

TP Active Directory-DNS-GPO

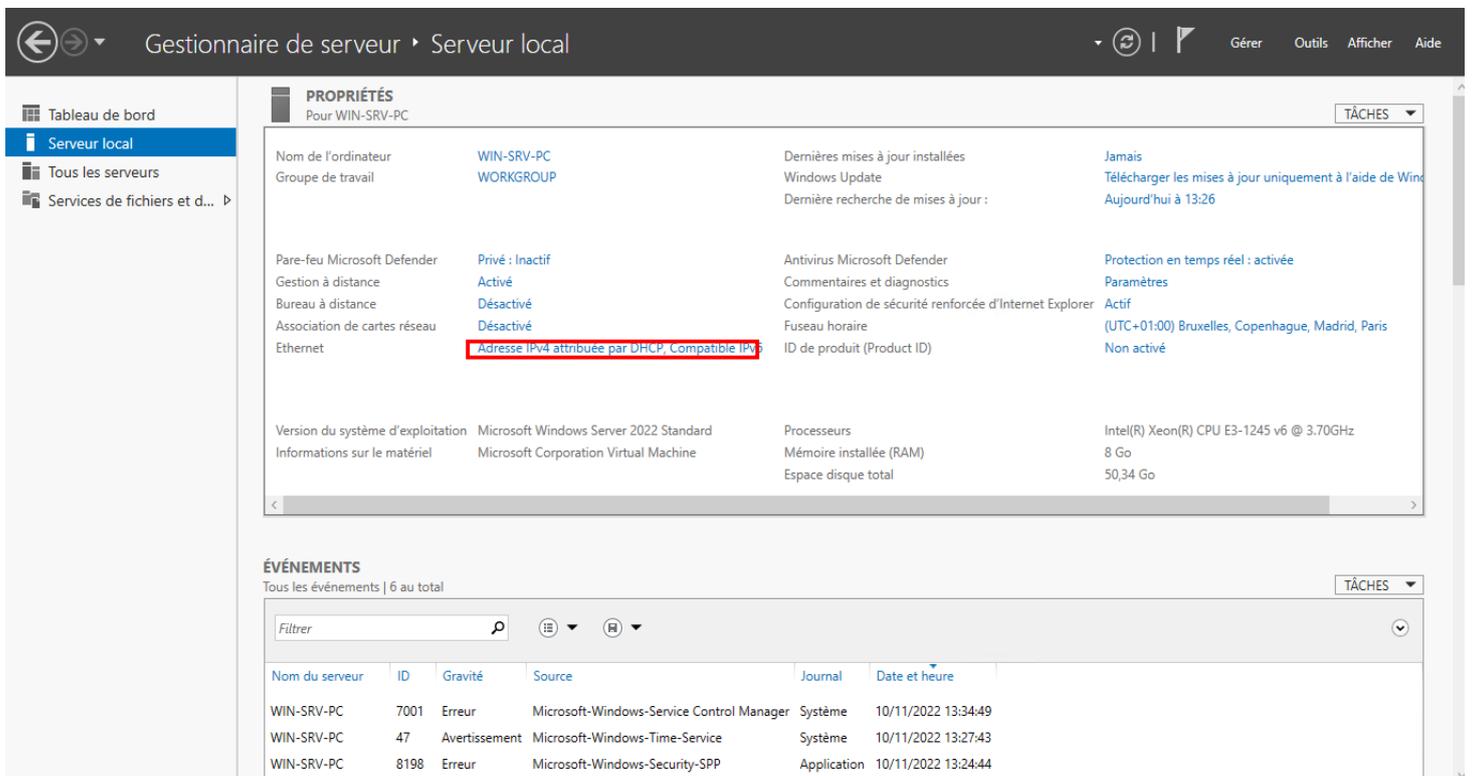
Dans ce TP nous allons voir comment installer et paramétrer des rôles AD, DS et DNS sur notre VM Windows serveur et le relier à notre client Windows 10 pro.

On créera également un utilisateur des unités d'organisation et des stratégies de groupe.

Pour cela on aura besoin d'une VM Windows server ainsi que Windows 10 pro.

I/Installation du serveur active directory

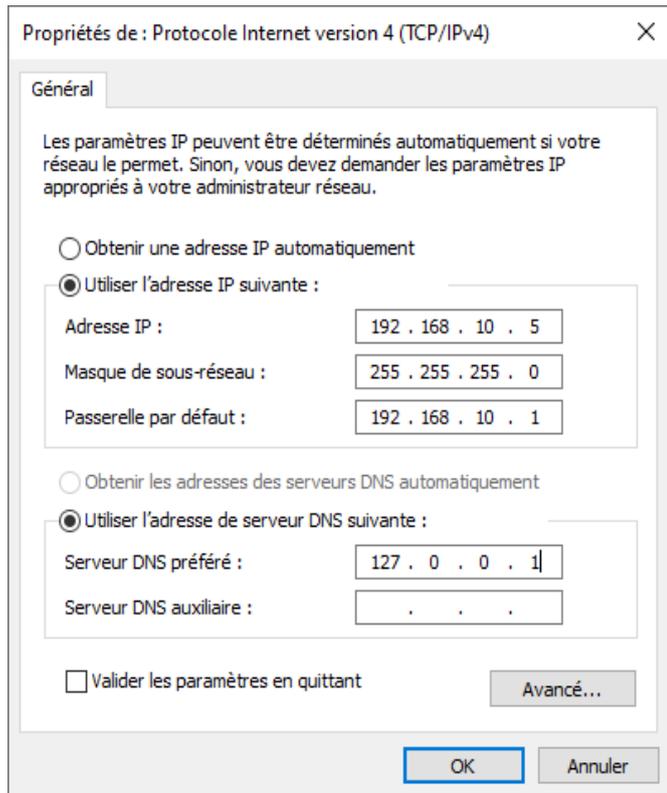
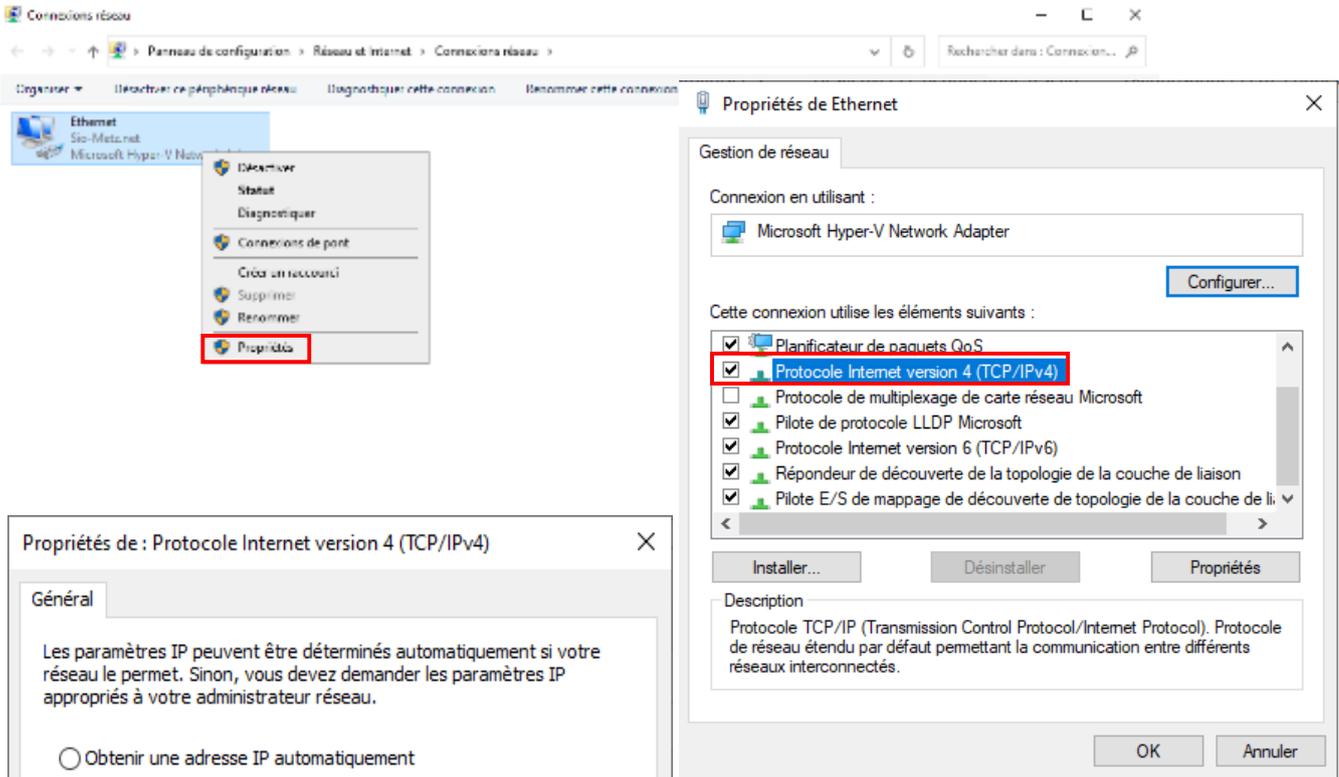
Pour commencer on lance notre VM Windows server et dans le gestionnaire de serveur on clique sur « Adresse IPv4 attribuée par DHCP, Compatible IPv6 ».



The screenshot shows the Windows Server 2022 Server Manager interface. The left sidebar shows the navigation pane with 'Serveur local' selected. The main area displays the 'PROPRIÉTÉS' (Properties) window for the 'Ethernet' adapter. The 'IPv4' tab is selected, and the 'Obtenir l'adresse IPv4 par DHCP' option is highlighted with a red box. Below the properties window, the 'ÉVÉNEMENTS' (Events) window is visible, showing a list of events.

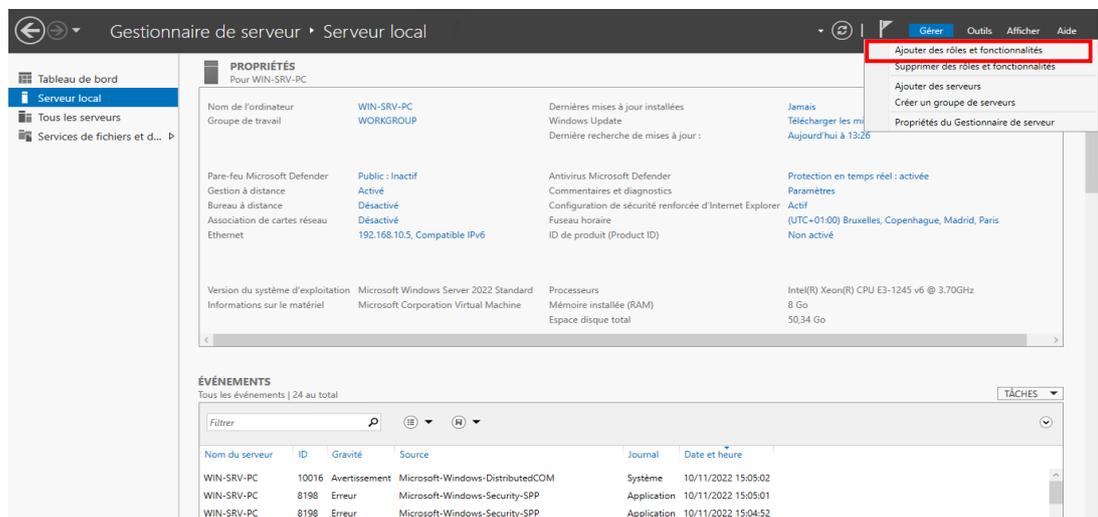
Nom du serveur	ID	Gravité	Source	Journal	Date et heure
WIN-SRV-PC	7001	Erreur	Microsoft-Windows-Service Control Manager	Système	10/11/2022 13:34:49
WIN-SRV-PC	47	Avertissement	Microsoft-Windows-Time-Service	Système	10/11/2022 13:27:43
WIN-SRV-PC	8198	Erreur	Microsoft-Windows-Security-SPP	Application	10/11/2022 13:24:44

Puis clic droit sur « Ethernet » puis « propriétés » et enfin « Protocole Internet version 4 ».

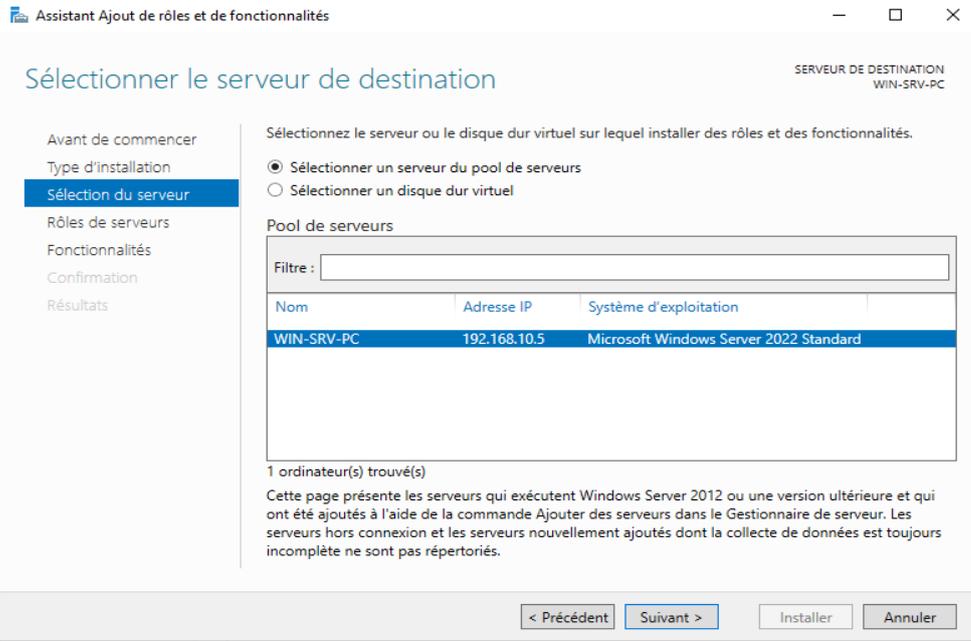


On entre les adresses suivantes (IP, Masque, Passerelle et DNS à adapter au réseau).

Une fois les paramètres DNS en place on retourne sur la page de notre serveur, dans l'onglet « Gérer » on clique sur « Ajouter des rôles et fonctionnalités ».

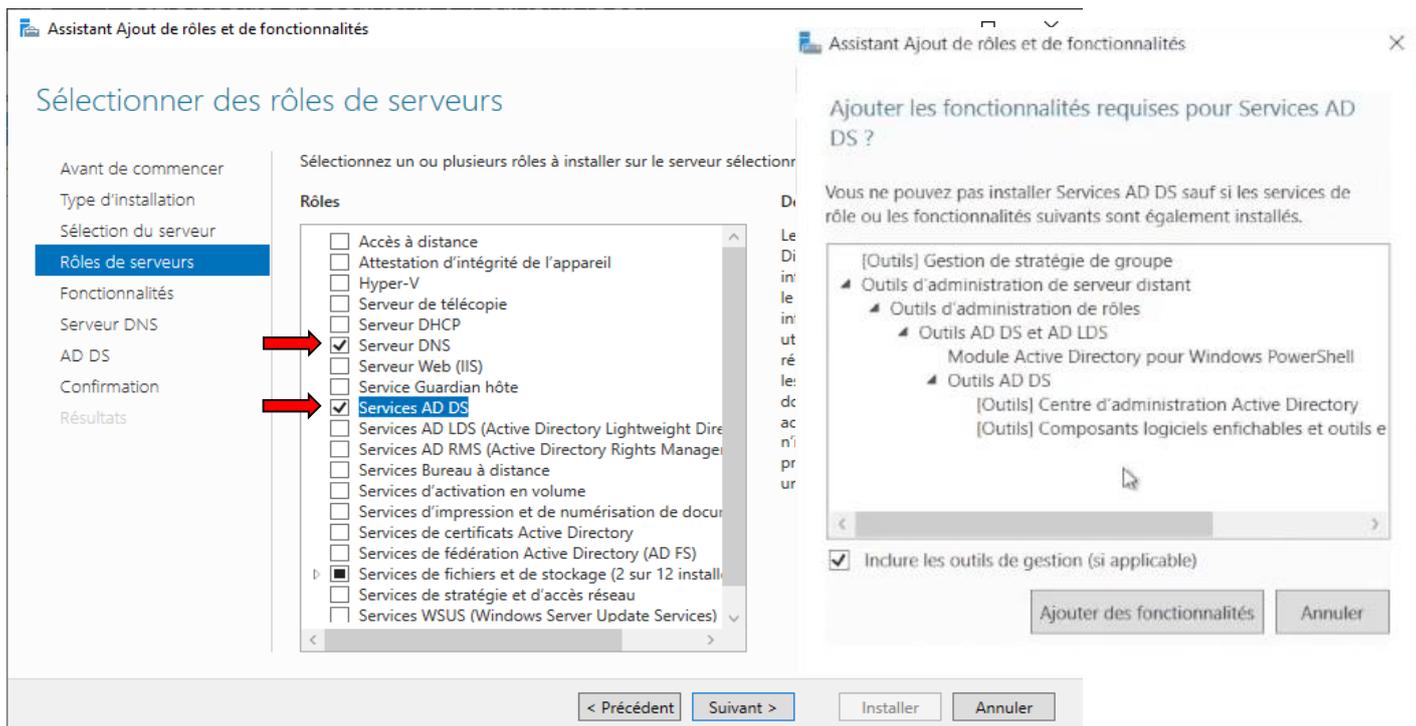


Ensuite on va simplement suivre les indications d'installation pour mettre en place notre serveur active directory.

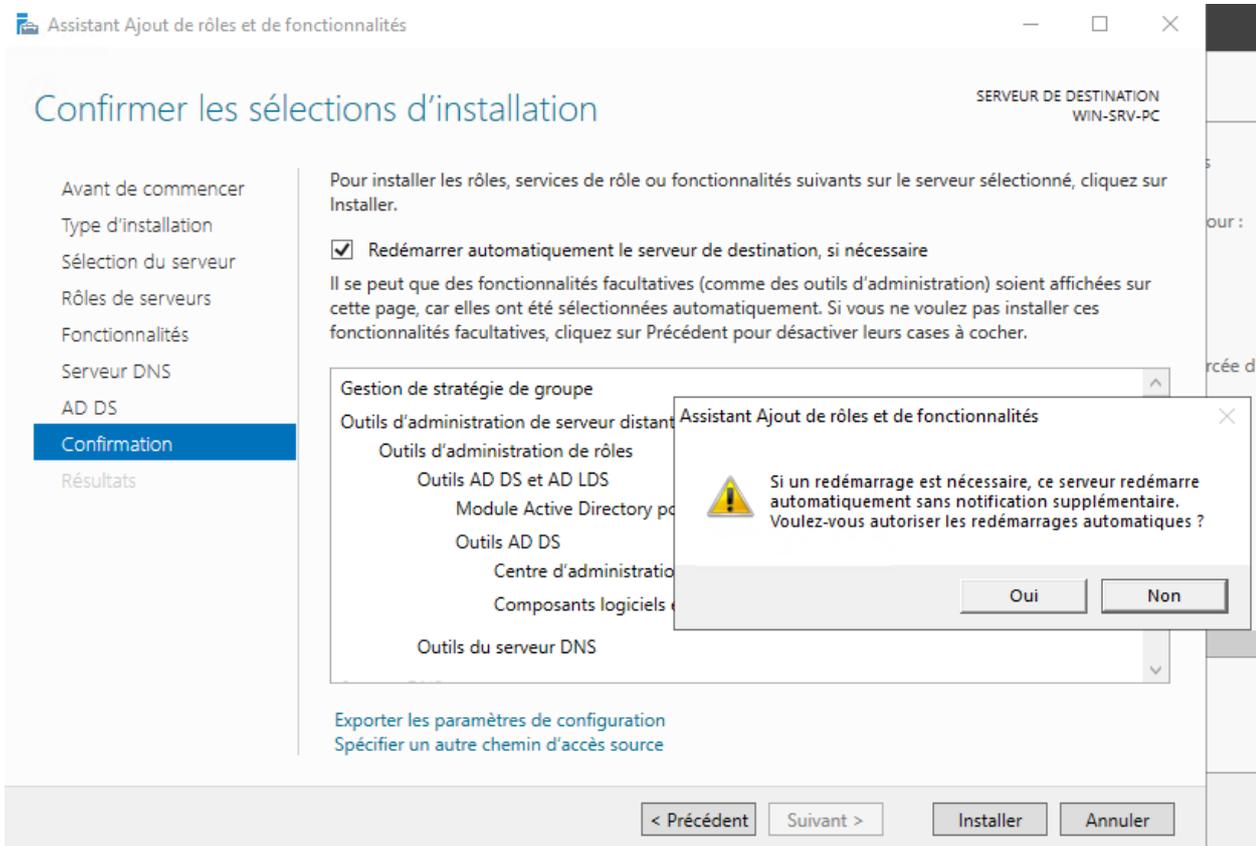


On voit que notre serveur est bien présent.

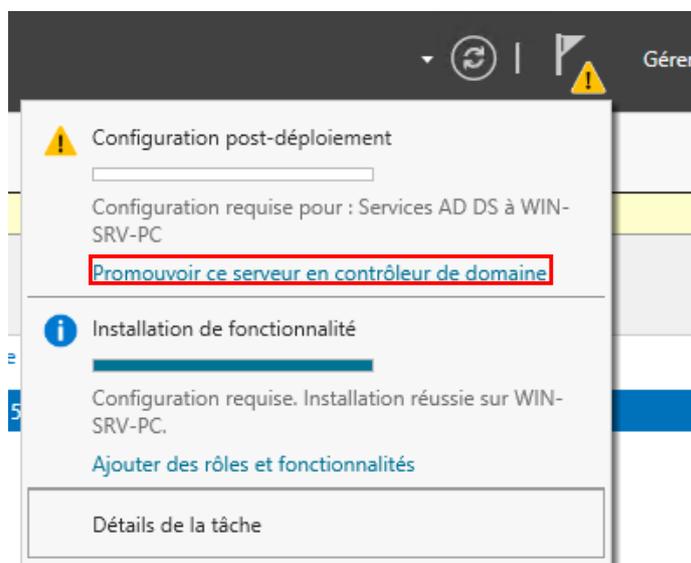
Ici on coche « Serveur DNS » (pour faire le lien entre le nom d'hôte et l'adresse ip), « Services AD DS » (pour gérer le domaine et les utilisateurs) et on peut également ajouter les outils d'administration pour plus de facilité.



Puis on va cliquer sur suivant jusqu'à arriver sur la page de confirmation, on n'oublie pas de cocher la case de redémarrage automatique et on peut lancer l'installation.

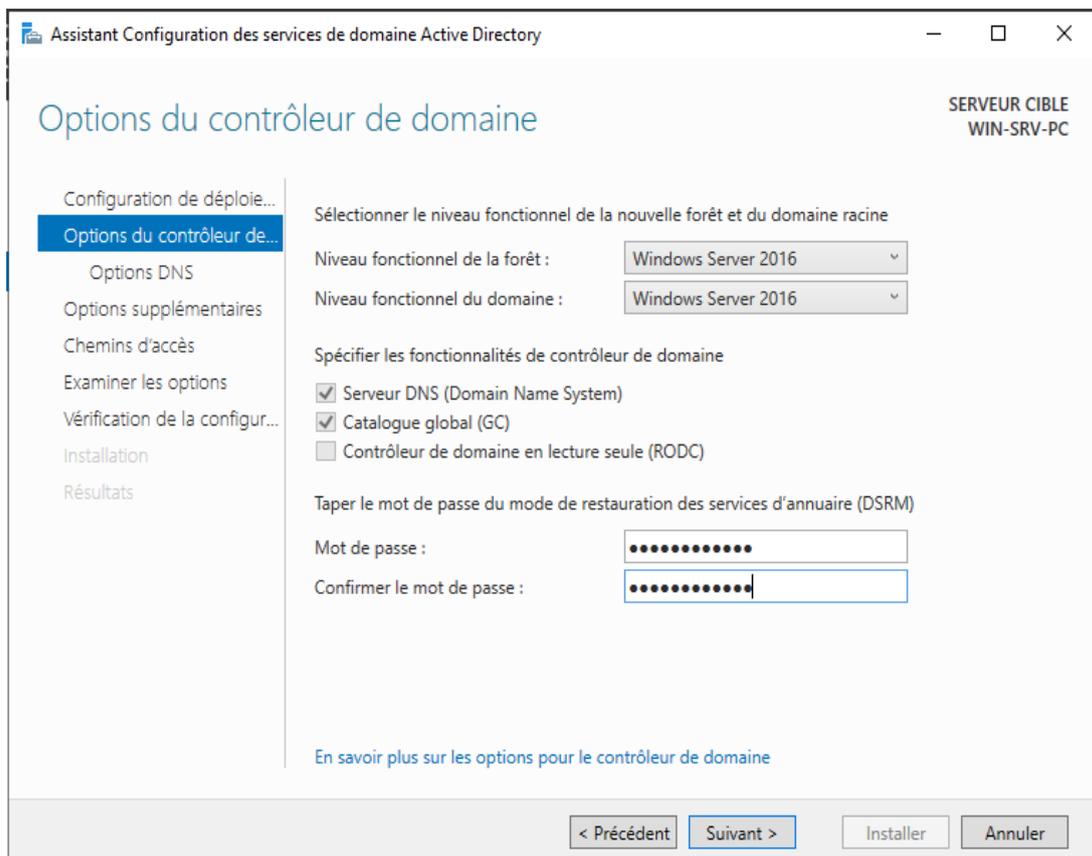
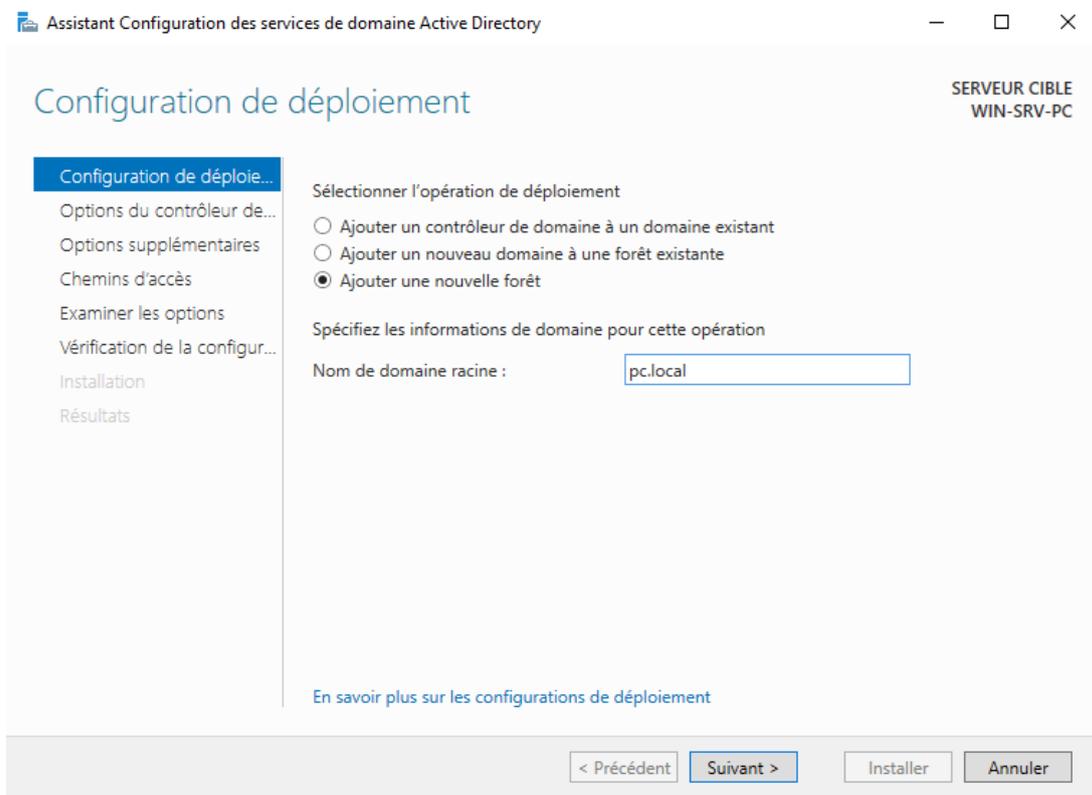


On peut voir que nos rôles se sont bien installés. On va pouvoir promouvoir notre serveur en contrôleur de domaine.

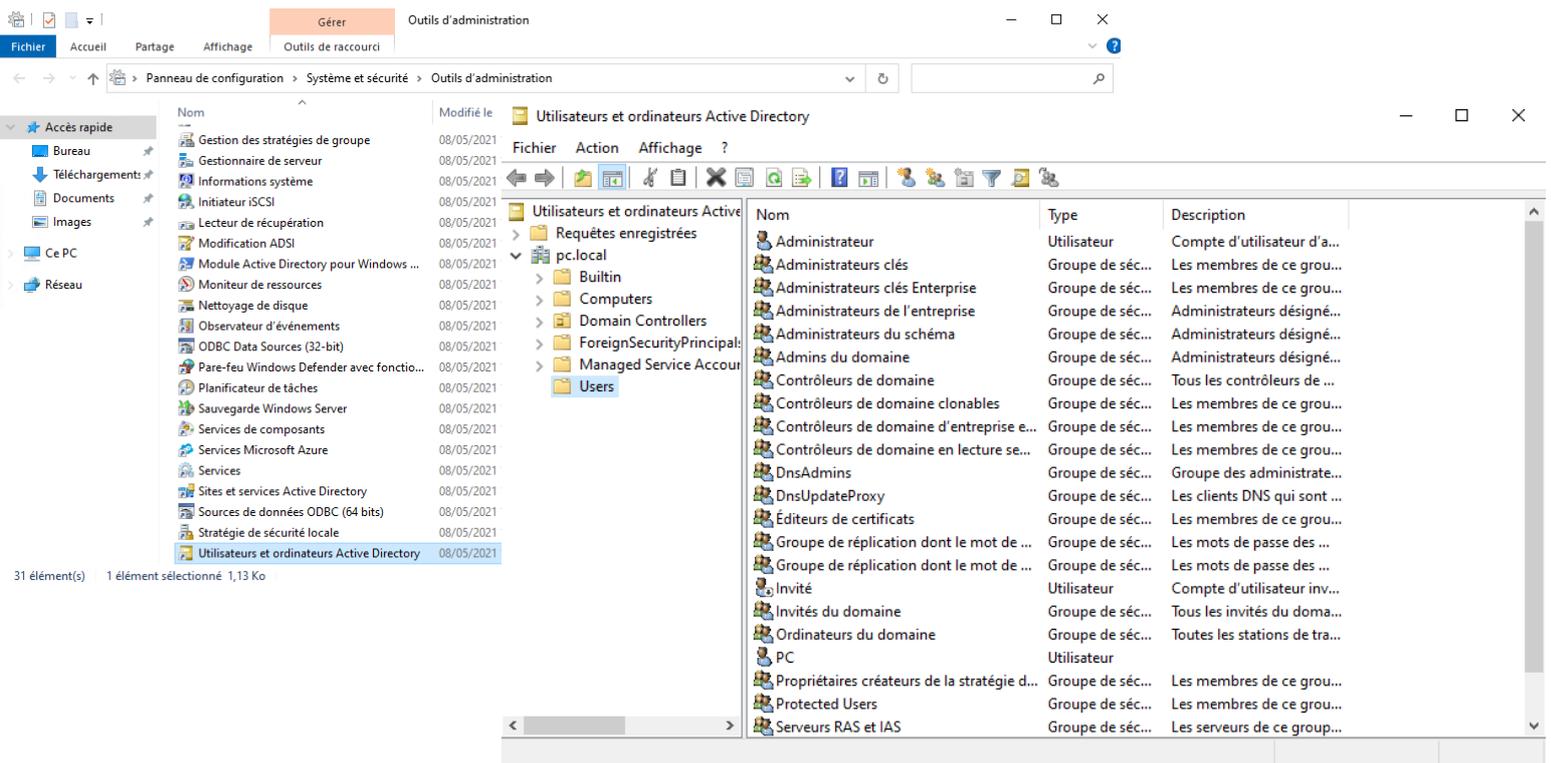
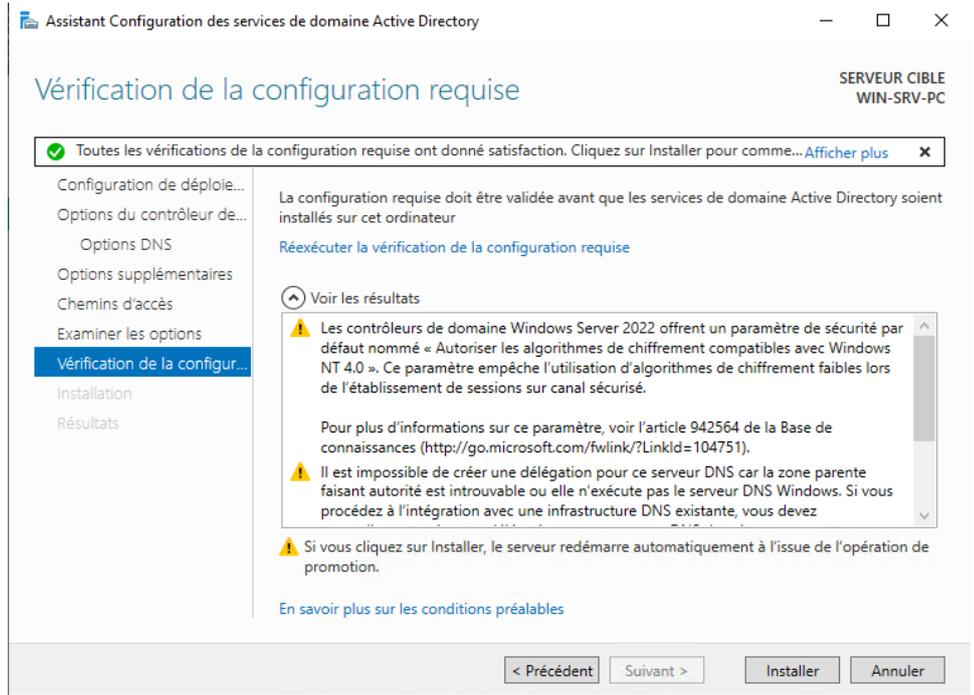


Etant donné qu'on part de zéro on va ajouter une nouvelle forêt (ensemble de domaine) et créer un nom de domaine.

On détermine ensuite le niveau fonctionnel qu'on adapte en fonction des autres domaines, dans notre on va donc choisir le niveau le plus élevé. Enfin on définit un mot de passe de restauration.



On vérifie le nom NetBIOS attribué et les chemins d'accès jusqu'à arriver sur la page suivante ou on pourra finalement lancer l'installation.

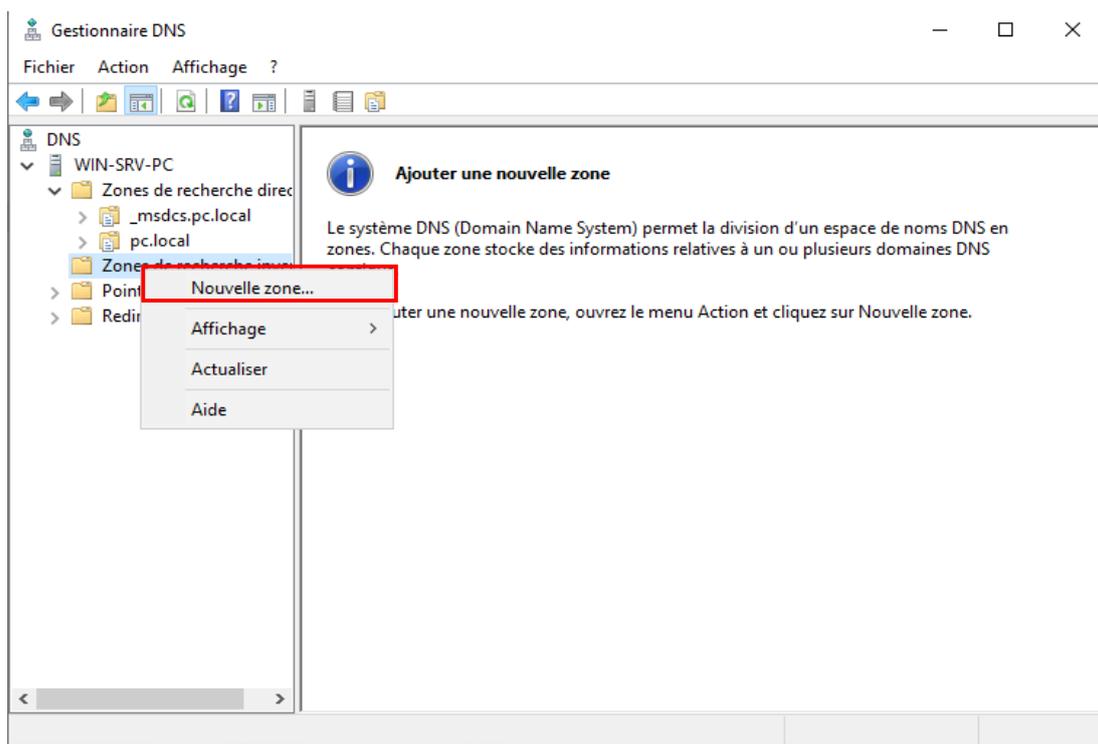
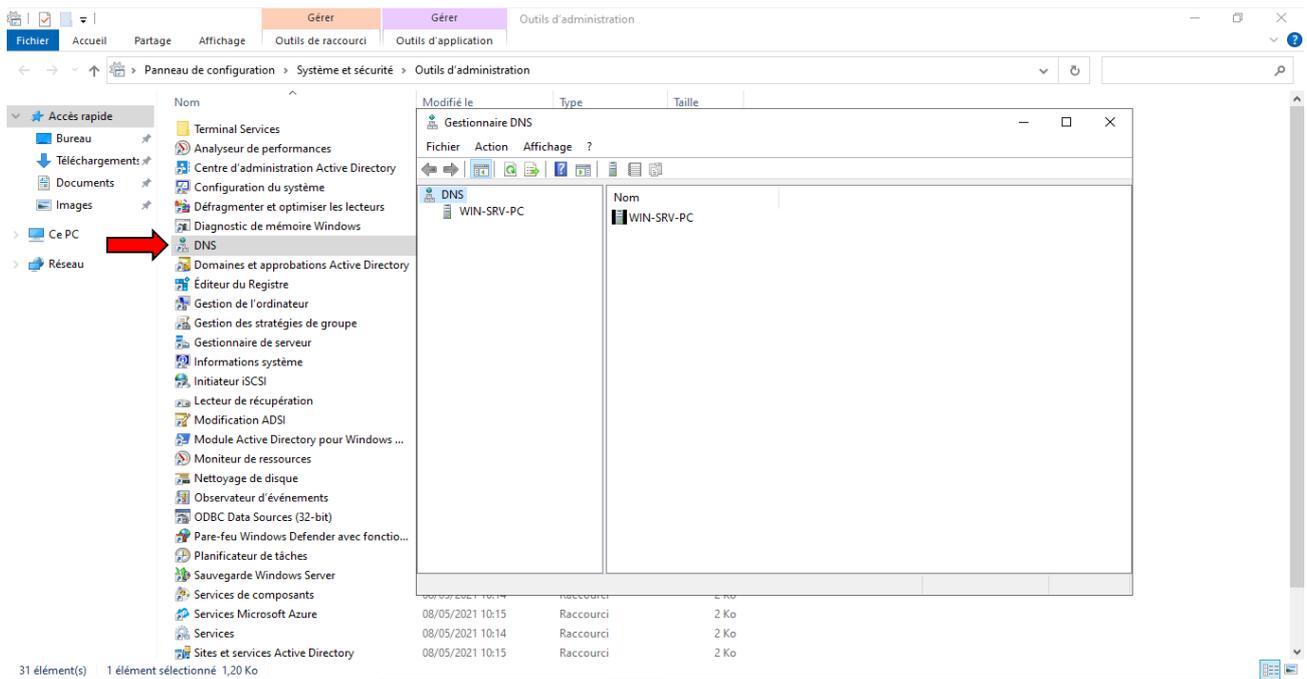


Après l'installation on peut vérifier dans les outils d'administration puis « Utilisateurs et ordinateurs Active Directory » que notre serveur active directory est fonctionnel, ici dans « pc.local » on peut voir l'unité d'organisation « Users » avec les utilisateurs par défaut.

II Paramétrage DNS zone de recherche inversée

La recherche DNS inversée permet de faire la liaison entre une IP et un nom (l'inverse pour une recherche directe). On pourra donc faire la résolution de nom dans les deux sens.

On retourne dans les outils d'administration, dans l'onglet DNS ou on ira chercher « Zone de recherche inversée » pour créer une nouvelle zone.



Assistant Nouvelle zone

**Nom de la zone de recherche inversée**

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



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

ID réseau :

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

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

Nom de la zone de recherche inversée :

On clique sur suivant, on coche « Zone publique » puis la deuxième case qui effectuera une mise à jour de la zone DNS vers tous les contrôleurs de domaine du domaine, on laissera le réglage IPv4, enfin arrivé ici ou on entre l'ID du réseau.

On autorise les mises à jour uniquement de manière sécurisée et on peut valider.

Par défaut les enregistrements préalables à la création de la zone ne se mettent pas dans la zone de recherche inversée, on va donc faire un clic droit sur notre nom de serveur et cocher « Mettre à jour l'enregistrement de pointeur (PTR) associé ».

Gestionnaire DNS

Fichier Action Affichage ?

DNS

- WIN-SRV-PC
 - Zones de recherche direc
 - _msdcs.pc.local
 - pc.local
 - Zones de recherche inver
 - 10.168.192.in-addr.arpa
 - Points d'approbation
 - Redirecteurs conditionne

Nom	Type
_msdcs	
_sites	
_tcp	
_udp	
DomainDnsZones	
ForestDnsZones	
(identique au dossier parent)	Source de nom (SOA)
(identique au dossier parent)	Serveur de noms (NS)
(identique au dossier parent)	Hôte (A)
win-srv-pc	Hôte (A)

Propriétés de : win-srv-pc

Hôte local (A) Sécurité

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

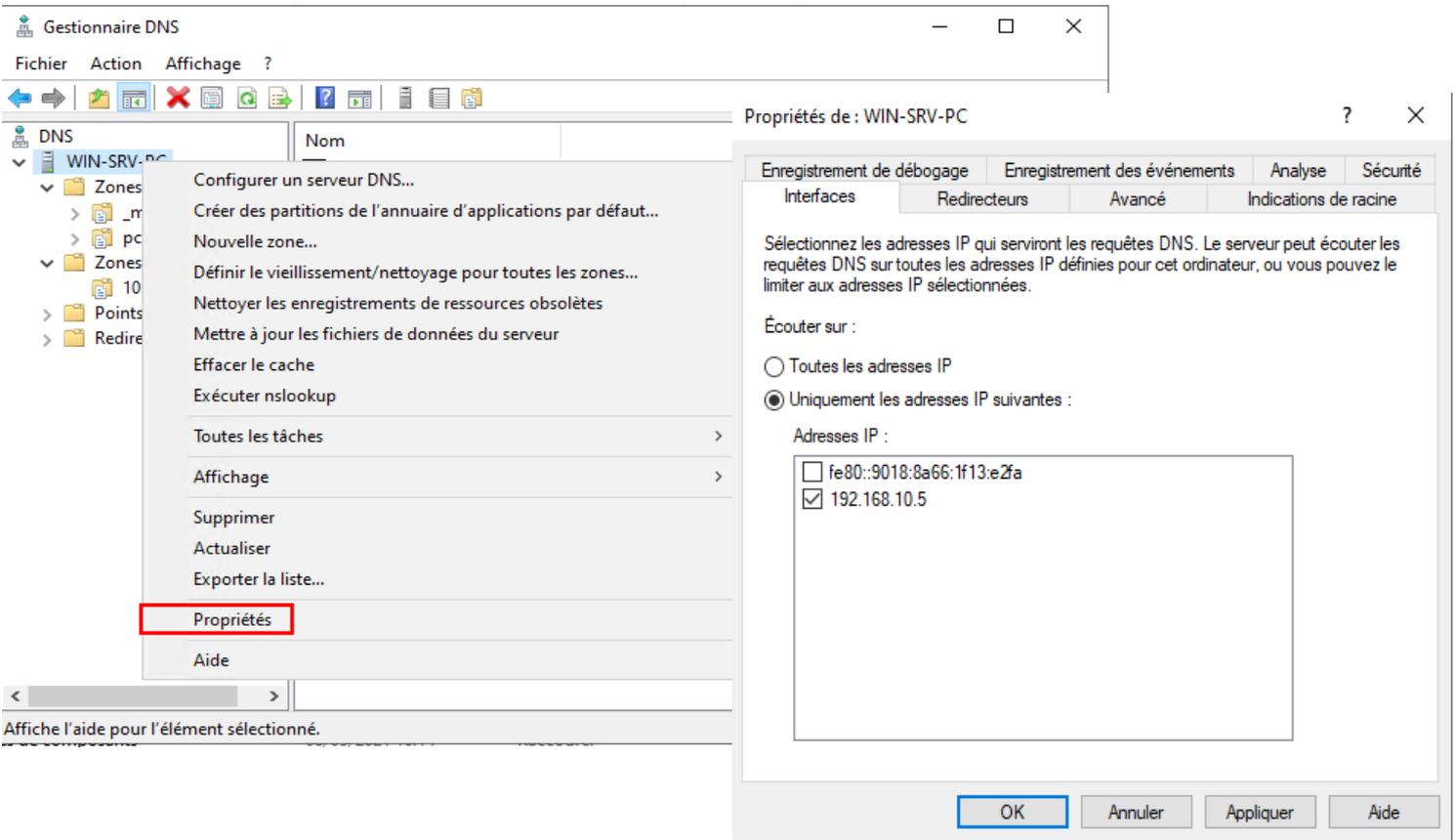
Nom de domaine pleinement qualifié (FQDN) :

Adresse IP :

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

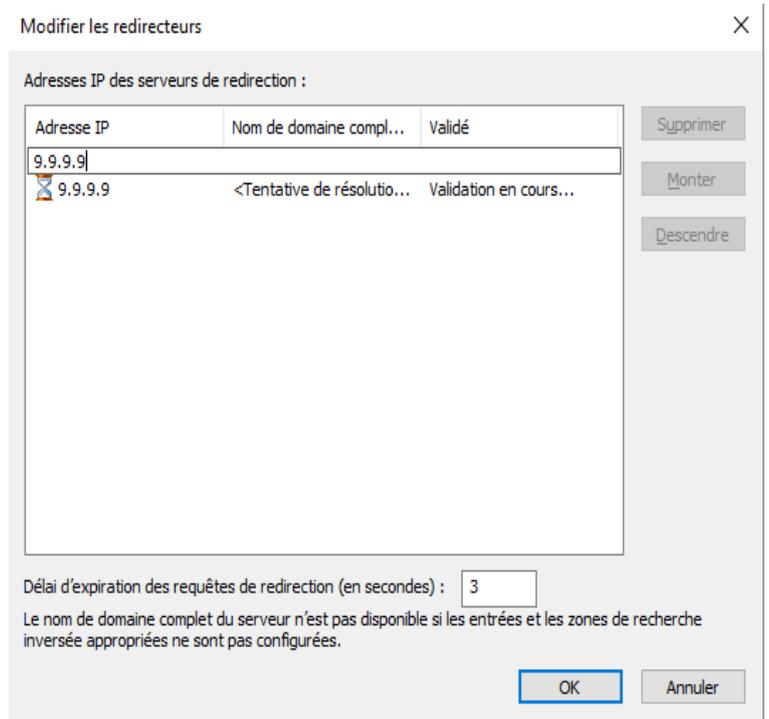
OK Annuler Appliquer

Si on n'utilise pas l'IPv6 il est préférable de décocher la case d'adresse IPv6 et donc de garder uniquement les réponses sur l'IPv4. Pour cela on va simplement faire un clic droit sur le nom de notre serveur, puis dans « Propriétés » décocher la case concernée.



Enfin on définira un redirecteur, dans le cas où le serveur n'arrive pas à faire la résolution de nom il posera la question à ce redirecteur.

Pour les requêtes internet par exemple qui seront transférées à un autre serveur DNS du côté d'internet, on choisira l'adresse 9.9.9.9.



Le serveur DNS est bien paramétré on peut le vérifier en ouvrant le cmd et en faisant un « ping nomdedomaine », on s'aperçoit que la requête aboutit donc notre configuration est fonctionnelle.

```
C:\Users\user>ping pc.local

Envoi d'une requête 'ping' sur pc.local [192.168.10.5] avec 32 octets de données :
Réponse de 192.168.10.5 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 192.168.10.5:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

III Mise en place de stratégies de groupe (GPO)

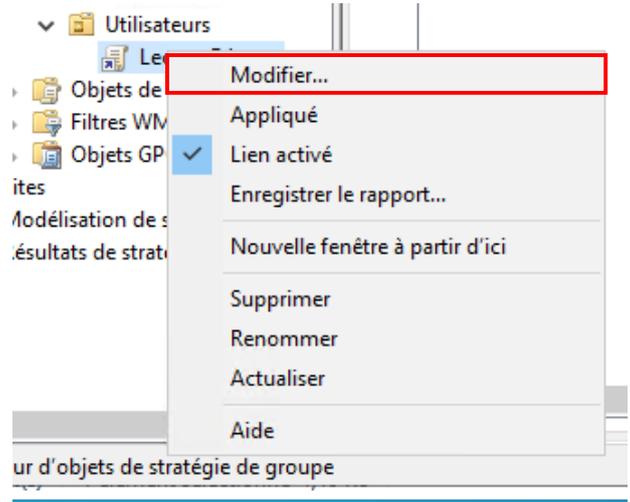
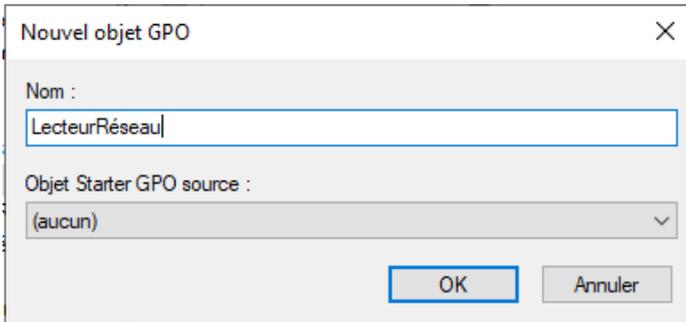
Le but des stratégies de groupes est d'automatiser certains paramètres pour les appliquer à tous les futurs utilisateurs du domaine, cela nous évitera de devoir faire le paramétrage pour chaque PC ou utilisateur.

On revient dans les outils d'administration et on ira cette fois dans « Gestion des stratégies de groupes ».

The screenshot shows the Windows Administrative Tools window. On the left, the 'Gestion des stratégies de groupe' (Group Policy Management) console is open, displaying a tree view of the 'Forêt : pc.local' domain. The 'Utilisateurs' (Users) folder is selected. A right-click context menu is open over the 'Utilisateurs' folder, and the option 'Créer un objet GPO dans ce domaine, et le lier ici...' is highlighted with a red box. A red arrow points to the 'Utilisateurs' folder in the tree view.

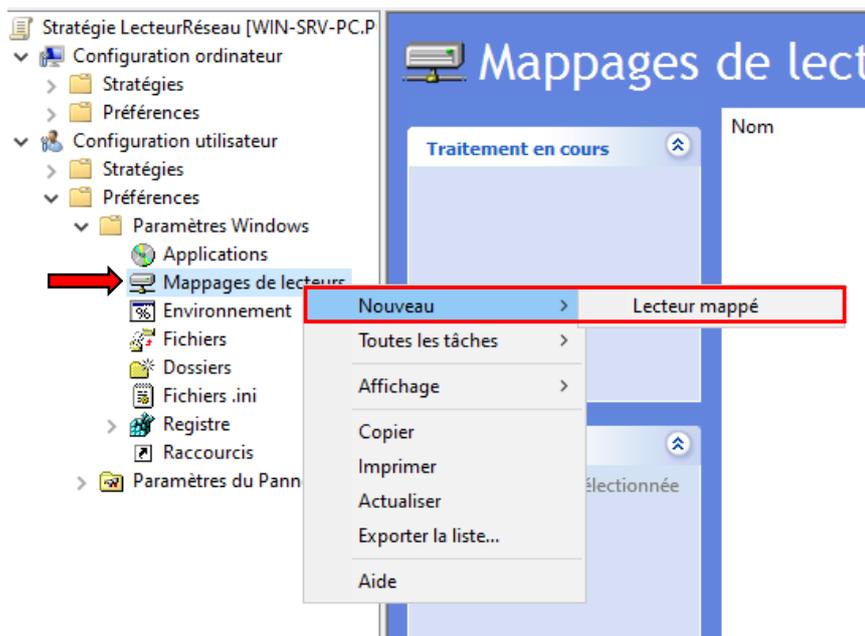
Une fois dans le gestionnaire, on déroule l'arborescence jusqu'à arriver sur « Utilisateurs » puis on fait un clic droit pour aller dans « Créer un objet GPO dans ce domaine, et le lier ici ».

On va créer une stratégie pour donner accès à un lecteur réseau donc on donnera un nom assez explicite. Dans le menu utilisateur on fait un clic droit sur l'objet qu'on vient de créer puis « Modifier ».



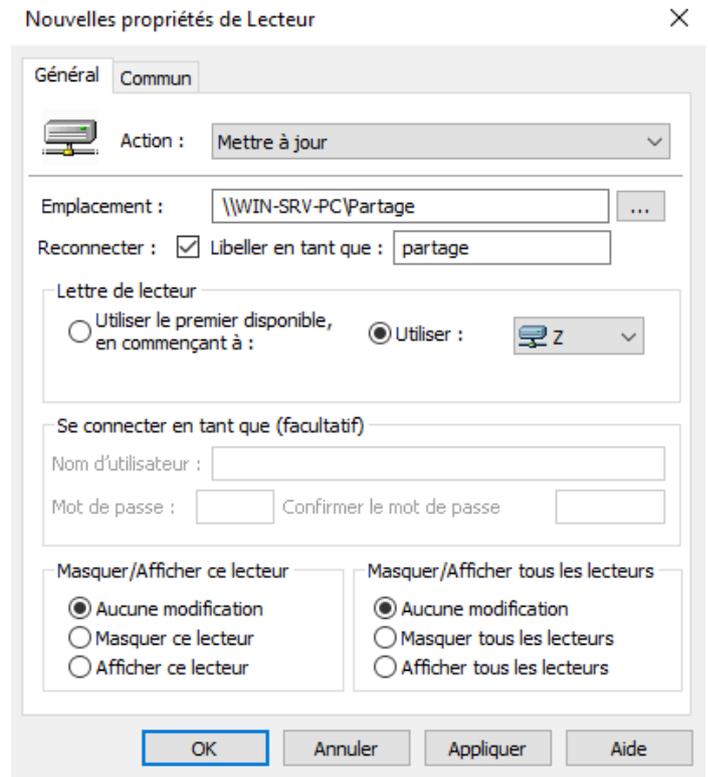
Ici on va aller dans « Configuration utilisateur », « Préférences », « Paramètres Windows » puis « Mappages de lecteurs ».

Selon le mode de paramétrage que l'on souhaite faire on optera pour la configuration utilisateur ou la configuration ordinateur, la configuration utilisateur permet de configurer un paramètre pour un utilisateur quel que soit l'ordinateur qu'il utilise, la configuration ordinateur permet à n'importe quel utilisateur se connectant à l'ordinateur choisit d'accéder aux données paramétrés.

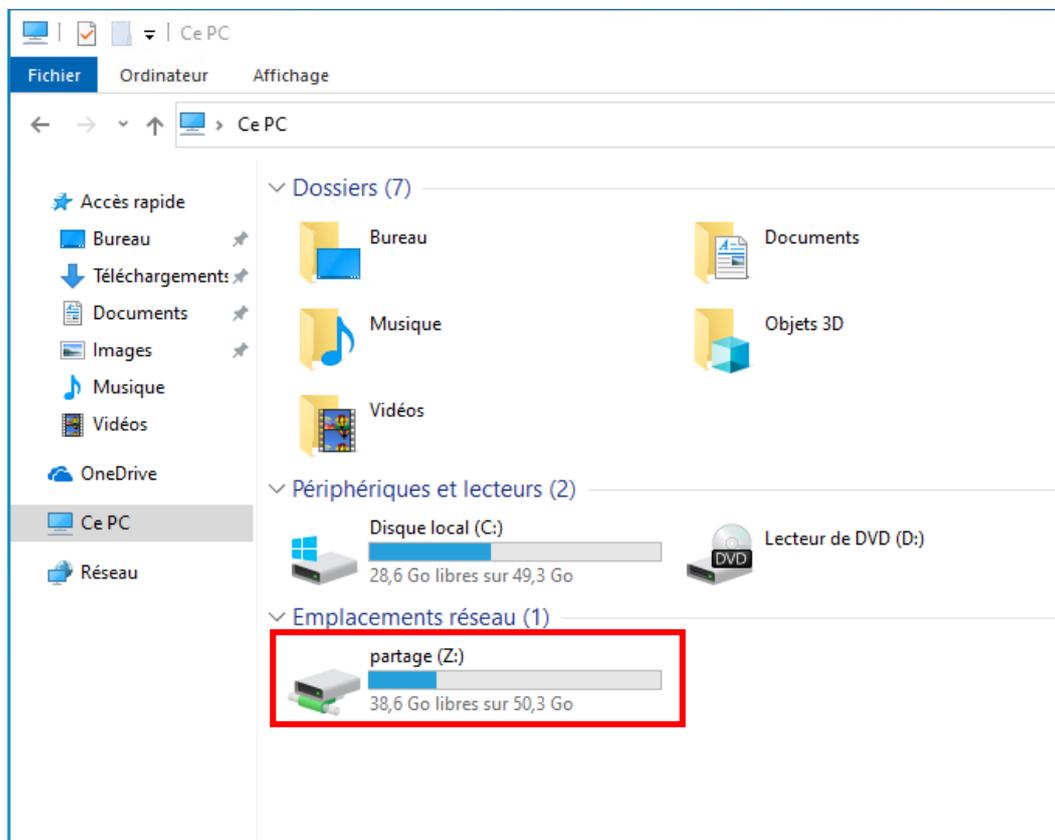


Le fait de sélectionner « Mettre à jour » modifiera la lettre du lecteur si elle est déjà prise sur un ordinateur, ensuite on renseigne l'emplacement du lecteur et lui donne un nom approprié, puis on choisit une lettre à notre lecteur, il est préférable de choisir une lettre en commençant par la fin pour éviter qu'elle soit déjà prise par un autre périphérique.

Ceci fait on peut appliquer les paramètres et cliquer sur « OK » .



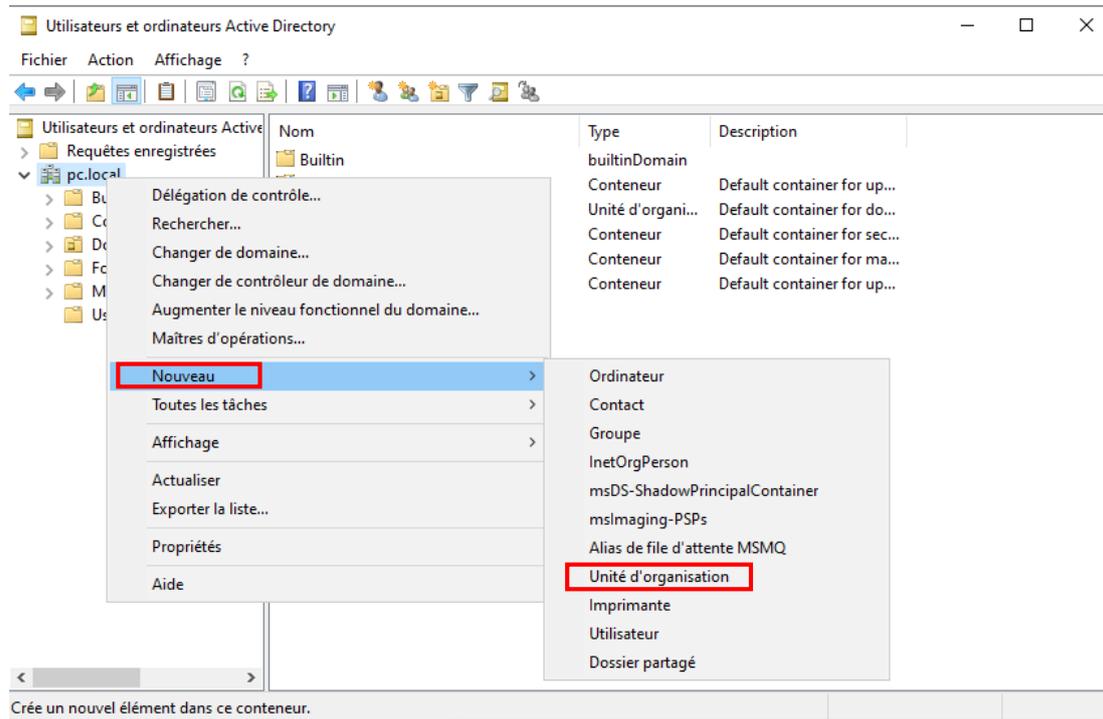
On peut maintenant retourner sur notre client pour vérifier si la stratégie mise en place est bien effective, on voit que le lecteur « partage (Z :) est bien visible et accessible.



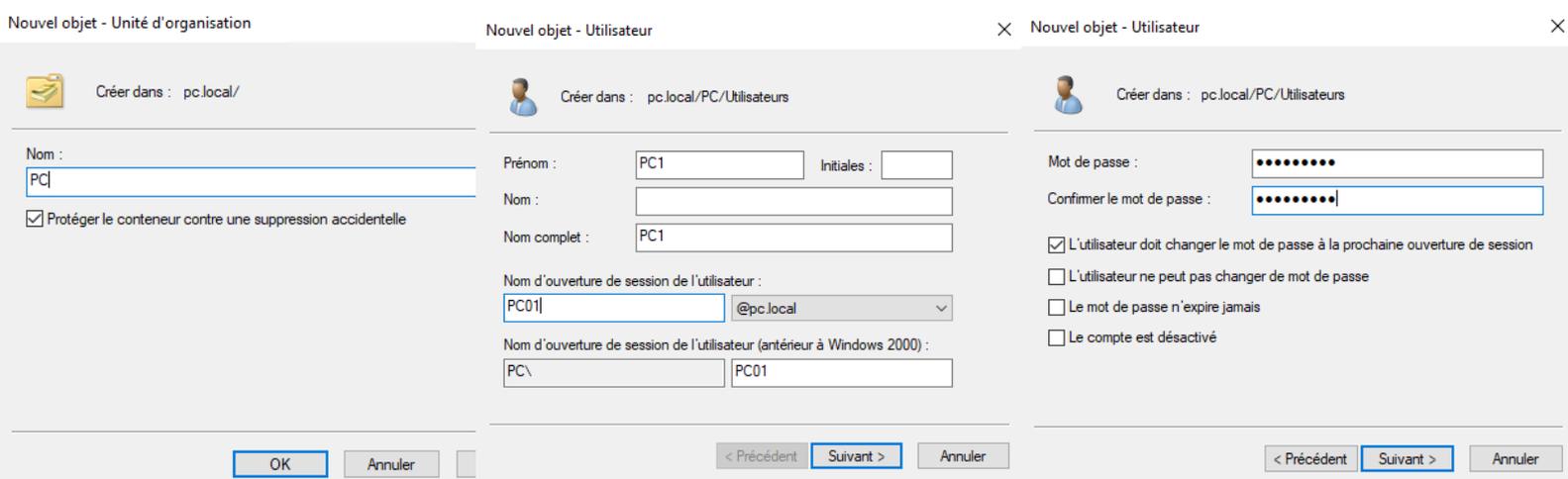
IV/ Intégration au domaine AD

Maintenant nous allons intégrer un poste client à notre serveur active directory.

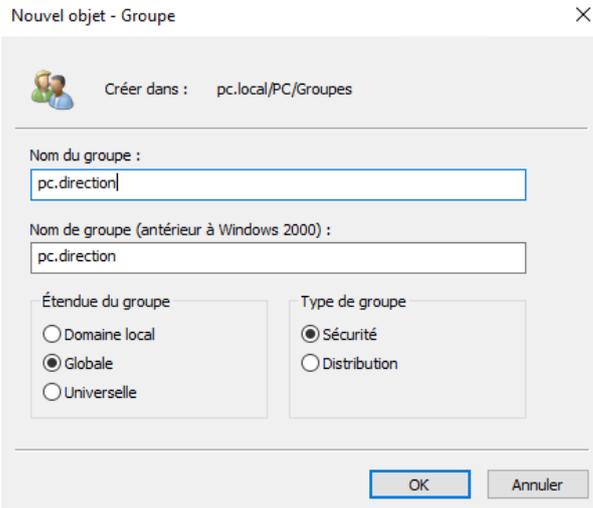
Dans les outils d'administration on va aller dans « Utilisateurs et ordinateurs Active Directory », puis clic droit sur notre serveur, « Nouveau », « Unité d'organisation ».



On créer tout d'abord une unité d'organisation (ici « PC ») puis dans cette unité on va créer notre utilisateur et lui choisir un mot de passe.



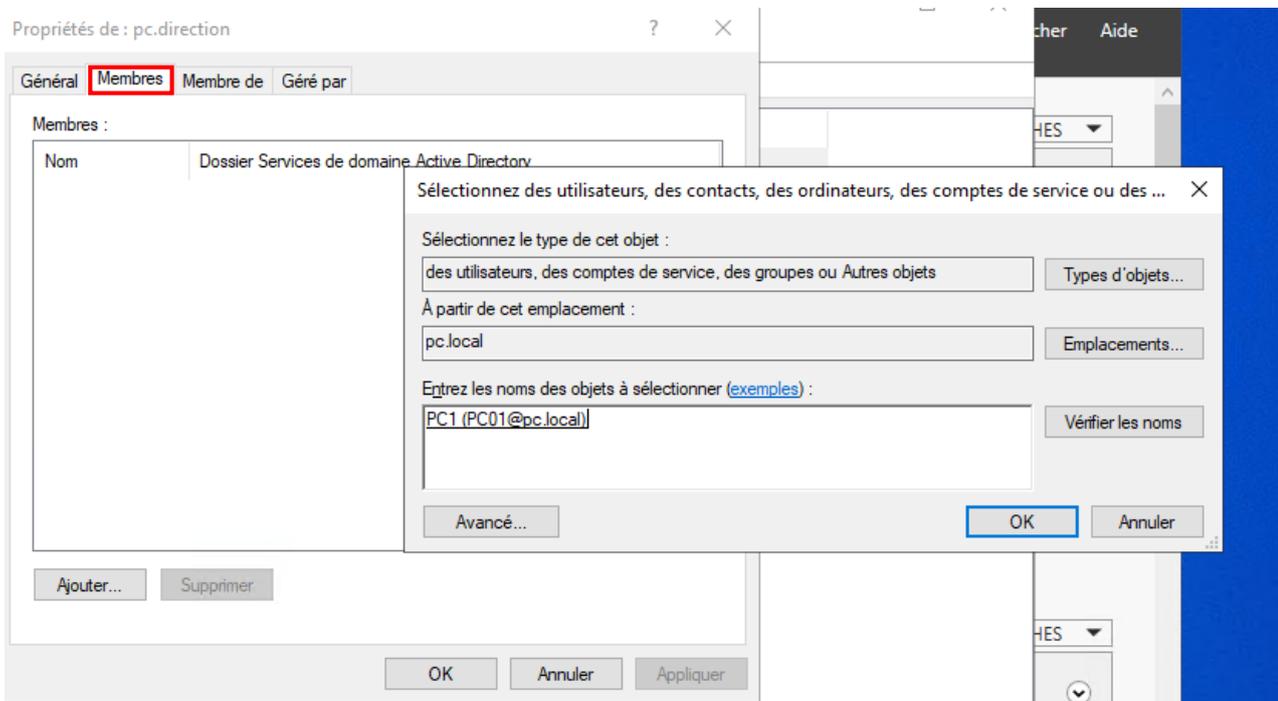
On va ensuite créer un groupe pour cet utilisateur, pour pouvoir les droits de plusieurs utilisateurs à la fois.



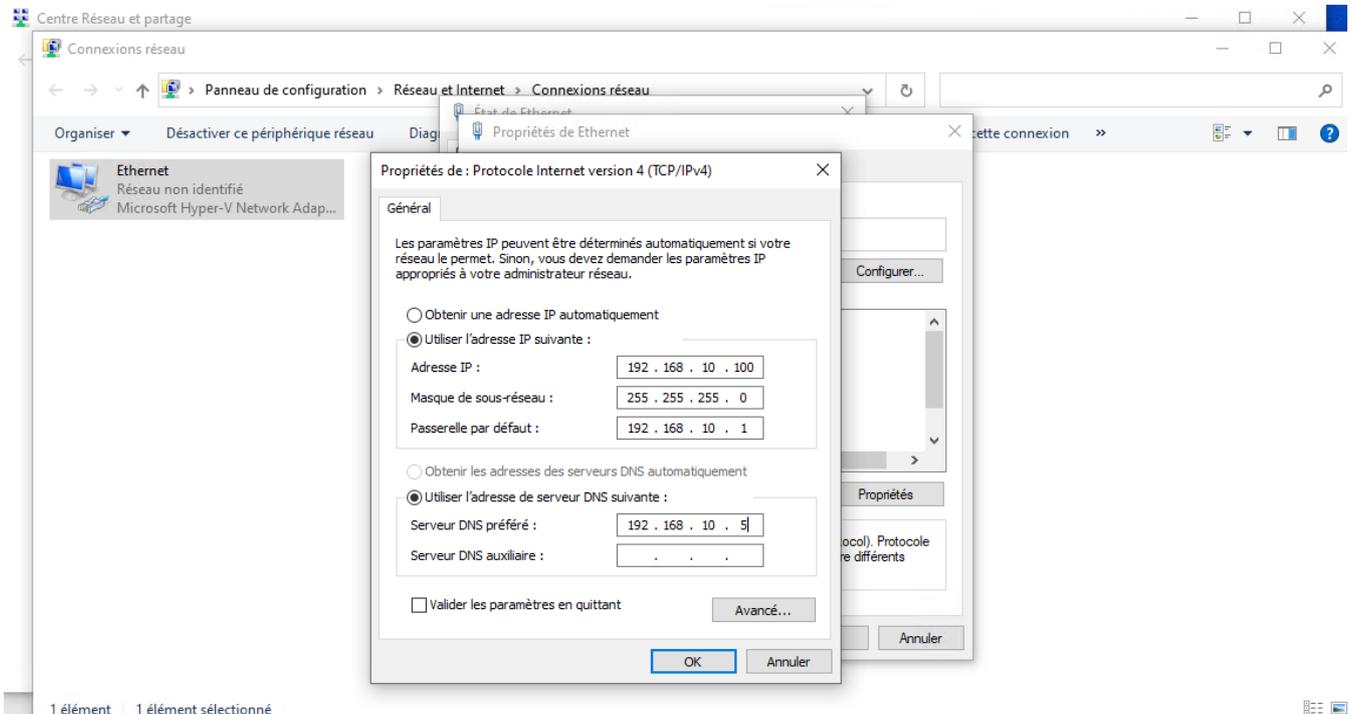
Dans le type de groupe on choisira sécurité pour les droits d'accès ou distribution pour les listes de distribution email.

Pour l'étendue du groupe, domaine local sera pour le domaine en cours uniquement, globale pour tous les domaines de la forêt mais uniquement des utilisateurs de notre domaine, et enfin universelle sera pour tous domaines de la forêt et tous les utilisateurs peu importe le domaine de la forêt.

Une fois notre groupe créer on clique sur celui-ci et on y ajoute dans l'onglet membre notre utilisateur.



On va maintenant se rendre sur notre VM Windows 10 pro et dans un premier temps paramétrer les adresses DNS, on se rend donc dans le panneau de configuration, « réseau et internet » puis « connexion réseau », ensuite clic droit propriétés, « adresse IPv4 » et ici on renseigne manuellement l'adresse IP (par défaut dans notre réseau donc ici 192.168.10.xxx) le masque de sous-réseau la passerelle et le serveur DNS préféré.



Pour vérifier si tout fonctionne correctement on va ouvrir le cmd (Touche « Windows » + « R » et taper « cmd ») en tapant la commande « ipconfig /all » on pourra voir si on retrouve bien nos informations, puis on fera une requête « ping » (taper « ping 192.168.10.5 ») pour voir si la connexion entre le client et le serveur est bien établie.

```
C:\Windows\system32\cmd.exe
DHCP activé. . . . . : Non
Configuration automatique activée. . . . . : Oui
Adresse IPv6 de liaison locale . . . . . : fe80::31f7-70d4-e0f6-8d42%12 (préféré)
Adresse IPv4. . . . . : 192.168.10.100 (préféré)
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . : 192.168.10.1
IAID DHCPv6 . . . . . : 100668765
DUID de client DHCPv6. . . . . : 00-01-00-01-2A-AB-B3-90-00-15-5D-08-0D-3B
Serveurs DNS. . . . . : 192.168.10.5
                       9.9.9.9
NetBIOS sur Tcpip. . . . . : Activé

C:\Users\user>192.168.10.5
'192.168.10.5' n'est pas reconnu en tant que commande interne
ou externe, un programme exécutable ou un fichier de commandes.

C:\Users\user>ping 192.168.10.5
Envoi d'une requête 'Ping' 192.168.10.5 avec 32 octets de données :
Réponse de 192.168.10.5 : octets=32 temps<1ms TTL=128

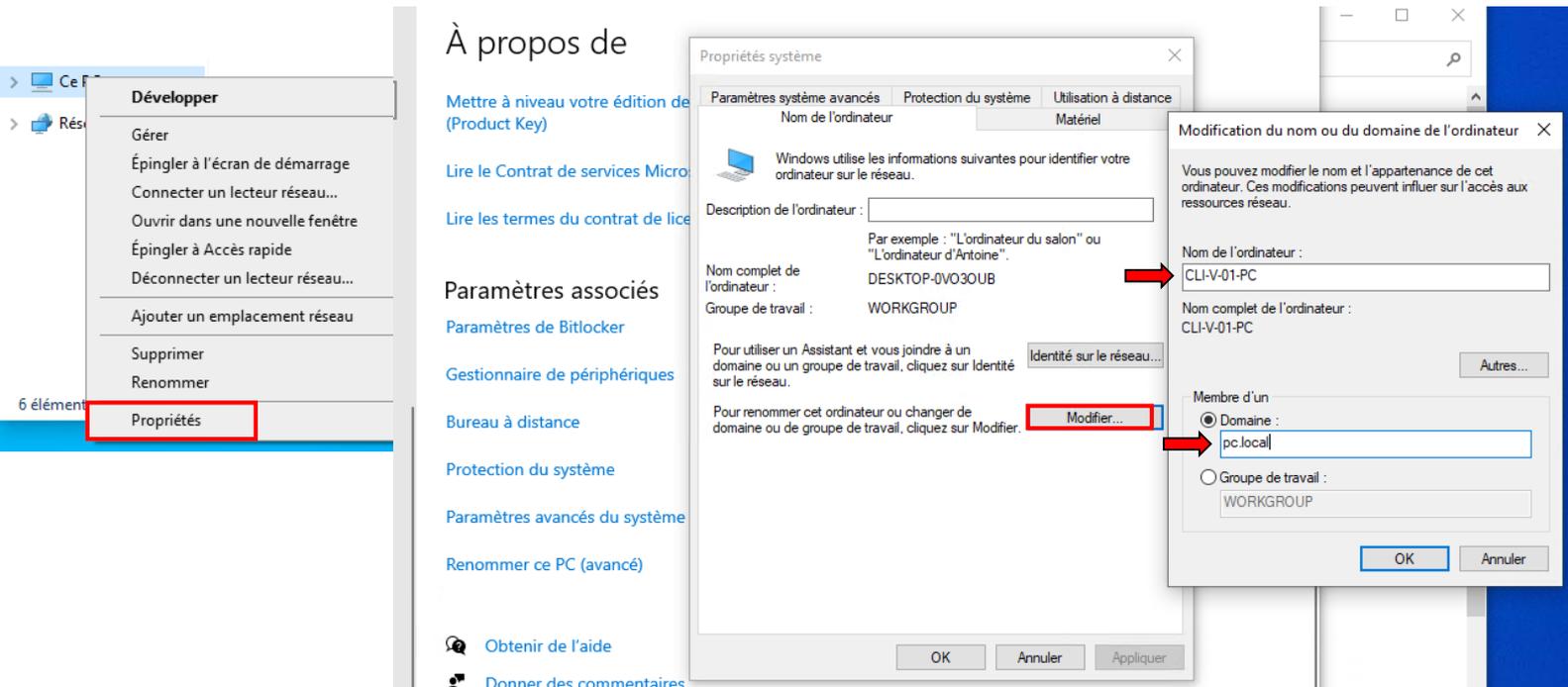
Statistiques Ping pour 192.168.10.5:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\user>
```

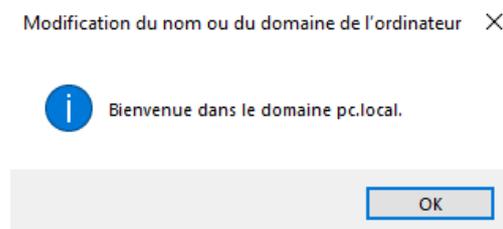
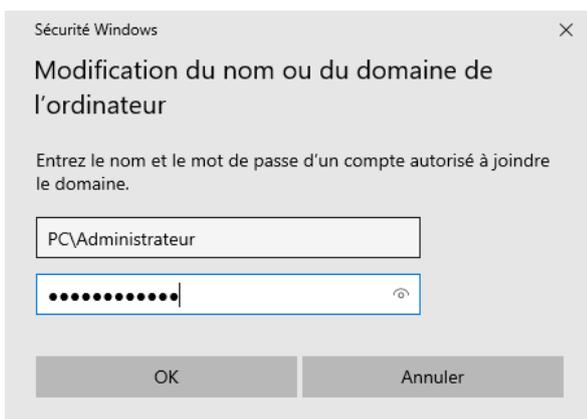
Avec la commande « nslookup » on vérifie si on est bien sur notre serveur avec la bonne adresse.

```
C:\Users\user>nslookup
Serveur par défaut : WIN-SRV-PC.pc.local
Address: 192.168.10.5
```

Maintenant on va pouvoir intégrer notre pc au domaine, dans l'explorateur de fichier on fait un clic droit sur « Ce PC », « Propriétés », ensuite dans les propriétés système on va modifier le nom de l'ordinateur pour un plus clair et l'intégrer à notre domaine.

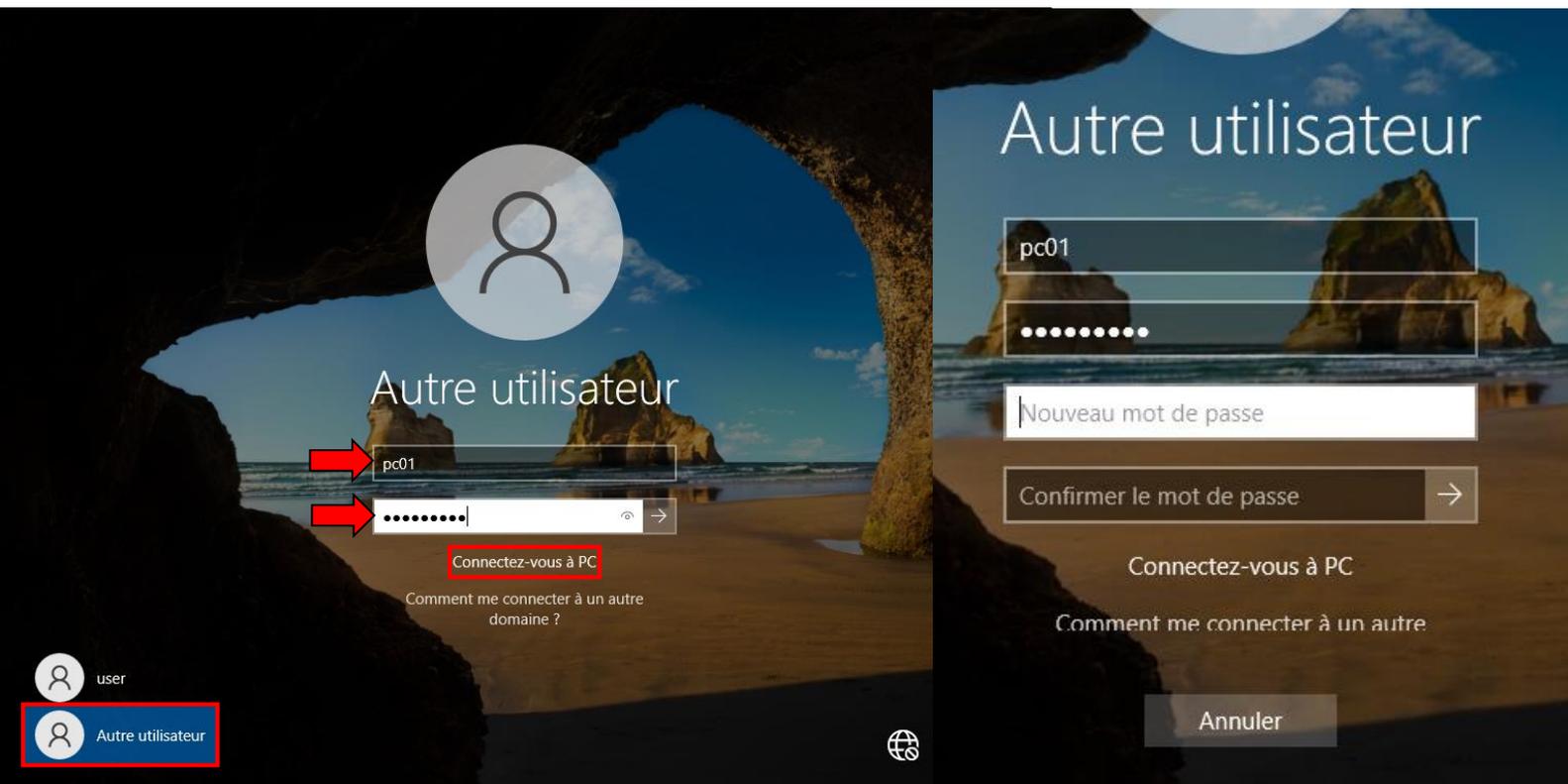


Après avoir cliqué sur « OK » on va nous demander de nous authentifier, on va donc se connecter avec le compte administrateur du domaine et le mot de passe du domaine (pour l'identifiant il sera ici noté « nomdedomaine\Administrateur »). On peut voir avec le pop-up qui apparait que nous sommes bien dans le domaine.

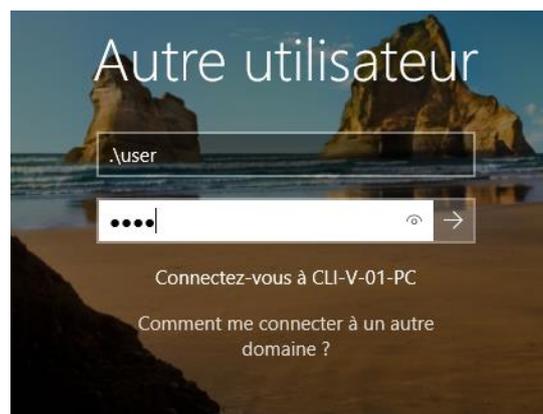


Pour que le changement prenne effet on fera un redémarrage.

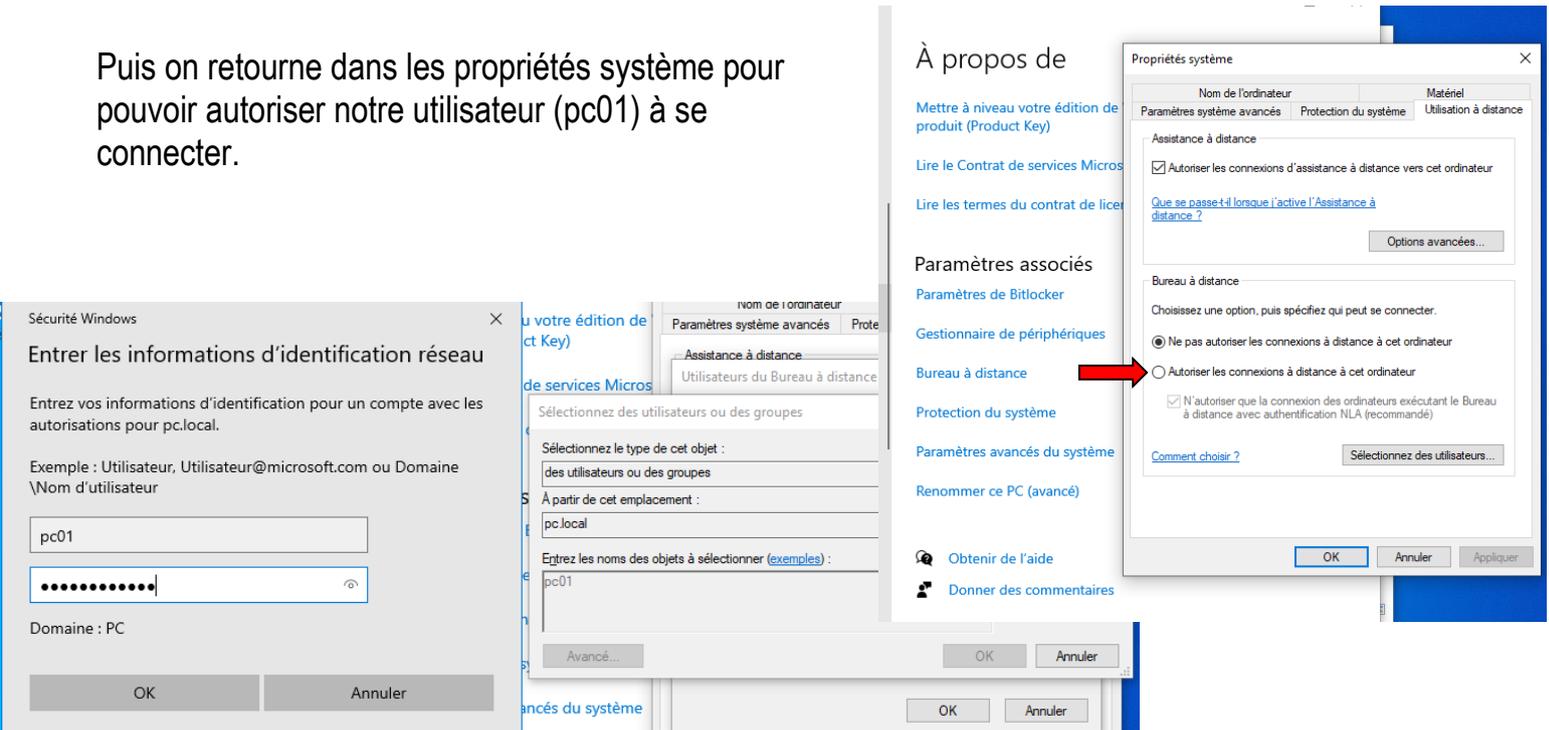
Une fois la machine redémarré on va pouvoir tester si notre utilisateur peut se connecter, en faisant « Autre utilisateur » on remplit simplement les champs «Identifiant » et « mot de passe » avec les informations qu'on a choisi plus tôt (on remarque également qu'on nous propose directement de nous connecter à notre domaine). Comme on l'avait coché plus haut on nous demande de changer notre mot de passe après notre première connexion, cela aura surtout du sens pour que les utilisateurs choisissent directement leur propre mot de passe, dans notre cas on va le changer pour le test.



Si un message d'erreur apparaît par rapport à la connexion via le bureau à distance c'est à cause du fait que dans notre cas on utilise une machine virtuelle qui utilise le protocole bureau à distance, on va donc se reconnecter avec le compte précédent (ici « user »).



Puis on retourne dans les propriétés système pour pouvoir autoriser notre utilisateur (pc01) à se connecter.



Une authentification nous sera demander encore une fois on entrera à nouveau nos identifiant administrateur.

Cette manipulation est spécifique à notre cas, en temps normal ça serait plutôt déconseillé d'autoriser les connexion bureau à distance pour éviter d'éventuelles failles de sécurité.

V/ Conclusion

Pour conclure nous avons pu mettre en place un serveur active directory paramétré ses adresse DNS ainsi qu'une recherche DNS inversé, nous avons également établi une stratégie de groupe pour pouvoir accéder à un lecteur réseau, des unités d'organisations et finalement créé un utilisateur qu'on aura fait rejoindre notre domaine.