

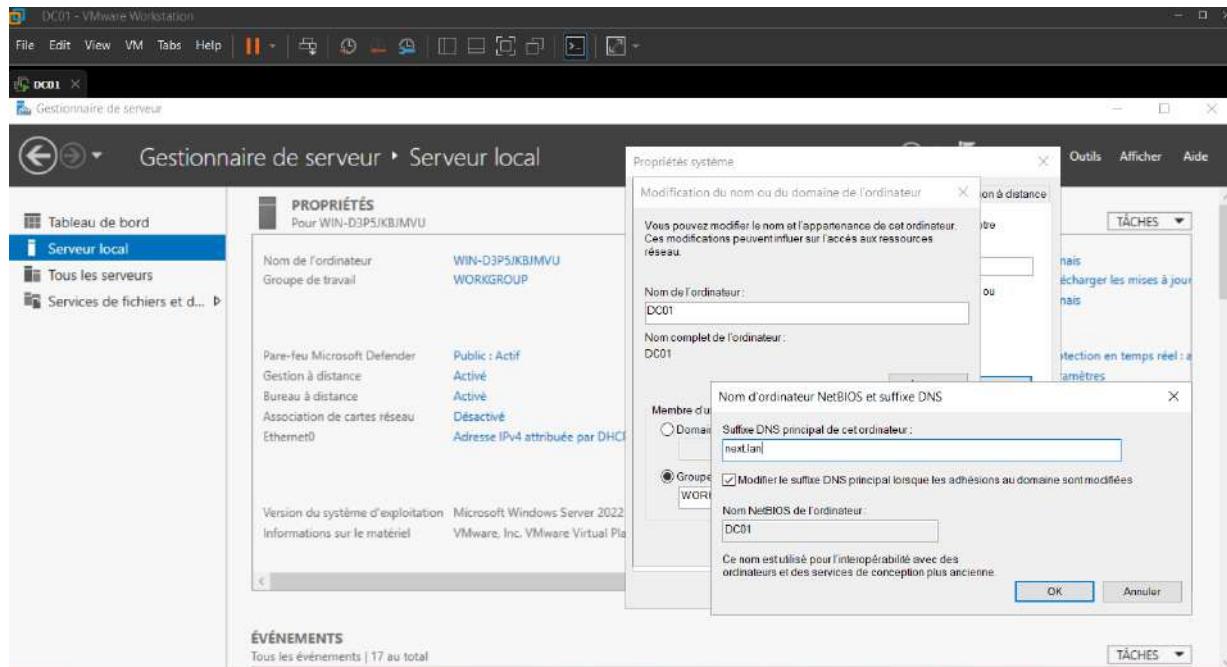
Administration Windows Serveur

Table des matières

Configuration du système	2
Configuration et installation du rôle DNS.....	4
Ajouter un serveur DNS secondaire.....	9
Création d'une forêt Active Directory.....	12
Ajout d'un contrôleur (CD) supplémentaire à un domaine.	14
Installation et configuration du service DHCP	18
Intégration d'un client Windows dans un domaine AD.....	24
Gestion des services AD DS.....	26
Gestion de l'annuaire du domaine.....	32
Gestion des groupes et permission.....	39
Mise en place d'un profil itinérant.....	45
Gestion de l'annuaire et configuration des profils utilisateurs.	49
Gestion des stratégies de groupe.	57
Démonstration GPO	62
Le dossier partagé SYSVOL	73
Mise en place d'un serveur d'impression.....	74
Glossaire	81

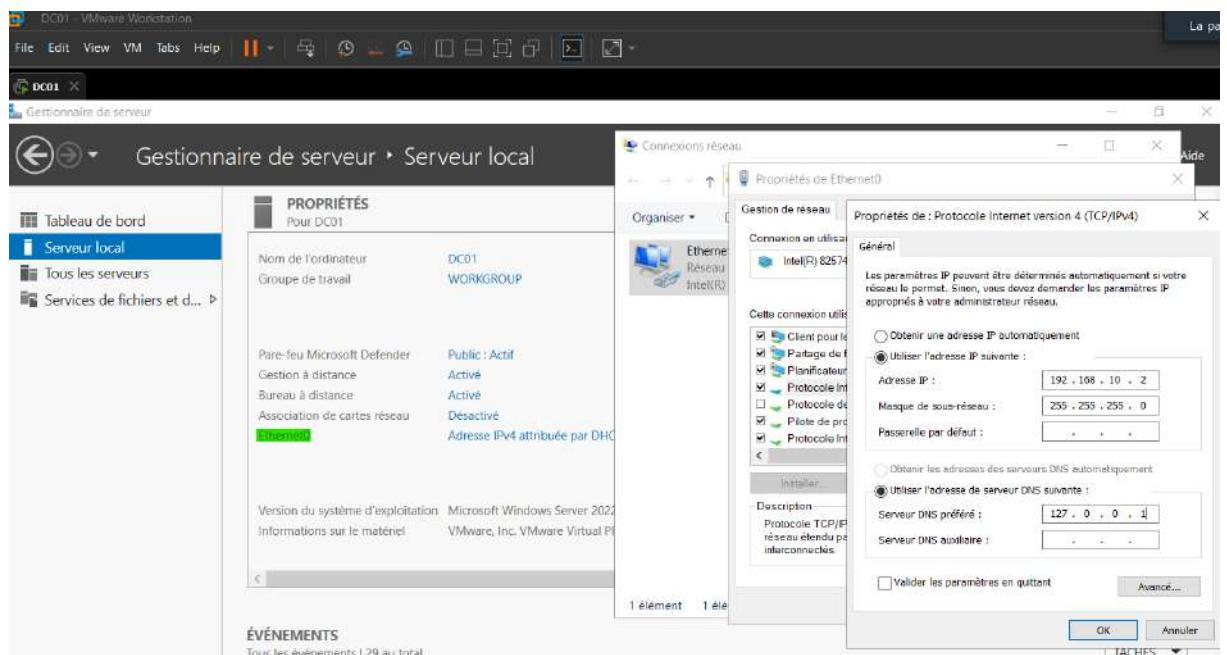
Configuration du système

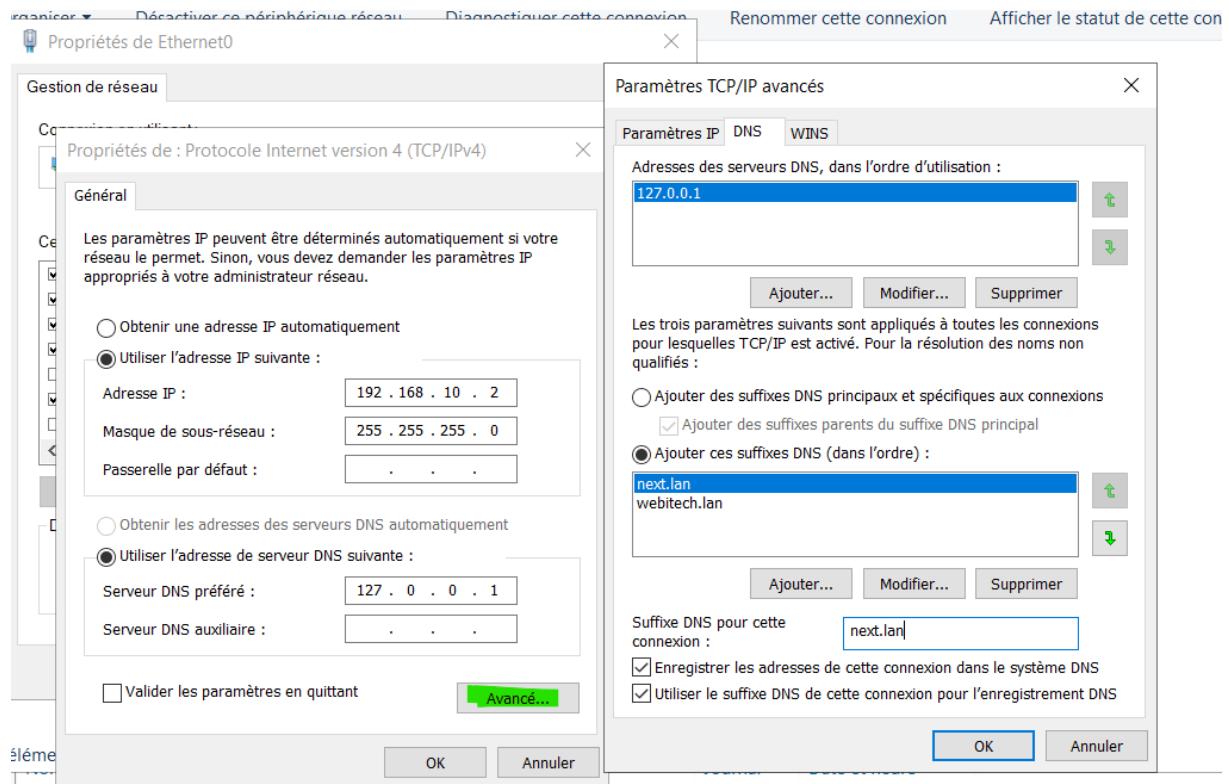
1) Renommer le serveur



On indique le nom et son suffixe DNS (votre futur nom de domaine). On valide pour redémarrer le système.

2) Adressage IP





On renseigne comme suffixe DNS pour cette connexion le domaine principal de l'hôte.

```

Administrator : C:\Windows\system32\cmd.exe
Microsoft Windows [version 10.0.20348.169]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur>ipconfig /all

Configuration IP de Windows

Nom de l'hôte . . . . . : DC01
Suffixe DNS principal . . . . . : next.lan
Type de noeud. . . . . : Hybride
Routage IP activé . . . . . : Non
Proxy WINS activé . . . . . : Non
Liste de recherche du suffixe DNS.: next.lan
                                         webitech.lan

Carte Ethernet Ethernet0 :

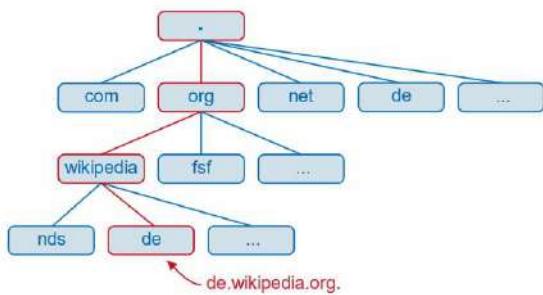
Suffixe DNS propre à la connexion. . . . . : next.lan
Description. . . . . : Intel(R) 82574L Gigabit Network Connection
Adresse physique . . . . . : 00-0C-29-1C-FA-C6
DHCP activé. . . . . : Non
Configuration automatique activée. . . . . : Oui
Adresse IPv4. . . . . : 192.168.10.2(préféré)
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . :
Serveurs DNS. . . . . : 127.0.0.1
NetBIOS sur Tcpip. . . . . : Activé

C:\Users\Administrateur>

```

On vérifie les informations depuis l'invité de commande.

Configuration et installation du rôle DNS



Permet de faire le lien entre un nom de domaine et une adresse IP.

Obligatoire dans le cas d'un Domaine Active Directory

FQDN (Full Qualified Domain Name) : Nom complet d'une machine, constitué d'étiquettes (label) séparées par des points.

Source : wikipedia.org

Zone de recherche directe : Nom -> IP

Zone de recherche indirecte IP -> Nom

The screenshot shows the 'Gestionnaire de serveur' interface. On the left, the 'Tableau de bord' navigation pane is visible with options like 'Serveur local', 'Tous les serveurs', and 'Services de fichiers et de...'. The main window displays the 'Assistant Ajout de rôles et de fonctionnalités' (Add Roles and Features Wizard). The 'Sélectionner des rôles de serveurs' (Select Server Roles) step is selected. In the 'Avant de commencer' (Before you begin) section, 'Type d'installation' (Installation type) is set to 'Ajouter des rôles et fonctionnalités sur un serveur existant' (Add roles and features to an existing server). In the 'Rôles de serveurs' (Server Roles) section, 'Serveur DNS' (DNS Server) is checked and highlighted in green. The 'Description' panel provides information about the DNS role, stating it allows name resolution over TCP/IP and is easier to manage if installed on the same server as Active Directory. Below this, a table lists the selected role:

Name	Install State
DNS	Installed

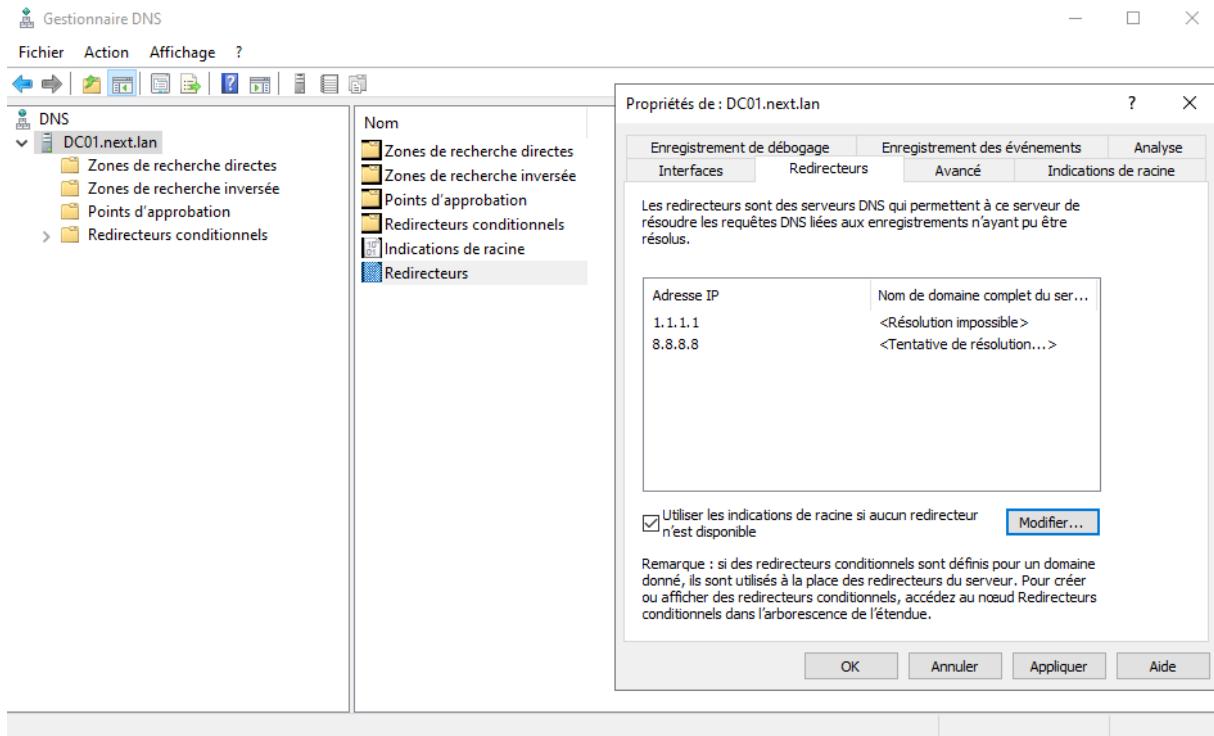
At the bottom, PowerShell command lines show the configuration:

```
PS C:\Users\Administrateur> Get-WindowsFeature -name dns
Display Name
-----
[X] Serveur DNS
```

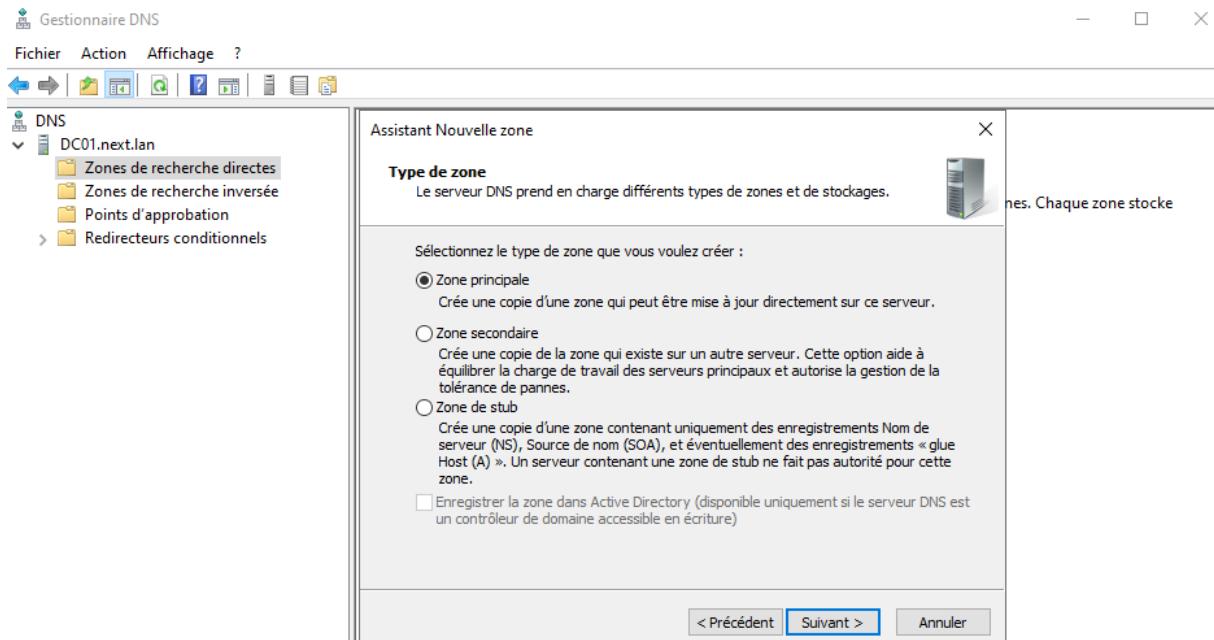
```
PS C:\Users\Administrateur> Install-WindowsFeature -name DNS
```

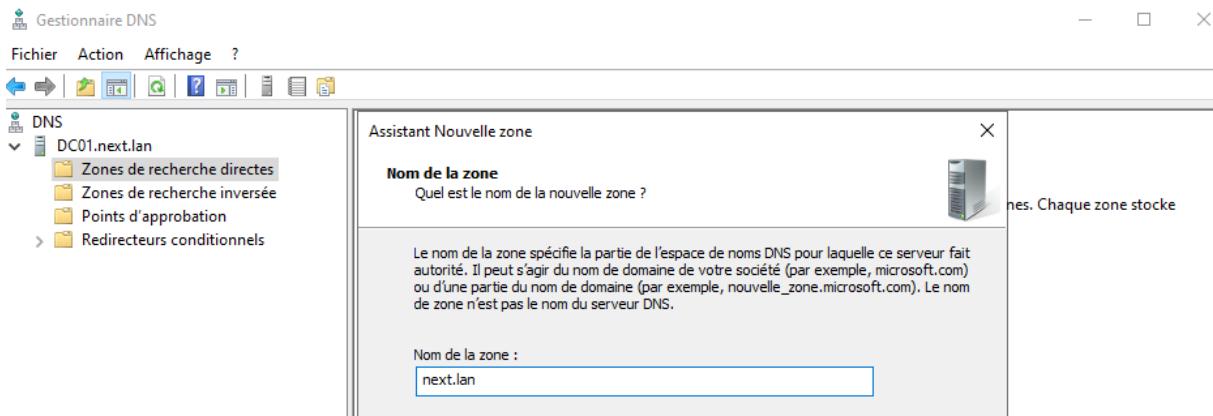
Ajouter le rôle DNS (graphique et ligne de commande)

Si le serveur à une connexion vers internet on peut préciser des adresses de serveur DNS pour la redirection des requêtes. Mais si votre serveur n'a pas internet ce n'est pas nécessaire de le préciser.

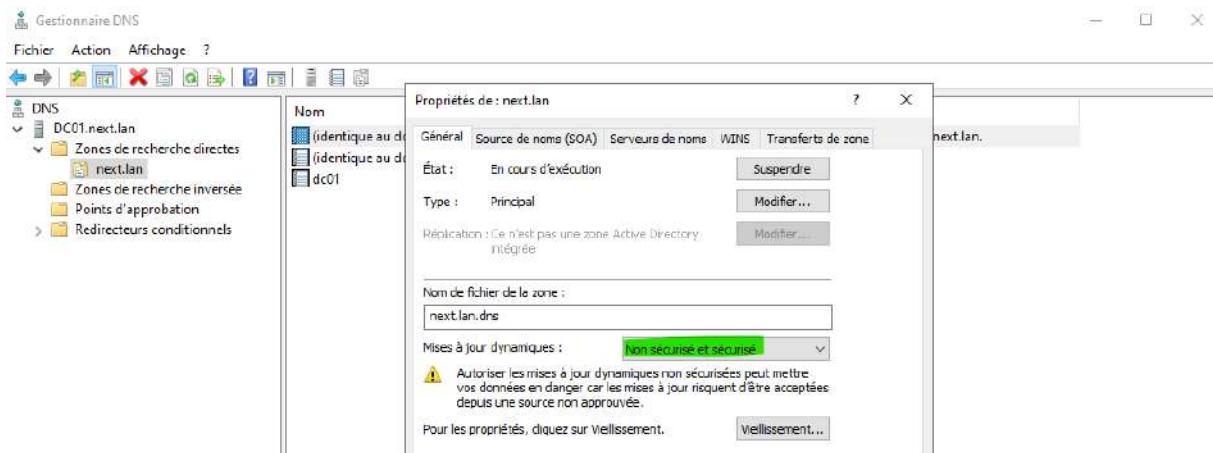


On crée une zone de recherche directe

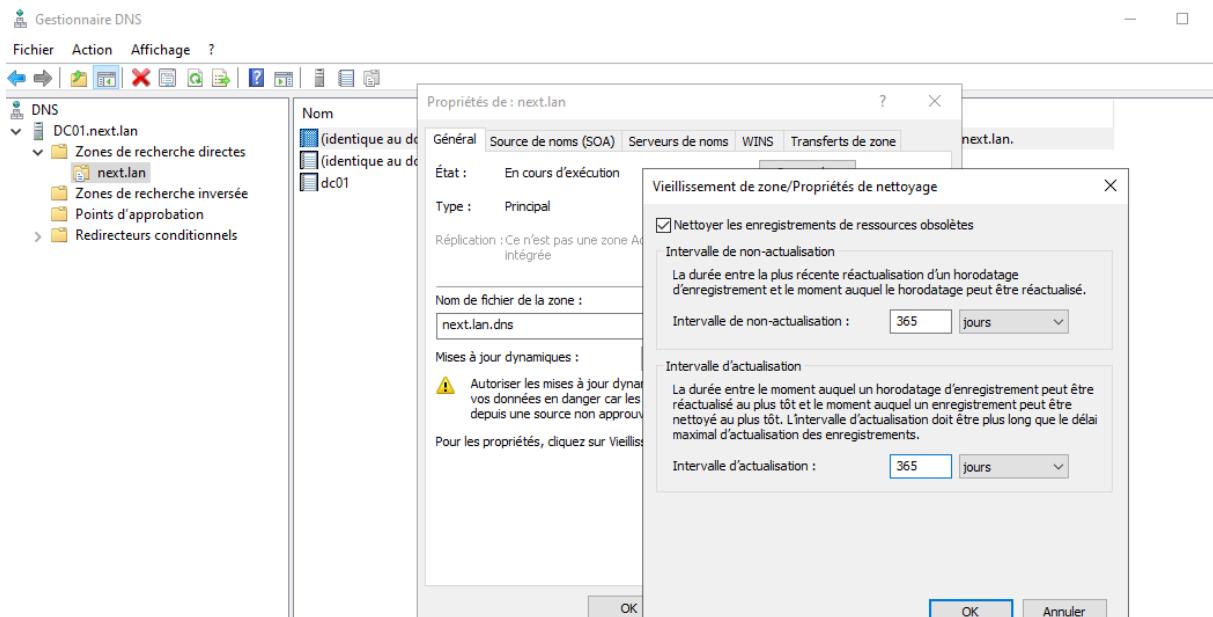




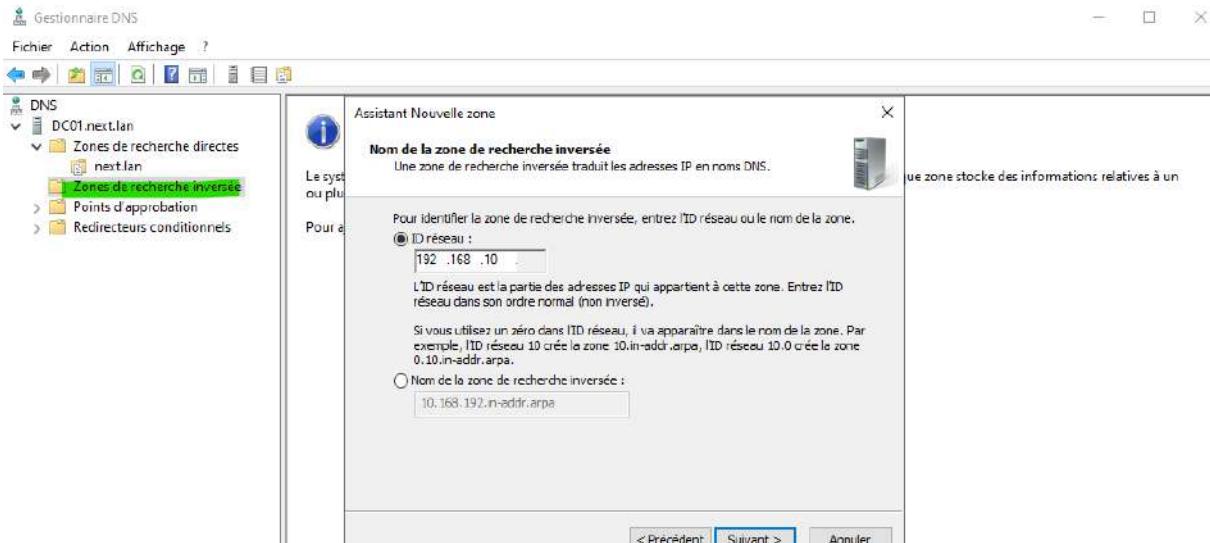
On indique la zone DNS pour notre futur domaine.



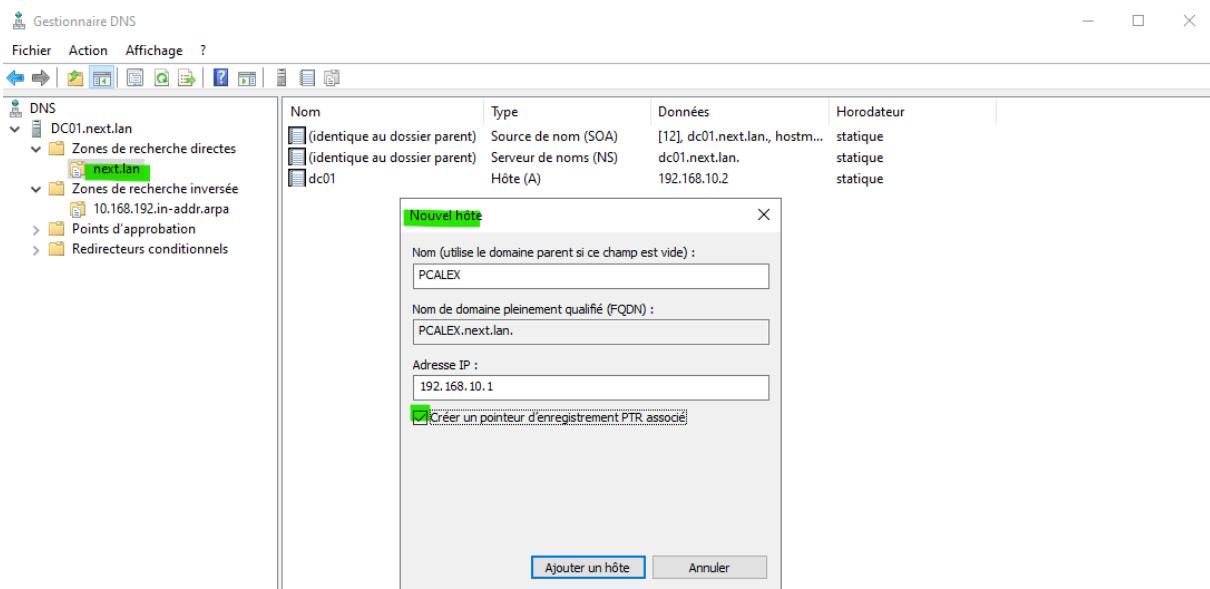
On vérifie que la zone accepte les mises à jour dynamiques en sécurisé et non sécurisé.



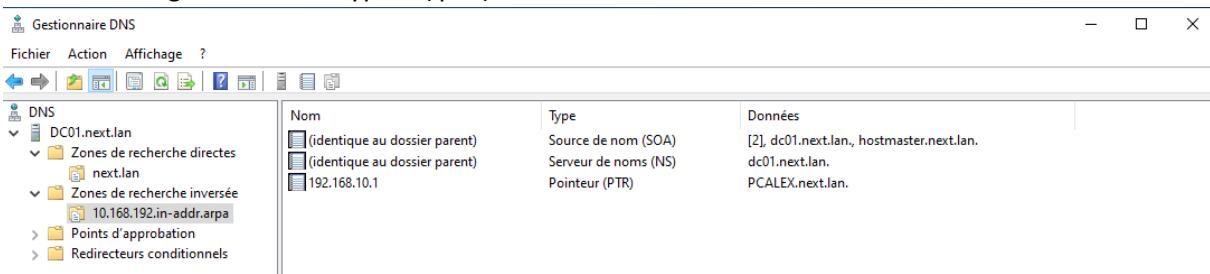
On peut préciser le nombre de jour à conserver un enregistrement s'il n'est pas actualisé. (Optionnel)



On crée la zone de recherche inversé comme serveur maître comme pour la zone de recherche directe.



Créer un enregistrement de type A (ipv4).



Automatiquement après avoir sélectionné le PTR un enregistrement sera créé dans la zone inverse.

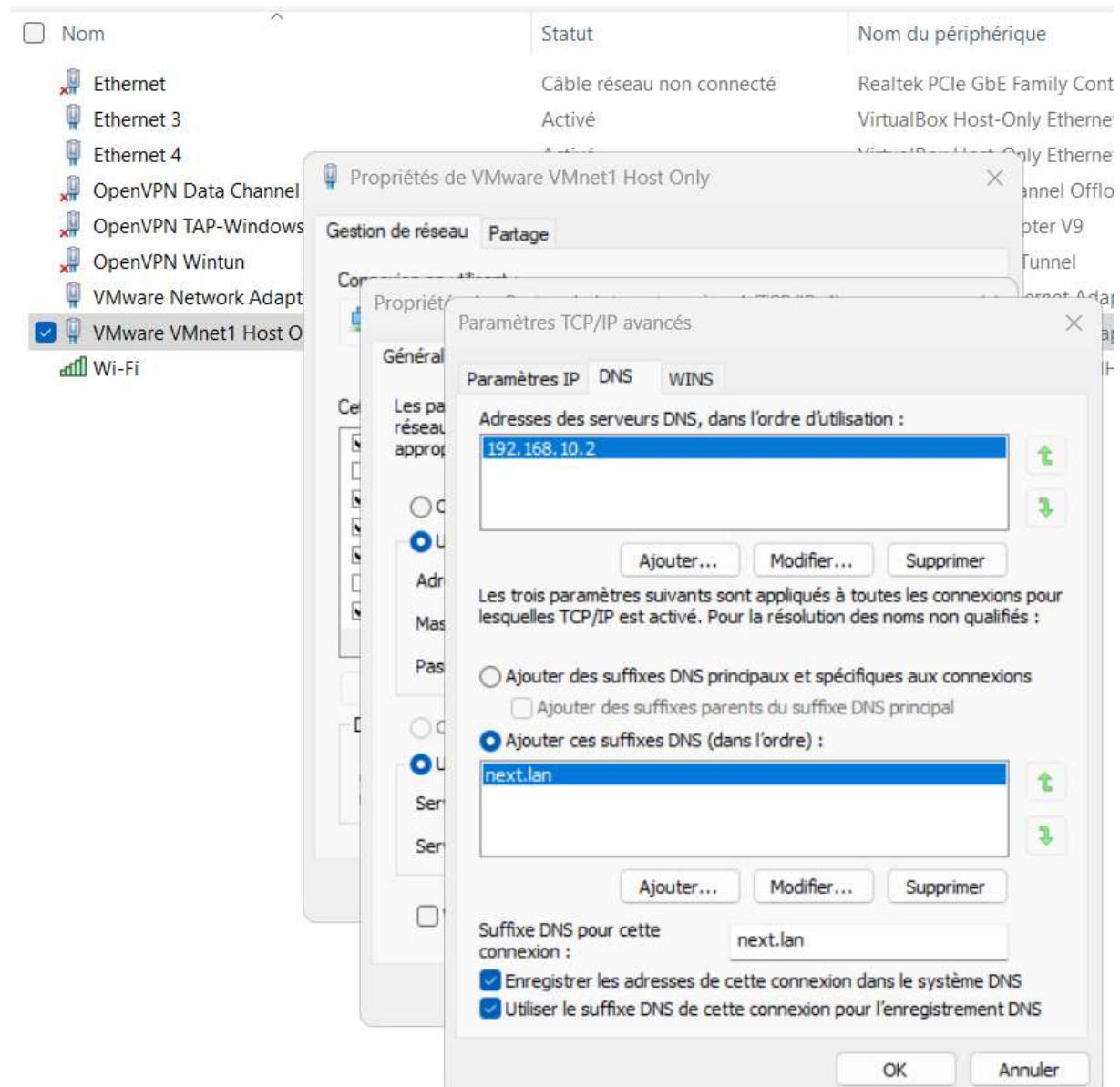
```
C:\Users\Alex>nslookup PCALEX.next.lan 192.168.10.2
Serveur : Unknown
Address: 192.168.10.2

Nom : PCALEX.next.lan
Address: 192.168.10.1

C:\Users\Alex>nslookup 192.168.10.1 192.168.10.2
Serveur : Unknown
Address: 192.168.10.2

Nom : PCALEX.next.lan
Address: 192.168.10.1
```

On vérifie avec la commande NSLOOKUP pour interroger le serveur DNS sur les enregistrements.



On indique sur la carte réseau virtuel de la machine physique les informations pour communiquer avec le serveur DNS (machine virtuel) et sélectionne les options pour s'enregistrer.

```
C:\Users\Alex>ipconfig /registerdns
```

Nom	Type	Données	Horodateur
(identique au dossier parent)	Source de nom (SOA)	[23] dc01.next.lan, hostmas...	statique
(identique au dossier parent)	Serveur de noms (NS)	dc01.next.lan.	statique
ALEXPC	Hôte (A)	192.168.10.1	10/10/2023 16:0
dc01	Hôte (A)	192.168.10.2	statique

On vérifie sur le serveur DNS si le client a été enregistré.

Ajouter un serveur DNS secondaire

Depuis le serveur maître on déclare un enregistrement de type NS (name server) dans la zone.

On indique l'adresse IP du serveur secondaire pour le transfert de notre zone directe. Il est possible d'indiquer le paramètre (uniquement vers les serveurs déclaré dans les serveurs de noms).

Depuis le serveur secondaire on ajoute une zone de recherche directe en zone secondaire.

Gestionnaire DNS

Fichier Action Affichage ?

DNS

- DC02
 - Zones de recherche directes
 - Zones de recherche inversée
 - Points d'approbation
 - Redirecteurs conditionnels

Assistant Nouvelle zone

Type de zone

Le serveur DNS prend en charge différents types de zones et de stockages.

Sélectionnez le type de zone que vous voulez créer :

- Zone principale
Crée une copie d'une zone qui peut être mise à jour directement sur ce serveur.
- Zone secondaire
Crée une copie de la zone qui existe sur un autre serveur. Cette option aide à équilibrer la charge de travail des serveurs principaux et autorise la gestion de la tolérance de pannes.
- Zone de stub
Crée une copie d'une zone contenant uniquement des enregistrements Nom de serveur (NS), Source de nom (SOA), et éventuellement des enregistrements « glue Host (A) ». Un serveur contenant une zone de stub ne fait pas autorité pour cette zone.

Assistant Nouvelle zone

Nom de la zone

Quel est le nom de la nouvelle zone ?

Le nom de la zone spécifie la partie de l'espace de noms DNS pour laquelle ce serveur fait autorité. Il peut s'agir du nom de domaine de votre société (par exemple, microsoft.com) ou d'une partie du nom de domaine (par exemple, nouvelle_zone.microsoft.com). Le nom de zone n'est pas le nom du serveur DNS.

Nom de la zone :
next.lan

Assistant Nouvelle zone

Serveurs DNS maîtres

La zone secondaire est copiée à partir d'un ou de plusieurs serveurs DNS.

Spécifiez les serveurs DNS à partir desquels vous voulez copier la zone. Les serveurs sont contactés dans l'ordre indiqué.

Serveurs maîtres :

Adresse IP	Nom de domaine ...	Validé
<Cliquez ici pour ajouter une adresse IP ou un nom DNS>		
192.168.10.2	DC01.next.lan	OK

Supprimer

Monter

Descendre

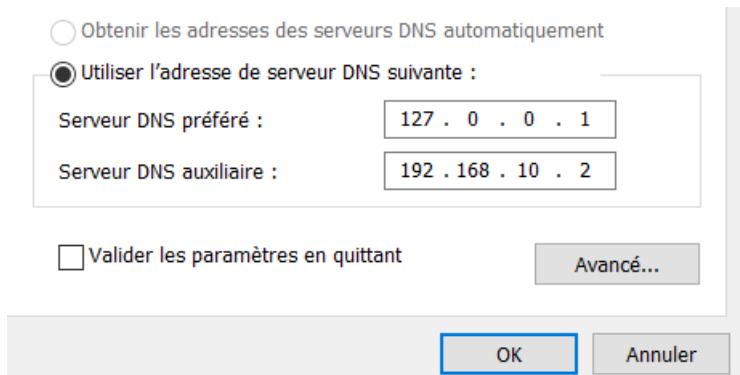
Pensez à actualiser la zone depuis le serveur secondaire ou vous pouvez faire une demande de transfert de zone.

Depuis le serveur secondaire ont obtiens la zone de recherche directe avec tous les enregistrements du serveur maître. On peut observer qu'on ne peut pas modifier la zone car le serveur secondaire n'a le droit qu'en lecture à cette zone.

The screenshot shows the Windows Server DNS Management console. On the left, a tree view shows 'DNS' and a selected node 'DC02'. Under 'DC02', there are several items: 'Zones de recherche directes', 'next.lan' (highlighted in grey), 'Zones de recherche inversée', 'Points d'approbation', and 'Redirecteurs conditionnels'. To the right, a table displays the contents of the 'next.lan' zone:

Nom	Type	Données	Horodateur
(identique au dossier parent)	Source de nom (SOA)	[26], dc01.next.lan, hostmas...	statique
(identique au dossier parent)	Serveur de noms (NS)	dc01.next.lan.	statique
(identique au dossier parent)	Serveur de noms (NS)	DC02.next.lan.	statique
ALEXPC	Hôte (A)	192.168.10.1	statique
dc01	Hôte (A)	192.168.10.2	statique
DC02	Hôte (A)	192.168.10.3	statique

Une fois la zone transférée, changer l'adressage DNS du serveur secondaire à partir de la carte réseau.



Création d'une forêt Active Directory

Role AD-DS

Active Directory Domain Services est un service annuaire qui permet d'organiser les objets dans un environnement Microsoft.

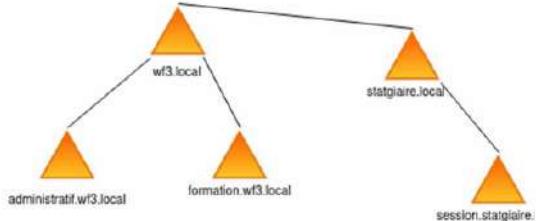
AD-DS permet de centraliser l'authentification des utilisateurs. Il permet d'autoriser, ou de ne pas autoriser l'accès à une ressource.

Les objets au sens AD sont principalement, les Utilisateurs, les Ressources (PC, imprimante, dossier partagé...) et les Groupes (pour regrouper les utilisateurs a)



Domaine Microsoft

Un domaine et ses sous-domaines représentent un arbre Active Directory. Cet arbre peut être inclus dans une forêt si d'autres domaines existent dans la même infrastructure.

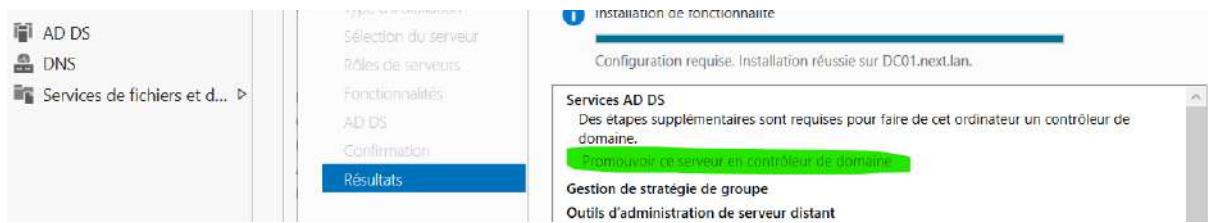


Ajouter le rôle.

Rôles de serveurs	<input type="checkbox"/> Accès à distance <input type="checkbox"/> Attestation d'intégrité de l'appareil <input type="checkbox"/> Hyper-V <input type="checkbox"/> Serveur de télécopie <input type="checkbox"/> Serveur DHCP <input checked="" type="checkbox"/> Serveur DNS (Installé) <input type="checkbox"/> Serveur Web (IIS) <input type="checkbox"/> Service Guardian hôte <input checked="" type="checkbox"/> Services AD DS <input type="checkbox"/> Services AD LDS (Active Directory Lightweight Dire
-------------------	--

Les services de domaine Active Directory (AD DS) stockent des informations à propos des objets du réseau et rendent ces informations disponibles pour les utilisateurs. Les administrateurs du réseau utilisent les contrôleurs de domaine pour donner aux utilisateurs du réseau accès aux ressources autorisées.

Promouvoir son serveur en tant que contrôleur de domaine afin de créer la forêt.



Options supplémentaires Ajouter un nouveau domaine à une forêt existante
Chemins d'accès Ajouter une nouvelle forêt
Examiner les options
Vérification de la config...
Installation
Résultats

Spécifiez les informations de domaine pour cette opération

Nom de domaine racine : next.lan

Options du contrôleur de domaine

SERVEUR CIBLE
DC01.next.lan

- Configuration de déploie...
Options du contrôleur de...
 Options DNS
 Options supplémentaires
 Chemins d'accès
 Examiner les options
 Vérification de la config...
 Installation
 Résultats

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

Niveau fonctionnel de la forêt : Windows Server 2016
Niveau fonctionnel du domaine : Windows Server 2016

Spécifier les fonctionnalités de contrôleur de domaine

- Serveur DNS (Domain Name System)
 Catalogue global (GC)
 Contrôleur de domaine en lecture seule (RODC)

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

Mot de passe : Confirmer le mot de passe :

On décoche délégation si nous n'avons pas de domaine enfant.

Options DNS

SERVEUR CIBLE
DC01.next.lan

- Configuration de déploie...
Options du contrôleur de...
 Options DNS
 Options supplémentaires
 Chemins d'accès

Spécifier les options de délégation DNS

- Crée une délégation DNS

Chemins d'accès

SERVEUR CIBLE
DC01.next.lan

- Configuration de déploie...
Options du contrôleur de...
 Options DNS
 Options supplémentaires
 Chemins d'accès
 Examiner les options

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

Dossier de la base de données : C:\Windows\NTDS
Dossier des fichiers journaux : C:\Windows\NTDS
Dossier SYSVOL : C:\Windows\SYSVOL

Ajout d'un contrôleur (CD) supplémentaire à un domaine.

On va rajouter un deuxième serveur Windows qui va être contrôleur de domaine d'un domaine existant afin d'augmenter la haute disponibilité.

Afin de rajouter notre 2eme serveur il est conseillé de supprimer les zones DNS secondaire directe t'inversé s'ils ont été créés.

Pour la configuration de la carte réseau on va indiquer en serveur préféré DNS l'adresse du contrôleur de domaine du serveur principal.

Assistant Ajout de rôles et de fonctionnalités

Progression de l'installation

SERVEUR DE DESTINATION
DC02.next.lan

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

AD DS

Confirmation

Résultats

Afficher la progression de l'installation

Installation de fonctionnalité

Configuration requise. Installation réussie sur DC02.next.lan.

Services AD DS

Des étapes supplémentaires sont requises pour faire de cet ordinateur un contrôleur de domaine.

Promouvoir ce serveur en contrôleur de domaine

Gestion de stratégie de groupe

Configuration de déploiement

Configuration de déploiement

Options du contrôleur de domaine

Options supplémentaires

Chemins d'accès

Examiner les options

Vérification de la configuration

Installation

Résultats

Selectionner l'opération de déploiement

Ajouter un contrôleur de domaine à un domaine existant

Ajouter un nouveau domaine à une forêt existante

Ajouter une nouvelle forêt

Spécifiez les informations de domaine pour cette opération

Domaine : next.lan

Fournir les informations d'identification pour effectuer cette opération

<Aucune information d'identification fournie>

SÉCURITÉ WINDOWS

SERVEUR CIBLE
DC02.next.lan

SERVEUR DE DESTINATION
DC02.next.lan

TÂCHES

Informations d'identification pour une opération de déploiement

Fournir des informations d'identification pour l'opération de déploiement

adminnext@next.lan

OK Annuler

Cours d'exécution. Examinez les étapes dans la barre de progression.

On peut décocher l'option CG car dans notre domaine nous avons déjà un serveur Contrôleur de domaine (CD) qui a ce rôle. Pour informations le CG va permettre d'accélérer les recherches des objets AD de l'annuaire d'un domaine de notre forêt car le serveur qui est Global catalogue (GC ou CG) dispose d'une copie des annuaires venant des autres domaines (attention il ne récupère pas tous les attributs attachés à un objet, il faut les définir à partir de la console schéma AD).

Dans l'exemple ci-dessous on peut cocher ou décocher la réPLICATION de cet attribut attaché à une classe.

The screenshot shows the 'Propriétés de : accountExpires' (Properties of : accountExpires) dialog box. In the 'Général' (General) tab, the attribute 'accountExpires' is listed with the following details:

- Description : Account-Expires
- Nom commun : Account-Expires
- ID d'objet X.500 : 1.2.840.113556.1.4.159
- Syntaxe et étendue
- Syntaxe : Entier long/Intervalle
- Minimum :
- Maximum :

A note at the bottom states: 'Cet attribut est à valeur simple.' (This attribute is a simple value). Below the general tab, there are several checkboxes:

- L'attribut est actif
- Indexer cet attribut
- Résolution de noms ANR (Ambiguous Name Resolution)
- Replicuer cet attribut dans le catalogue global (Replicate this attribute in the global catalog) - This checkbox is highlighted with a green border.
- L'attribut est copié lors de la duplication de l'utilisateur
- Indexer cet attribut pour des recherches en contenu

De plus le rôle CG est obligatoire aux moins pour un serveur CD d'une forêt AD et peu importe le domaine, car c'est celui-ci qui va permettre de renseigner le SID (identifiant pour les droits) des groupes universels lors de la connexion d'un utilisateur à son poste.

The screenshot shows the 'Options du contrôleur de domaine' (Domain Controller Options) step of the 'Assistant Configuration des services de domaine Active Directory' (Active Directory Domain Services Configuration Wizard).

The left sidebar menu includes:

- Configuration de déploiement
- Options du contrôleur de domaine (selected)
- Options DNS
- Options supplémentaires
- Chemins d'accès
- Examiner les options
- Vérification de la configuration
- Installation
- Résultats

The main pane displays the 'Spécifier les capacités du contrôleur de domaine et les informations sur le site' (Specify the domain controller capabilities and site information) section. It includes:

- Serveur DNS (Domain Name System)
- Catalogue global (GC)
- Contrôleur de domaine en lecture seule (RODC)
- Nom du site : PARIS
- Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)
- Mot de passe : (password field)
- Confirmer le mot de passe : (password confirmation field)

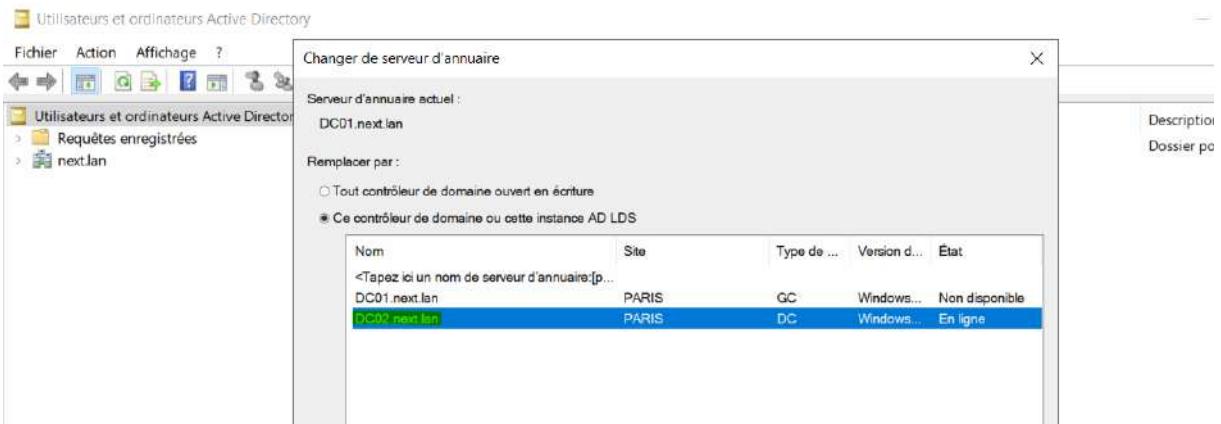


Après le redémarrage on peut observer dans la console des sites AD que le serveur DC02 apparait sur le même site donc on parle de réPLICATION intra-site.

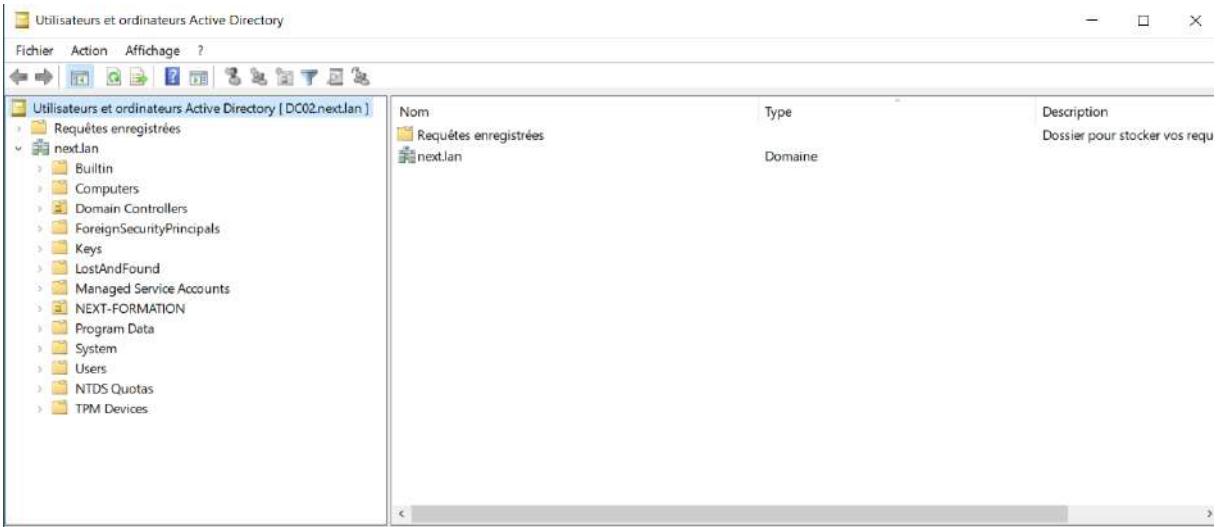
Nom	Domaine	Serveur pont	Type de contrôl...	Description
				Aucun élément à afficher dans cet aperçu.

Que ce soit depuis le serveur DC01 (soit notre premier contrôleur de domaine) ou le DC02 on peut accéder à l'annuaire AD car il le partage en commun depuis la base de données NTDS. Concrètement ces deux serveurs qui sont contrôleur de domaine du domaine NEXT possèdent les mêmes informations de la base NTDS (AD). Donc par exemple le même compte utilisateur admin.

Exemple depuis DC01.



Ici on est connecté depuis le DC01 mais on est sur l'annuaire avec le DC02.



Installation et configuration du service DHCP

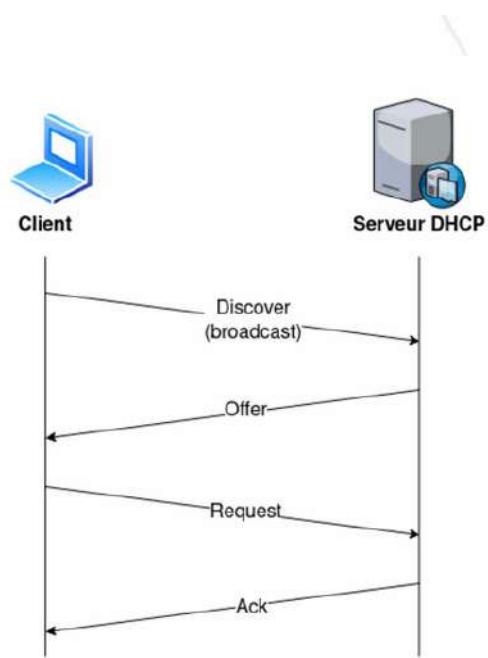
Service DHCP (Dynamic Host Configuration Protocol) :

Récupération d'une adresse IP de manière automatique.

Permet aussi de récupérer l'adresse IP de la passerelle, du serveur DNS...

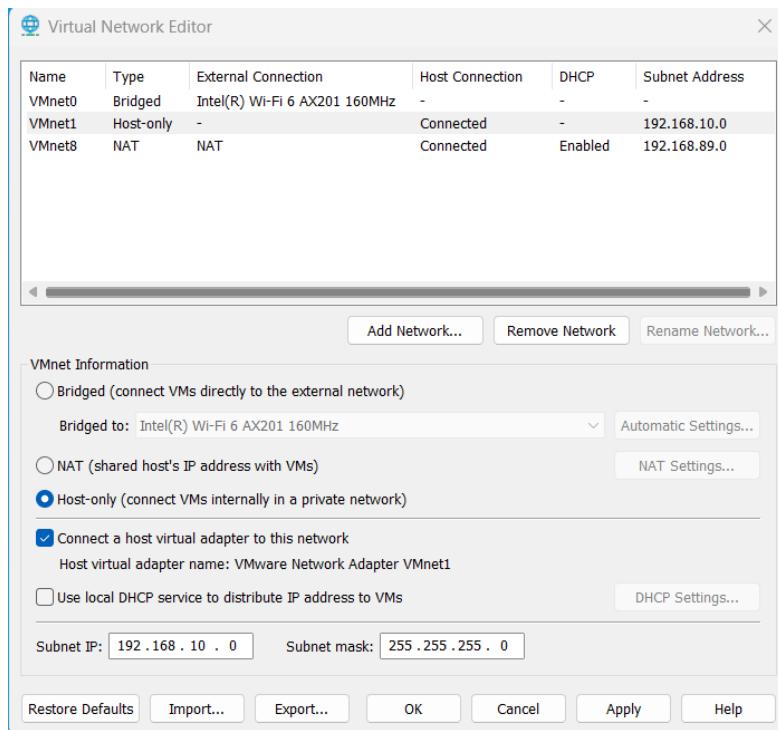
Emission d'un message DHCP discover (broadcast) par le client

Echange des messages Offer/Request et ACK pour obtenir une configuration réseau.

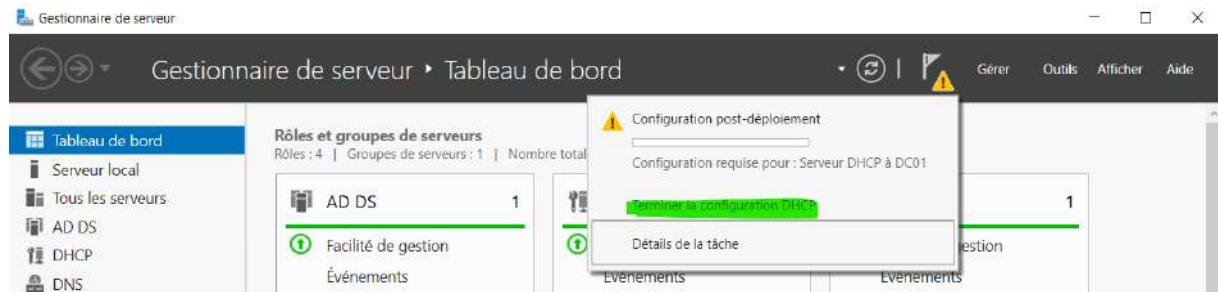


Ajouter le rôle DHCP depuis le serveur. (un serveur)

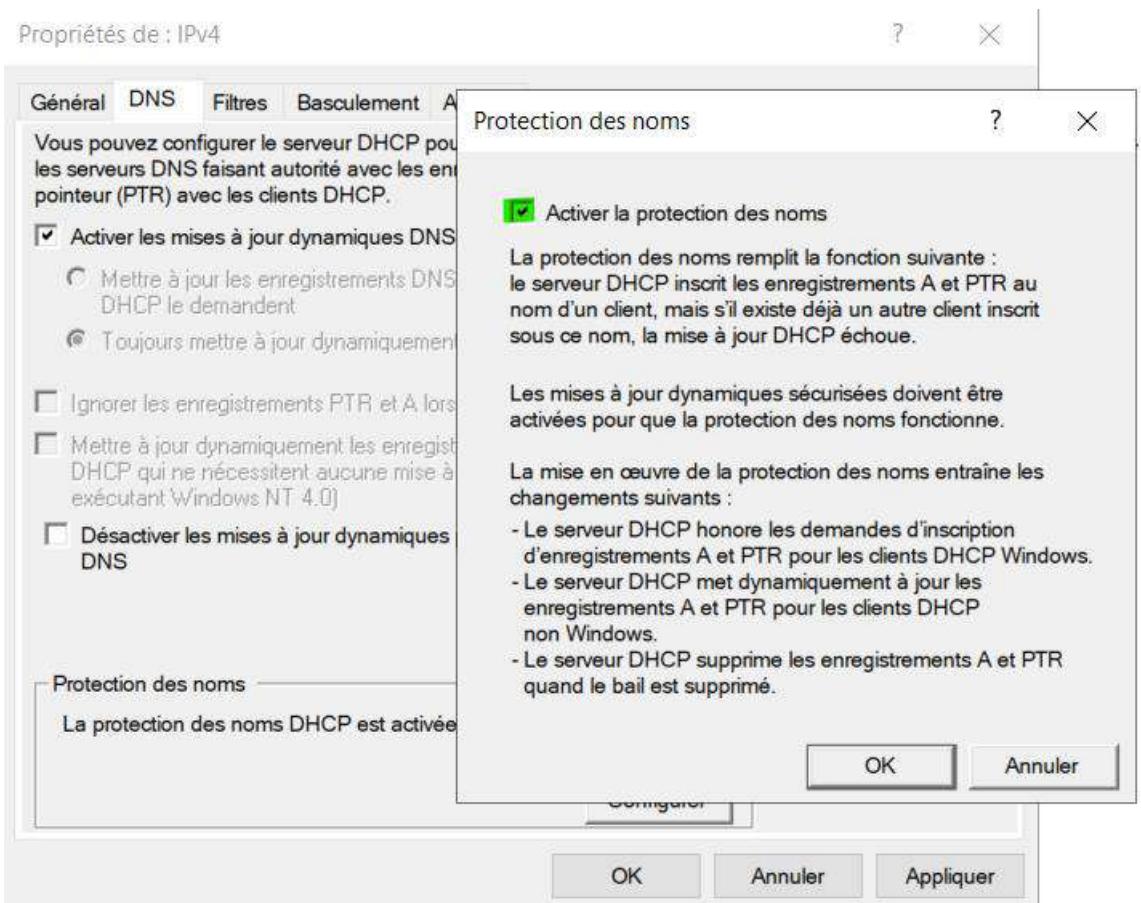
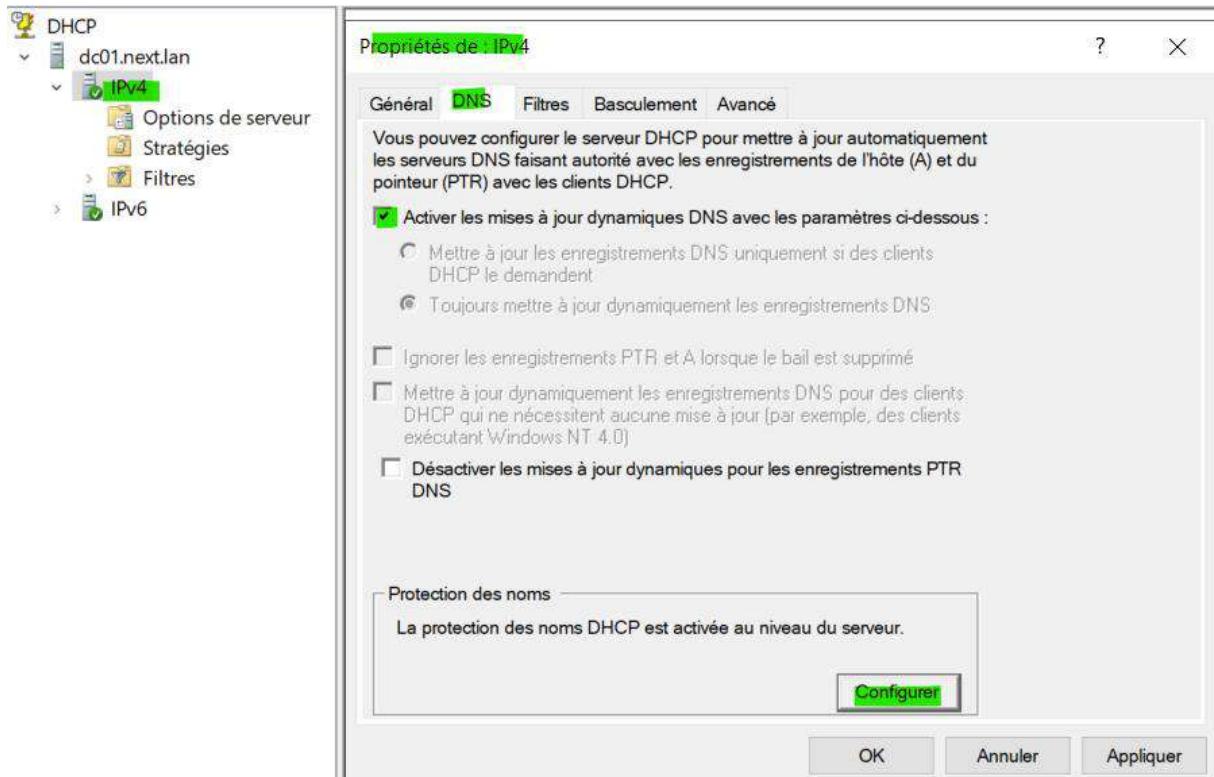
Attention pensez à désactiver le service DHCP du VMWare selon le profil réseau qui a été choisi.



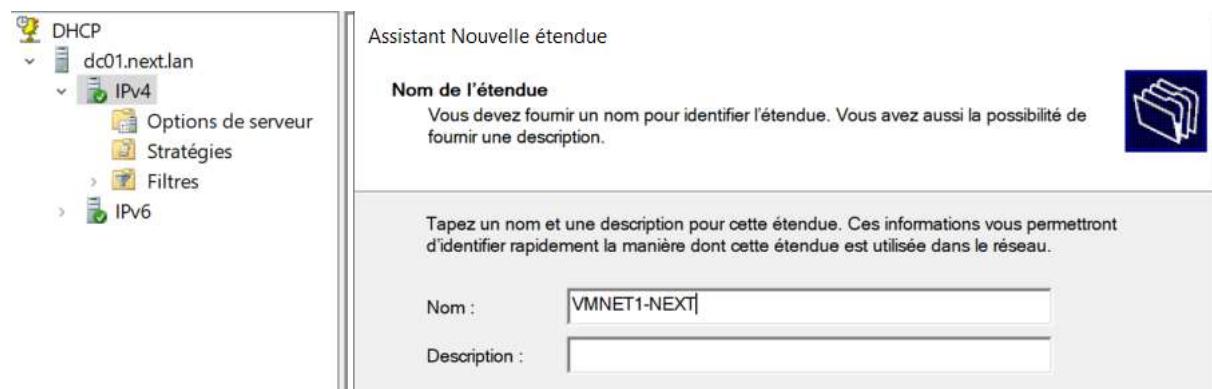
Une fois le rôle installé pensez à valider la configuration depuis la console gestionnaire de serveur.



Depuis la console de gestion on active l'enregistrement dynamique du DNS et la protection des noms.



Créer l'étendu pour votre réseau en indiquant ces paramètres.



This screenshot shows the 'Plage d'adresses IP' (IP Address Range) configuration page. It starts with a note: 'Vous définissez la plage d'adresses en identifiant un jeu d'adresses IP consécutives.' (You define the address range by identifying a set of consecutive IP addresses). Below this is a 'Paramètres de configuration pour serveur DHCP' (DHCP Server Configuration Parameters) section. It contains fields for 'Adresse IP de début' (Start IP Address) set to '192 . 168 . 10 . 1' and 'Adresse IP de fin' (End IP Address) set to '192 . 168 . 10 . 254'. The next section, 'Paramètres de configuration qui se propagent au client DHCP.' (DHCP Client Configuration Parameters), includes 'Longueur:' (Length) set to '24' and 'Masque de sous-réseau:' (Subnet Mask) set to '255 . 255 . 255 . 0'. At the bottom are navigation buttons: '< Précédent' (Previous), 'Suivant >' (Next), and 'Annuler' (Cancel).

On va exclure une plage de 1 à 10 afin d'éviter de les distribuer dans le réseau pour les clients.

DHCP

- dc01.next.lan
 - IPv4
 - Options de serveur
 - Stratégies
 - Filtres
 - IPv6

Assistant Nouvelle étendue

Ajout d'exclusions et de retard

Les exclusions sont des adresses ou une plage d'adresses qui ne sont pas distribuées par le serveur. Un retard est la durée pendant laquelle le serveur retardera la transmission d'un message DHCPOFFER.

Entrez la plage d'adresses IP que vous voulez exclure. Si vous voulez exclure une adresse unique, entrez uniquement une adresse IP de début.

Adresse IP de début : Adresse IP de fin :

Plage d'adresses exclue :
192.168.10.1 sur 192.168.10.10

Retard du sous-réseau en millisecondes :

DHCP

- dc01.next.lan
 - IPv4
 - Options de serveur
 - Stratégies
 - Filtres
 - IPv6

Assistant Nouvelle étendue

Durée du bail

La durée du bail spécifie la durée pendant laquelle un client peut utiliser une adresse IP de cette étendue.

La durée du bail doit théoriquement être égale au temps moyen durant lequel l'ordinateur est connecté au même réseau physique. Pour les réseaux mobiles constitués essentiellement par des ordinateurs portables ou des clients d'accès à distance, des durées de bail plus courtes peuvent être utiles.

De la même manière, pour les réseaux stables qui sont constitués principalement d'ordinateurs de bureau ayant des emplacements fixes, des durées de bail plus longues sont plus appropriées.

Définissez la durée des baux d'étendue lorsqu'ils sont distribués par ce serveur.

Limitée à :

Jours : Heures : Minutes :

DHCP

- dc01.next.lan
 - IPv4
 - Options de serveur
 - Stratégies
 - Filtres
 - IPv6

Assistant Nouvelle étendue

Configuration des paramètres DHCP

Vous devez configurer les options DHCP les plus courantes pour que les clients puissent utiliser l'étendue.

Une étendue peut avoir plusieurs configurations de paramètres DHCP. Vous pouvez configurer les paramètres pour une étendue spécifique ou pour tous les clients de l'ensemble de serveurs.

Pour une étendue spécifique :

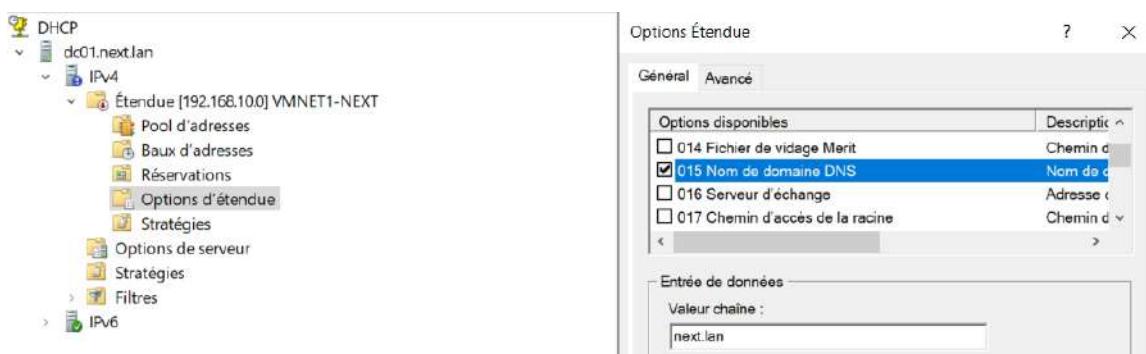
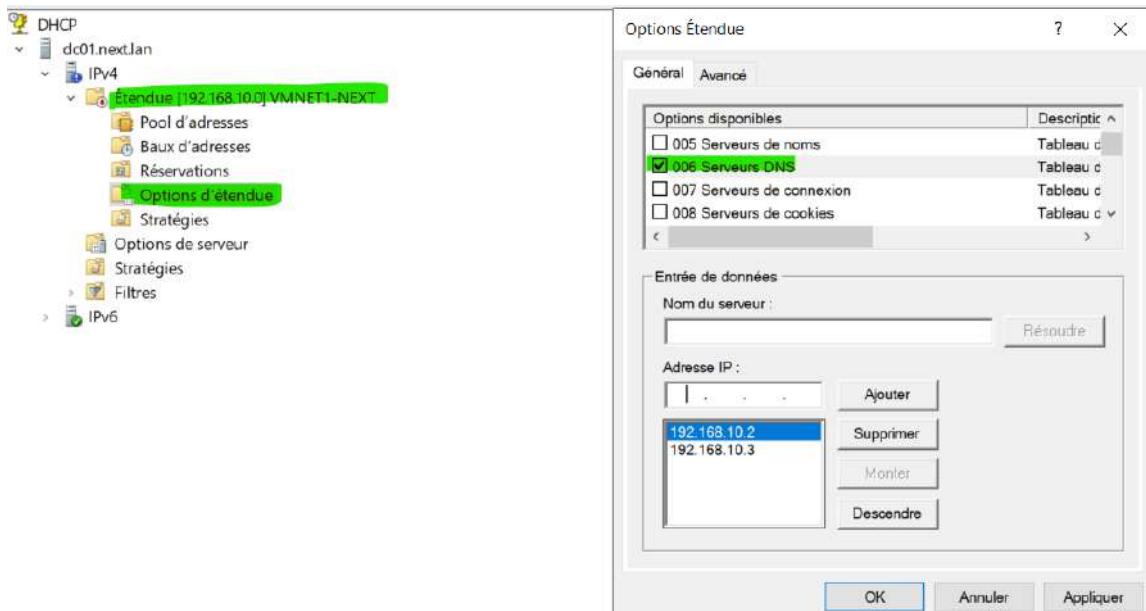
Lorsque les clients obtiennent une adresse, ils se voient attribuer des options DHCP, telles que les adresses IP des routeurs (passerelles par défaut), des serveurs DNS, et les paramètres WINS pour cette étendue.

Les paramètres que vous sélectionnez maintenant sont pour cette étendue et ils remplaceront les paramètres configurés dans le dossier Options de serveur pour ce serveur.

Voulez-vous configurer les options DHCP pour cette étendue maintenant ?

Oui, je veux configurer ces options maintenant
 Non, je configurerai ces options ultérieurement

Ajouter les options au niveau de l'étendu.



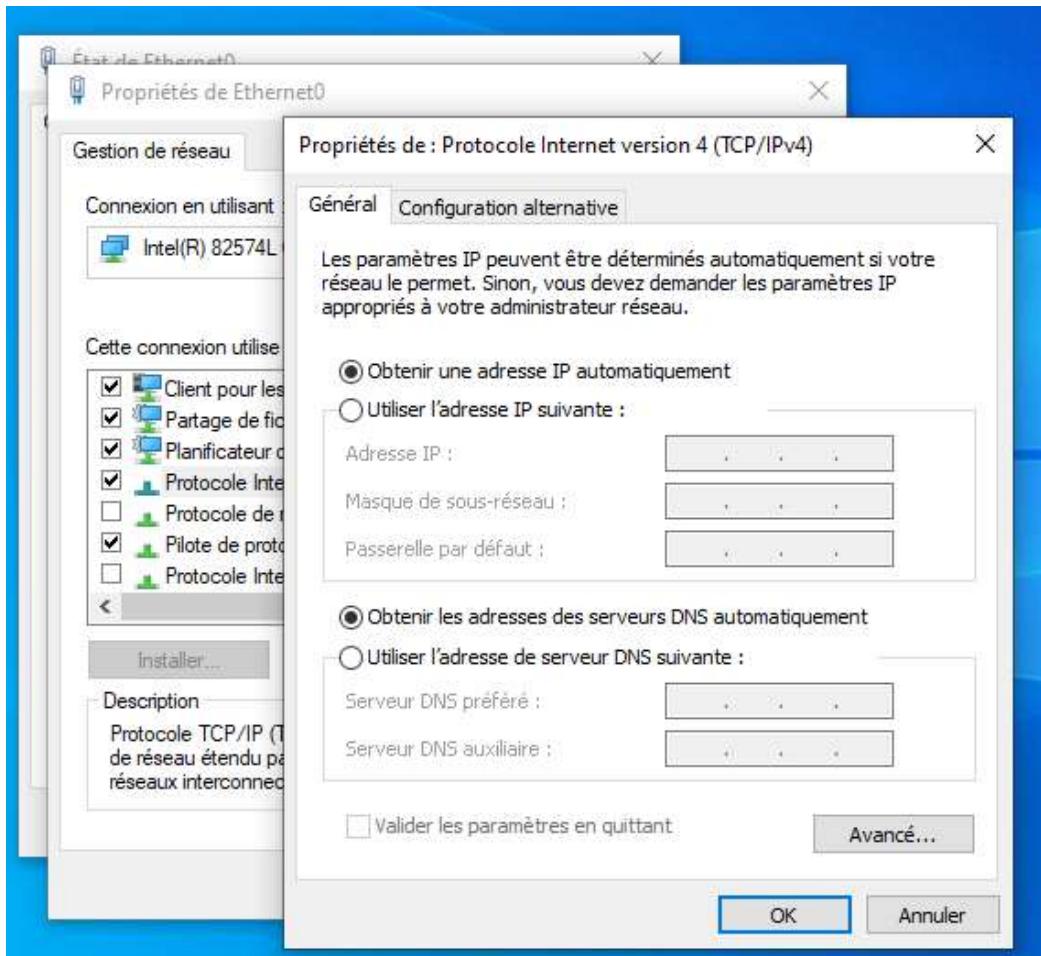
Aperçu des options.

Nom d'option	Fournisseur	Valeur	Nom de la stratégie
006 Serveurs DNS	Standard	192.168.10.2, 192.168.10.3	Aucun
015 Nom de domaine DNS	Standard	next.lan	Aucun

Pensez à activer l'étendu.

Intégration d'un client Windows dans un domaine AD.

Depuis le client, la carte réseau doit être en DHCP et recevoir toutes les informations d'adressage IP et DNS venant du DHCP. Pensez à mettre la carte réseau de la VM dans le bon profil réseau de VMware ou de votre logiciel de virtualisation.

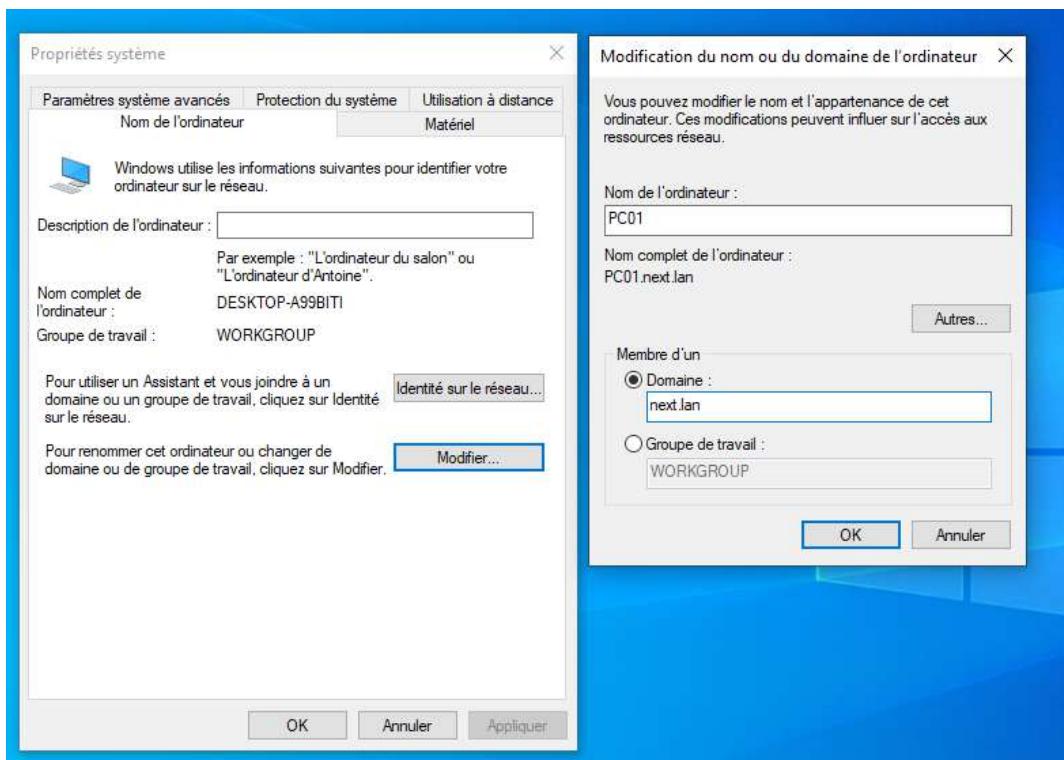


On va vérifier que le client est capable de résoudre le domaine :

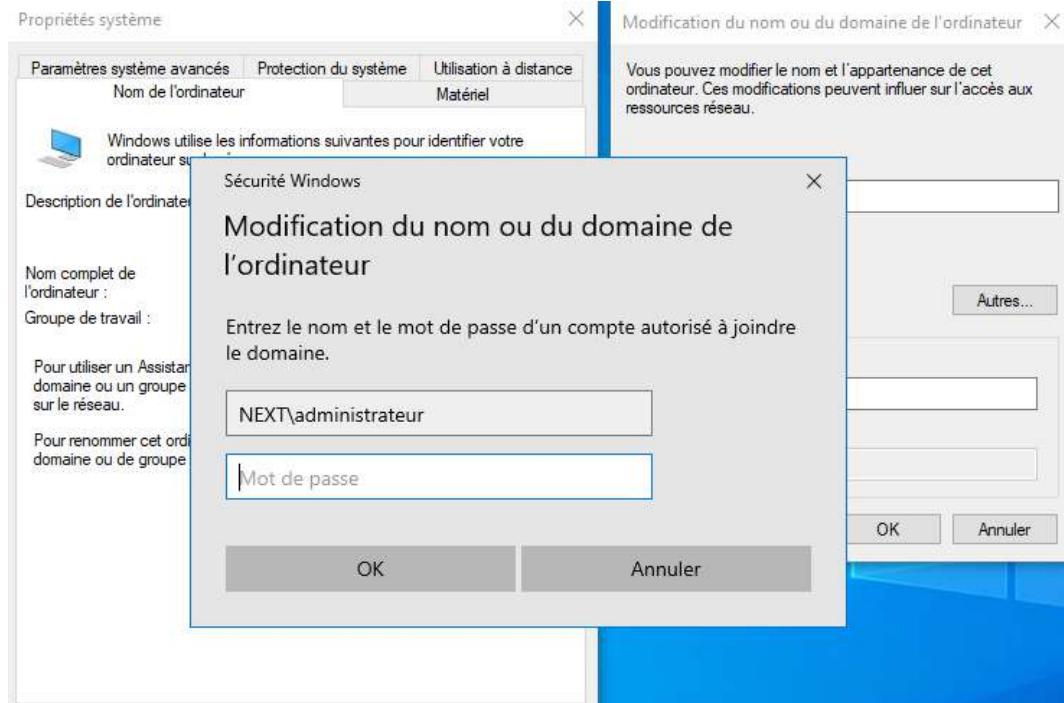
```
C:\Users\alx>nslookup next.lan
Serveur : DC01.next.lan
Address: 192.168.10.2

Nom : next.lan
Address: 192.168.10.2
```

Ajouter le client Windows en le renommant, indiqué le suffixe DNS.



Indiquer le compte utilisateur qui permet d'ajouter un ordinateur dans un domaine (compte du domaine AD)

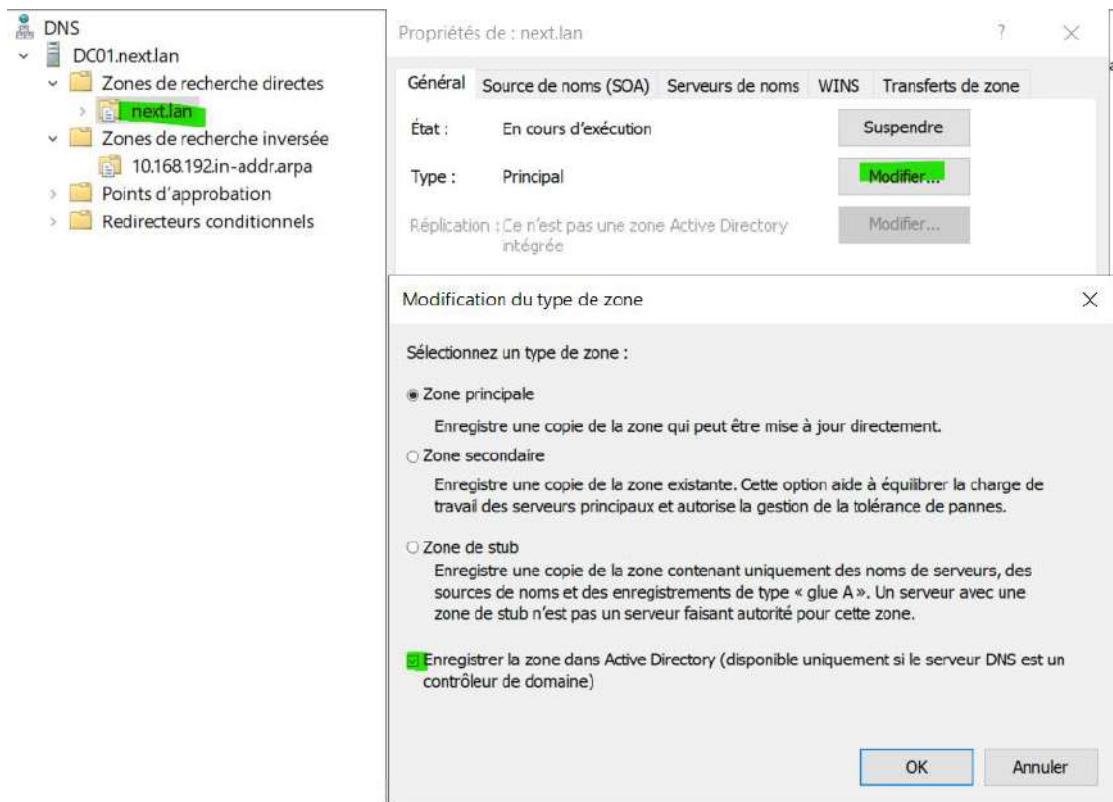


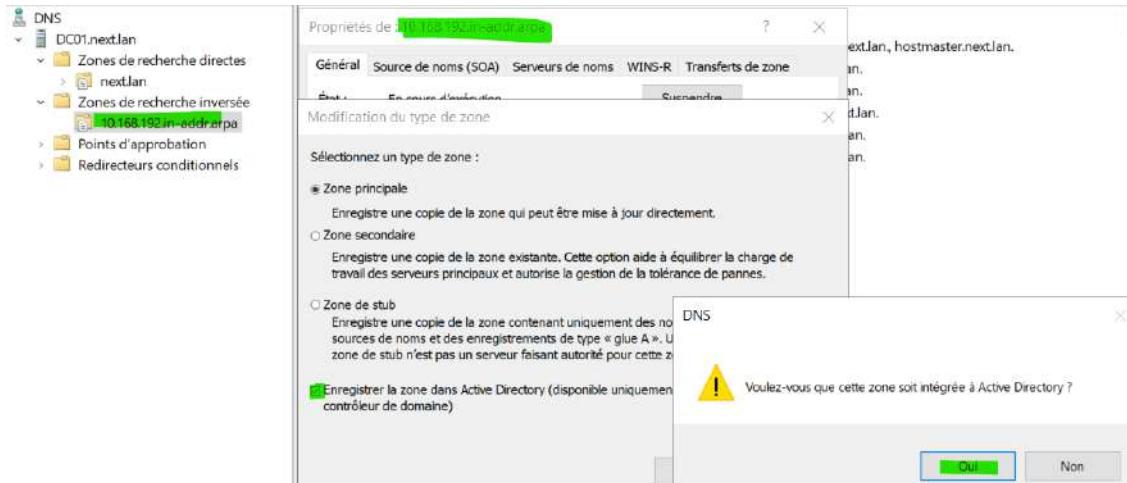
Gestion des services AD DS.

Gestion du DNS

Intégrer la zone DNS d'un domaine dans la base de données NTDS permet de rendre le service DNS en mode multi-maître, il n'y a plus de notions secondaires. En fonction de la durée de réplication de la base NTDS entre les serveurs, si la zone DNS a été intégré celle-ci sera mis à jour entre les serveurs.

Intégrer les zones de recherche directe et inversé dans la base de données Active Directory.

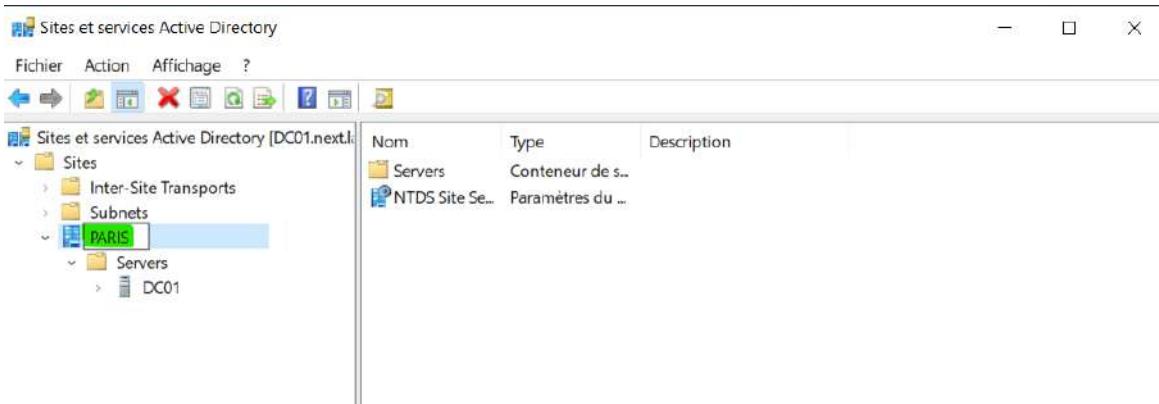




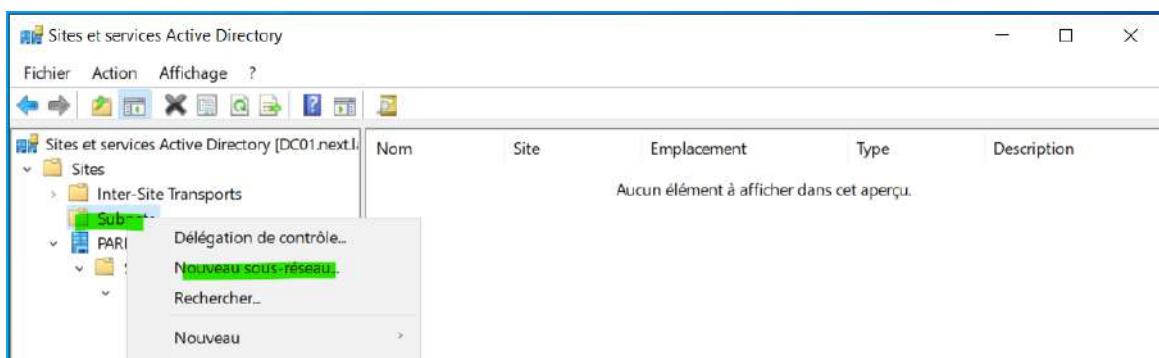
Gestion des sites & services AD

La console gestion des sites et services AD nous permet de définir l'emplacement des serveurs (Contrôleur de domaine) afin d'optimiser la réPLICATION inter-sites ou intra-site de la base de données NTDS (soit Active Directory) et les connexions entre les postes informatiques d'un domaine en fonction de sa localisation.

On renomme le site par défaut avec le site de nos serveurs.



On va associer un réseau en fonction de son site.



The screenshot shows the 'Sites et services Active Directory' console. On the left, the navigation pane shows a tree structure with 'Sites', 'Inter-Site Transports', 'Subnets', 'PARIS' (selected), 'Servers', 'DC01', and 'NTDS Settings'. The main pane displays a 'Nouvel objet - Sous-réseau' (New object - Subnet) dialog. It has a note about entering a network prefix using network notation (address/length). Below it are examples for IPv4 (157.54.208.0/20) and IPv6 (3FFE:FFFF:0:C000::/64). A 'Prefixe:' field contains '192.168.10.0/24'. A 'Nom du préfixe des services de domaine Active Directory:' field contains '192.168.10.0/24'. A 'Sélectionnez un objet du site pour ce préfixe.' section shows a list with 'Nom du site' and 'PARIS' selected. At the bottom, a table lists the newly created subnet:

	Nom	Site	Emplacement	Type	Description
	192.168.10.0/24	PARIS		Sous-réseau	

Gestion du schéma.

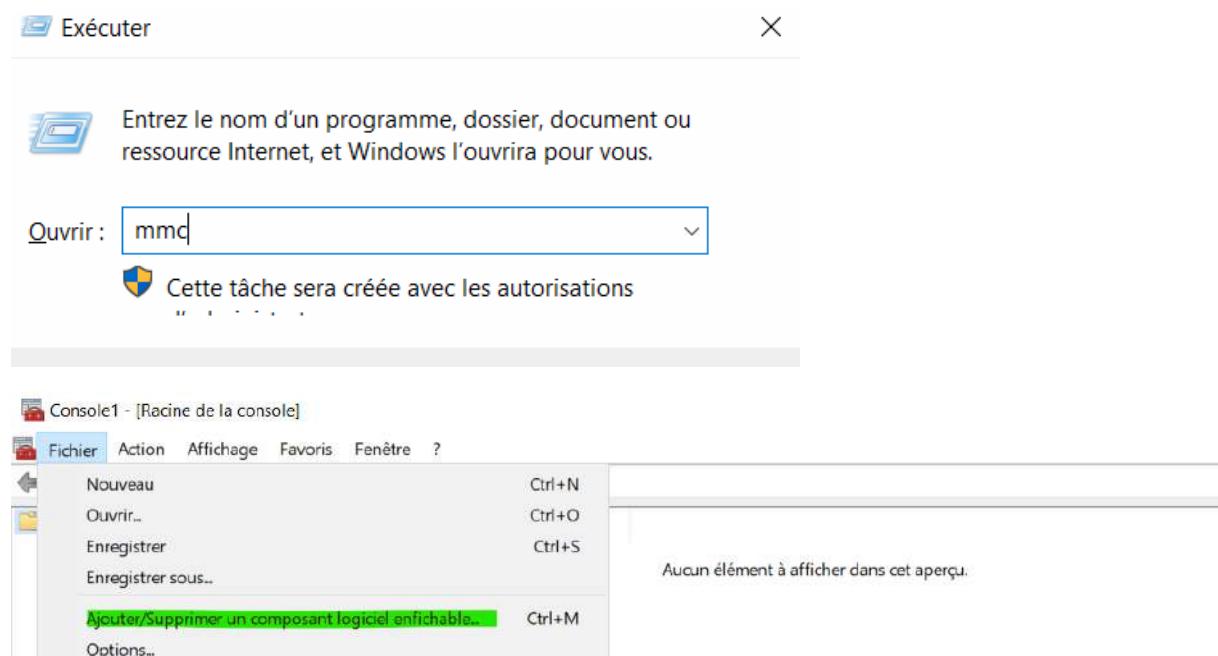
Depuis la console schéma active directory on va pouvoir modifier le schéma de notre entreprise (de la forêt). On pourrait ajouter un nouvel attribut à un objet AD. Exemple rajouter une catégorie GRADE pour les comptes utilisateurs de notre AD dans le cas d'une structure militaire.

On active la console pour le schéma.

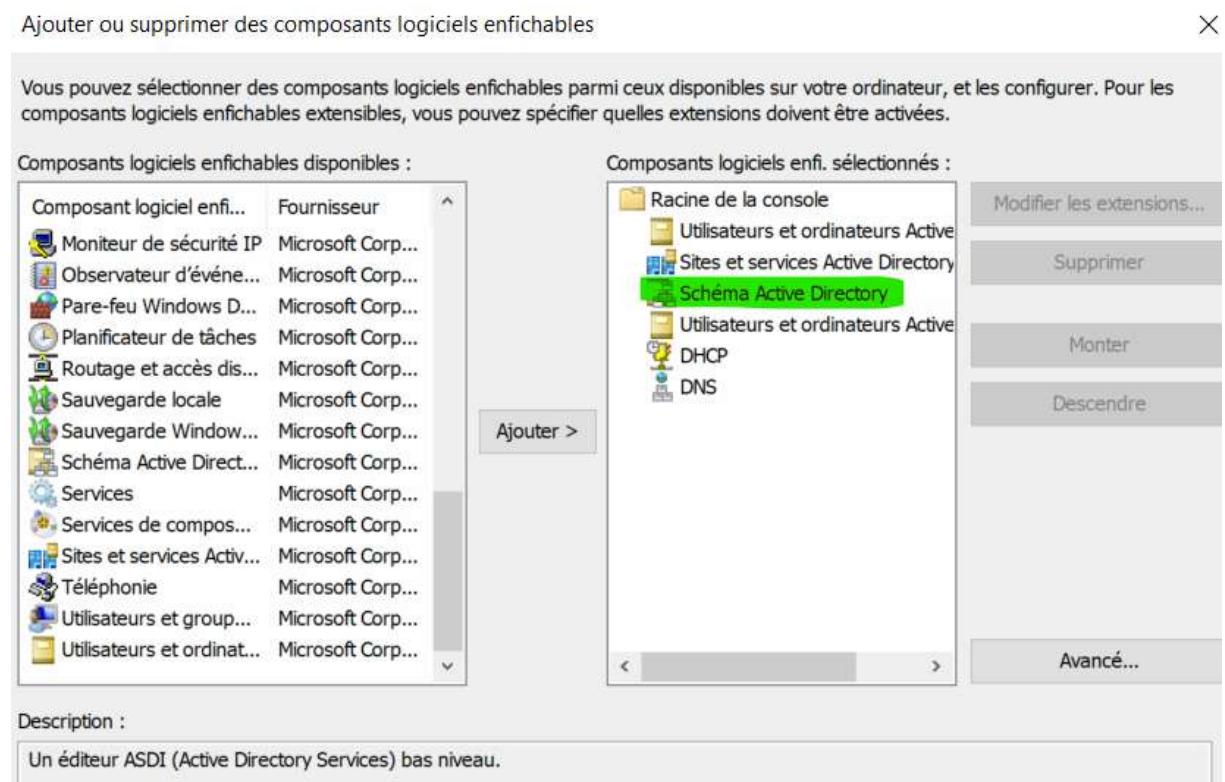
```
Administrator : C:\Windows\system32\cmd.exe
Microsoft Windows [version 10.0.20348.169]
(c) Microsoft Corporation. Tous droits réservés.

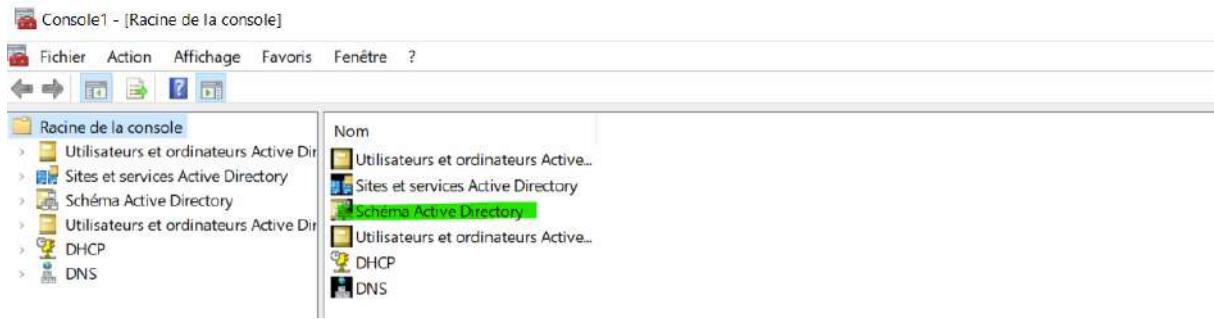
C:\Users\Administrateur>regsvr32 schmmgmt.dll
```

Ouvrir une console MMC



Ajouter les outils suivants dont la console pour la gestion du schéma.

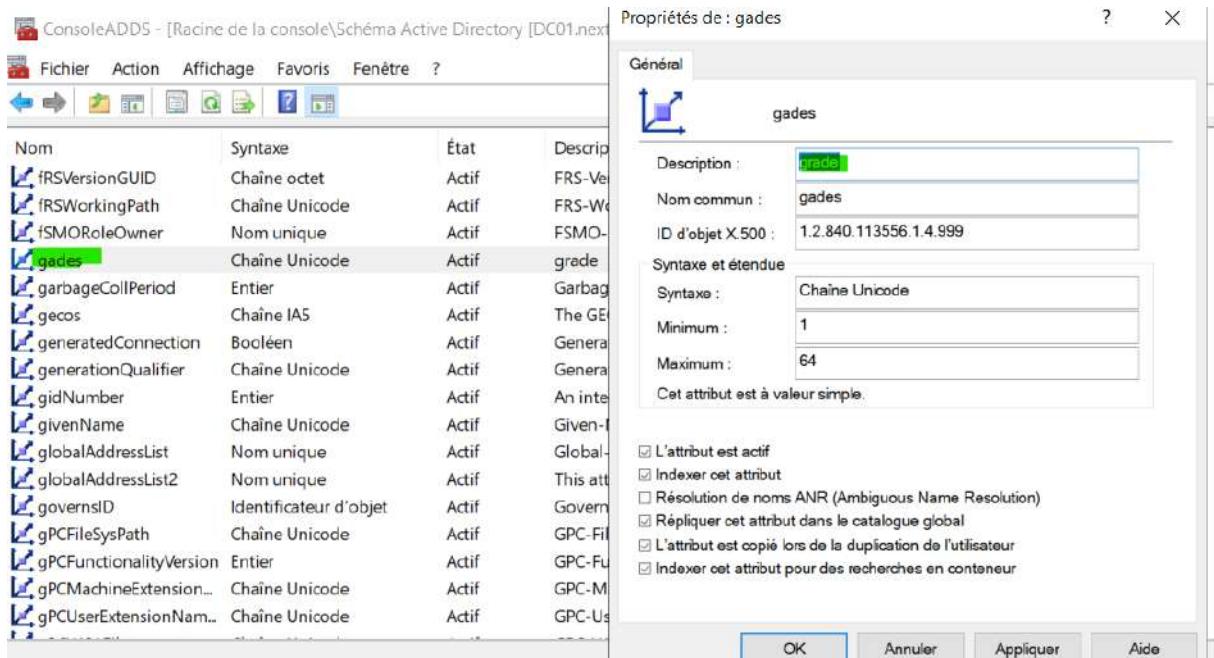




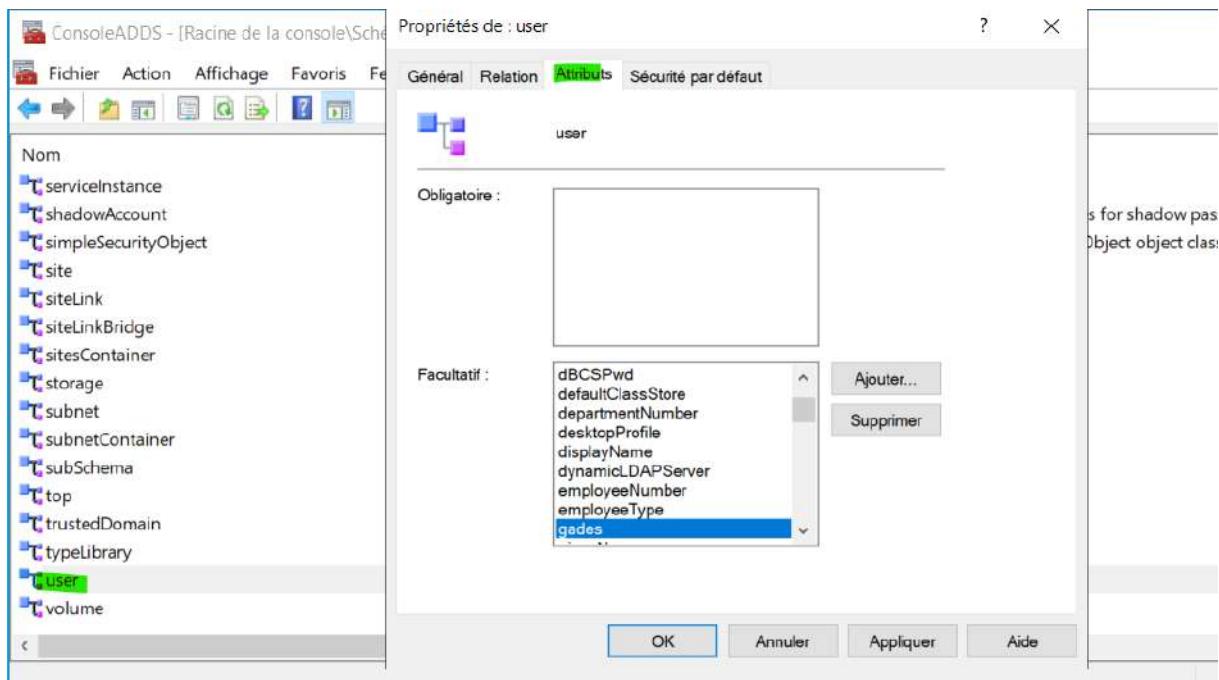
A travers le schéma on associe des attributs à des classes exemples description pour la classe ordi. On peut créer notre propre attribut et l'associer à une classe existante voir une nouvelle classe.

Exemple : rajouter une attribut GRADES à une classe USER. Un objet utilisateur de l'AD va contenir cet attribut qui peut être modifier en lui indiquant une valeur depuis l'annuaire.

On crée l'attribut dans l'onglet ATTRIBUT.



On associe l'attribut GRADE créé avec la classe USER.



Visualiser ou indiquer une valeur à cet attribut de l'objet utilisateur.

The screenshot shows the 'Utilisateurs et ordinateurs Active Directory [DC01.next.lan]' (Users and computers Active Directory [DC01.next.lan]) window. A user object named 'test01' is selected. On the right, the 'Propriétés' (Properties) dialog box is open, showing the 'Attributs' (Attributes) tab. The 'gedes' attribute is listed with the value 'CAPITAINES'. The 'Editeur d'attributs' (Attribute editor) button is highlighted with a green oval.

Voir ce lien pour de l'aide sur cette manipulation :

https://www.it-connect.fr/active-directory-comment-creer-un-attribut-personnalise/#II_Ouvrir_ledito...

Gestion de l'annuaire du domaine.

La gestion de l'annuaire AD va se manipuler à partir de la console utilisateurs et ordinateurs AD.

Quelques exemples à respecter comme bonne pratiques depuis l'annuaire :

- Organiser son annuaire avec les UO
- Renommer le compte administrateur & le groupe admin du domaine
- Délégation de contrôle
- Gestions des comptes utilisateurs et groupes
- Activer la corbeille AD

Il est possible de manager son annuaire avec la console centre d'administration AD, sachant qu'on ne peut activer la Corbeille AD qu'à partir cette console. Cela nous permet de retrouver un objet AD qui a été supprimé accidentellement.

Nom	Type	Description
ForeignSecurityPrincipals	Conteneur	Default container for security...
Infrastructure	Conteneur	Default container for infrastructure...
Keys	Conteneur	Default container for key objects...
LostAndFound	Conteneur	Default container for orphaned objects...
Managed Service Accounts	Conteneur	Default container for managed service accounts...
NTDS Quotas	msDS-Quota	Quota specifications container...
Program Data	Conteneur	Default location for storage of application data...
System	Conteneur	Builtin system settings

Pour retirer la suppression d'une UO ou d'un objet depuis l'annuaire il faut désactiver la sécurité de l'objet.

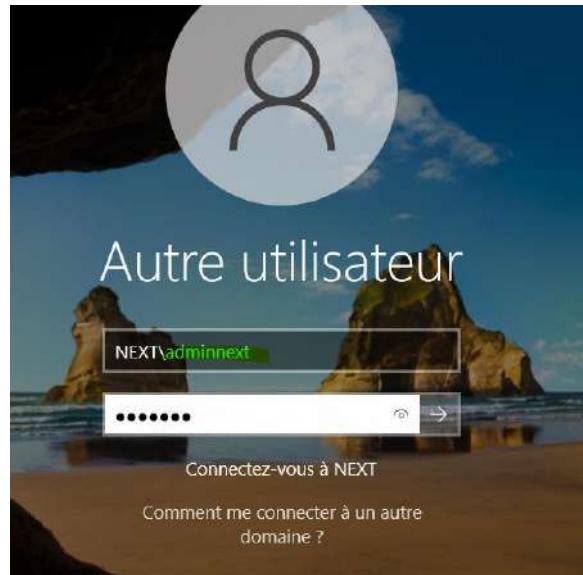


Nom	Type	Description
Propriétés de : TEST		
Général Géré par Objet Sécurité COM+ Éditeur d'attributs		
Norm canonique de l'objet :	next.lan/TEST	
Classe d'objets :	Unité d'organisation	
Créé le :	12/10/2023 13:55:01	
Modifié le :	12/10/2023 13:55:01	
Nombres de séquences de mise à jour (USN) :		
Actuel :	28700	
Original :	28699	
<input checked="" type="checkbox"/> Protéger l'objet des suppressions accidentelles		

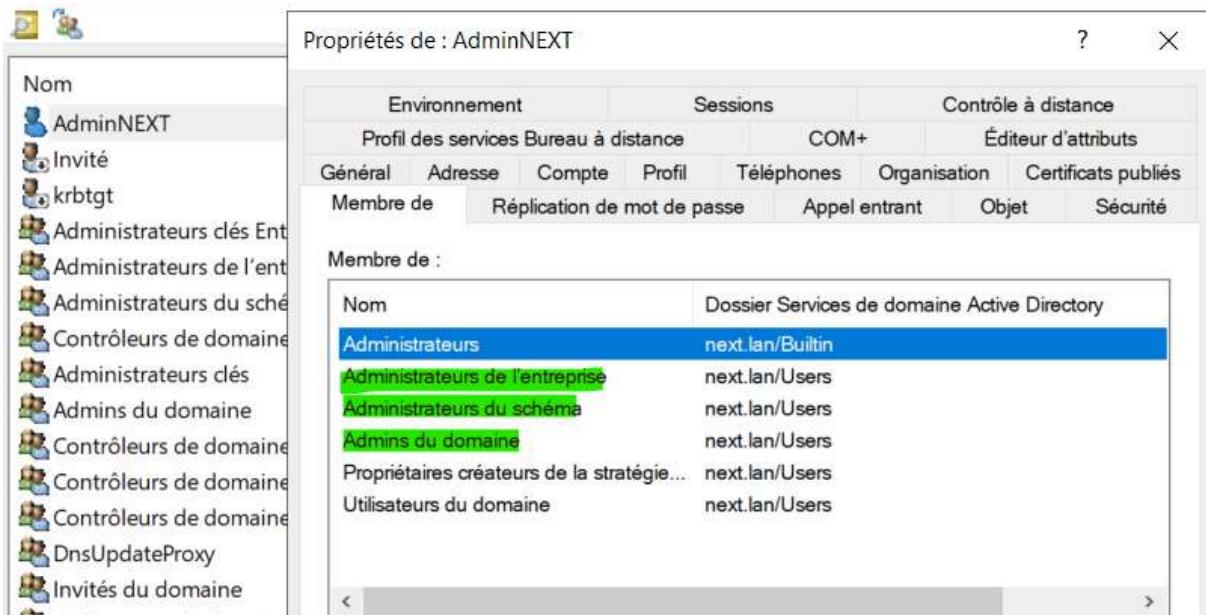
On retrouve l'objet supprimé dans le centre d'administration

Nom	Quand suppri...	Dernier parent...	Type	Description
test	10/12/2023 2:00	DC=next,DC=lan	Unité d'org...	

Renommer le compte utilisateur Administrateur avec le nom de votre domaine afin de l'identifier. Attention de renseigner correctement les UPN de connexion (User Principal Name) pour les identifications à saisir lors d'une connexion, ici nous avons deux possibilités. Une fois la modification effectuée pensez à vous déconnecter de la session et se reconnecter.

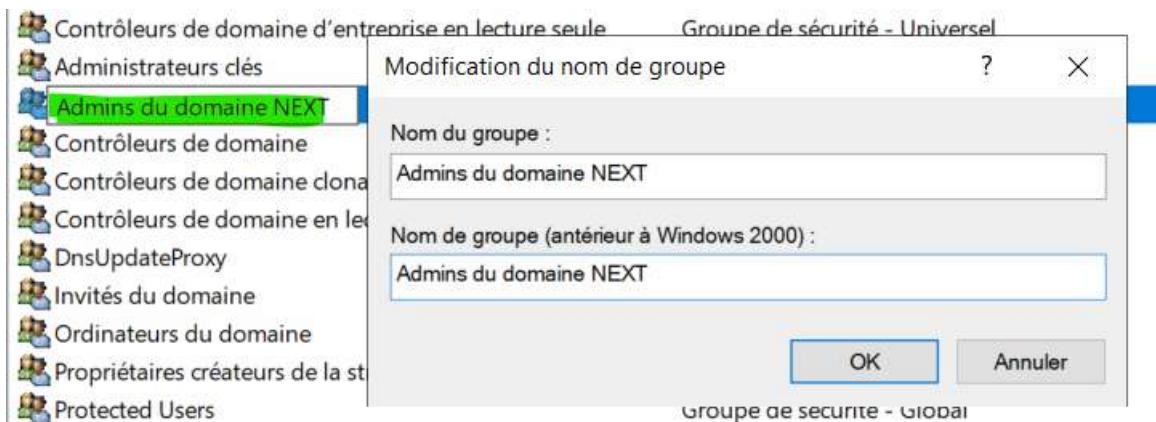


Pour informations, lors de la promotion du serveur en contrôleur de domaine pour notre premier domaine ce qui a généré une forêt AD, par défaut le compte administrateur local est devenu un compte de l'annuaire, mais conserve son mot de passe, le groupe administrateurs, et rajoute comme membre le groupe Admin entreprise, schéma et domaine.



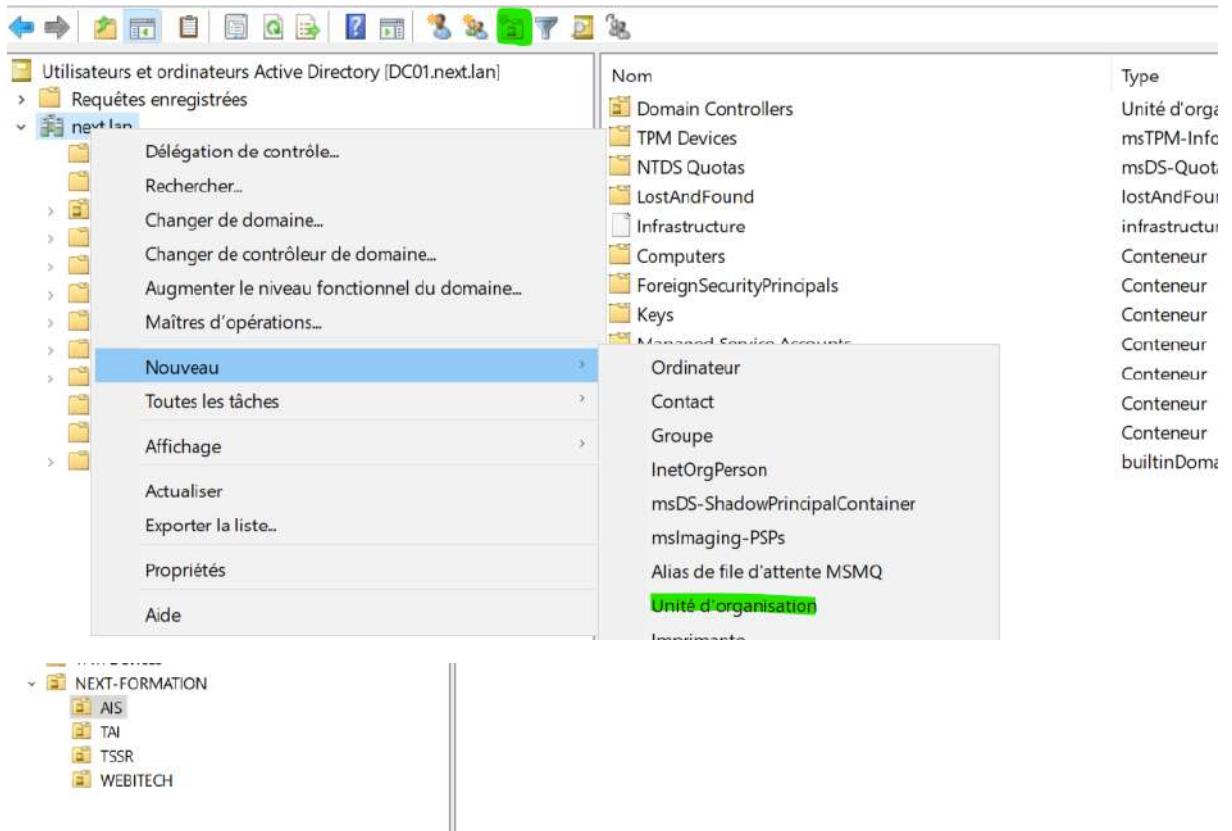
Rappel : le groupe admin de l'entreprise et schéma sont unique dans toute la forêt AD de l'entreprise. En revanche il y a un groupe admin différent pour chaque domaine de la forêt.

Il est recommandé de modifier le nom du groupe Admin du domaine comme pour le compte administrateur.

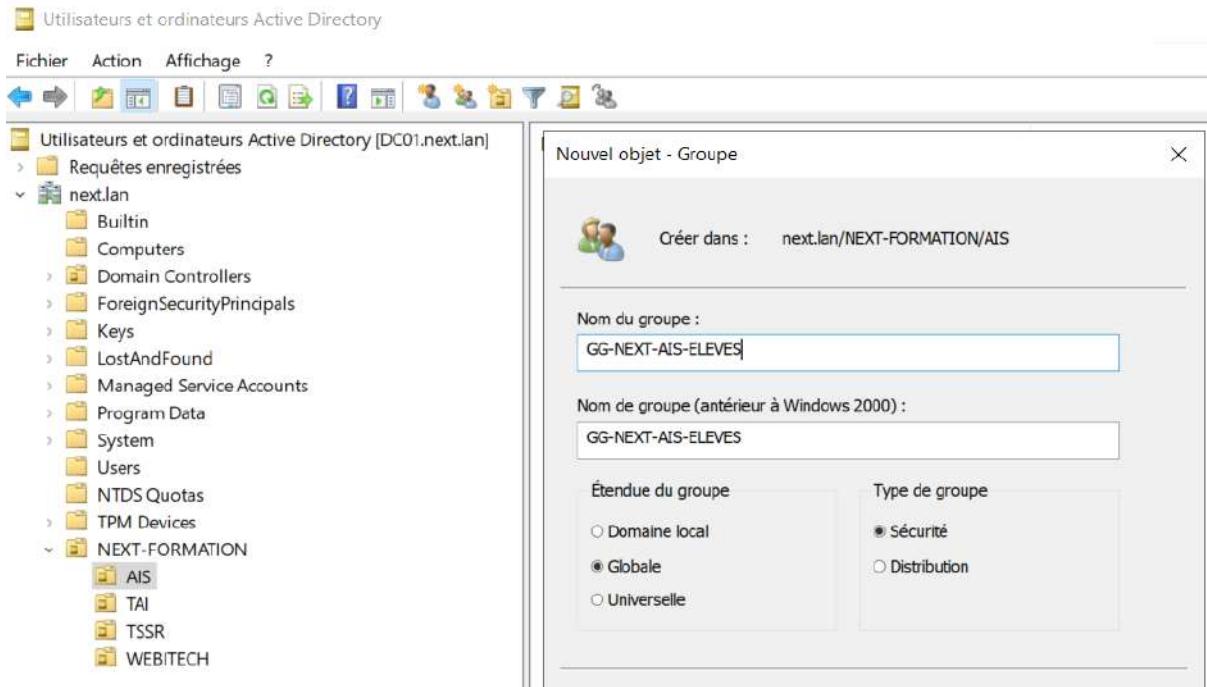


Organiser son AD avec des UO.

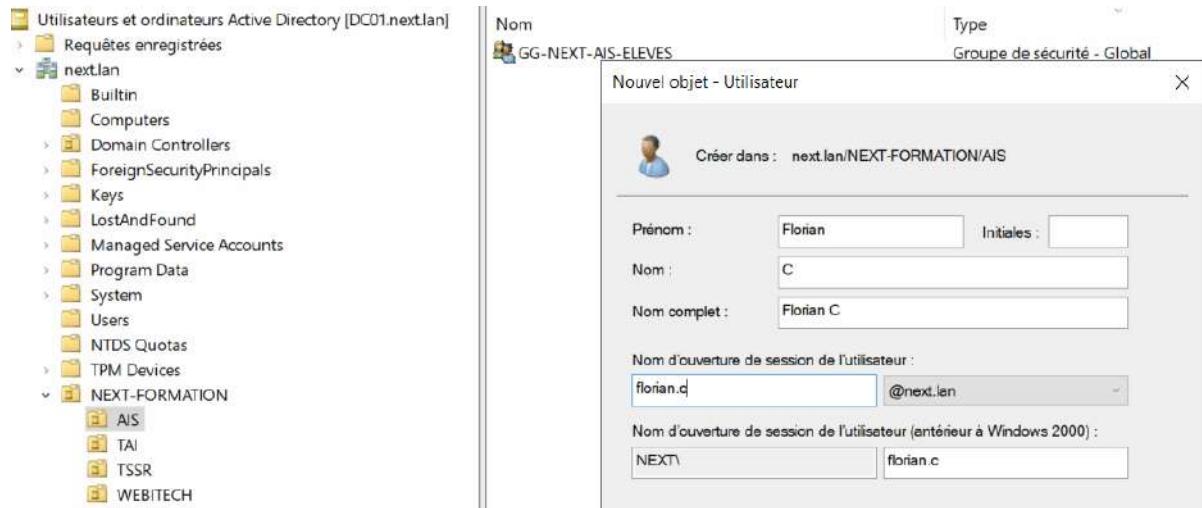
Les unités d'organisation vont nous permettre de classer par catégorie ou service nos utilisateurs, groupes, machine, afin d'appliquer des délégations de contrôle spécifique ou des GPO.



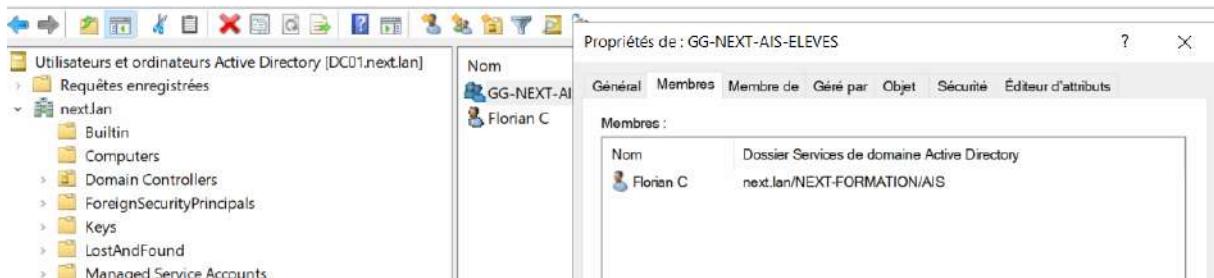
On va créer des groupes utilisateurs dans une UO.



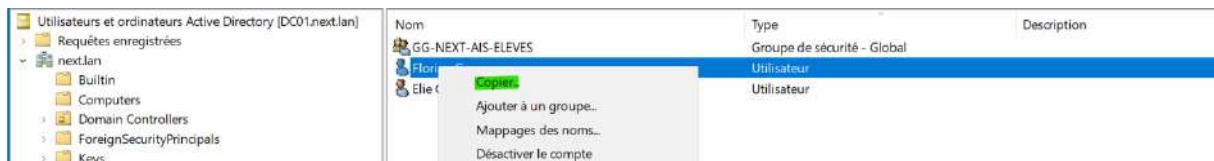
Créer un utilisateur.



On ajoute l'utilisateur dans le groupe GG



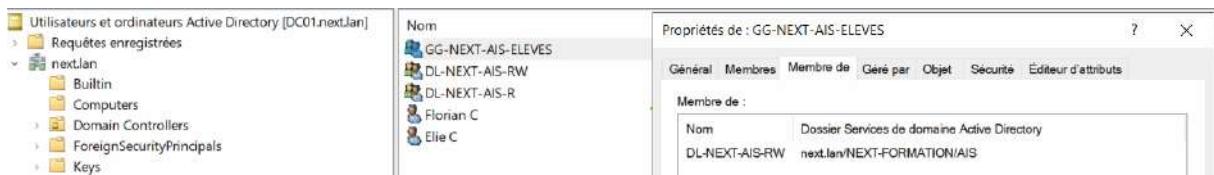
On peut copier à partir d'un utilisateur pour reprendre les mêmes droits lors de la création d'un nouvel utilisateur si besoins.



On va créer un groupe de type domaine local

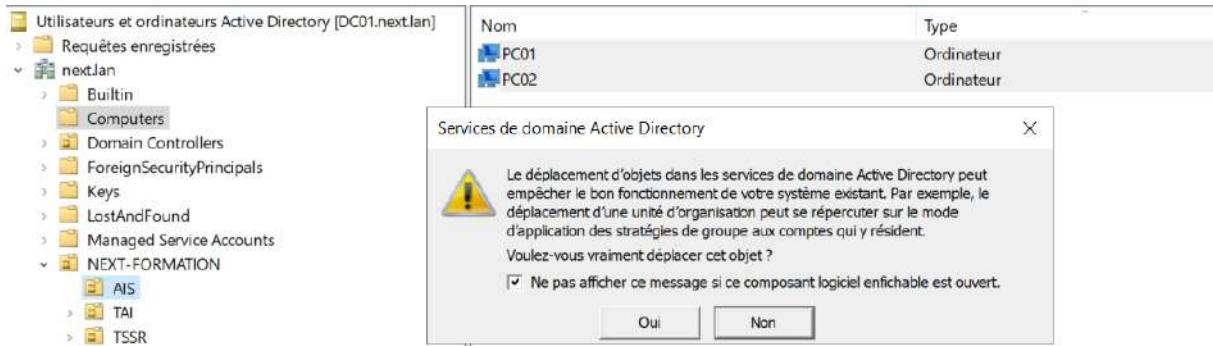


Le groupe GG-NEXT-AIS-ELEVES sera membre de DL-NEXT-AIS-RW



Ici dans les exemples les utilisateurs sont membre de GG-NEXT-AIS-ELEVES et le groupe global cité est membre de DL-NEXT-AIS-RW. Donc les utilisateurs sont membre de DL-NEXT....

On peut déplacer les machines dans les UO afin de les organiser.



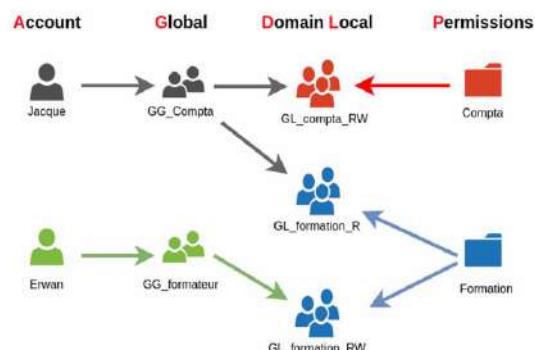
Gestion des groupes et permission.

ACL AGDLP

Microsoft préconise la méthode AGDLP (aussi nommée IGDLA) pour créer et gérer les droits d'accès (ACL). Les Utilisateurs sont organisés en groupes (correspondant généralement à leur fonction dans l'entreprise). Ces groupes sont à nouveau membres de groupes qui eux possèdent les droits.

Cette méthode permet de faciliter grandement la gestion des droits d'accès aux fichiers par exemple

Dans les forêts multi-domaines, la méthode devient AGUDLP avec l'ajout de groupe Universel



Afin de respecter les préconisations de Microsoft on va créer un dossier depuis notre CD et lui attribuer les droits (ACL) et autoriser le partage. Il est conseillé de stocker les dossiers dans un espace de stockage réservé (disque dur secondaire).

Disque 0	Réserve au système	(C:)	
De base 60,00 Go En ligne	100 Mo NTFS Sain (Système, Actif,	59,34 Go NTFS Sain (Démarrer, Fichier d'échange, Vidage sur incident)	568 Mo Sain (Partition de récupération)
Disque 1	DATA (E:)		
De base 99,98 Go En ligne	99,98 Go NTFS Sain (Partition de données de base)		
■ Non alloué ■ Partition principale			

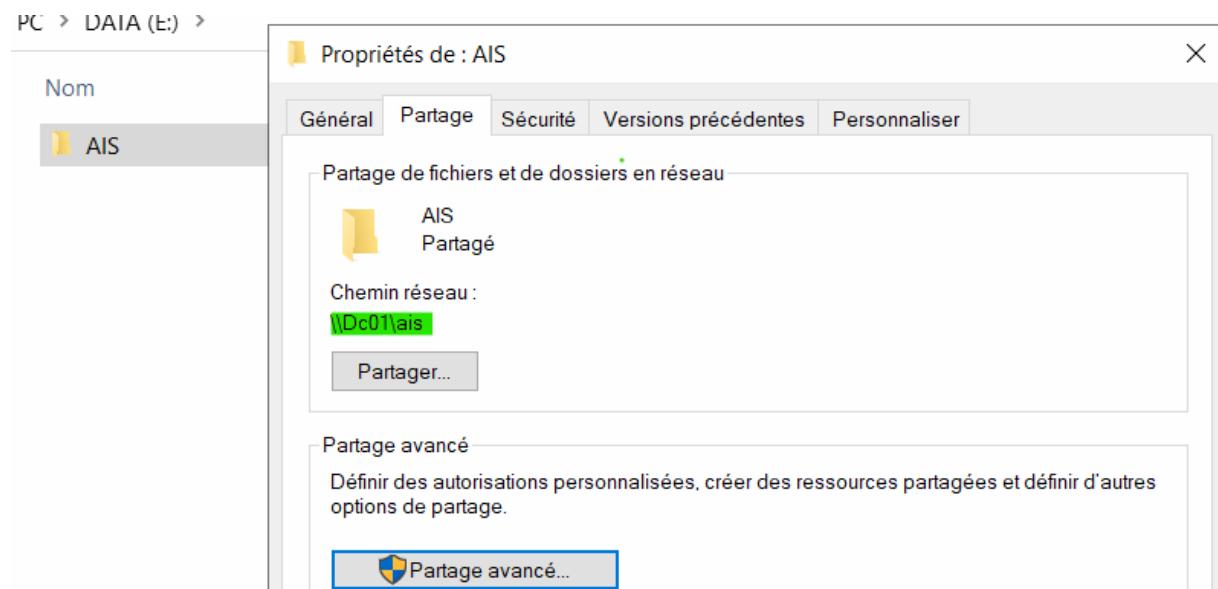
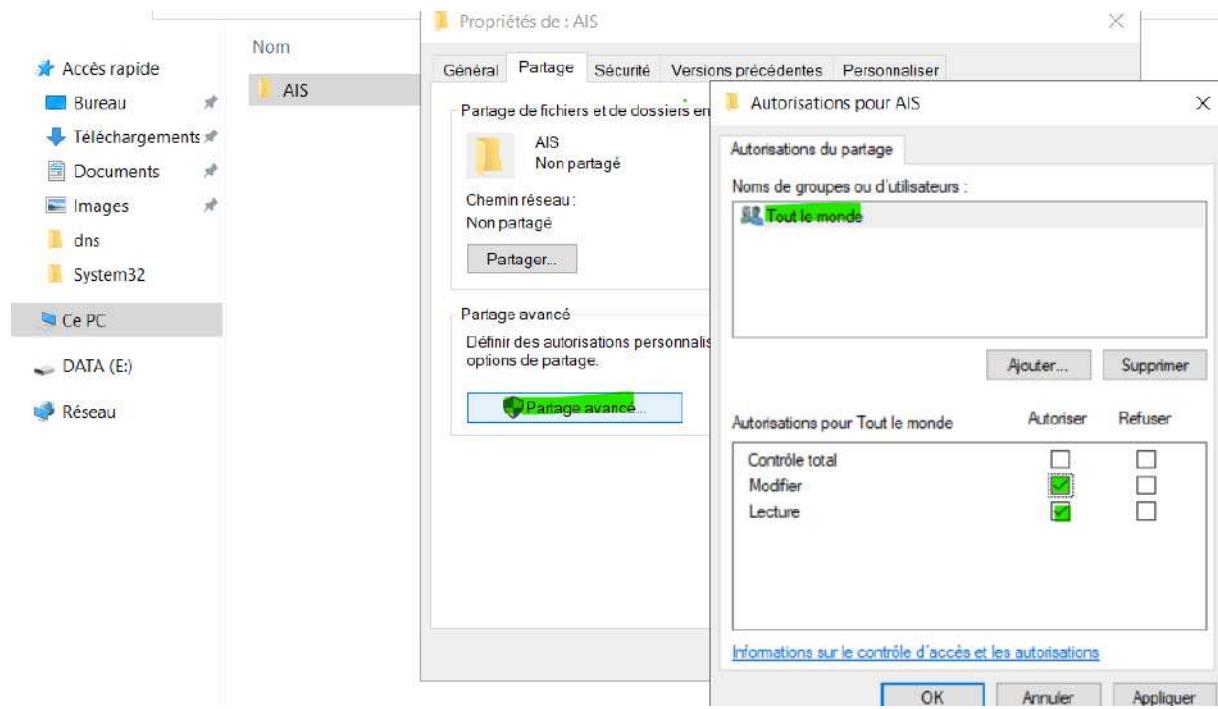
Ont créé un dossier dans le lecteur E:/ (ou le lecteur secondaire)

The screenshot shows the Windows File Explorer interface. The top navigation bar includes 'Fichier', 'Accueil', 'Partage', 'Affichage', 'Gérer' (which is highlighted in green), and 'Outils de lecteur'. Below the navigation bar, the path 'Ce PC > DATA (E:) >' is displayed. The main pane lists files and folders under 'DATA (E:)'. A folder named 'AIS' is visible, along with other items like 'Bureau' and 'Accès rapide'. The 'AIS' folder has a modified date of '12/10/2023 16:06' and is categorized as a 'Dossier de fichiers'.

On partage le dossier

The screenshot shows the Windows File Explorer interface with the 'DATA (E:)' drive selected. In the center, the 'Propriétés de : AIS' (Properties of AIS) dialog box is open. The 'Partage' (Sharing) tab is selected. Under 'Partage de fichiers et de dossiers en', it shows 'AIS' is 'Non partagé'. The 'Partage avancé' section contains a checked checkbox 'Partager ce dossier'. The 'Paramètres' section shows 'Nom du partage : AIS'. Below that, 'Ajouter' and 'Supprimer' buttons are visible. A limit for simultaneous users is set at '16777'. The 'Commentaires' and 'Autorisations' tabs are also visible at the bottom of the dialog. At the very bottom of the window, there are 'OK', 'Annuler' (Cancel), and 'Appliquer' (Apply) buttons.

On indique comme partage tout le monde.



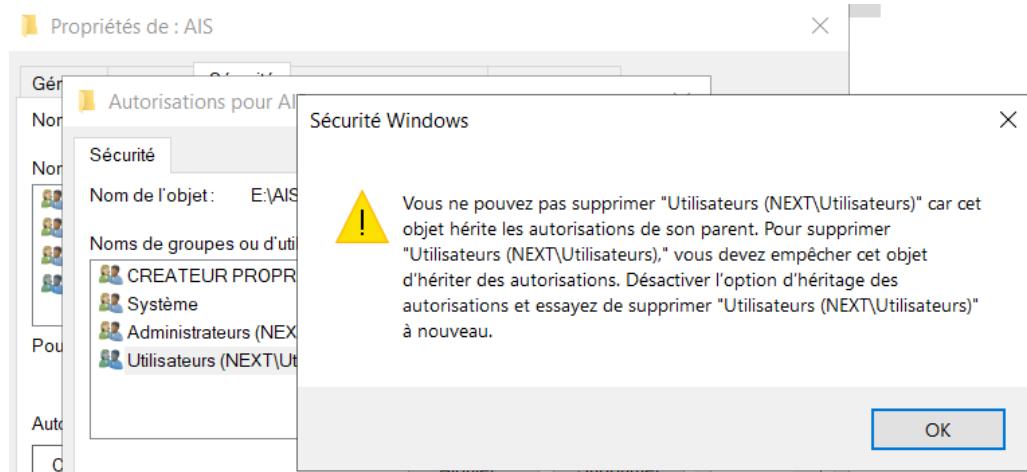
Cette commande vous permet de visualiser les partages existants sur le serveur en question.

```
C:\Users\Administrateur>net share

Nom partage Ressource Remarque .

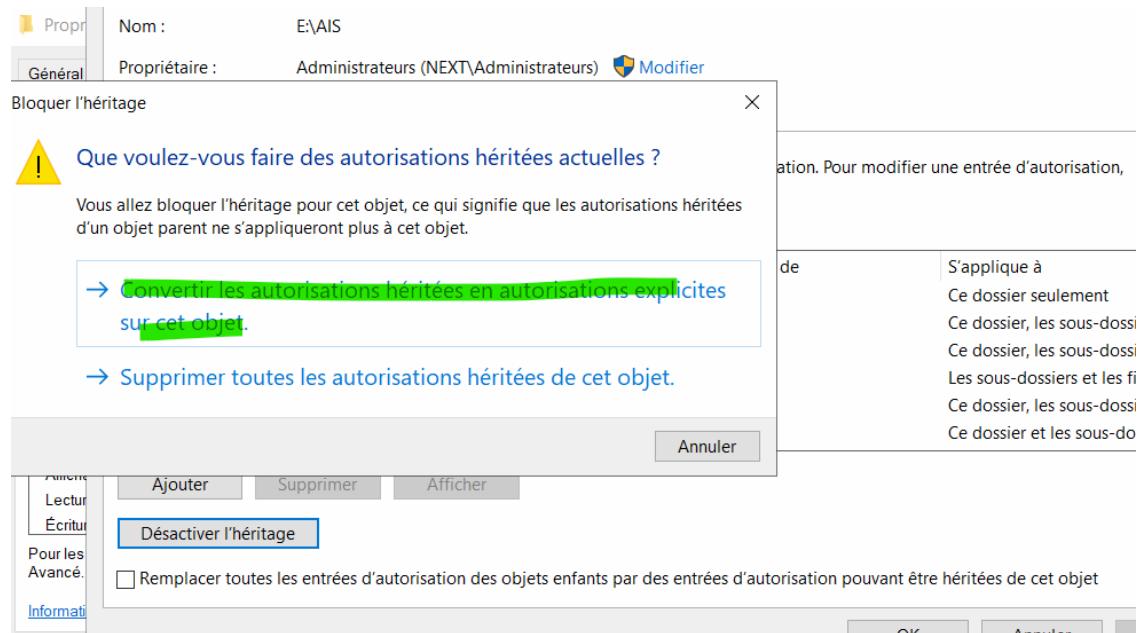
-----
IPC$ C:\ IPC distant
C$ E:\ Partage par défaut
E$ E:\ Partage par défaut
ADMIN$ C:\Windows Administration à distance
AIS E:\AIS
NETLOGON C:\Windows\SYSVOL\sysvol\next.lan\SCRIPTS Partage de serveur d'accès
SYSVOL C:\Windows\SYSVOL\sysvol Partage de serveur d'accès
La commande s'est terminée correctement.
```

On va retirer le groupe utilisateurs car par défaut tous les comptes user du domaine sont membre de ce groupe. Mais pour le retirer on va devoir désactiver l'héritage.

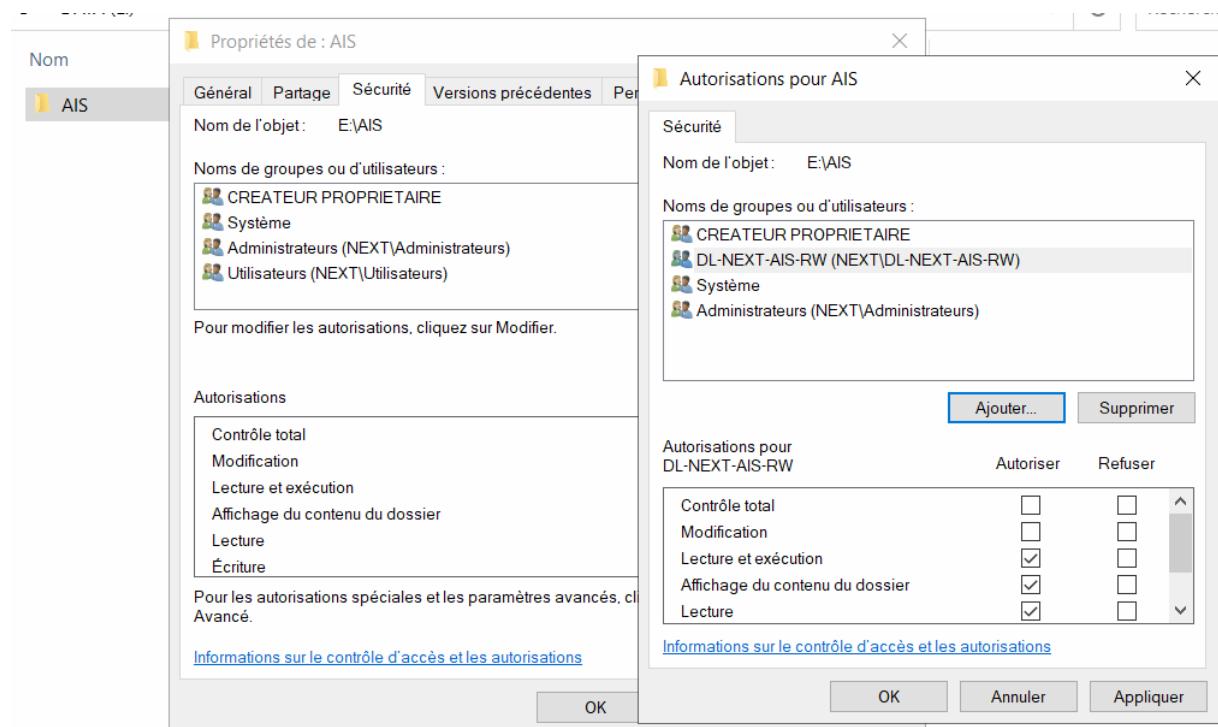


La solution :

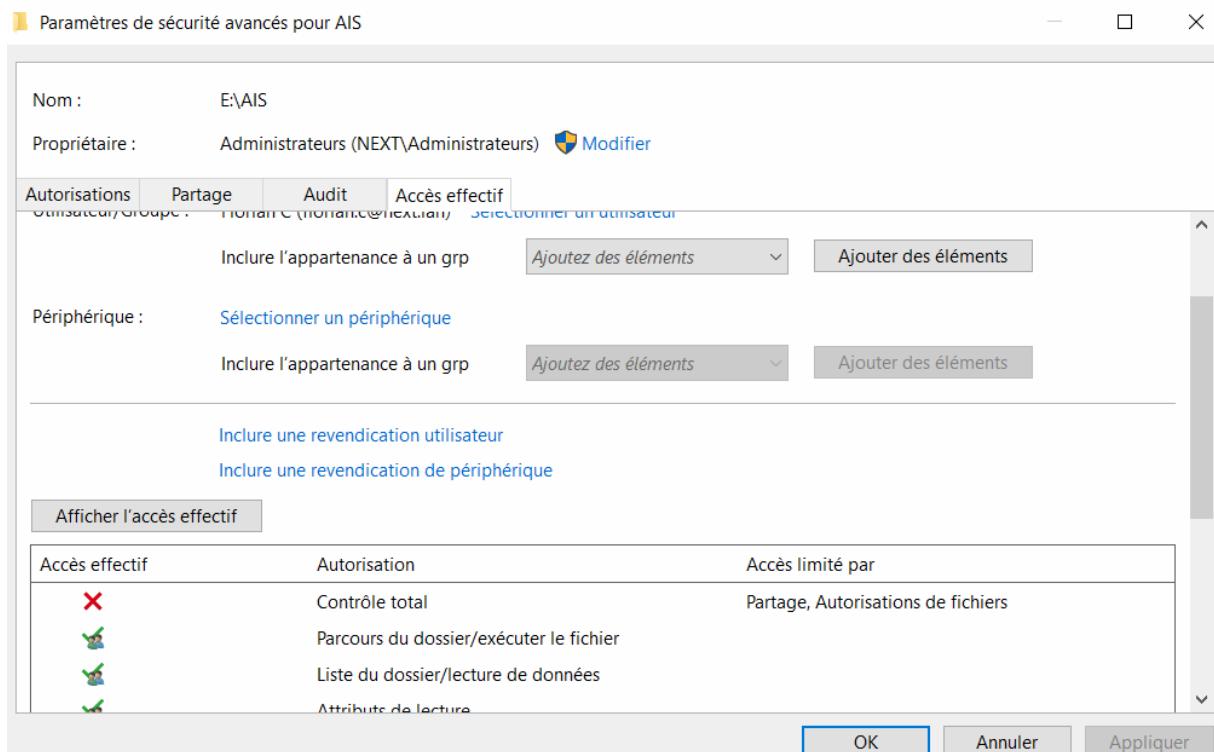
A screenshot of the Windows Properties dialog box for folder "AIS". The "Sécurité" tab is selected. It shows the object name as "E:\AIS" and the owner as "Administrateurs (NEXT\Administrateurs)". Under "Noms de groupes ou d'utilisateurs", "Utilisateurs (NEXT\Utilisateurs)" is listed. A note says: "Pour modifier les autorisations, cliquez sur Modifier...". Below it, a table shows permissions for "CREATEUR PROPRIETAIRE": "Contrôle total", "Modification", "Lecture et exécution", "Affichage du contenu du dossier", "Lecture", and "Écriture". At the bottom, there's an "Avancé..." button. To the right, a detailed view shows the same information with an additional table for "Entrées d'autorisations" and a "Désactiver l'héritage" button.



On peut maintenant supprimer le groupe Utilisateurs et rajouter notre groupe DL.



On peut vérifier l'accès d'un utilisateur à un dossier partagé avec les accès effectifs.



Mise en place d'un profil itinérant.

Le profil itinérant va permettre de conserver le profil d'un utilisateur lorsqu'il se connecte pour la première fois sur un ordinateur sur un serveur distant par exemple notre contrôleur de domaine au lieu d'être conserver en local dans la machine.

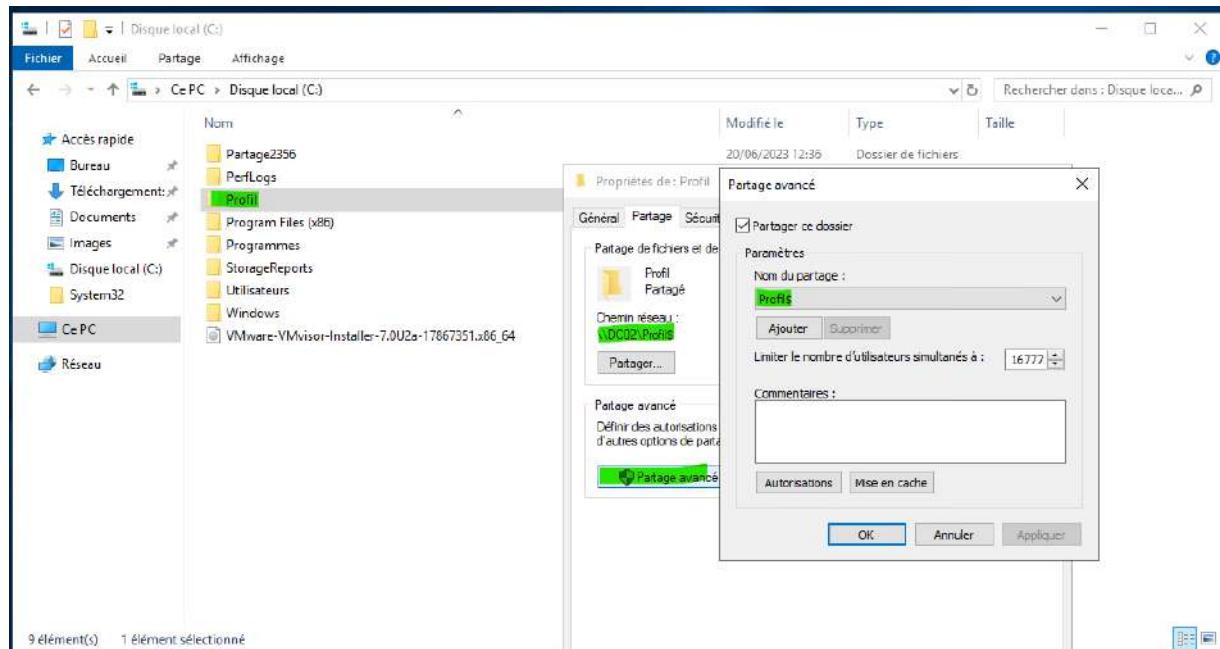
Cette mise en place est utile et plus sécurisée car les données de l'utilisateur seront disponibles que depuis un serveur et quand un utilisateur se connecte à sa session il va charger son profil user à partir du serveur et non en local.

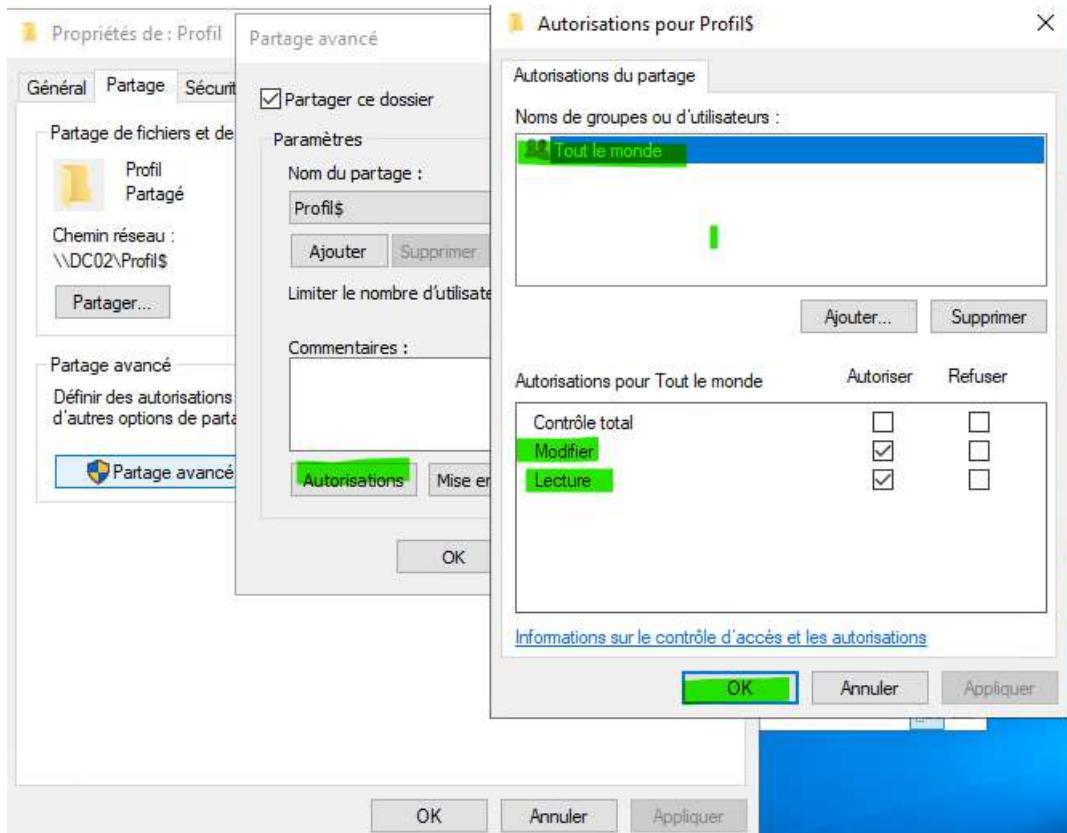
L'avantage si l'utilisateur change de service dans l'entreprise et utilise un autre poste informatique en se connectant avec sa session, il va récupérer tous ses données déposées dans le bureau.

Etapes 1 : Créer un dossier partagé depuis le serveur qui va stocker les profils des utilisateurs du domaine.

1) Créer le dossier et le partager

On crée le dossier, on le partage avec un nom de partage caché et comme autorisation on autorise tout le monde en lecture et écriture.





Etapes 2 : Indiquer sur le profil AD de l'utilisateur le chemin pour son profil itinérant.

Depuis l'annuaire depuis la console, modifier le chemin du profil de l'user.

Attention indiquée bien le chemin du serveur qui partage le dossier Profil\$ (chemin réseau soit \\) et pour éviter une erreur de saisie indiqué la variable %username%.

Nom	Type
ERWAN	Ordinateur
KEVIN	Ordinateur
PCALEXPROF	Ordinateur
PCKEVIN	Ordinateur
Alex AH. hasar	Utilisateur
Enwan ES. Sahbi	Utilisateur
Kevin KR. Ringuet	Utilisateur

Etapes 3 : Vérification du profil itinérant.

Pour vérifier si le profil est devenu itinérant depuis Windows 10 ou 11 (client) avec l'utilisateur du domaine connecté :

À propos de

Spécifications de Windows

Édition	Windows 10 Professionnel
Version	21H2
Installé le	15/06/2023
Build du système d'exploitation	19044.3086
Expérience	Windows Feature Experience Pack 1000.19041.1000.0

Copier

Mettre à niveau votre édition de Windows ou modifier la clé de produit (Product Key)

Lire le Contrat de services Microsoft qui s'applique à nos services

Lire les termes du contrat de licence logiciel Microsoft

Paramètres associés

Paramètres de Bitlocker

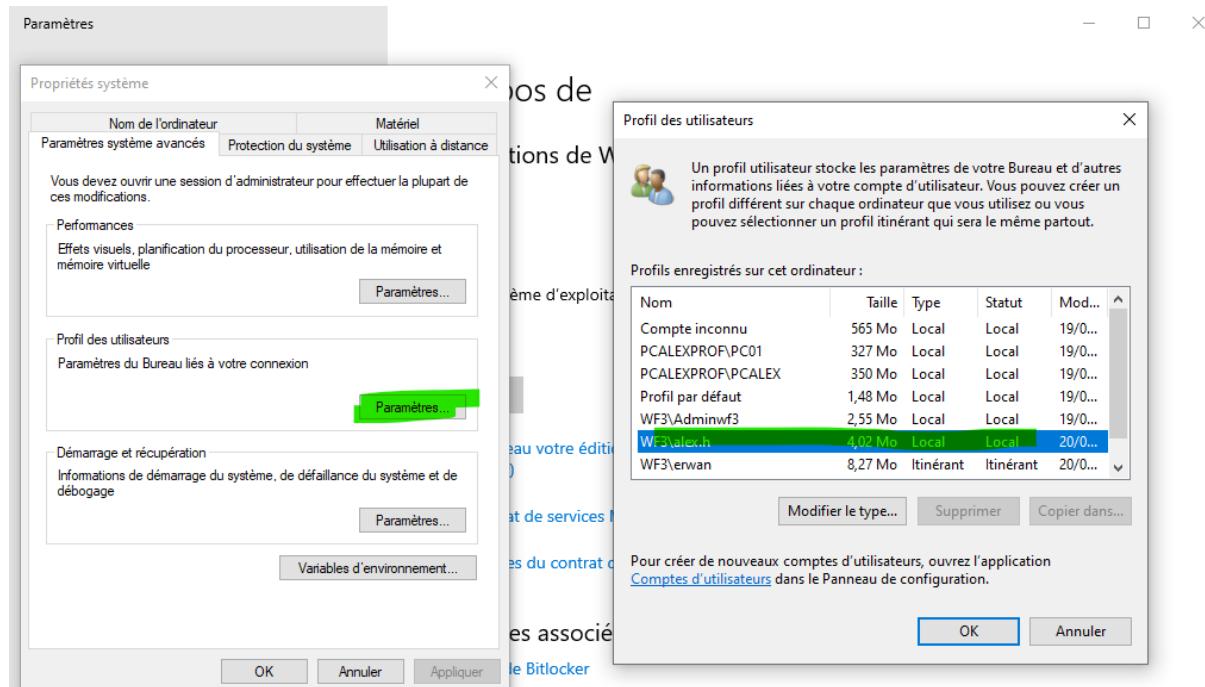
Gestionnaire de périphériques

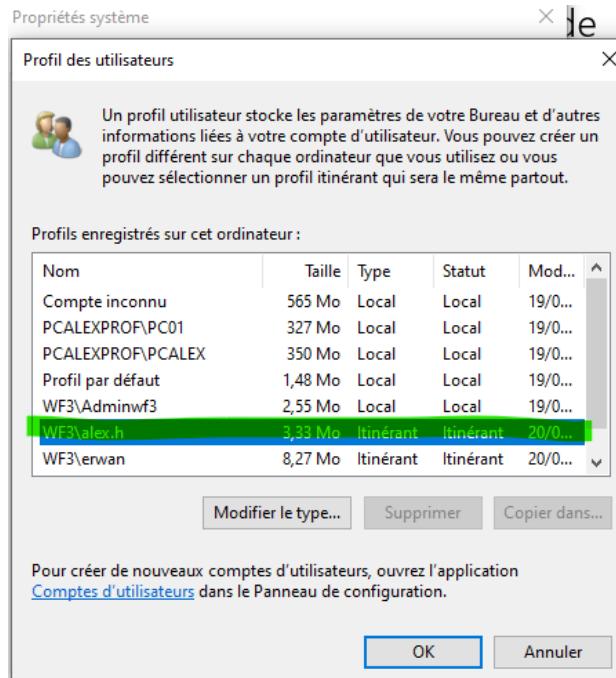
Bureau à distance

Protection du système

Paramètres avancés du système

Renommer ce PC (avancé)





Il doit être indiqué profil itinérant au lieu de local alors la manipulation est correcte. Sinon il y a erreur.

- 2) Vérifier le dossier Profil depuis le serveur afin de visualiser le profil utilisateur du domaine s'il a bien été créé automatiquement (ce n'est pas une action à faire manuellement !)

Gestion de l'annuaire et configuration des profils utilisateurs.

Depuis l'annuaire AD du domaine et depuis n'importe quels serveurs vérifier les connexions **UPN** d'un utilisateur du domaine afin de s'assurer des bonnes informations.

UPN = user principal name. Ce sont les identifiants à utiliser pour se connecter à un domaine depuis un compte user d'un domaine.

Exemple pour l'utilisateur ci-dessous.

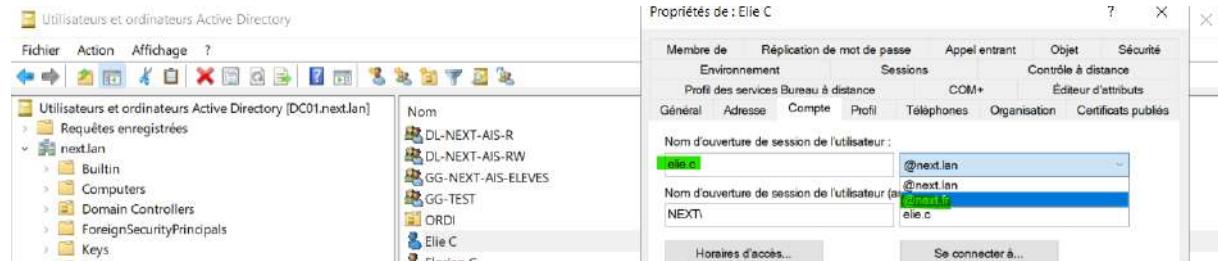
The screenshot shows the Windows Server Management Console with the 'Utilisateurs et ordinateurs Active Directory' snap-in. On the left, the navigation pane shows the domain structure under 'next.lan'. On the right, the 'Properties' window for user 'Elie C' is open. The 'Sessions' tab is selected. In the 'Nom d'ouverture de session de l'utilisateur' field, 'Elie C' is entered. Below it, 'Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000)' shows 'NEXT'. Under 'Options de compte', there are checkboxes for password change, account lockout, and password expiration. The 'Date d'expiration du compte' section indicates the account never expires ('Jamais').

Il est possible de rajouter un suffixe UPN supplémentaire liée à un domaine public exemple NEXT.FR

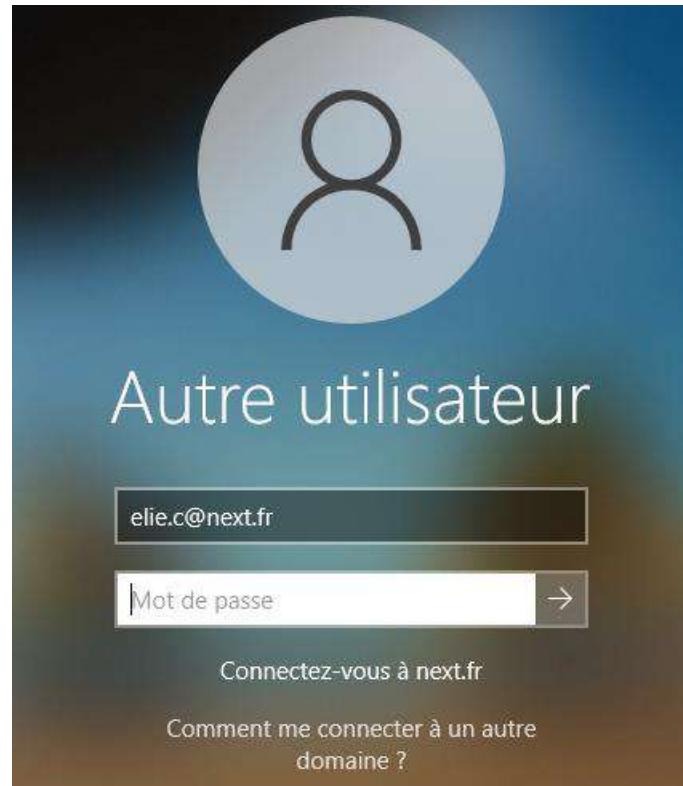
Depuis la console Domaine et approbation, on va ouvrir les propriétés et indiquer le suffixe public de notre domaine.

The screenshot shows the 'Domaines et approbations Active Directory' snap-in. The 'next.lan' domain is selected. A properties dialog box is open for 'Suffixes UPN'. It contains a list of existing suffixes: 'next.lan' and 'next'. A new suffix, 'next.fr', is being added to the list. The 'Ajouter' (Add) button is highlighted.

Maintenant si l'utilisateur possède une adresse de messagerie Outlook avec le nom de domaine public de l'entreprise on va pouvoir spécifier depuis l'annuaire sur le profil de l'utilisateur UPN de connexion avec le nom de domaine public. Ce qui va permettre à l'utilisateur de s'authentifier sur son poste de travail avec l'adresse de messagerie de l'entreprise.



Connexion depuis un poste utilisateur avec le suffix UPN.



On peut vérifier depuis le compte user les différents groupes à qui ont appartient et leurs SID (identifiant) dont le nôtre.

```
C:\Users\elie.c>whoami /all
Informations sur l'utilisateur
-----
Nom d'utilisateur SID
=====
next\elie.c      S-1-5-21-1061595489-2201516246-1858733890-1114

Informations de groupe
-----
Nom du groupe          Type           SID
=====
Tout le monde          Groupe bien connu S-1-1-0
BUILTIN\Administrateurs Alias          S-1-5-32-545
AUTORITE NT\INTERACTIF Groupe bien connu S-1-5-4
OUVERTURE DE SESSION DE CONSOLE Groupe bien connu S-1-2-1
AUTORITE NT\Utilisateurs authentifiés Groupe bien connu S-1-5-11
AUTORITE NT\Cette organisation Groupe bien connu S-1-5-15
LOCAL                 Groupe bien connu S-1-2-0
NEXT\GG-NEXT-AIS-ELEVES Groupe          S-1-5-21-1061595489-2201516246-1858733890-1112
Identité déclarée par une autorité d'authentification Groupe bien connu S-1-18-1
NEXT\DL-NEXT-AIS-RW   Alias          S-1-5-21-1061595489-2201516246-1858733890-1115
Etiquette obligatoire\Niveau obligatoire moyen    Nom            S-1-16-8192
```

Pour information ces valeurs on les retrouve dans l'annuaire dans l'onglet attribut. Exemple voici le SID de GG-NEXT-AIS-ELEVES à qui ont appartient avec le compte elie.c

Attribut	Valeur
top	group
	607c8319-d9a3-4b15-aedd-937904752864
	S-1-5-21-1061595489-2201516246-1858733890-1112
cn	<non défini>
objectClass	<non défini>
member	<non défini>
memberCount	<non défini>

Concernant la gestion de l'objet d'un utilisateur ont depuis l'annuaire :

- Réinitialiser le mot de passe
- Spécifier les heures de connexion autorisée
- Spécifier un mappage
- Spécifier un profil itinérant

Utilisateurs et ordinateurs Active Directory [DC01.next.lan]

- Requêtes enregistrées
- next.lan
 - Builtin
 - Computers
 - Domain Controllers
 - ForeignSecurityPrincipals
 - Keys
 - LostAndFound
 - Managed Service Accounts
 - NEXT-FORMATION
 - AIS
 - TAI
 - TSSR
 - WEBITECH
 - Program Data

Nom	Type
DL-NEXT-AIS-R	Groupe de sécurité - Domaine local
DL-NEXT-AIS-RW	Groupe de sécurité - Domaine local
GG-NEXT-AIS-ELEVES	Groupe de sécurité - Global
GG-TEST	Groupe de sécurité - Global
ORDI	Unité d'organisation
Elie C	
Florian C	

Utilisateurs et ordinateurs Active Directory [DC01.next.lan]

Horaires d'accès pour Elie C

Horaires d'accès pour Elie C	OK	Annuler
0 • 2 • 4 • 6 • 8 • 10 • 12 • 14 • 16 • 18 • 20 • 22 • 0		
Tous		
Lundi		
Mardi		
Mercredi		
Jeudi		
Vendredi		
Samedi		
Dimanche		

Options de compte :

- L'utilisateur devra changer le mot de passe.
- L'utilisateur ne peut pas changer de mot de passe.
- Le mot de passe n'expire jamais.
- Enregister le mot de passe en utilisant u...

De lundi au dimanche : 00:00 à 23:59

- Mappage réseau

1ère méthode :

On indique un lecteur réseau qui sera monté sur la session de l'utilisateur afin d'accéder au partage.
(Mappage réseau depuis l'AD)

Utilisateurs et ordinateurs Active Directory [DC01.next.lan]

Fichier Action Affichage ?

Utilisateurs et ordinateurs Active Directory [DC01.next.lan]

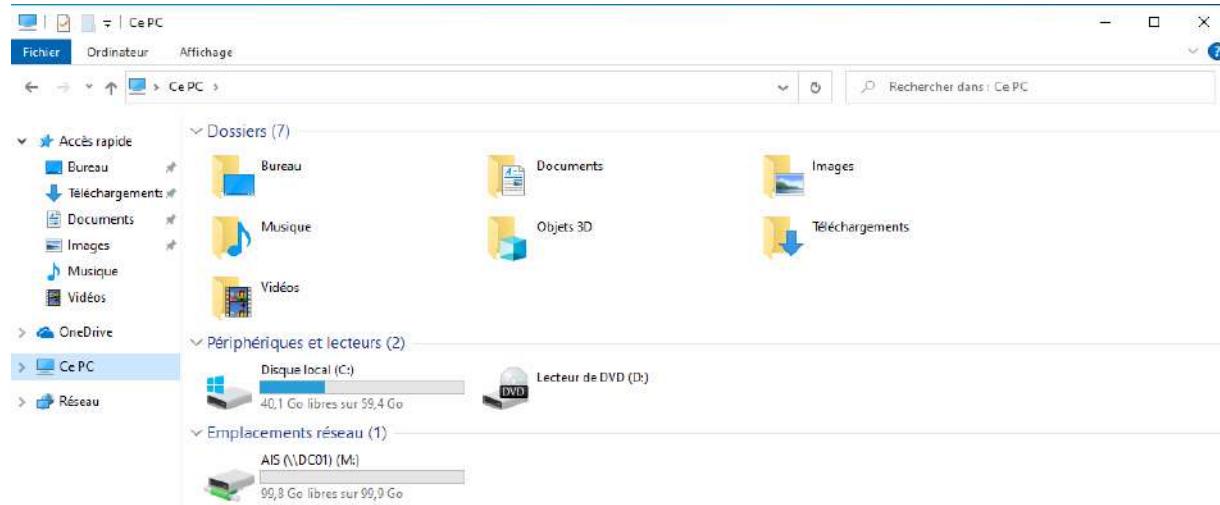
Requêtes enregistrées

next.lan

- Builtin
- Computers
- Domain Controllers
- ForeignSecurityPrincipals
- Keys
- LostAndFound
- Managed Service Accounts
- NEXT-FORMATION
 - AIS
 - TAI
 - TSSR
 - WEBITECH
- Program Data

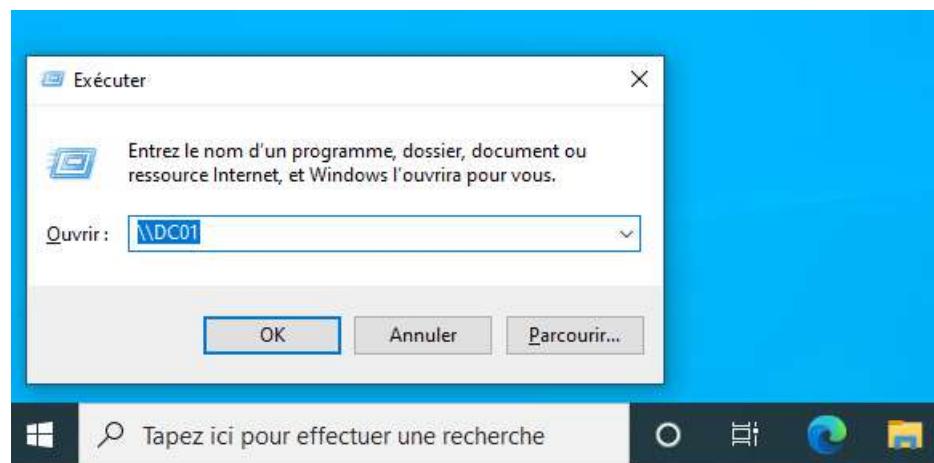
Membre de	Réplication de mot de passe	Appel entrant	Objet	Sécurité
Environnement	Sessions	Contrôle à distance		
Profil des services	Bureau à distance	COM+	Éditeur d'attributs	
Général	Adresse	Compte	Profil	Téléphones
Profil utilisateur				
Chemin du profil : <input type="text"/>				
Script d'ouverture de session : <input type="text"/>				
Dossier de base				
<input type="radio"/> Chemin d'accès local : <input type="text"/>				
<input checked="" type="radio"/> Connecter : <input type="text"/> à : <input type="text"/>				

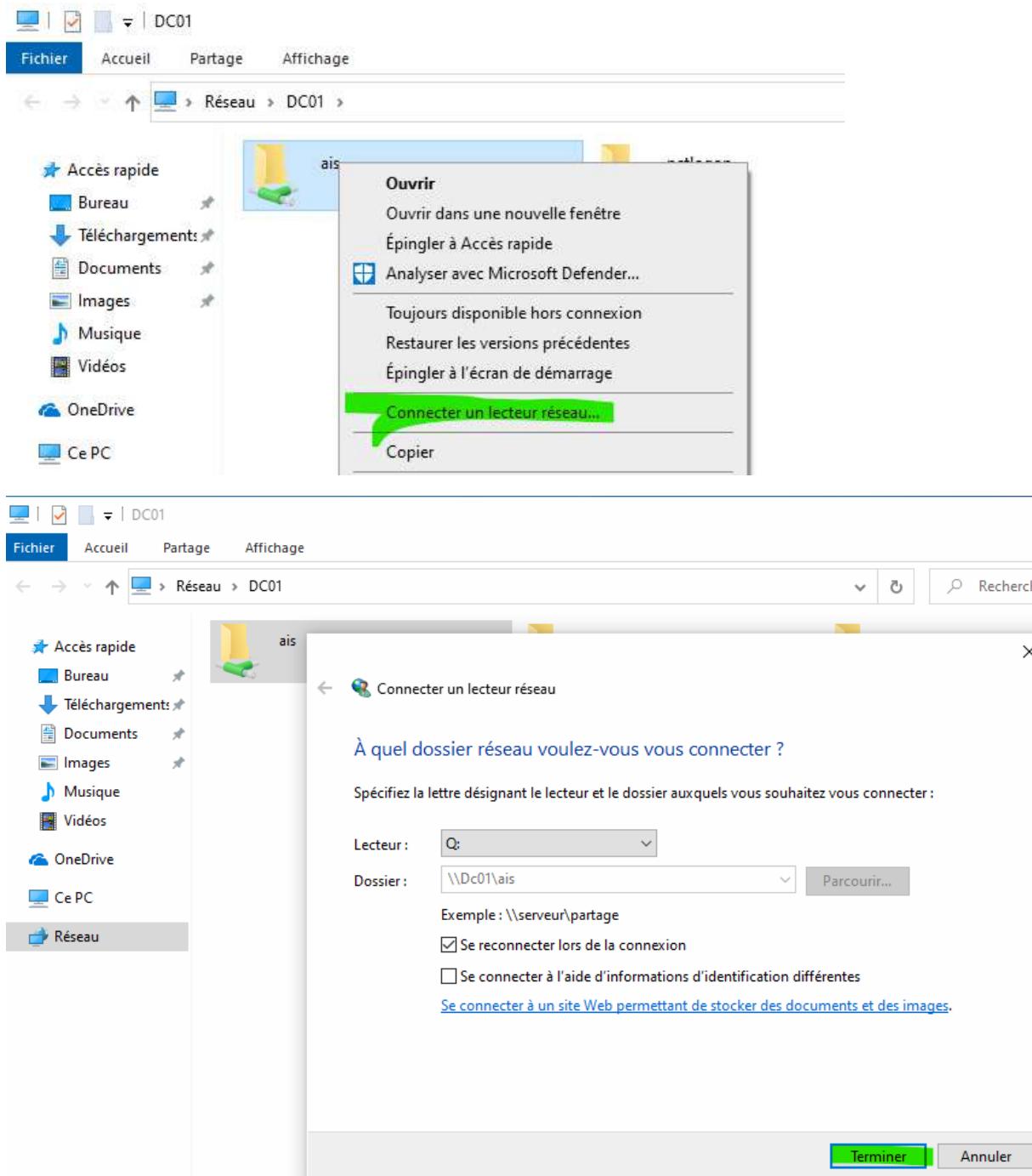
Depuis le client on peut observer un montage de lecteur réseau



2^{ème} méthode :

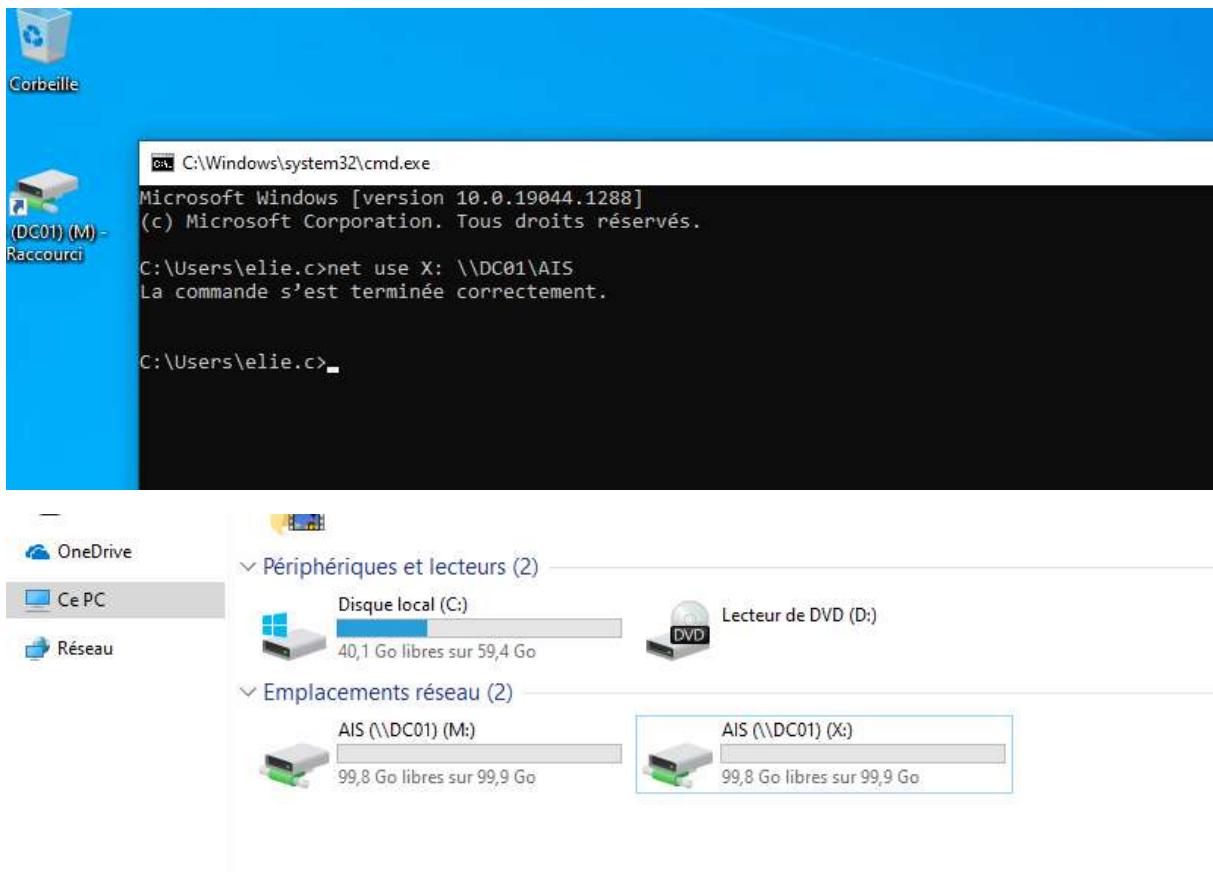
Depuis le client on peut monter des lecteurs réseau en indiquant un chemin UNC.





3^{ème} méthode :

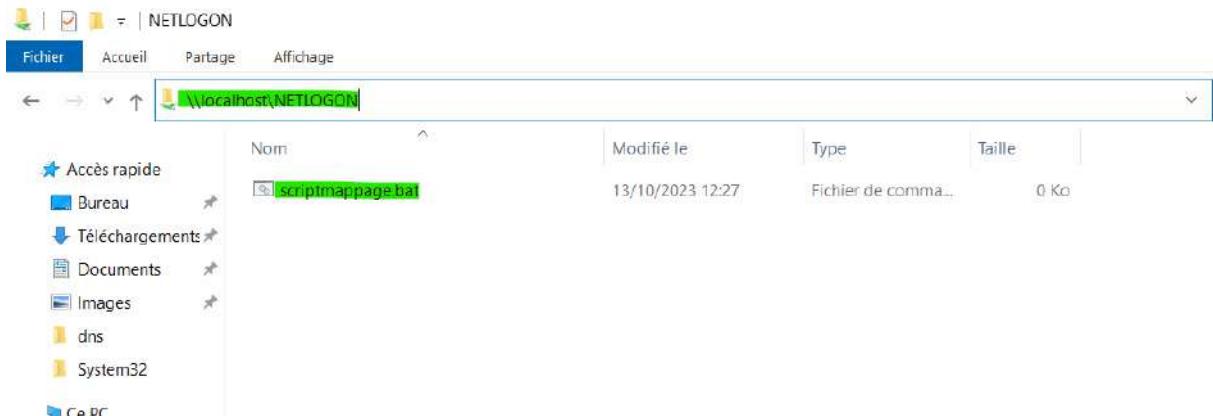
Depuis l'invité de commande avec le client on peut accéder et monter un partage.



4^{ème} méthode :

On peut utiliser un script depuis le serveur AD, l'avantage est de pouvoir déclarer plusieurs chemins dans un seul fichier et on peut le modifier à l'avenir si besoins afin de les mettre à jour.

Depuis un des serveurs contrôleur de domaine, on va déposer le script dans le dossier NETLOGON qui est disponible en réseau il suffit d'indiquer le chemin UNC comme ci-dessous depuis le serveur.



Attention le fichier est en format .BAT

The screenshot shows a Windows File Explorer window with the following details:

- Address Bar:** Réseau > localhost > NETLOGON
- File List:** Nom (Name) column shows 'scriptmappage.bat'.
- Properties Window:** 'scriptmappage.bat - Bloc-notes' is open, displaying the following content:

```
net use * /delete /Y
net use X: \\DC01\AIS
```
- Left Navigation:** Accès rapide (Quick Access), Bureau, Téléchargements, Documents, Images, dns, System32.
- Bottom Left:** Utilisateurs et ordinateurs Active Directory (User and Computer Active Directory).
- Bottom Right:** Properties dialog for 'Elie C':
 - General tab: Script d'ouverture de session : `scriptmappage.bat`
 - Session tab: Bureau à distance (Remote Desktop)
 - Security tab: Contrôle à distance (Remote Control)

Vérification depuis le client et on remarque qu'à l'ouverture de session on aura le mappage monté grâce au script du serveur.

The screenshot shows a Windows File Explorer window with the following details:

- Left Navigation:** OneDrive, Ce PC (highlighted), Réseau.
- Right Content:**
 - Périphériques et lecteurs (2):** Disque local (C:) (Local Disk (C:)), Lecteur de DVD (D:)
 - Emplacements réseau (1):** AIS (\\\DC01) (M:)

Gestion des stratégies de groupe.

Une GPO va permettre de modifier le registre au niveau de la machine ou de l'utilisateur.

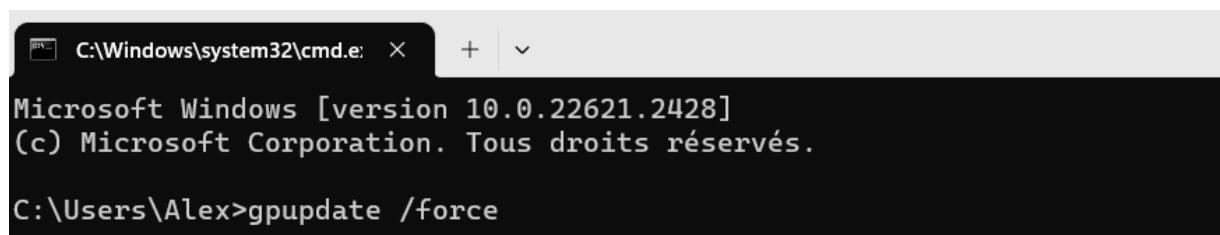
On peut découper l'étendu de la GPO en deux : les GPO local ou des GPO avec Active Directory.

Exemple d'utilisation d'une GPO : déployer l'installation d'un logiciel sur des machines du parc informatique qui sont répertoriées dans l'AD ou interdire le CMD des utilisateurs.

Une GPO peut s'appliquer de plusieurs façons et voici l'ordre sur lesquels ils vont être appliqués :

- Local (GPO local par machine, cette GPO s'applique seulement sur la machine hôte.) Pour lancer la console des GPO en local, il faut taper la commande avec la fenêtre exécuter : gpedit.msc
- GPO sites & services AD, cette GPO sera disponible dès qu'on est dans un environnement AD DS et ce type de GPO s'applique sur les serveurs aux niveaux de la console sites et services AD DS.
- GPO domaine, une GPO domaine va modifier le comportement de tous les objets AD DS du domaine en question.
- GPO UO, on applique une stratégie seulement à une UO ciblé qui va contenir des utilisateurs, groupes, ordinateurs du domaine soit des objets Active Directory.

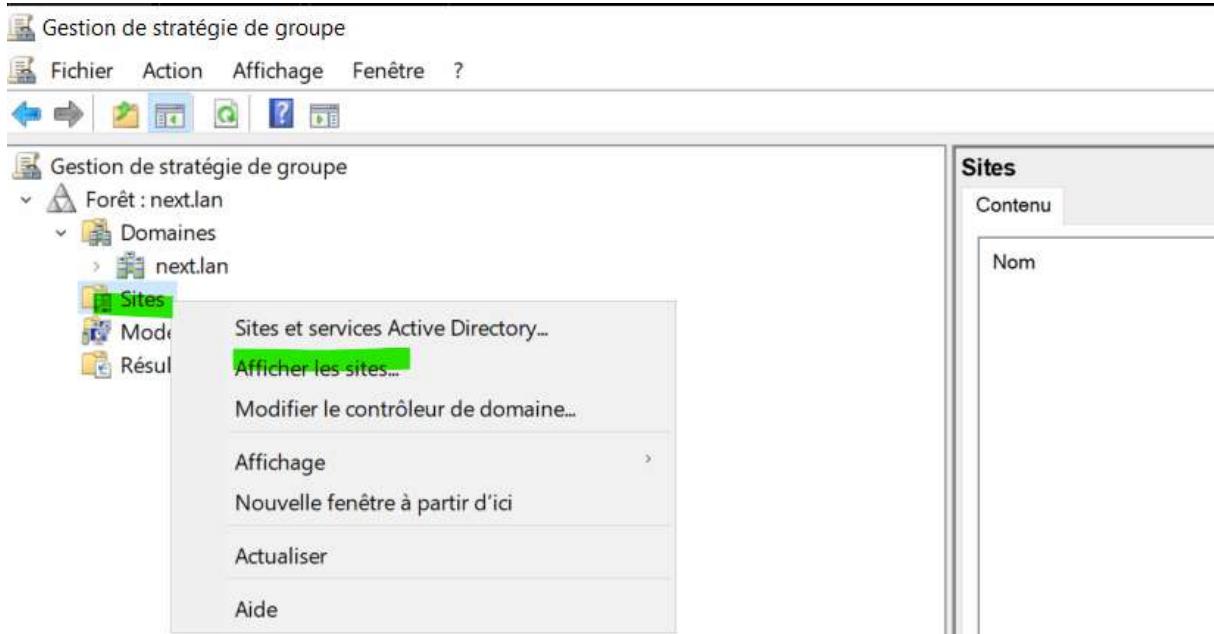
Après avoir configurer un paramètre depuis la console on peut forcer l'application de la GPO sur notre système (local) avec la commande suivante ou selon certains il est nécessaire de redémarrer le système d'exploitation :



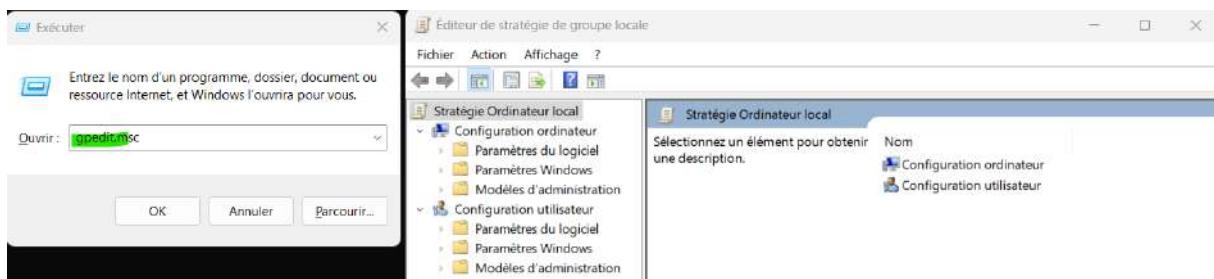
```
C:\Windows\system32\cmd.e: + ▾
Microsoft Windows [version 10.0.22621.2428]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\Alex>gpupdate /force
```

- Exemple de GPO sites & services AD



- Console pour effectuer des GPO en local. (On ne parle de domaine AD ici)



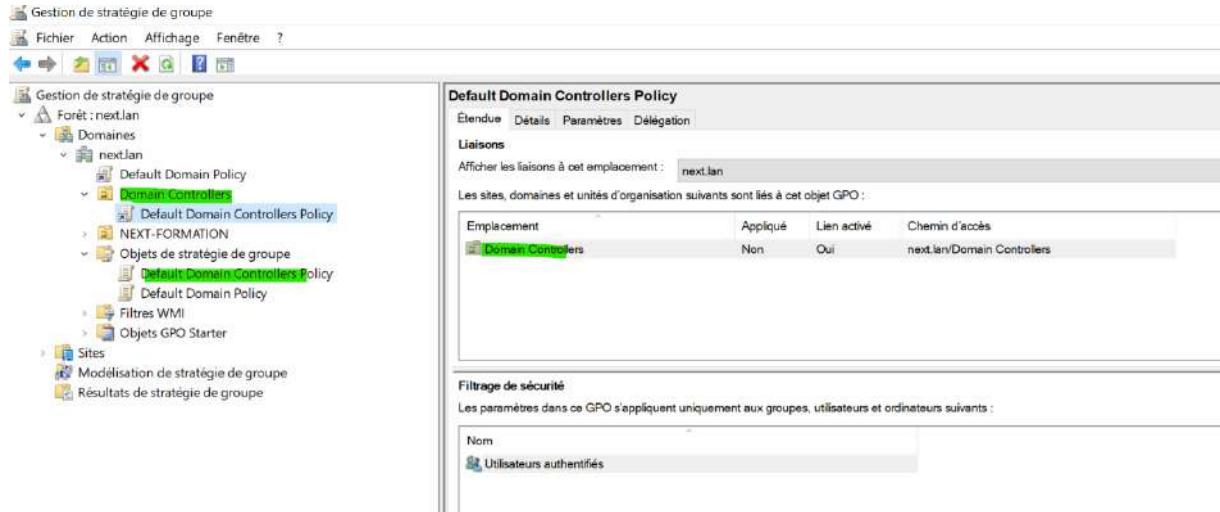
- Application des GPO au niveau du domaine.



- Application d'une GPO sur UO

Comme on peut le remarquer ce sont les UO qu'on observe qui sont présent dans l'annuaire AD. Donc il est important de prendre en compte l'emplacement de nos objets AD dans l'annuaire afin d'appliquer une GPO.

Par exemple dans l'exemple ci-dessous le système à crée une GPO qui se nomme Default Domain Controller Policy. Cette règle à été liée à l'unité d'organisation qui se nomme Controller Domain et qui se trouve dans l'annuaire. Dans cette UO contiens les objets ordinateurs dont les contrôleurs de domaine.



1^{er} Manipulation : Désactivation de la complexité des mots de passe pour la création des comptes.

On va modifier la GPO par défaut qui se nomme Default Domain Policy (qui s'applique au domaine) afin d'appliquer la désactivation des mots de passe complexe sur tout notre domaine. Donc tous les objets que ce soit UO, Ordi ou user seront concerné par cette modification.



Fichier Action Affichage ?

Stratégie Default Domain Policy [DC01.NEXT.LAN]

- Configuration ordinateur
 - Stratégies
 - Paramètres du logiciel
 - Paramètres Windows
 - Stratégie de résolution de noms
 - Scripts (démarrage/arrêt)
 - Paramètres de sécurité
 - Stratégies de comptes
 - Stratégie de mot de passe
 - Stratégie de verrouillage du compte
 - Stratégie Kerberos
 - Stratégies locales

Stratégie

Paramètres de stratégie	
Assouplir les limites de longueur minimale du mot de passe	Non défini
Audit de la longueur minimale du mot de passe	Non défini
Conserver l'historique des mots de passe	24 mots de passe mémorisés
Durée de vie maximale du mot de passe	42 jours
Durée de vie minimale du mot de passe	1 jours
Enregistrer les mots de passe en utilisant un chiffrement réversible	Désactivé
Le mot de passe doit respecter des exigences de complexité	Désactivé
Longueur minimale du mot de passe	3 caractères

Pour appliquer cette GPO on va utiliser la commande GPUPDATE /FORCE.

```
C:\ Administrateur : C:\Windows\system32\cmd.exe
Microsoft Windows [version 10.0.20348.169]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur>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.

C:\Users\Administrateur>
```

On peut visualiser les paramètres de notre GPO depuis la console

Gestion de stratégie de groupe

Forêt : nextlan

- Domaines
 - nextlan
 - Default Domain Policy
 - Domain Controllers
 - NEXT-FORMATION
- Objets de stratégie de groupe
 - Default Domain Controllers Policy
 - Default Domain Policy
 - Filtres WMI
 - Objets GPO Starter
- Sites
- Modélisation de stratégie de groupe
- Résultats de stratégie de groupe

Default Domain Policy

- Étendue
- Détails
- Paramètres**
- Délégation
- État

Général

- Détails
- Liaisons
- Filtrage de sécurité
- Délégation

Configuration ordinateur (activée)

Stratégies

Paramètres Windows

Stratégies de comptes/Stratégie de mot de passe

Stratégie	Paramètre
Antériorité maximale du mot de passe	42 jours
Antériorité minimale du mot de passe	1 jours
Appliquer l'historique des mots de passe	24 mots de passe mémorisés
Enregistrer les mots de passe en utilisant un chiffrement réversible	Désactivé
Le mot de passe doit respecter des exigences de complexité	Désactivé
Longueur minimale du mot de passe	3 caractères

Stratégies de comptes/Stratégie de verrouillage du compte

Vérifier également que cette GPO est bien active.

The screenshot shows the 'Gestion de stratégie de groupe' (Group Policy Management) interface. On the left, a tree view shows the forest 'next.lan' with its domains ('next.lan'), objects ('Objets de stratégie de groupe') which include 'Default Domain Controllers Policy' and 'Default Domain Policy', and other options like 'Sites' and 'Modélisation de stratégie de groupe'. On the right, the 'Default Domain Policy' is selected, and its details are displayed in a card:

Default Domain Policy	
	Étendue Détails Paramètres Délegation État
Domaine :	next.lan
Propriétaire :	Admins du domaine NEXT (NEXT\Admins du domaine NEXT)
Créé le :	11/10/2023 12:04:54
Modifié le :	11/10/2023 12:15:14
Version utilisateur :	0 (AD), 0 (SYSVOL)
Version ordinateur :	3 (AD), 11 (SYSVOL)
ID unique :	{31B2F340-016D-11D2-945F-00C04FB984F9}
État (GPO) :	Activé
Commentaire :	

N'oubliez de vérifier que notre GPO est liée à bonne destination (dans notre cas domaine).

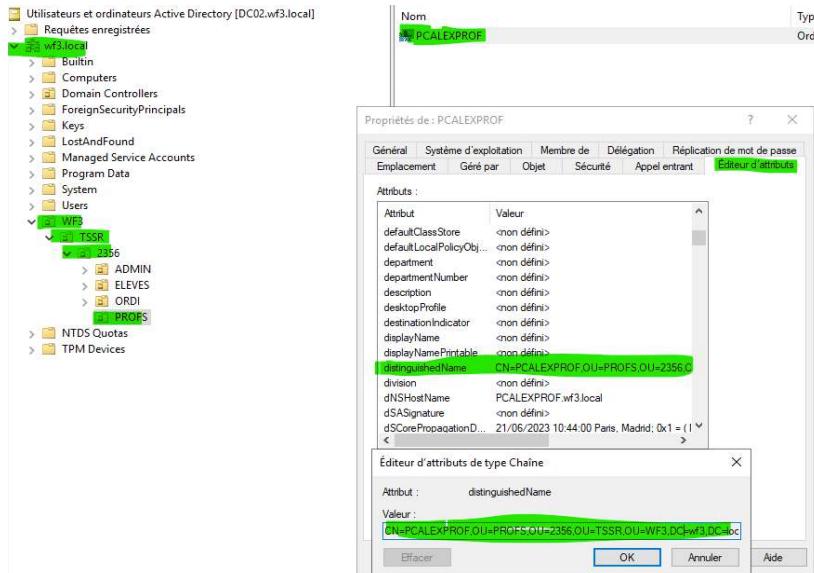
Tester la création d'un user dans l'annuaire avec 3 caractères comme mot de passe.

Démonstration GPO

Démo 1 : Appliquer un fond écran commun.

On souhaite déployer un fond écran pour toutes les machines de l'unité d'organisation (UO) PROF. Voici le chemin LDAP de l'objet ordinateur du PCALEXPROF que nous recherchons pour l'application de la GPO. Pour afficher ce chemin LDAP il faut activer la fonctionnalité avancée depuis l'annuaire et se rendre dans l'objet en question pour afficher l'éditeur d'attribut.

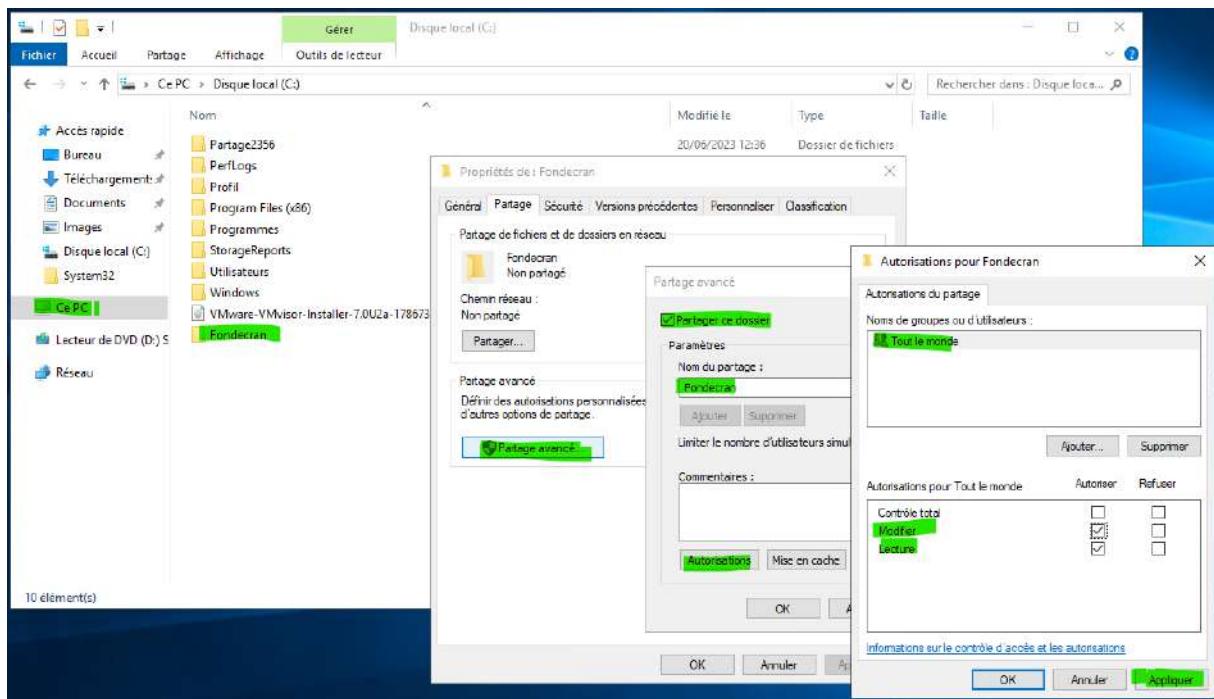
CN=PCALEXPROF,OU=PROFS,OU=2356,OU=TSSR,OU=WF3,DC=wf3,DC=local.



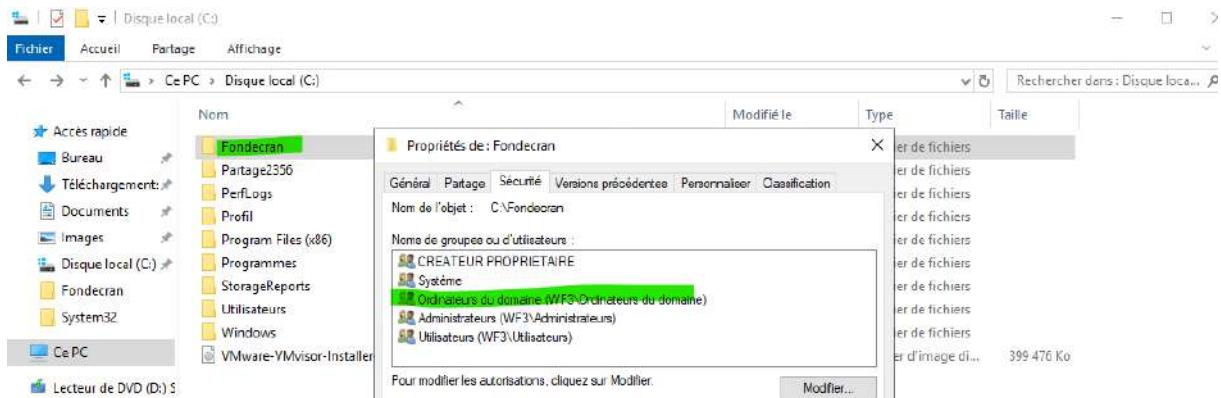
Pour appliquer notre image, il faut créer un partage depuis le serveur pour que ce fichier soit accessible en réseau depuis les machines utilisateurs car sans ce partage alors aucune personne ne peut récupérer un fichier en local. Dans notre cas, on souhaite déployer une image par le réseau donc il est important de placer cette image dans un partage.

On crée le dossier dans la racine du serveur qui va partager le fichier et on partage ce dossier comme indiqué avec les droits d'accès nécessaires.

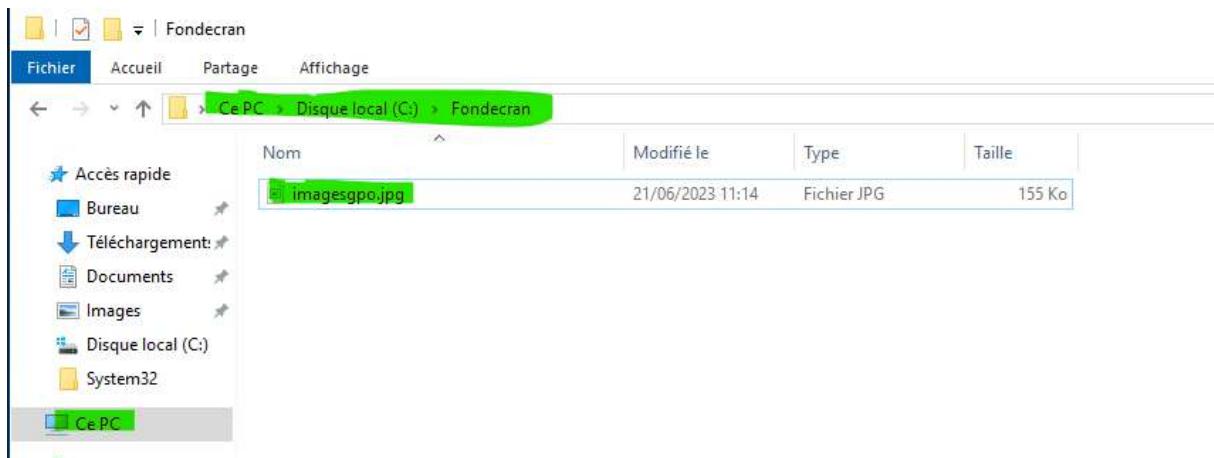
Pour le partage, on laisse le groupe « tout le monde » comme autorisation.



On rajoute le groupe *Ordinateurs du domaine* dans l'onglet sécurité du dossier partagé.



Dans ce dossier, on dépose une image au format .PNG par exemple.



Pour la prochaine étape :

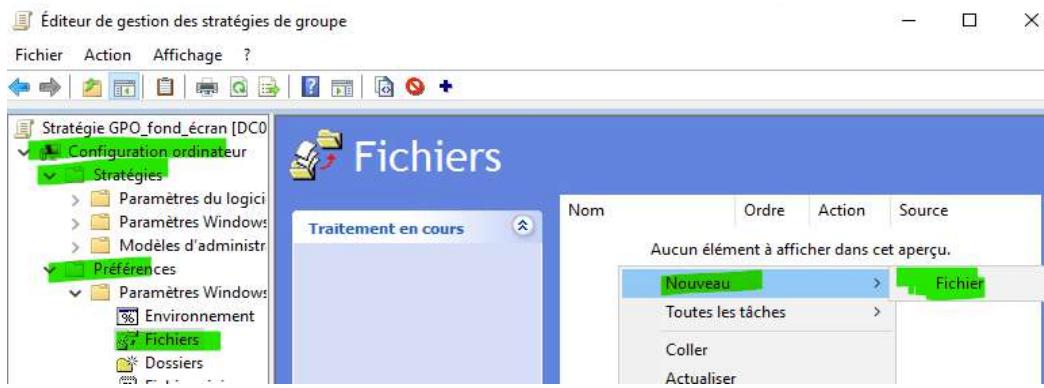
Depuis la console Gestion des stratégies de groupe, on va chercher notre unité d'organisation qui possède l'objet ordinateur PCALEXPROF dans notre cas.

Puis, on va créer une GPO dans cette UO pour qu'elle soit liée directement. Attention : cela ne veut pas dire qu'elle est configurée, ici on précise cette GPO sera appliquée seulement à cette UO et attention à la hiérarchie.

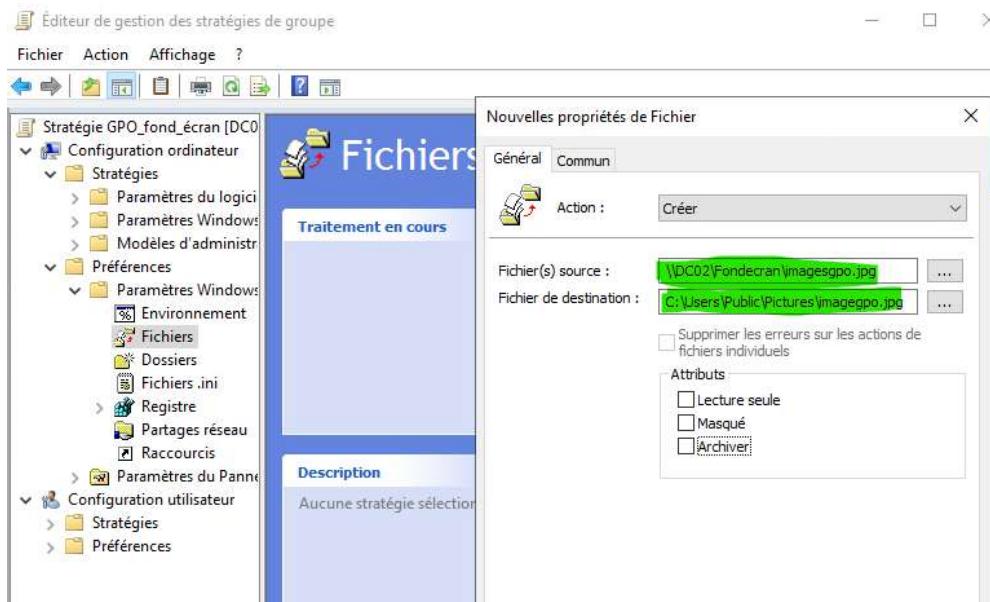
The screenshot shows the 'Gestion de stratégie de groupe' (Group Policy Management) console. On the left, the navigation pane shows the forest 'wf3.local' with its domains: 'wf3.local' (containing 'Default Domain Policy' and 'Domain Controllers' with 'Default Domain Controllers Policy'), 'WF3' (containing 'TSSR' which has '2356' (containing 'ADMIN', 'ELEVES', 'ORDI') and 'PROFS'), and 'Objets de strat.' (containing 'Filtres WMI' and 'Objets GPO Strat.'). A context menu is open over the 'PROFS' OU, with the following options visible: 'Créer un objet GPO dans ce domaine, et le lier ici...', 'Lier un objet de stratégie de groupe existant...', and 'Bloquer l'héritage'. The 'PROFS' OU is highlighted with a green box. On the right, the details pane shows the 'PROFS' object with tabs for 'Objets de stratégie de groupe liés', 'Héritage de stratégie de groupe', and 'Délegation'. Below the tabs is a tree view of the inheritance chain. A second screenshot below shows the 'GPO_fond_écran' policy object created under 'PROFS', with its details pane showing 'Emplacement' set to 'PROFS', 'Appliqué' set to 'Non', and 'Liens actifs' set to 'Oui'. The 'Chemin d'accès' is listed as 'wf3.local/WF3/TSSR/2356/PROFS'.

Désormais, nous allons passer à la configuration de celle-ci, et comme il s'agit d'une GPO qui va modifier le comportement d'une machine d'un domaine (dans notre cas modifier le fond d'écran de la machine) alors la stratégie va concerner une configuration ORDINATRICE.

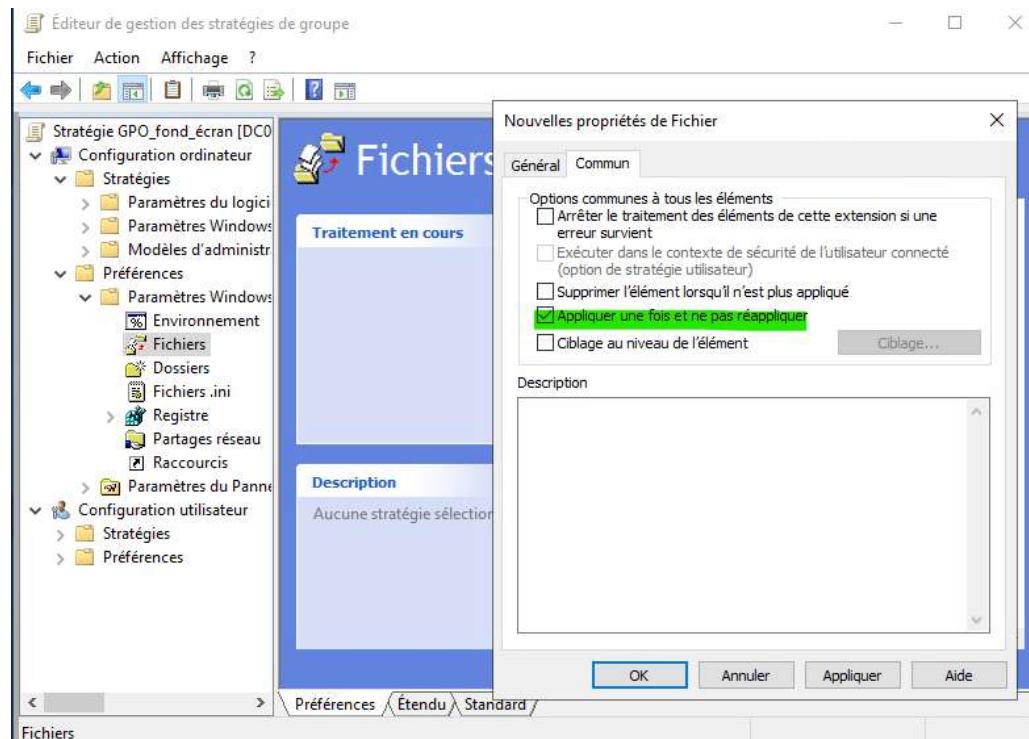
The screenshot shows the 'Gestion de stratégie de groupe' (Group Policy Management) console. The navigation pane is identical to the previous screenshot. The 'PROFS' OU is highlighted with a green box. The 'GPO_fond_écran' policy object is selected, and a context menu is open over it, with the option 'Modifier...' highlighted. The details pane for 'GPO_fond_écran' shows tabs for 'Étendue', 'Détails', and 'Paramètres'. The 'Liaisons' section indicates that the policy is linked to the 'wf3.local' domain. The 'Emplacement' is set to 'PROFS'. The 'GPO_fond_écran' object is also visible in the navigation pane under 'wf3.local/WF3/TSSR/2356/PROFS'.



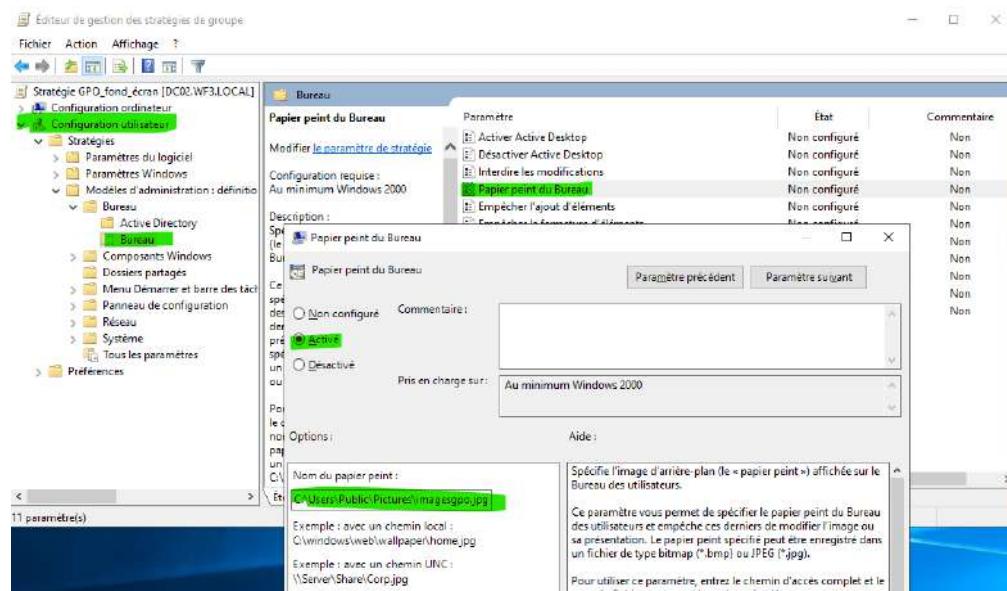
Dans la source on va déclarer le chemin UNC (chemin réseau du fichier qui se trouve dans le serveur). Pour la destination, ce paramètre permet de copier l'image dans l'emplacement local des clients donc ici on indique qu'on souhaite copier le fichier imagegpo.jpg dans le dossier public en local sur les machines du domaine.



On va appliquer ce paramètre (la copie du fichier depuis la source en réseau vers la destination en local) qu'une seul fois cela évite de recopier inutilement ce fichier à plusieurs reprises.



On va maintenant dans la même GPO indiqué un paramètre qui permet de lancer l'image depuis l'emplacement local des machines comme celle-ci a été copié depuis le serveur en réseau.



A partir du client, on va forcer l'application de la GPO avec la commande GPUPDATE /FORCE ou tout simplement vous pouvez redémarrer le client.

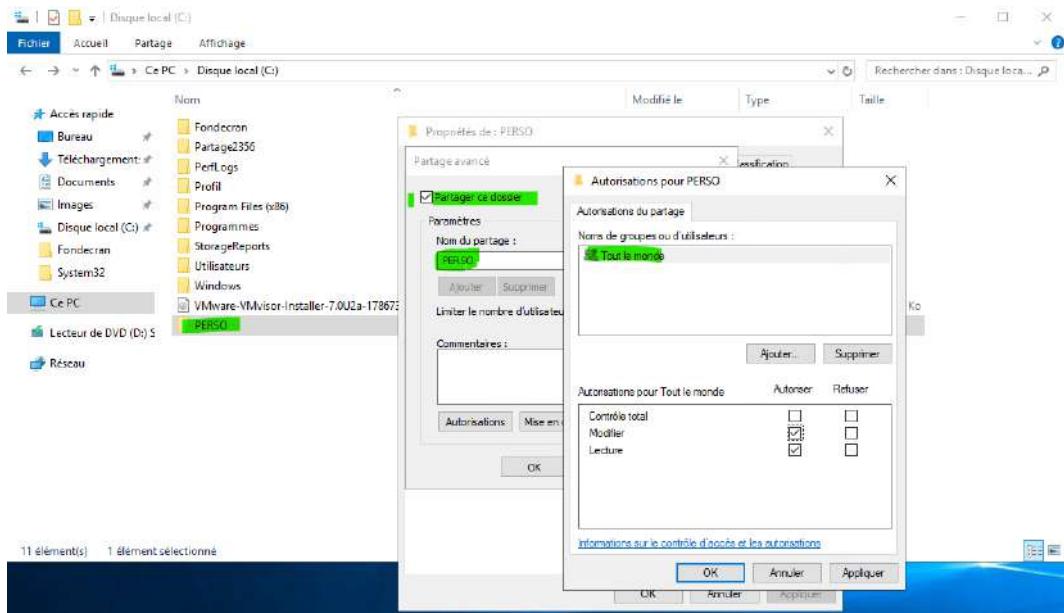
Aide pour la procédure :

https://www.it-connect.fr/copier-et-deployer-un-fond-decran-par-gpo/#IV_Appliquer_le_fond_decran

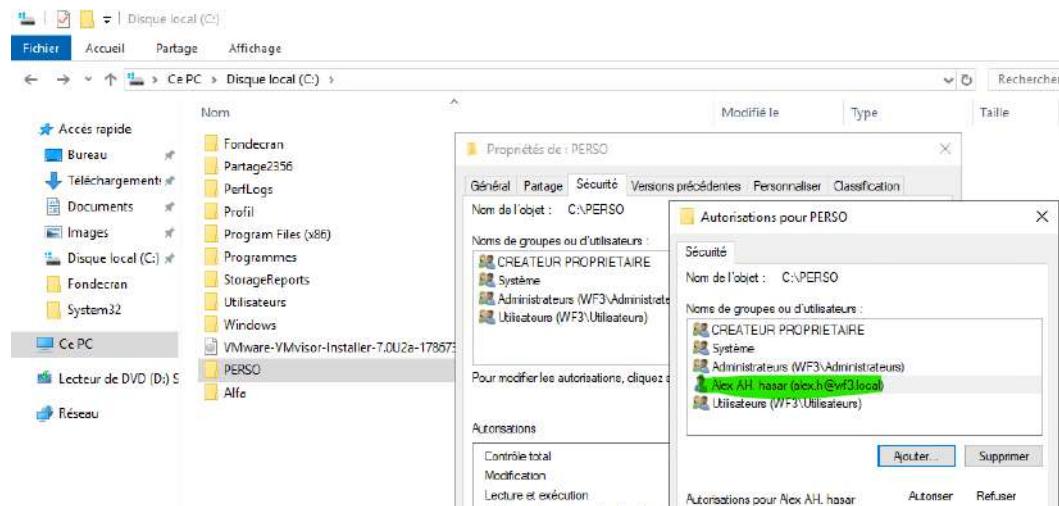
Démo 2 : appliquer un script à l'ouverture de session.

L'objectif est de connecter un lecteur réseau sur client via une GPO mais cette GPO va exécuter un script au format .bat.

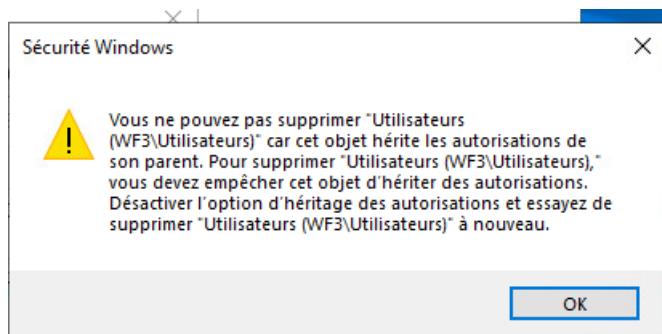
En premier, on va créer un répertoire nommée PERSO depuis le serveur et on partage ce dossier.



Ici, je précise l'utilisateur ALEX pour l'accès à ce dossier, et je retire le groupe Utilisateurs pour éviter que d'autres utilisateurs du domaine puissent y accéder car par défaut tout le monde du domaine est membre de ce groupe.



Si vous obtenez ce message lors de la suppression du groupe Utilisateurs, il faut désactiver l'héritage pour ce dossier car celui-ci hérite de son parent des droits d'accès par défaut.



A screenshot of the Windows Properties dialog box for a folder named "PERSO" located at "C:\PERSO". The "Sécurité" (Security) tab is selected. The "Noms de groupes ou d'utilisateurs :" (Names of groups or users) section lists "CREATEUR PROPRIETAIRE", "Système", "Administrateurs (WF3\Administrateurs)", and "Utilisateurs (WF3\Utilisateurs)". Below this, a note says "Pour modifier les autorisations, cliquez sur Modifier..." (To change permissions, click on Modify...) and a "Modifier..." button is highlighted with a green box. The "Autorisations pour CREATEUR PROPRIETAIRE" (Permissions for CREATEUR PROPRIETAIRE) section shows various permissions like "Contrôle total" (Full Control), "Modification", "Lecture et exécution", etc., with checkboxes for "Autoriser" (Allow) and "Refuser" (Deny). At the bottom, a note says "Pour les autorisations spéciales et les paramètres avancés, cliquez sur Avancé." (For special permissions and advanced settings, click on Advanced...) and an "Avancé" button is highlighted with a green box.

Paramètres de sécurité avancés pour PERSO

Nom :	C:\PERSO			
Propriétaire :	Administrateurs (WF3\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
Auto...	CREATEUR PROPRIÉTAIRE	Contrôle total	Objet parent	Les sous-dossiers et les fichiers...
Auto...	Système	Contrôle total	Objet parent	Ce dossier, les sous-dossiers et...
Auto...	Administrateurs (WF3\Administr...	Contrôle total	Objet parent	Ce dossier, les sous-dossiers et...
Auto...	Utilisateurs (WF3\Utilisateurs)	Spéciale	Objet parent	Ce dossier et les sous-dossiers
Auto...	Utilisateurs (WF3\Utilisateurs)	Lecture et exécution	Objet parent	Ce dossier, les sous-dossiers et...

[Ajouter](#) [Supprimer](#) [Afficher](#)

[Désactiver l'héritage](#)

On va conserver les groupes actuels et ensuite on va pouvoir supprimer une fois l'héritage désactivé.

Paramètres de sécurité avancés pour PERSO

Nom :	C:\PERSO			
Propriétaire :	Administrateurs (WF3\Administrateurs)			
Autorisations	Bloquer l'héritage			
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
Auto...	CREATEUR PROPRIÉTAIRE	Contrôle total	Objet parent	Les sous-dossiers et les fichiers...
Auto...	Système	Contrôle total	Objet parent	Ce dossier, les sous-dossiers et...
Auto...	Administrateurs (WF3\Administr...	Contrôle total	Objet parent	Ce dossier, les sous-dossiers et...
Auto...	Utilisateurs (WF3\Utilisateurs)	Spéciale	Objet parent	Ce dossier et les sous-dossiers
Auto...	Utilisateurs (WF3\Utilisateurs)	Lecture et exécution	Objet parent	Ce dossier, les sous-dossiers et...

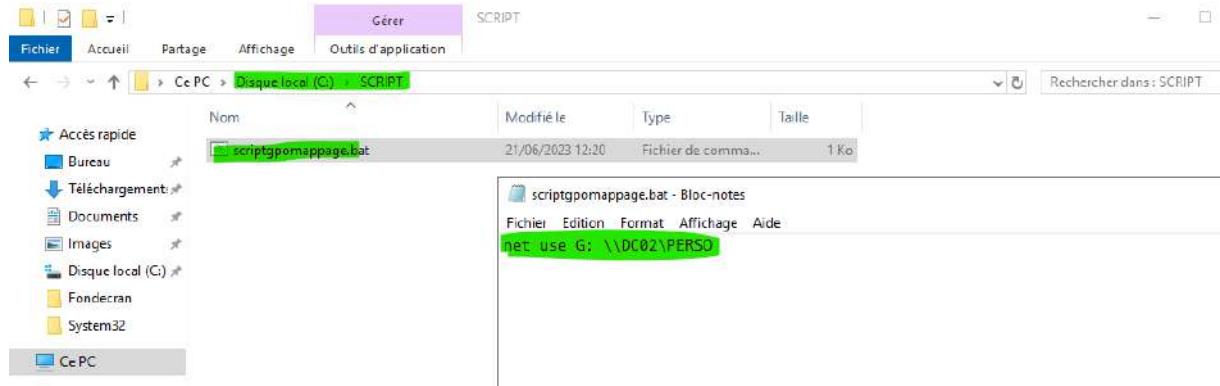
[Ajouter](#) [Supprimer](#) [Afficher](#)

[Désactiver l'héritage](#)

Remplacer toutes les entrées d'autorisation des objets enfants par des entrées d'autorisation pouvant être héritées de cet objet

[OK](#) [Annuler](#) [Appliquer](#)

On va créer un deuxième dossier SCRIPT où l'on va déposer un fichier texte avec la commande qui permet de monter un lecteur réseau et ensuite nous allons modifier le format txt en format .bat, le fichier va devenir un programme exécutable.



La commande NET USE permet d'indiquer le lecteur réseau que va utiliser le client.

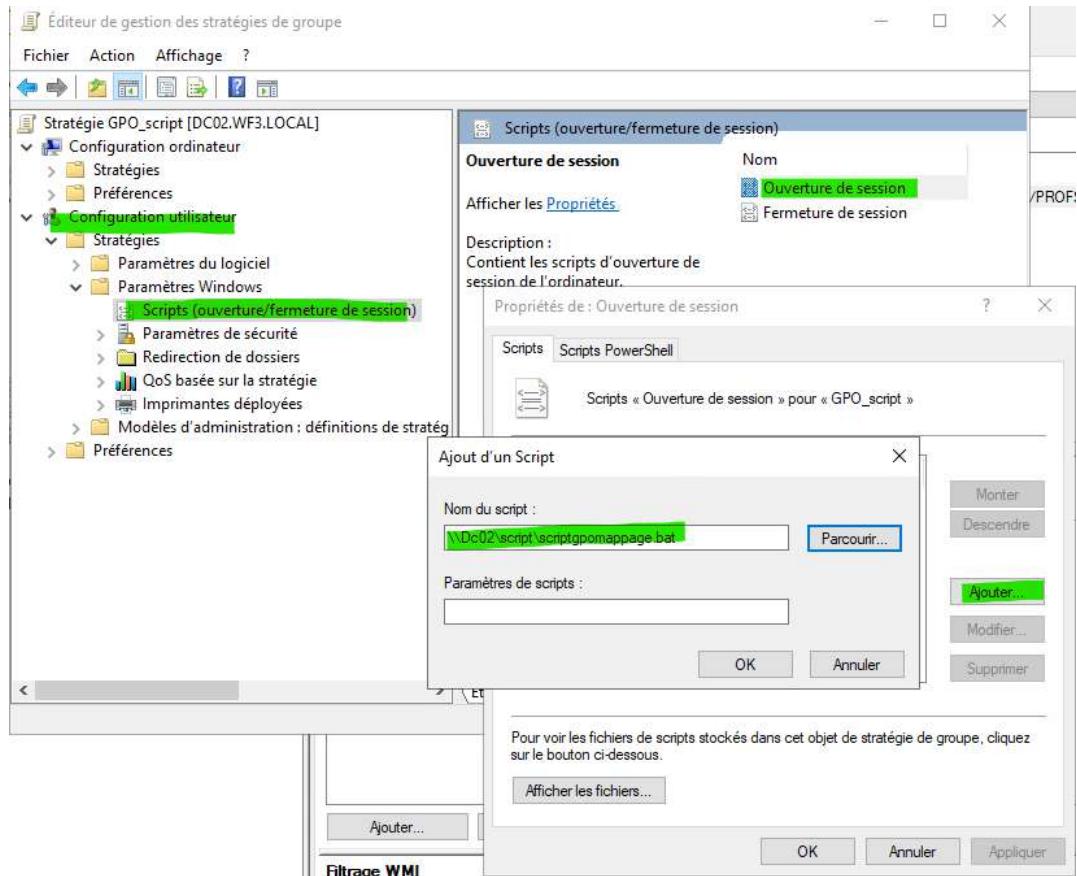
Dans ce script, on va monter un lecteur réseau G : qui pointe vers le dossier partagé PERSO que nous avons créé et partagé dans les étapes précédentes.

Etapes suivante : mise en place

On va pouvoir maintenant créer la GPO pour l'utilisateur, et dans cette GPO on va indiquer l'exécution du script au démarrage de la session.

Ordre des liens	Objet de stratégie de groupe
1	GPO_fond_écran
2	GPO_script

On indique l'emplacement RESEAU du fichier .bat et non pas un emplacement local (attention).

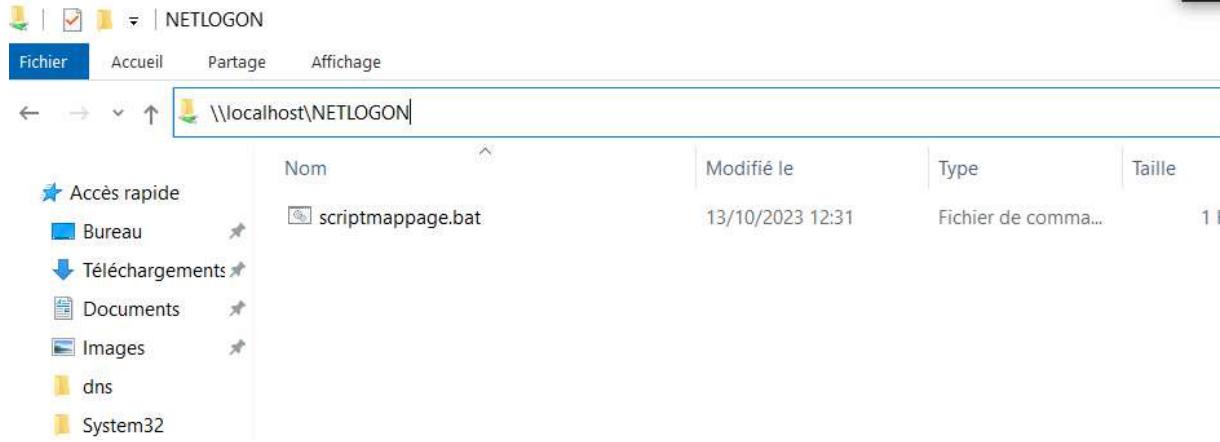


On peut maintenant se connecter sur le CLIENT avec un utilisateur du domaine.

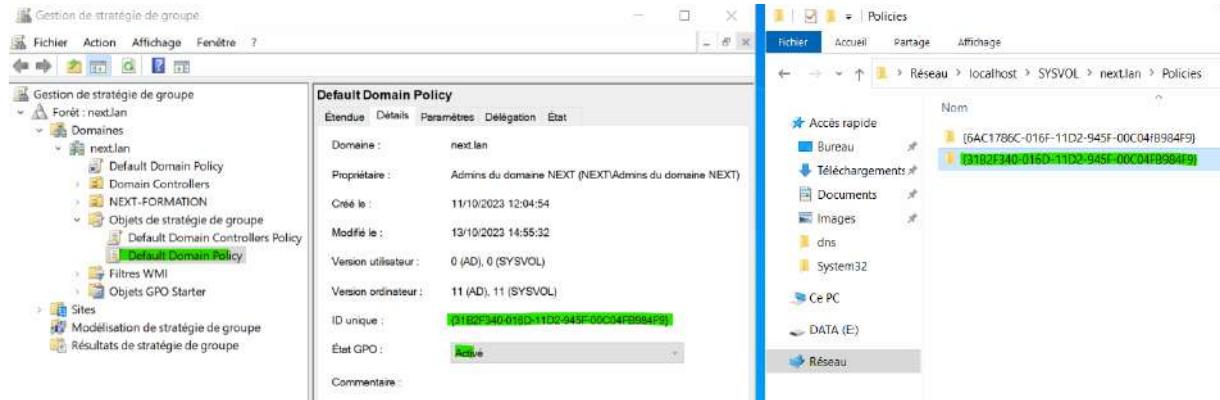
Attention si la GPO n'a pas fonctionné n'hésitez pas à exécuter le script directement en réseau depuis son chemin UNC cela va permettre de détecter les dysfonctionnements.

Le dossier partagé SYSVOL

Ce dossier sera utilisé pour déposer des scripts comme à l'ouverture de session vue précédemment.



On retrouve également les GPO.



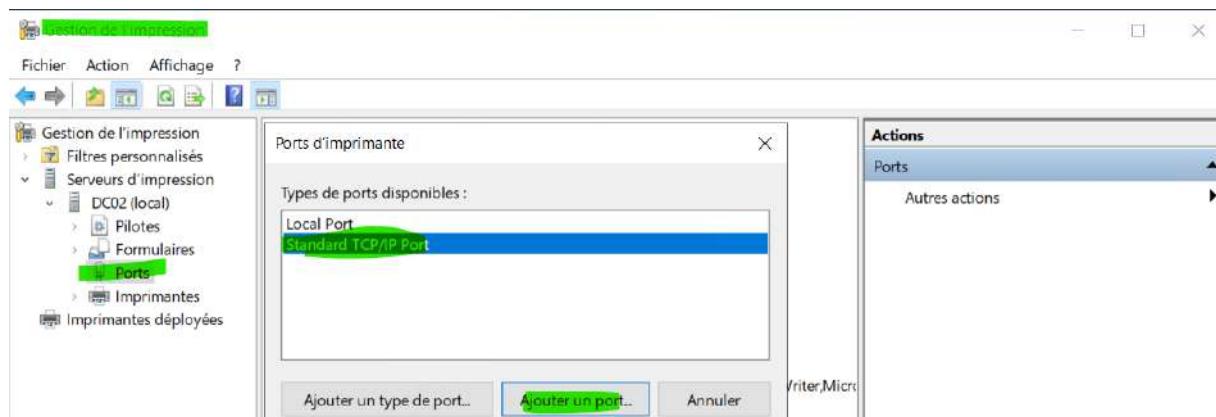
Mise en place d'un serveur d'impression.

Etapes 1 : ajouter le rôle

- Ajouter le rôle services des impressions et de numérisation depuis le serveur Windows.

Etapes 2 : ajouter une imprimante en réseau depuis le serveur d'impression

- En premier il faut que l'imprimante soit en DHCP, ensuite depuis le serveur DHCP créer une réservation avec l'adresse MAC de l'imprimante qu'il faut récupérer.
- Si vous n'avez pas d'imprimante cette opération ne peut pas être effectuée.
- On va créer un port depuis le serveur d'impression pour indiquer le protocole TCP/IP en indiquant l'IP de l'imprimante à ajouter.



L'adresse IP à indiquer va dépendre si vous disposez d'une imprimante physique ou une manipulation virtuelle dans tous les cas il faut indiquer une adresse IP et si vous avez une imprimante physique alors indiquer l'IP de l'imprimante reçue par la réservation du DHCP.

Lors de la recherche de l'imprimante il est normal que ce soit long si vous n'avez pas réellement d'imprimante mais il ne faut arrêter l'opération. Le système Windows va automatiquement simuler une imprimante.

Assistant Ajout de port imprimante TCP/IP standard

Ajouter un port

Pour quel périphérique voulez-vous ajouter un port ?



Entrez un nom d'imprimante ou une adresse IP, et le nom du port pour le périphérique désiré.

Nom ou adresse IP de l'imprimante :

192.168.1.60

Nom du port :

192.168.1.60

Assistant Ajout de port imprimante TCP/IP standard

Informations supplémentaires requises concernant le port
Le périphérique n'a pas pu être identifié.



Ce périphérique est introuvable sur le réseau. Vérifiez que :

1. Le périphérique est allumé.
2. Vous êtes connecté au réseau.
3. Le périphérique est configuré correctement.
4. L'adresse de la page précédente est correcte.

Si vous pensez que l'adresse est incorrecte, cliquez sur Précédent pour revenir à la page précédente. Corrigez l'adresse et effectuez une nouvelle recherche sur le réseau. Si vous êtes sûr que l'adresse est correcte, sélectionnez le type de périphérique ci-dessous.

Type de périphérique

Standard Generic Network Card

Personnalisé

Paramètres...

< Précédent Suivant > Annuler

Gestion de l'impression

Fichier Action Affichage ?



	Gestion de l'impression
>	
>	
>	DC02 (local)
>	
>	
>	
>	
	Imprimantes déployées

Nom du port	Description du ...	Type de p...
192.168.1.50	Port TCP/IP stan...	Écrire
192.168.1.60	Port TCP/IP stan...	Écrire
COM1:	Port local	Écrire
COM2:	Port local	Écrire
COM3:	Port local	Écrire
COM4:	Port local	Écrire
FILE:	Port local	Écrire
LPT1:	Port local	Écrire
LPT2:	Port local	Écrire

Une fois le port créé on peut ajouter l'imprimante en indiquant le port utilisé (celui qu'on vient de créer)



Assistant Installation d'imprimante réseau

Installation de l'imprimante

Choisissez une méthode d'installation.

- Rechercher les imprimantes du réseau
- Ajouter une imprimante TCP/IP ou de services Web par adresse IP ou nom d'hôte
- Ajouter une nouvelle imprimante via un port existant :
- Créer un autre port et ajouter une nouvelle imprimante :

Assistant Installation d'imprimante réseau

X

Pilote d'imprimante

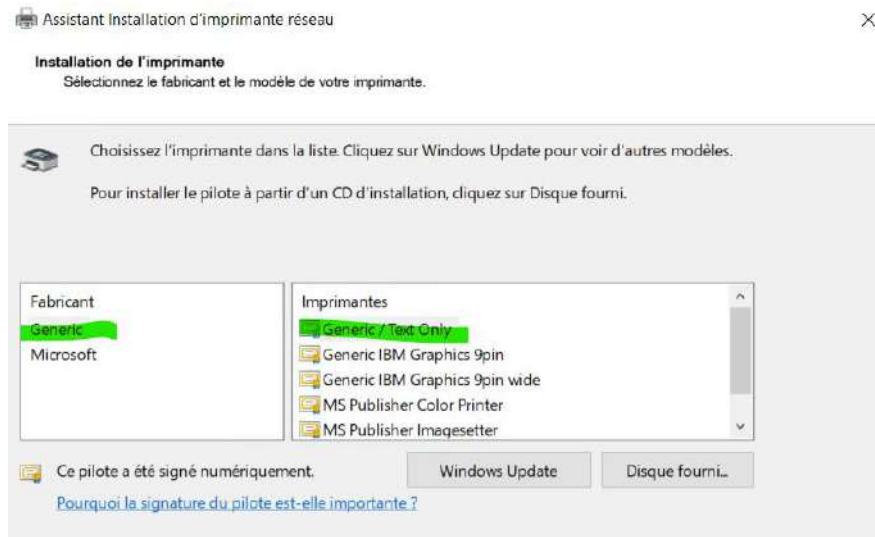
Choisissez un pilote pour la nouvelle imprimante.

- Utiliser le pilote d'imprimante sélectionné par l'Assistant

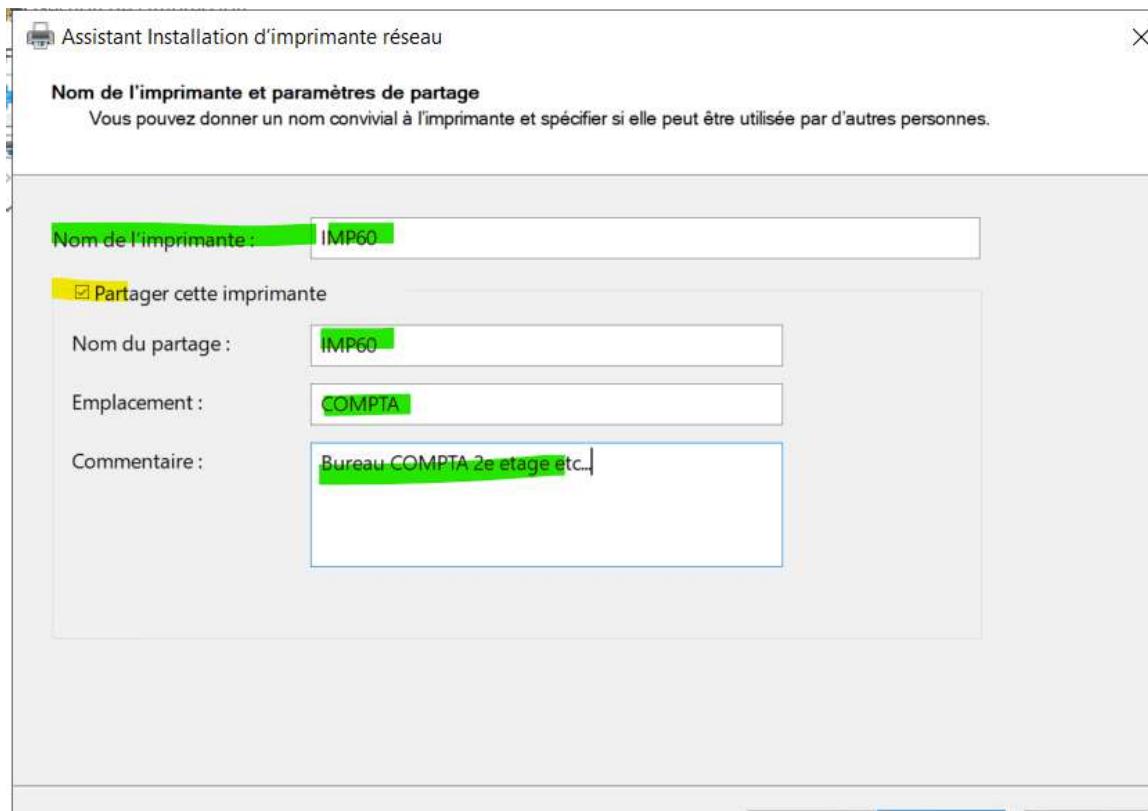
- Utiliser un pilote d'imprimante existant sur l'ordinateur

- Installer un nouveau pilote

Attention s'il s'agit d'une vraie imprimante il faut indiquer le fichier pour le pilote. Mais il s'agit d'une imprimante virtuelle alors laissé par défaut les paramètres.



Dans cette fenêtre on indique le nom de l'imprimante pour l'inventaire du serveur mais également le nom du partage de l'imprimante et pour information le nom du partage peut être différent du nom de l'imprimante. Pour que les utilisateurs puissent connecter cette imprimante en réseau depuis leurs machines il faut laisser la case Partager cette imprimante cochée. Cette action va permettre à ce serveur d'impression de partager l'imprimante dans le réseau.



Gestion de l'impression

Fichier Action Affichage ?

Nom de l'imprimante	Statut de la file...	Travaux...	Nom du serveur
IMP50	Prêt	0	DC02 (local)
IMP60	Prêt	0	DC02 (local)
Microsoft Print to PDF	Prêt	0	DC02 (local)
Microsoft Print to PDF (redirecti...)	Prêt	0	DC02 (local)
Microsoft XPS Document Writer	Prêt	0	DC02 (local)

Gestion de l'impression
Filtres personnalisés
Serveurs d'impression
DC02 (local)
Pilotes
Formulaires
Ports
Imprimantes
Imprimantes déployées

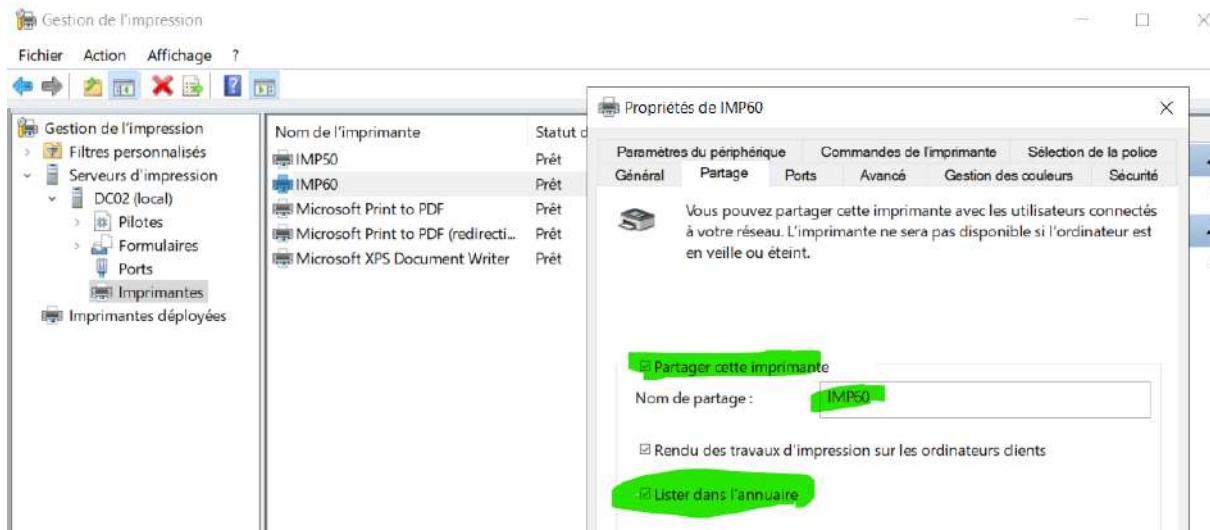
- On peut lister cette imprimante dans l'annuaire Active Directory de son domaine pour permettre la recherche de cette objet imprimante à travers l'annuaire ce qui va permettre à des utilisateurs qui recherche une imprimante dans l'annuaire la retrouver plus facilement et d'en avoir connaissance de son existence.

Gestion de l'impression

Fichier Action Affichage ?

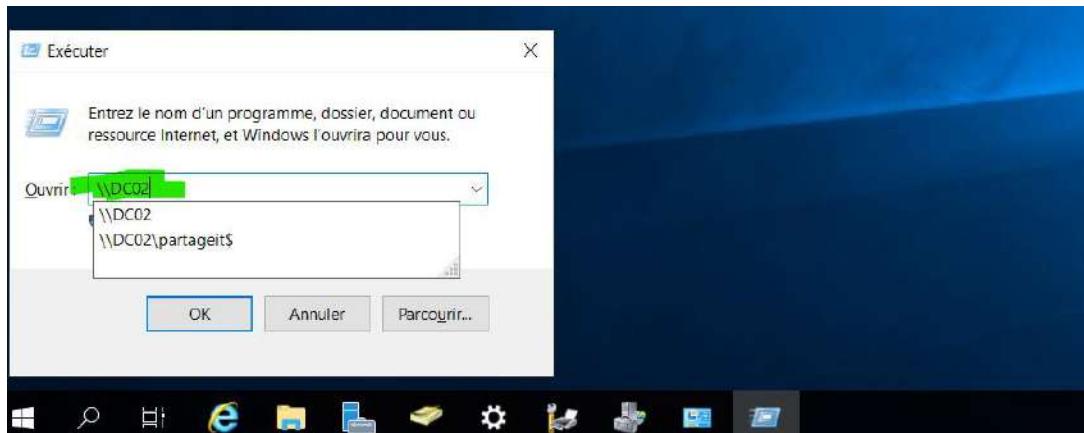
Nom de l'imprimante	Statut de la file...	Travaux...	Nom du serveur	Actions
IMP50	Prêt	0	DC02 (local)	Imprimantes
IMP60				Ouvrir la file d'attente de l'imprimante... Autres actions Suspendre l'impression IMP60 Répertorier dans l'annuaire Autres actions Déployer avec la stratégie de groupe.. Définir des valeurs d'impression par défaut... Gérer le partage... Autres actions Imprimer une page de test Activer l'impression directe pour les filiales Propriétés...
Microsoft Print to PDF				
Microsoft Print to PDF (
Microsoft XPS Docume				

Gestion de l'impression
Filtres personnalisés
Serveurs d'impression
DC02 (local)
Pilotes
Formulaires
Ports
Imprimantes
Imprimantes déployées



Etapes 3 : connecter l'imprimante sur le client.

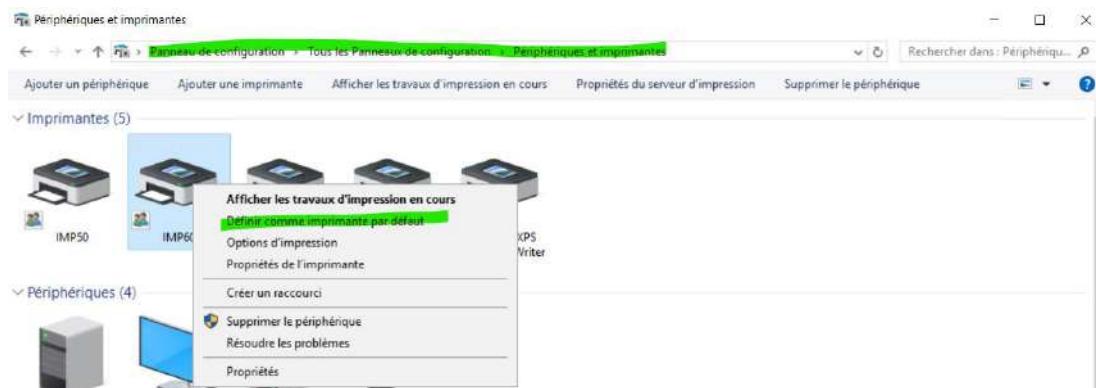
Pour vérifier que cette imprimante est partagée depuis un client indiqué le chemin UNC du serveur d'impression.



- Vous devriez voir l'imprimante en réseau apparaître et il suffit de cliquer sur la bonne imprimante souhaitée pour l'installer (double clic ou cliquer sur connecter)
- Il n'y a pas besoin d'installer les pilotes ou d'installer l'imprimante manuellement sur le client toute l'opération s'effectue en réseau.



Forcer l'utilisation de cette imprimante comme par défaut pour les utilisateurs.



Glossaire

DHCP : Dynamic Host Configuration Protocol

DNS : Domain Name System

FQDN : Full Qualified Domain Name (nom de domaine complet)

AD : Active Directory

AD-DS : Active Directory Domain Services (le rôle pour installer un contrôleur de domaine)

GPO : Group Policy Object (stratégie de groupe)

ACL : Access Control List (gestion des droits d'accès aux ressources)

OU : Organizational Units

AGDLP Access Global Domain Local Permissions

Base SAM : base Security Account Manager, gestion des mots de passe locaux sous Windows