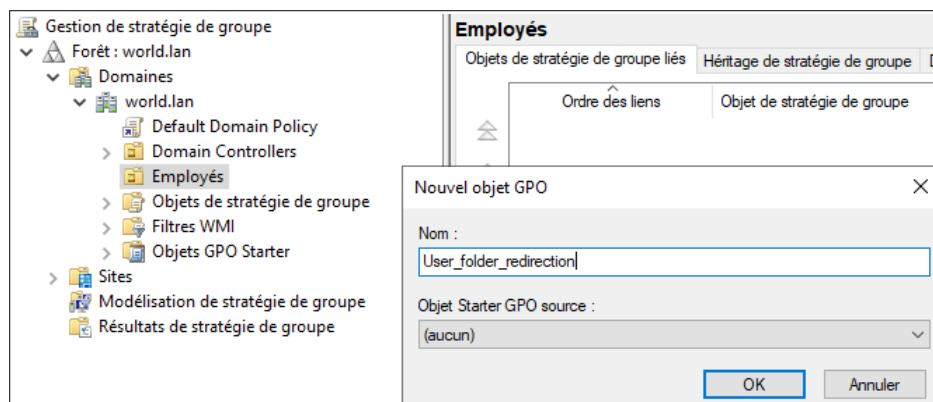
Type	Principal	Accès	Hérité de	S'applique à
Autori...	Système	Contrôle total	Aucun	Ce dossier, les sous-dossie
Autori...	Administrateurs (WORLD\Administrateurs)	Contrôle total	Aucun	Ce dossier, les sous-dossie
Autori...	CREATEUR PROPRIETAIRE	Contrôle total	Aucun	Les sous-dossiers et les ficl
Autori...	USER-REDIR (WORLD\USER-REDIR)	Spéciale	Aucun	Ce dossier seulement

Suivant → Créer → Fermer

Maintenant que le répertoire de stockage des documents utilisateurs est créé avec les bonnes permissions, passons à la **GPO** qui va permettre d'appliquer la redirection des dossiers à tous les utilisateurs.

Ouvrir l'outil « **Gestion de stratégie de groupe** »

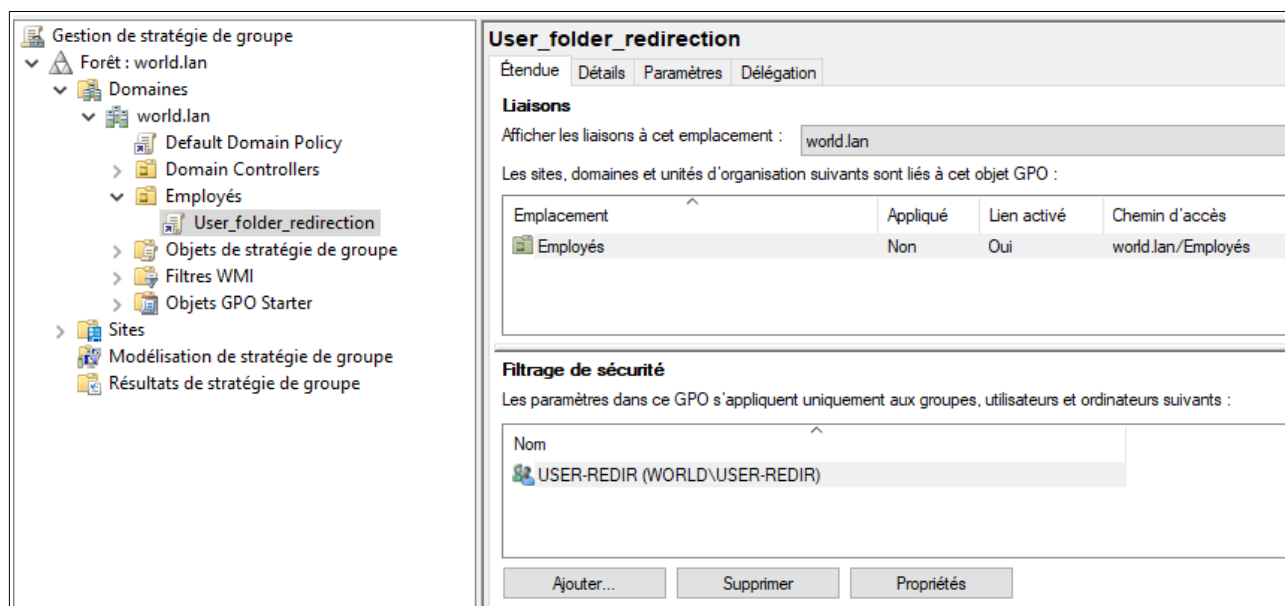
Dérouler le menu de gauche pour créer (clic droit) une GPO sur l'OU « Employés »



Double-cliquez sur la GPO créée

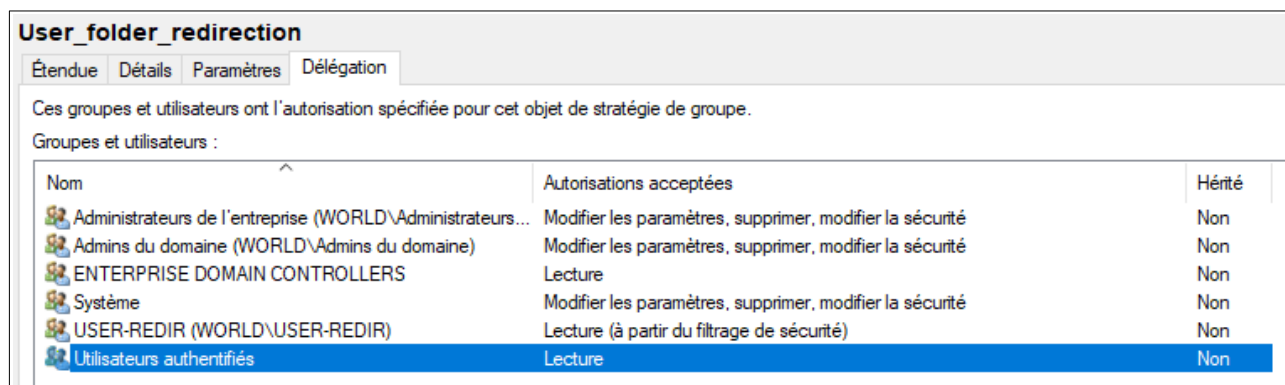
Dans la zone « Filtrage de sécurité »

Supprimez les Utilisateurs authentifiés et ajoutez le groupe USER-REDIR



Passez ensuite à l'onglet **Délégation**

Ajoutez "Utilisateurs authentifiés" en "Lecture" uniquement.



Clic droit sur la GPO – Modifier

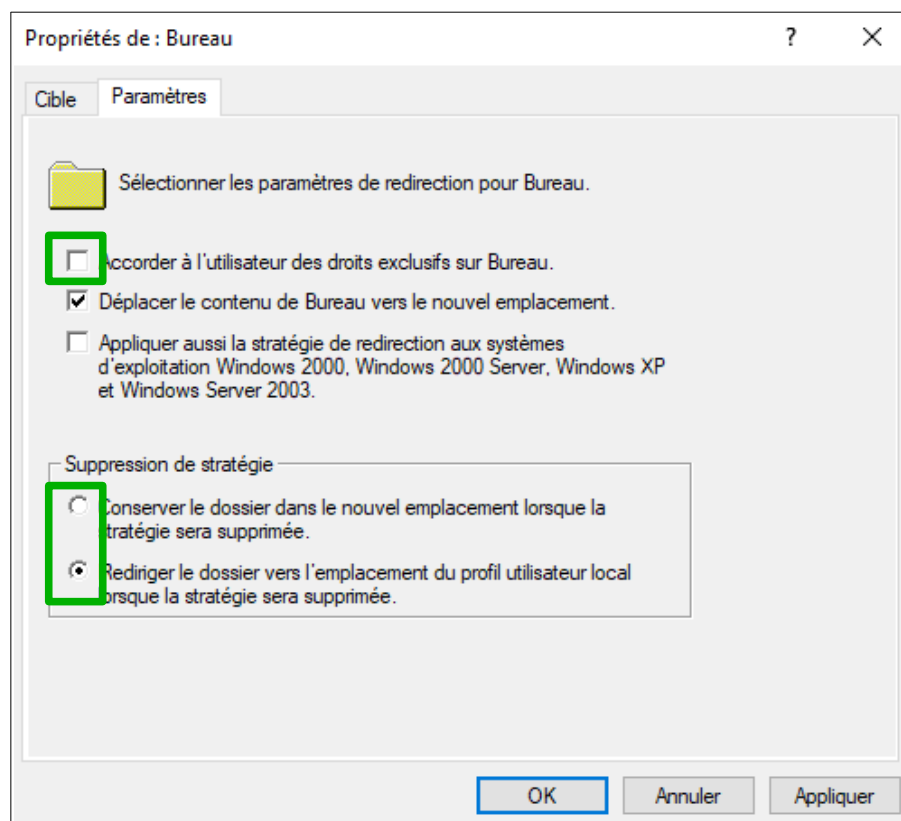
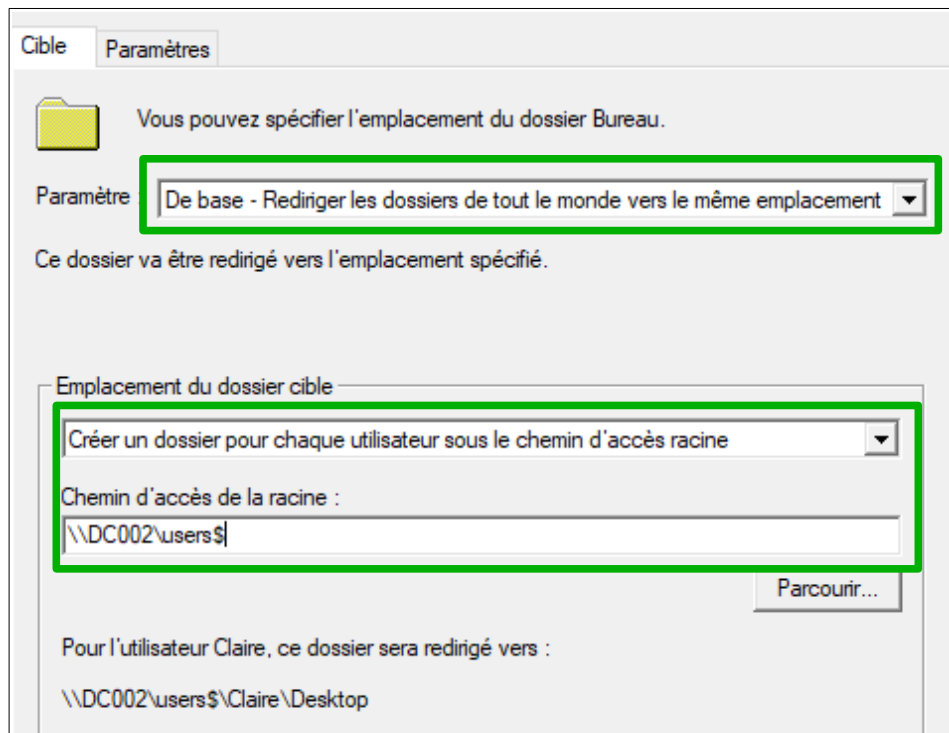
Une GPO s'applique à des utilisateurs ou des ordinateurs. Dans notre cas, on l'applique à des utilisateurs.

Utilisateurs → Stratégie → Paramètres Windows → Redirection de dossiers. Dans la partie droite vous voyez les différents répertoires utilisateurs qu'il est possible de rediriger vers le stockage.

/!\ On ne peut rediriger qu'un dossier à la fois.

Exemple pour **Bureau**

Clic droit sur Bureau → Propriétés



Phase de test

Sur une machine Windows 10 : se connecter avec un utilisateur.

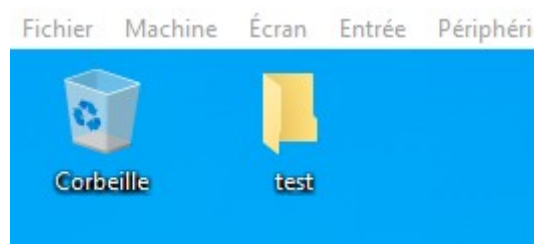
Lancer une console PowerShell

Forcez l'application de la GPO avec la commande :

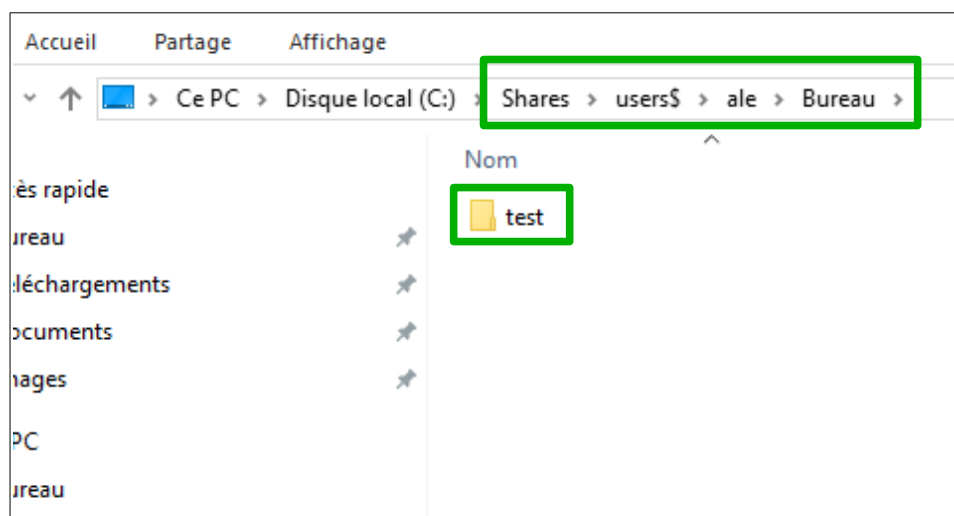
```
gpupdate /force
```

Fermer la session, se reconnecter.

Créez un répertoire test sur le Bureau.



Allez vérifier sur le serveur !



Faire de même avec tous les répertoires des utilisateurs qui sont re-dirigeables,

Testez avec d'autres utilisateurs

Testez si vous le souhaitez avec une seconde machine Windows 10 pour vérifier que le dossier apparaît bien sur le Bureau.

Vers l'infini et au-delà !

1. Configurer un controleur de domaine avec Samba v4

https://wiki.samba.org/index.php/Setting_up_Samba_as_an_Active_Directory_Domain_Controller

2. Authentifier les utilisateurs sur une machine Debian via un Active Directory.