[2023-2024]

# Tutoriel Serveur Annuaire

ADMINISTRATION D'ACTIVE DIRCTORY

FIRAS RASSAA

# I. Introduction

## A. Les protocoles indispensables de l'Active Directory

Les trois protocoles LDAP, DNS et Kerberos. Sont vitaux au bon fonctionnement de l'Active Directory. Ils assurent 3 fonctions critiques :

- La gestion de l'annuaire (LDAP)
- La communication et la résolution des noms (DNS)
- L'Authentification et la gestion des sessions (Kerberos)

### 1. Le protocole LDAP

#### a) Présentation

Le protocole LDAP (Lightweight Directory Access Protocol) permet de gérer des annuaires, notamment grâce à des requêtes d'interrogations et de modification de la base d'informations. L'Active Directory est un annuaire LDAP.

Les communications LDAP s'effectuent sur le port 389, en TCP, du contrôleur de domaine cible. Il existe une déclinaison du protocole LDAP appelée LDAPS (LDAP over SSL) est qui apporte une couche de sécurité supplémentaire avec du chiffrement.

#### b) Contenu

L' Active Directory est l'annuaire LDAP de Windows Serveur. Il contient un ensemble d'unités d'organisation ("Organisation Units" en anglais = OU), représentées sous la forme de dossiers qui forment l'arborescence générale. Ensuite, on trouve tous les différents types d'objets classiques :

- Utilisateurs
- Ordinateurs
- Groupes
- Contrôleurs de domaine
- Serveurs
- imprimante

Pour chaque classe d'objets, il stocke les attributs correspondants et les différentes valeurs de ces attributs pour chaque instance d'un objet.

**Par exemple :** Il va stocker toutes les informations relatives à l'utilisateur Marc Dupuis :

- Les **informations** sont les attributs (nom, prénom, description, mot de passe, email, etc.)
- **Utilisateur** est la classe d'objet
- **Marc Dupuis** est l'objet

#### c) Structure

Un annuaire est un ensemble d'entrées, ces entrées étant elles-mêmes constituées de plusieurs attributs. Un attribut, quant à lui, est spécifique et dispose d'un nom qui lui est propre, d'un type et d'une ou plusieurs valeurs.

Chaque entrée dispose d'un identifiant unique qui permet de l'identifier rapidement, de la même manière que l'on utilise les identifiants dans les bases de données pour identifier rapidement une ligne. L'identifiant unique d'un objet est appelé GUID, pour"identificateur unique global", "Global Unique ID", en anglais.

Un nom unique est également attribué à chaque objet, le DN pour "Nom Distinct". "Distinguished Name", en anglais. Il se compose du nom de domaine auquel appartient l'objet ainsi que du chemin complet pour y accéder dans l'annuaire. C'est le chemin à suivre dans l'arborescence d'unités d'organisation (OU) pour arriver jusqu'à cet objet.

Par exemple, le chemin d'accès correspondant à un objet "utilisateur" nommé "Marc Dupuis", du domaine "bts.local" et étant stocké dans une unité d'organisation (OU) nommée "informatique" contenant elle-même une OU nommée "système" :

bts.local, informatique, système, Marc Dupuis

Se traduira en chemin LDAP par la chaîne :
cn=Marc Dupuis, ou=systeme, ou=informatique, dc=bts,dc=local

Cette chaîne correspond au DN (unique) de l'objet.

Dans un chemin LDAP vers un objet, on trouve toujours la présence du domaine sous la forme "dc=bts, dc=local", correspondant à bts.local" dans cet exemple.

## 2. Le protocole DNS

Le DNS (Domain Name System) est utilisé en permanence, notamment pour la navigation sur Internet et à chaque fois que l'on communique avec un serveur, pour ne citer que ces deux cas de figure.

Il en est de même pour l'Active Directory qui fonctionne de pair avec le DNS. Sans le DNS l'Active Directory ne fonctionne pas. C'est d'ailleurs pour ça que lors de la mise en place de l'Active Directory, l'installation du serveur DNS est proposée.

Le protocole DNS est utilisé pour la résolution des noms. Cela permet aux postes clients de localiser les contrôleurs de domaine au sein d'un système d'information. De la même manière, en joignant un poste client dans un domaine, on renseigne le nom de ce domaine, comme "bts.local". Une requête DNS est lancée à la recherche de l'adresse IP correspondant à ce nom. Le contrôleur de domaine traite alors cette requête.

Le serveur DNS crée une zone correspondant à un domaine. Il y conserve de nombreux enregistrements. On y trouve les contrôleurs de domaine, entre autres, mais il existe une multitude d'enregistrements annexes, indispensable au bon fonctionnement de l'Active Directory :
- Enregistrement pour localiser le "**Primary Domain Controller**" : correspondant au

contrôleur de domaine qui dispose d'un ou plusieurs **rôles FSMO** (Flexible Single Master Operation ). Le "maître d'opération" pour certaines tâches sensibles
- Enregistrement pour localiser un contrôleur de domaine qui est catalogue global.
- Enregistrement pour localiser les KDC du domaine (Centre de distribution de clés).
- Enregistrement pour localiser les contrôleurs de domaine du domaine cible.
- Enregistrer simplement la correspondance nom/adresse IP des différents contrôleurs de domaine. Il est également possible de créer un second enregistrement avec les adresses IPv6.
- Enregistrer les contrôleurs de domaine via le GUID pour assurer la localisation dans toute la forêt. Il même est possible d'enregistrer l'ensemble des ordinateurs d'un domaine dans le DNS. Ainsi, un ordinateur de l'entreprise pourra être joint via : pc-01.bts.local s'il se nomme "pc-01".

Le rôle DNS peut être installé sur le contrôleur de domaine principal ou sur un autre serveur DNS du système d'information. Ce serveur DNS peut être sous Windows mais aussi sous Linux en utilisant le paquet "Bind 9" qui requiert une configuration particulière.

Les contrôleurs de domaine doivent être capables d'écrire dans la zone DNS qui leur correspond, ceci dans le but de gérer les enregistrements dynamiquement. Lors de la création d'un domaine, tous les enregistrements nécessaires au bon fonctionnement du système seront créés automatiquement.

### 3. Le protocole Kerberos

Le protocole Kerberos est assure la gestion de l'authentification au sein d'un domaine, de manière sécurisée, avec un mécanisme de distribution de clés. Il n'intervient ni dans l'annuaire (LDAP), ni dans la résolution de noms (DNS).

#### a) Fonctionnement

Chaque contrôleur de domaine dispose d'un service de distribution de clés de sécurité, appelé "Centre de distribution de clés", "Key Distributtion center" en anglais : KDC. Il réalise 2 services :
- Un service d'authentification. "Authentication Service" – AS, en anglais

Ce service distribue des tickets spéciaux appelés "TGT" pour "Ticket-Granting Ticket" qui permettent d'effectuer d'autres demandes d'accès auprès du service d'émission de tickets, la "Ticket-Granting Service" , "TGS".

Avant qu'un client puisse obtenir un accès sur un ordinateur du domaine, il doit obtenir un TGT depuis le service d'authentification du domaine cible. Une fois que le service d'authentification retourne le TGT, le client dispose de l'autorisation pour effectuer sa demande auprès du TGS.

Ce TGT obtenu pourra être réutilisé jusqu'à ce qu'il expire, mais la première demande qui déclenchera la création d'un nouveau TGT requiert toujours un passage par le service d'authentification.

- Un service d'émission de tickets, le "Ticket-Granting Service" - TGS)

Ce service distribue des tickets aux clients pour la connexion de la machine du domaine. Quand un utilisateur se connecte à un ordinateur par son identifiant et son mot de passe, il contacte le service d'émission de tickets correspondant au domaine auquel appartient l'ordinateur et obtient (s'il est reconnu) un TGT. Pour obtenir un ticket d'accès sur l'ordinateur, le TGT est présenté. S'il est accepté, l'utilisateur obtient alors un ticket TGS.

Ces 2 services ont chacun des tâches et un processus précis. Ce mécanisme d'authentification permet d'accéder aux ressources d'un domaine. Sans Kerberos, il n'y a pas d'authentification, sans authentification, il n'y a pas d'accès.
Si le centre de distribution de clés (KDC) est indisponible sur le réseau local, l'Active Directory est indisponible également et le contrôleur de domaine ne fonctionne plus.

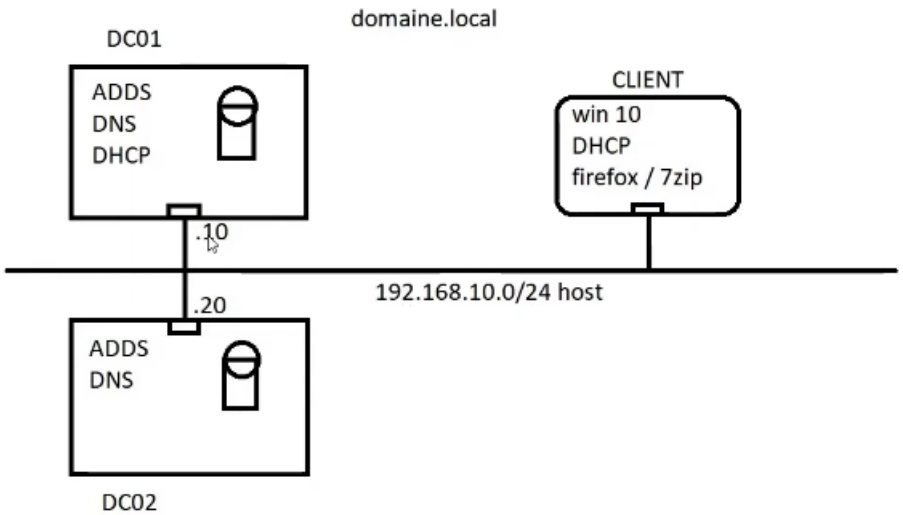
b) Contenu d'un ticket Kerberos

Un ticket Kerberos contient de nombreuses informations qui permettent d'identifier l'élément auquel il est attribué. Par exemple, pour un utilisateur, il contient son nom, son mot de passe, l'identité du poste initial ainsi que la durée de validité du ticket et sa date d'expiration.

Par ailleurs, les tickets TGS et TGT contiennent une clé de session qui permet de chiffrer les communications suivantes afin de sécuriser les échanges

## II-Installation d'une machine virtuelle

A-Présentation du Tp



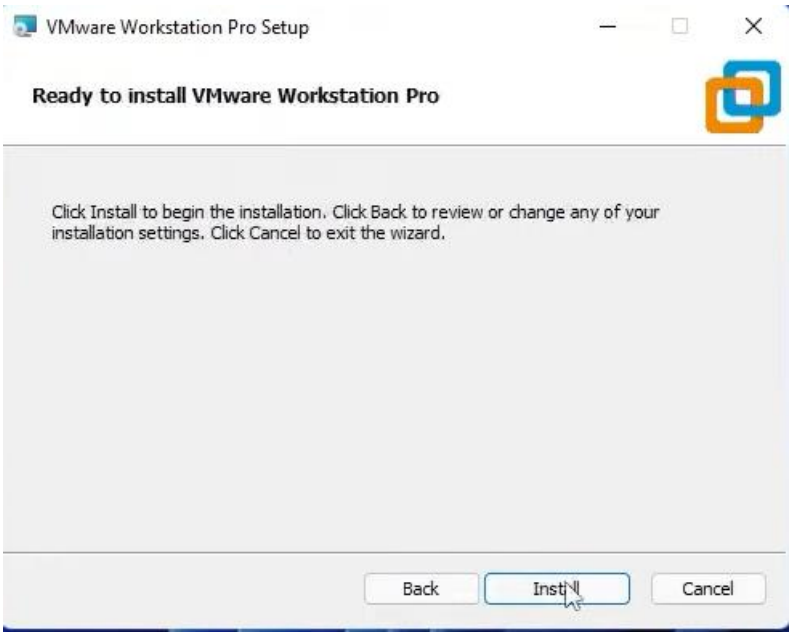
Pour ce tp nous allons créer un domaine que l'on nommera domaine.local, dans ce domaine nous aurons 3 machine dont un serveur avec un adds, dns, dhcp et un stockage de fichier, il y aura un autre serveur avec un adds et un dns et on répliquera le stockage de fichier enfin on montera une machine client en windows 10 avec un dhcp et grâce à des gpo on lui installera firefox et 7zip

Nous avons utilisé Vmware qui est un hyperviseur qui permettra de mettre 3 machines : avec Windows Server2016 et Windows 10 afin de créer un serveur annuaire et créer un domaine.

- Aller sur internet et chercher Vmware afin de créer plus tard trois machines virtuelles

**https://www.vmware.com/products/workstation-pro/workstation-pro-evaluation.html**

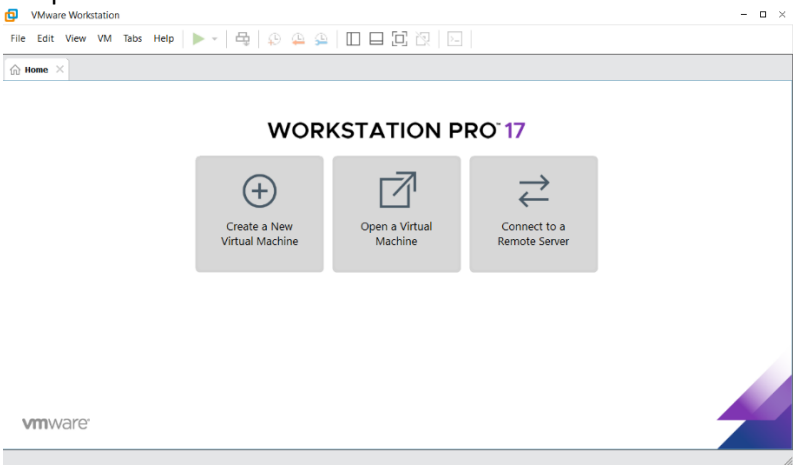

**Télécharger la version compatible à votre Pc**



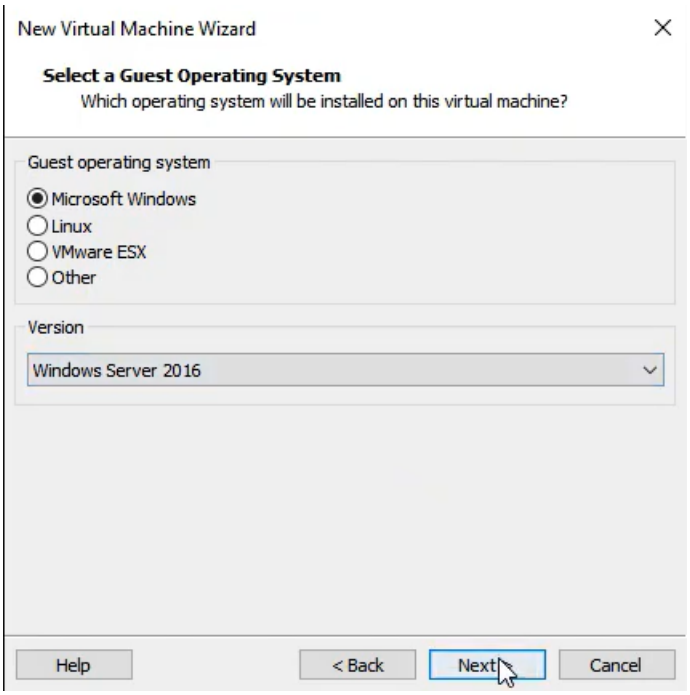

Une fois l'installation terminer crée vos machine virtuelle.

## III-Création d'une machine virtuelle avec Windows Server 2016

-Cliquer sur créer une nouvelle machine virtuelle

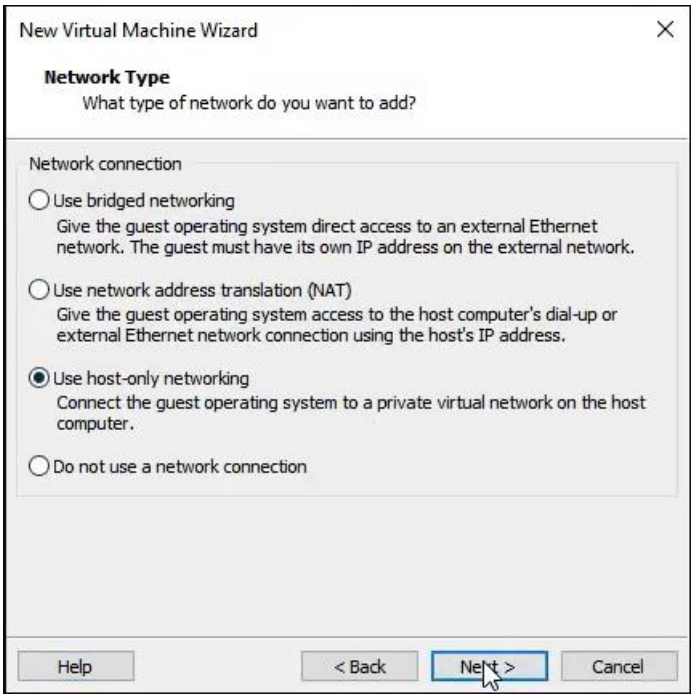



Pour la machine serveur choisissez l'OS windows serveur 2016




-Renommer votre machine à votre manière, pour ma part la première machine sera renommée en DC01, la deuxième en DC02 enfin la dernière en Client

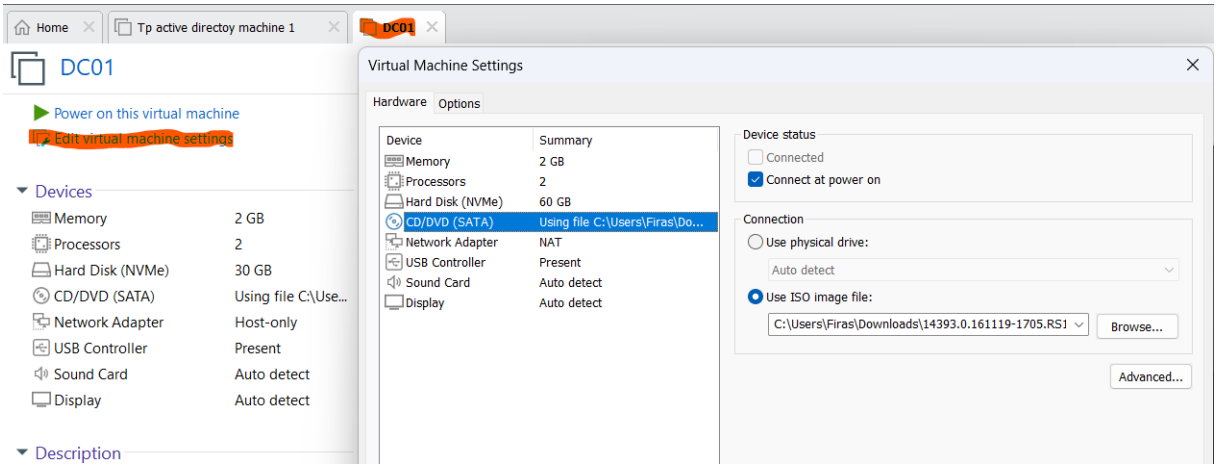
Pour les machines serveur mettez vous en host-only comme sur l'image ci-dessous




Pour la machine client choisissez windows 10 64 bit.
Pour les 3 machine, il faut un disque virtuelle de 30 giga

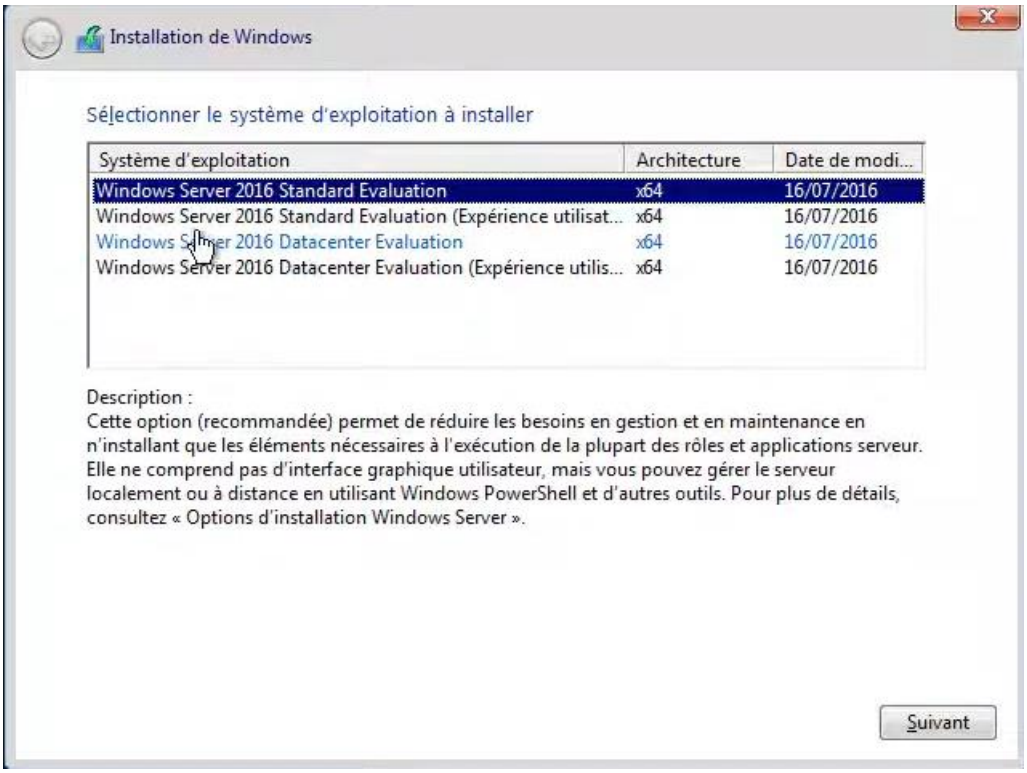
Ensuite télécharger l'ISO de Windows Server 2016 sur le site de Microsoft (https://www.microsoft.com/fr-fr/evalcenter/download-windows-server-2016)

Pour installer l'ISO ? Aller sur votre machine serveur, « edit virtual machine settings », CD/DVD
Puis installer l'ISO que vous avez télécharger

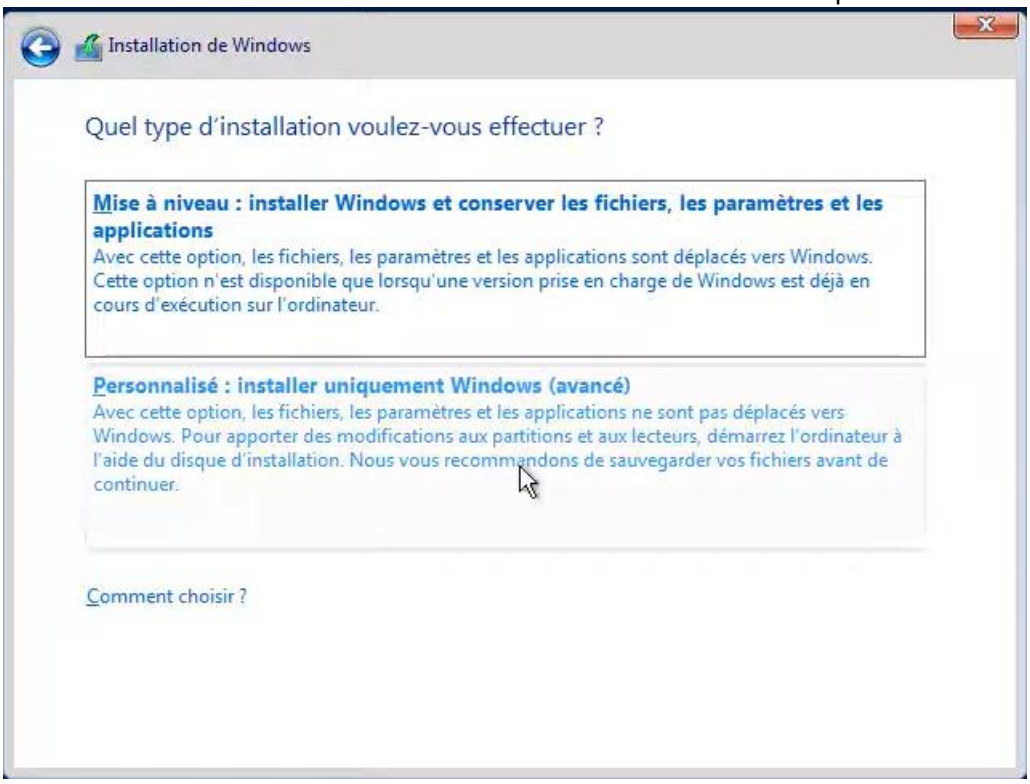



Enfin lancer votre machine.

Choisissez le windows server 2016 Datacenter Evaluation pour avoir une interface graphique




Suivez l'installation de Windows et ensuite choisissez une installation personnaliser.



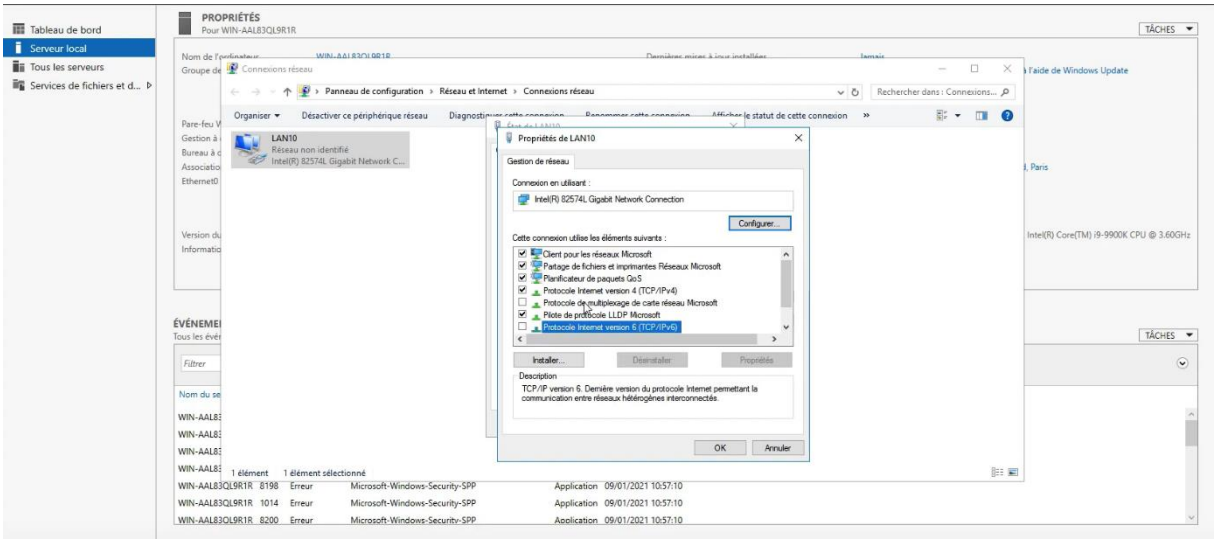
Enfin redémarrer votre serveur, puis au redémarrage entrez votre mot de passe personnel.

## IV-Configuration du Gestionnaire de Serveur

### A-Modification du réseau et du nom de serveur

Pour s'organiser correctement on se fie au schéma de l'architecture réseaux et la première chose à faire c'est de changer le nom et l'adresse Ip en fonction du schéma

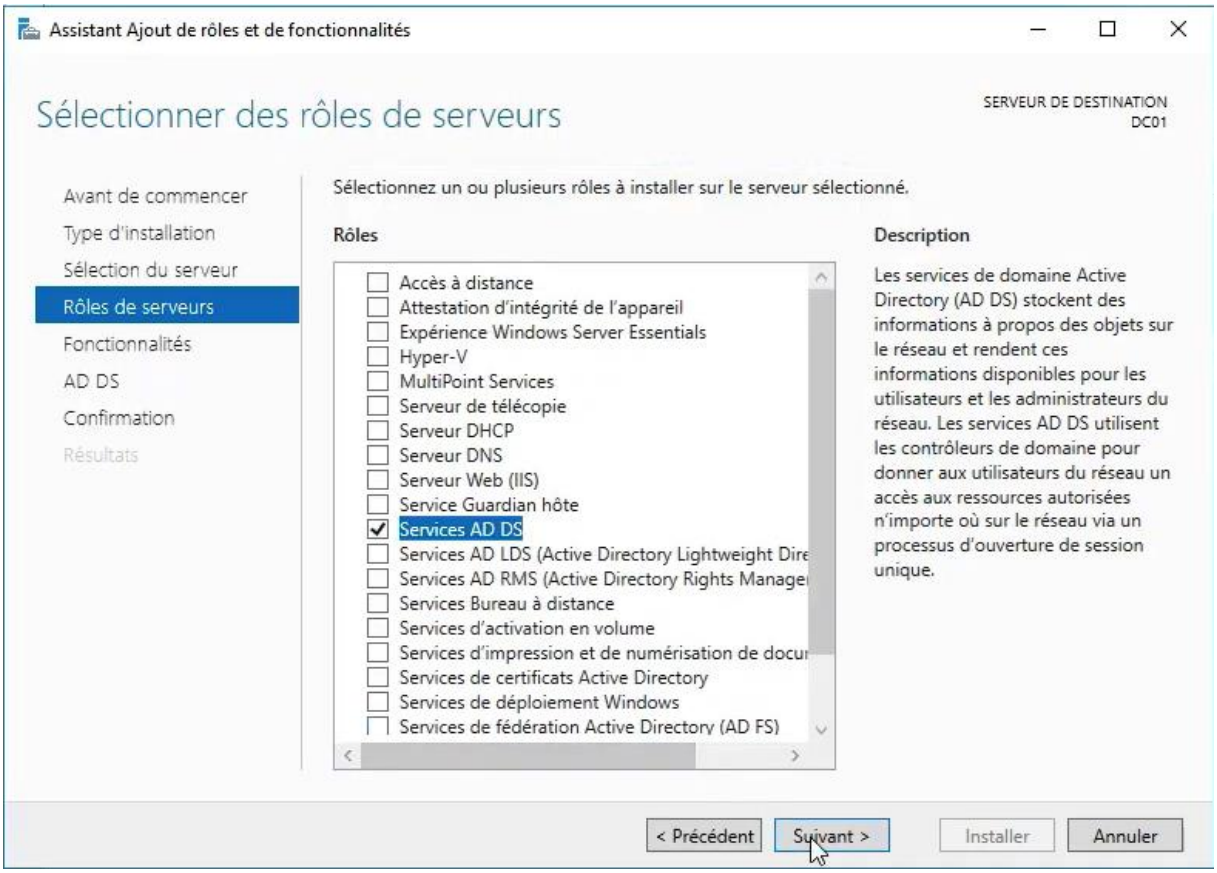
Donc pour cela aller dans le serveur local puis cliquer sur votre carte réseau puis renommer la en Lan 10 pour cette machine
-Ensuite aller dans les propriétés du réseaux et décocher l'ipv6
-Enfin cliquer sur le protocole ipv4 pour changer les paramètre réseau



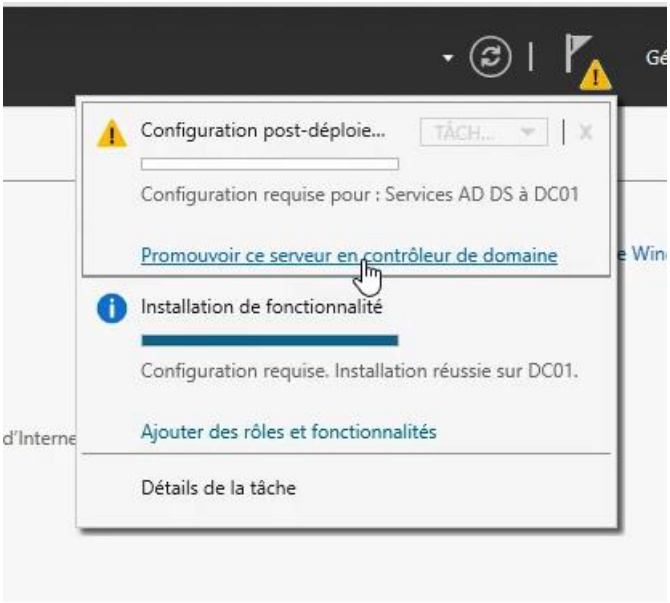

Pour la machine DC01 l'adresse IP à entrer est 192.168.10.10 , pareil pour le DNS car le serveur aura son propre DNS

### B-Installation de l'ADDS, DHCP et du DNS

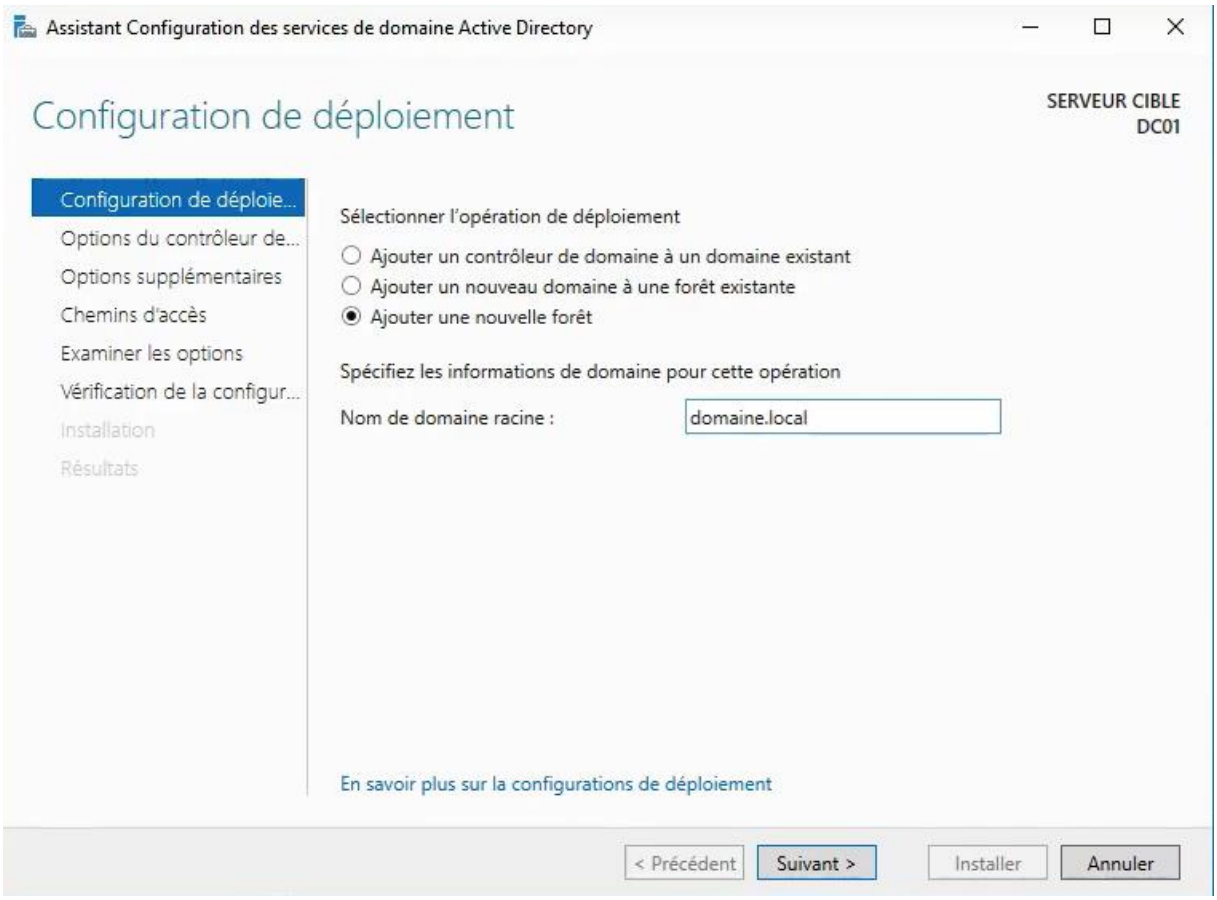
Dirigez vous sur l'onglet gérer → ajouter des rôles et fonctionnalité
Puis une page s'ouvrira cliquer sur suivant cocher « Installation basée sur un rôle ou une fonctionnalité » suivant → vérifier que vous êtes bien sur le serveur DC01→ cocher l'adds et ajouter la fonctionnalité, puis installer.



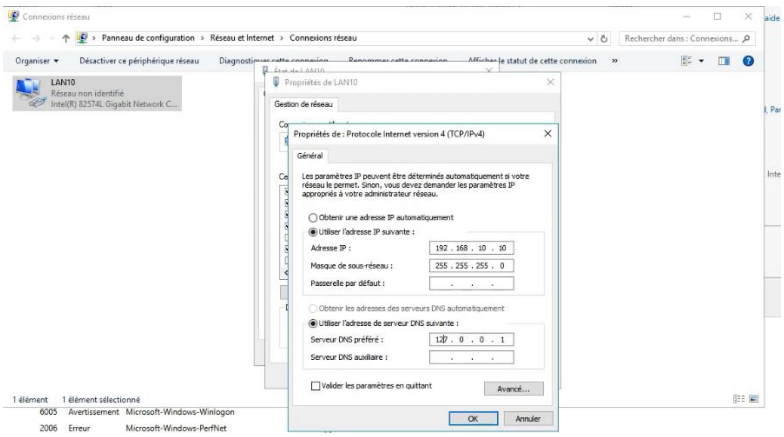

Une fois l'installation terminer un drapeau s'affichera, il faudra alors promouvoir en contrôleur de domaine.



Il faudra donc ajouter une nouvelle forêt d'après l'architecture réseau du Tp la forêt ce nomme domaine.local

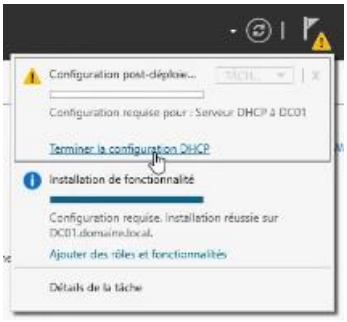



Entrez un mot de passe en cas de restauration des services d'annuaire puis terminer l'installation.
L'ordinateur vas se redémarrer automatiquement pour terminer l'installation de l'adds.
Lors du redémarrage vous pouvez constater que le domaine a bien été pris en compte, il faut directement vérifier l'adresse IP du DNS. Il faut remettre la même adresse.



Pour l'installation du DHCP faites la même procédure que l'ADDS et DNS

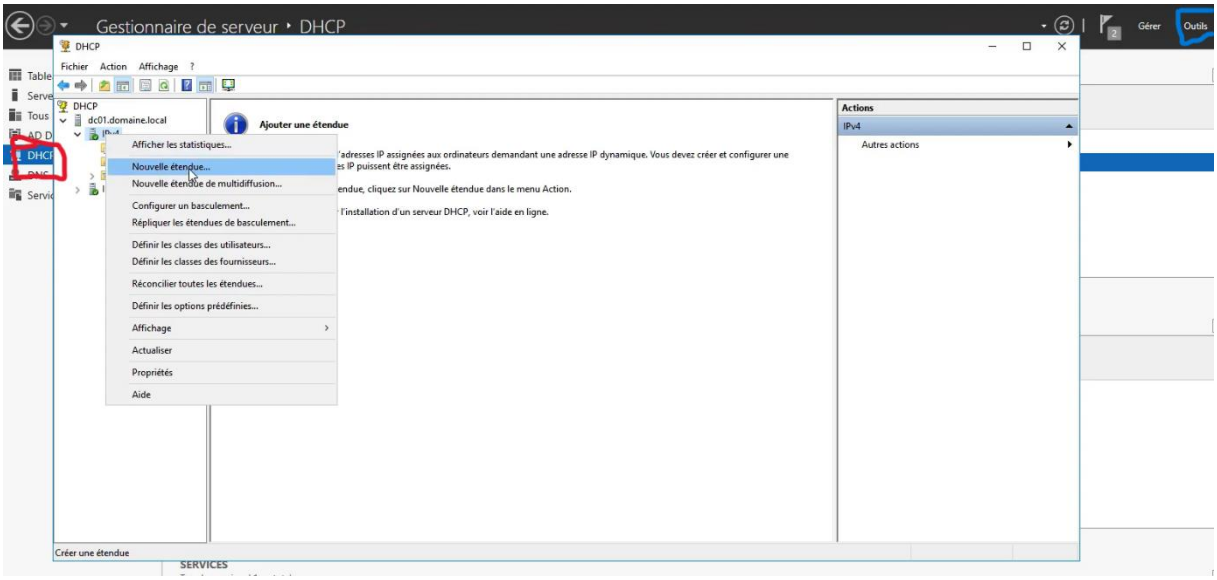
Une fois l'installation faite un drapeau s'affichera pour terminer la configuration du DHCP.7




Vérifier que les informations d'identification sont correcte puis cliquer sur terminer.

## C-Configuration du DHCP

Il faut donc créer une nouvelle étendu pour cela rendez-vous sur le dhcp, cliquer sur outils→DHCP, clique droit sur ipv4 pour créer une nouvelle étendue, nommer la puis ajouter une adresse ip de début et de fin pour ce tp on prendra 192.168.10.100 et comme adresse de fin on prendra 192.168.10.200 , ensuite vérifier que l'adresse du DNS est bonne puis terminer la config



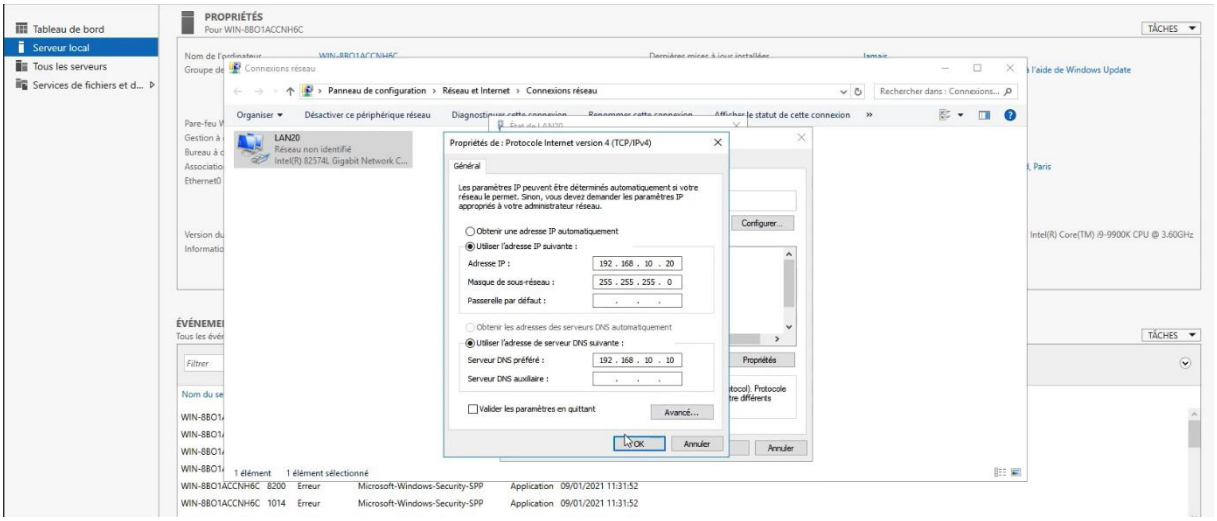

Nous avons donc terminer la configuration de notre première machine serveur.

## V-Configuration de la seconde machine virtuelle

### A-Modification de l'ip et du nom de serveur

Lancer la machine DC02, pour rappel nous allons installer l'ADDS et le DNS sur cette machine, configurer Windows de la même manière que la machine DC01 après l'installation le serveur doit redémarrer.

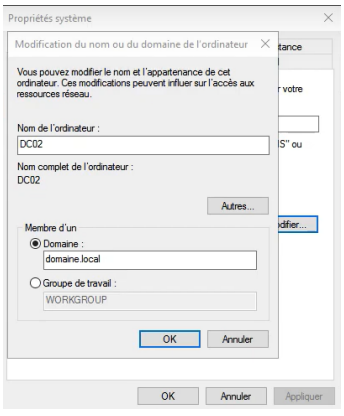
Pour commencer, il faut vérifier le nom et l'ip du serveur, renommer la carte réseau en LAN20, ensuite aller dans les propriétés de la carte réseau décocher l'ipv6 et entrer dans l'ipv4




Pour le DNS on lui spécifie l'adresse du premier serveur comme il n'a pas d'adds et dns encore installer cela vas l'aider à reconnaître le serveur dc01 et rejoindre le domaine
Puis changer le nom de l'ordinateur en DC02, l'ordinateur redémarrera.

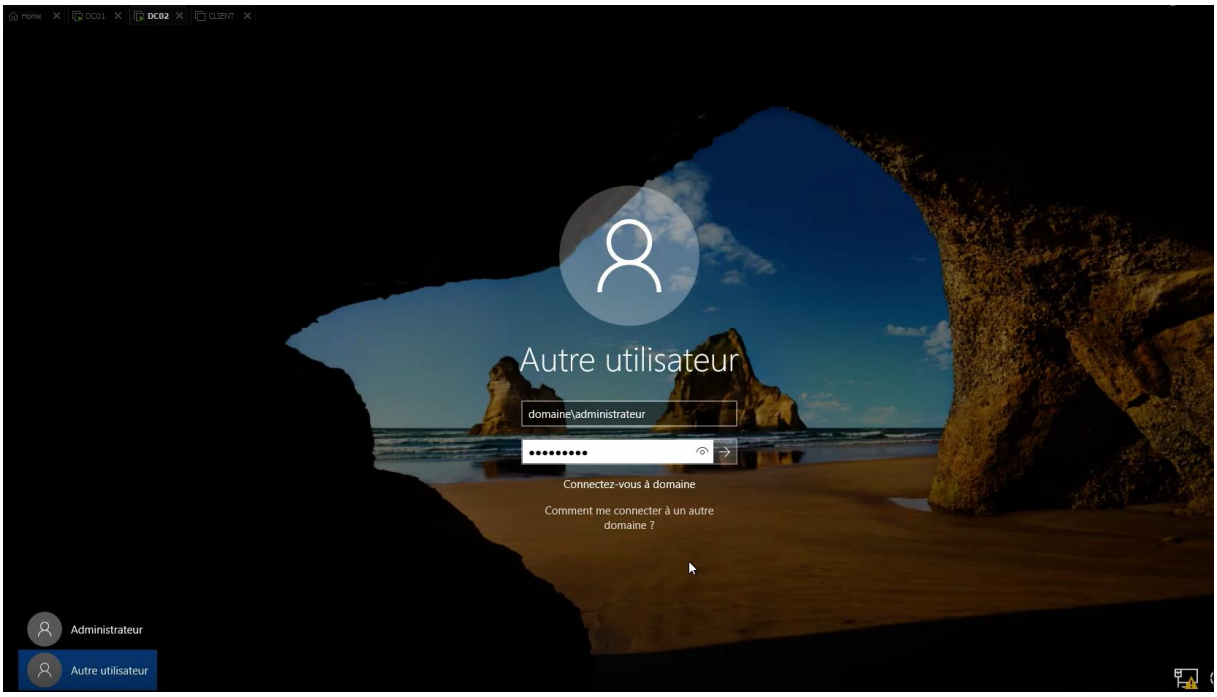
### B-Rejoindre le domaine

Pour rejoindre le domaine cliquer sur groupe de travail « WORKGROUP » → modifier → domaine → connecter vous au domaine.local → entrer le mot de passe administrateur

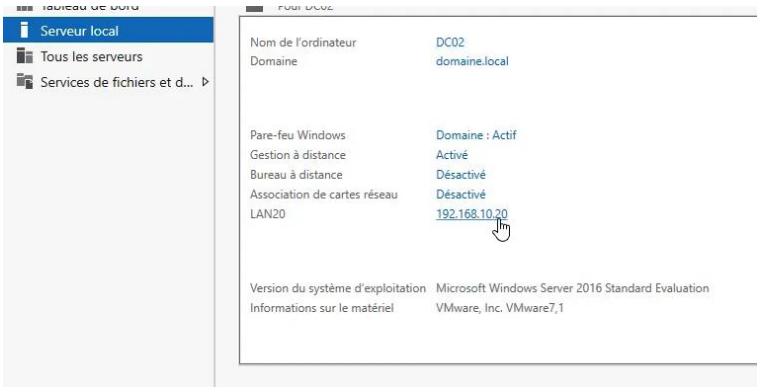



puis l'ordinateur vas redémarrer.

Pour vous connecter au domaine, utiliser un autre utilisateur et entrer les information du domaine.

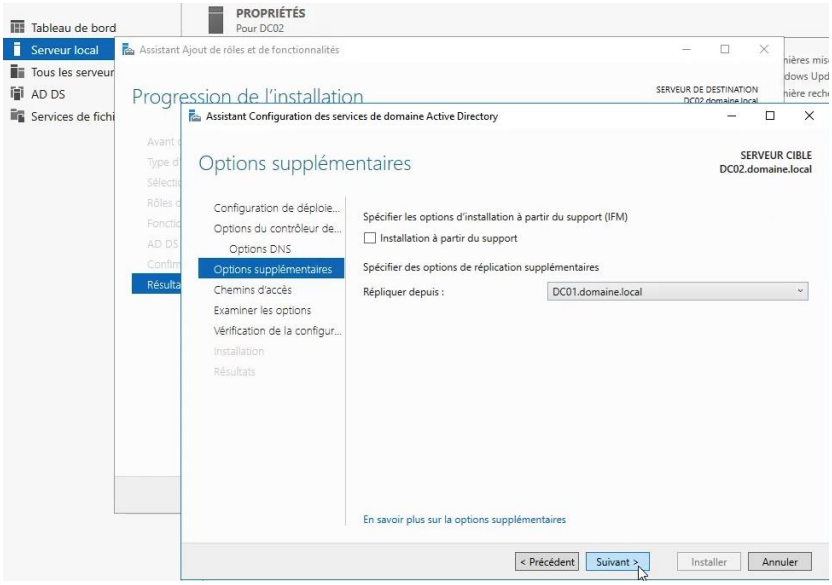



Une fois que vous êtes connecter vous verrez que vous êtes bien sur le bon domaine



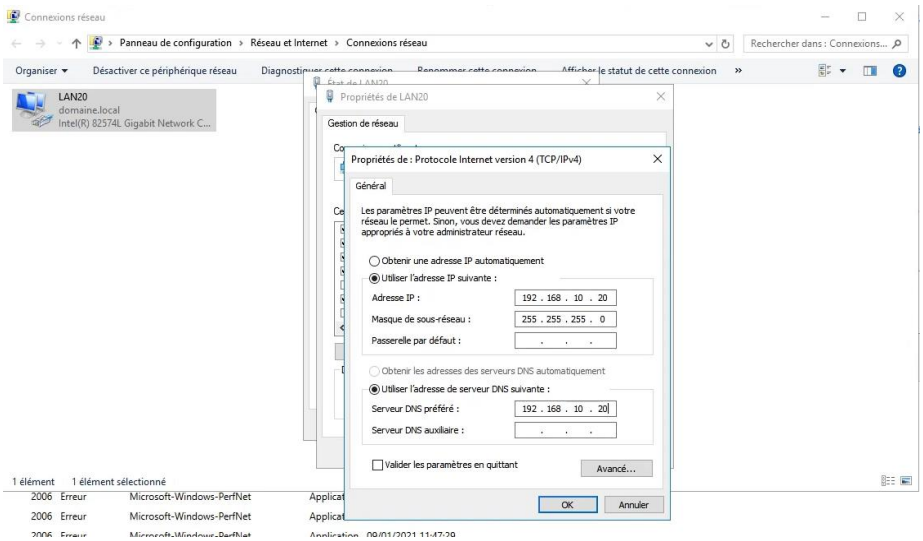

## C-Installation de l'ADDS et du DNS sur le DC02

Pour l'installation de l'ADDS appliquer les mêmes étapes qu'avec la machine DC01.
Une fois l'installation faite cliquer sur promouvoir un contrôleur de domaine puis ajouter le sur un domaine existant, pour notre part on l'ajoute sur le domaine.local

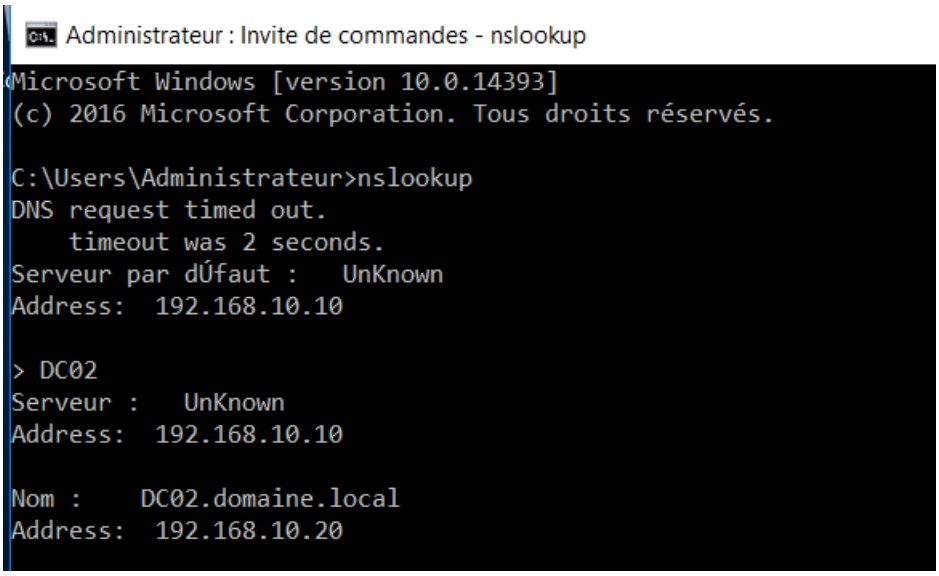



Répliquer bien sur le DC01.domaine.local et non pas sur tout contrôleur de domaine. Enfin terminer l'installation, vous serez déconnecter automatiquement une fois la configuration du serveur correctement configuré.

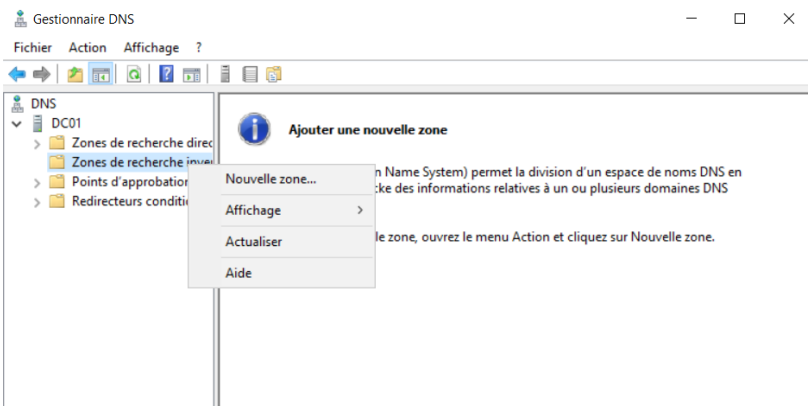
Pour le DNS, aller dans les propriétés de la carte réseau vous verrez que l'adresse IP du serveur DNS sera celle du serveur DC01, maintenant que le serveur DC02 a son propre DNS vous pouvez lui ajouter son adresse IP 192.168.10.20. Retirer l'adresse DNS auxiliaire qui s'ajoute automatiquement lors du redémarrage.



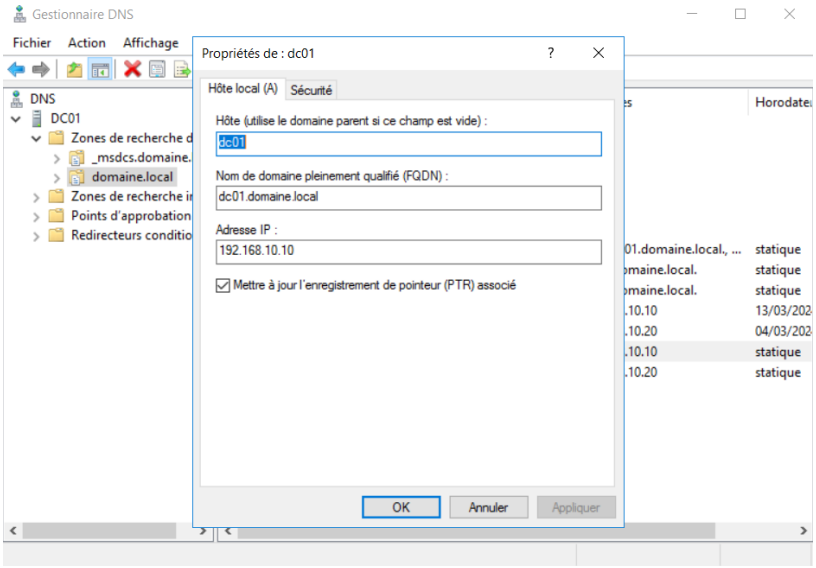
Une fois que vous avez changer l'adresse du serveur DNS actualiser le serveur et pour être sur que l'adresse IP a bien été répliquer, dirigez vous dans la machine serveur DC01, dans le terminal de commande et taper nslookup puis DC02.




Le serveur unknown correspond au serveur DC01 pour régler cela il faut aller dans outils → DNS → DC01




Faite clic droit sur zone de recherche inversé puis cliquer suivant jusqu'à ajouter l'adresse du serveur.
Pour que la zone de recherche inversé soit effective il faut retourner dans le domaine.local et cocher « mettre à jour l'engagement de porteur »




Vous pouvez retourner sur le terminal de commande et tapez nslookup pour vérifier que le serveur dc01 est bien reconnu.

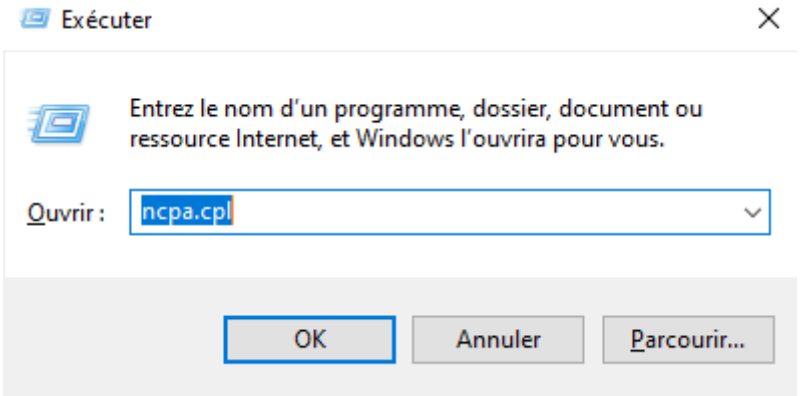
## VI-Configuration de la machine Client

Ajouter l'iso de Windows 10 pour la machine client, vous pouvez la retrouver sur le site de Microsoft

Ensuite démarrer la machine et suivez l'installation. Attention à la version que vous installer il faut installer la version pro pour pouvoir joindre la machine au domaine.
Une fois l'installation terminer on redémarre puis suivre les étapes proposer.

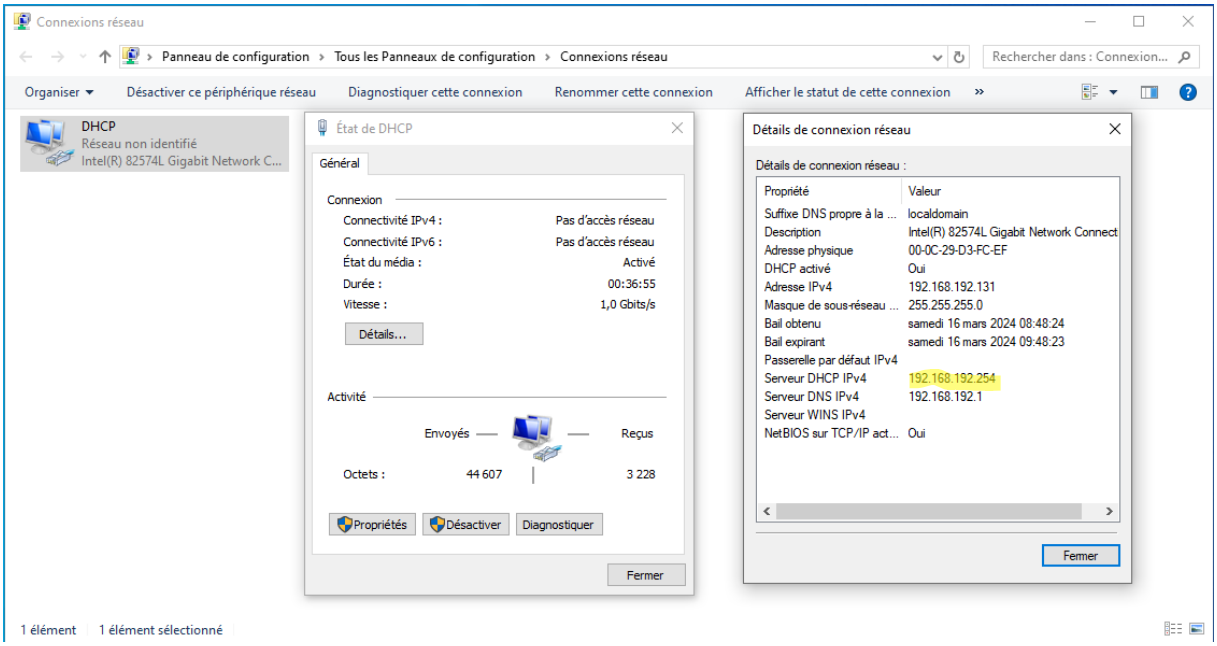
Enfin une fois l'installation complète terminer installer les vmware tools.

Maintenant la première chose à vérifier est sa configuration réseau pour cela exécuter la commande Windows+R

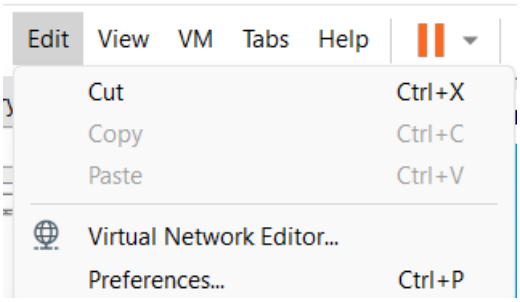


Aller dans les propriétés de la carte réseau, décocher l'ipv6 et vérifier bien qu'en ipv4 nous sommes en automatique.

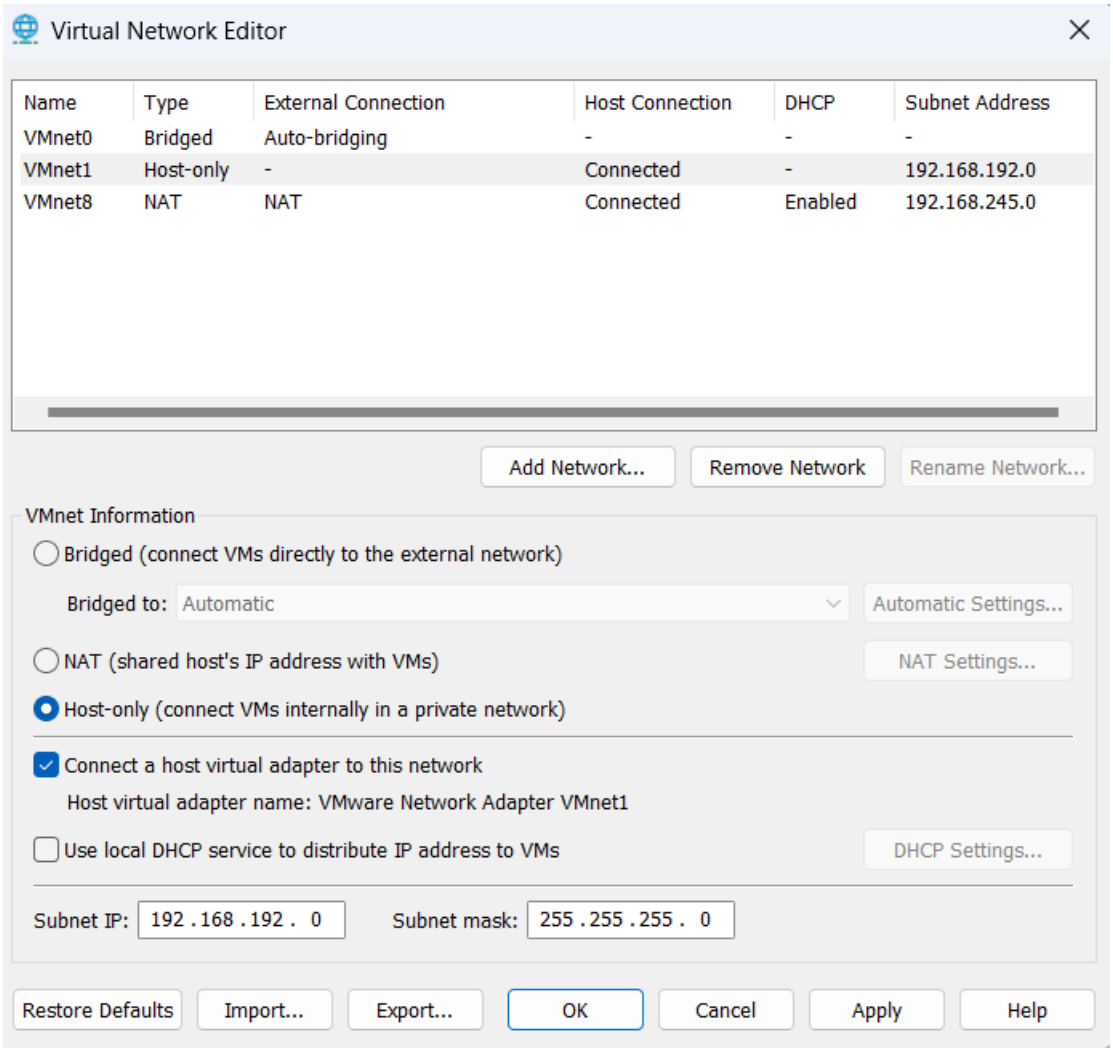
Comme nous avons configurer un DHCP sur le serveur DC01, normalement le client est connecté en DHCP, aller dans les détails de la carte réseau pour vérifier que c'est bien le cas



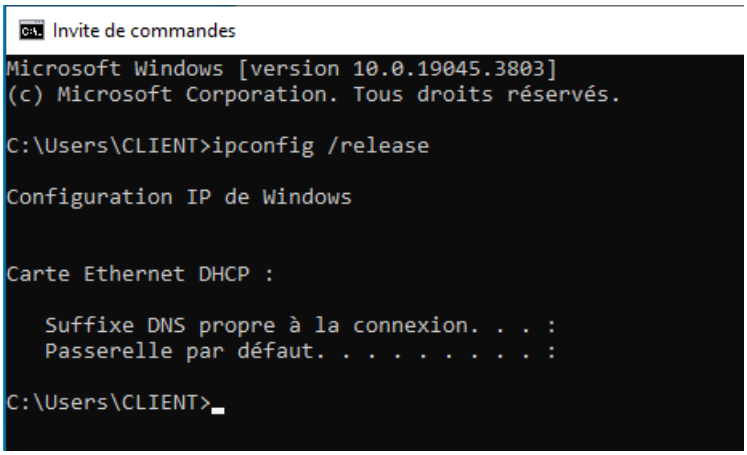

Si vous n'avez pas la bonne adresse du DHCP, dirigez-vous sur edit, Virtual Network Editor




Une fois le Virtual Network Editor ouvert cliquer sur change settings, cliquer sur oui puis sur le host only il faut décocher le « use local dhcp service … »




Pour mettre à jour la configuration aller sur le terminal de commande et taper « ipconfig /release »

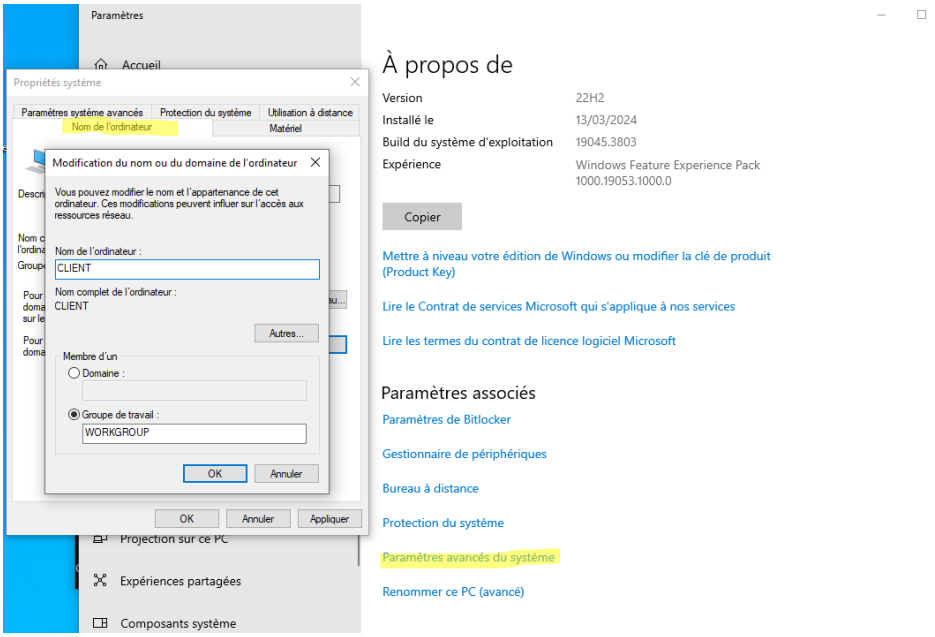



Puis pour lui reconfigurer les paramètres réseau taper dans le cmd « ipconfig /renew » ensuite taper « ipconfig /all »

```
C:\Users\CLIENT>ipconfig /all

Configuration IP de Windows

   Nom de l'hôte . . . . . . . . . . . . : DESKTOP-FRT3CIU
   Suffixe DNS principal . . . . . . . :
   Type de noeud. . . . . . . . . . . . : Hybride
   Routage IP activé . . . . . . . . . . : Non
   Proxy WINS activé . . . . . . . . . . : Non
   Liste de recherche du suffixe DNS.: domaine.local

Carte Ethernet DHCP :

   Suffixe DNS propre à la connexion. . . : domaine.local
   Description. . . . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Adresse physique . . . . . . . . . . . : 00-0C-29-D3-FC-EF
   DHCP activé. . . . . . . . . . . . . . : Oui
   Configuration automatique activée. . . : Oui
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.10.101(préféré)
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Bail obtenu. . . . . . . . . . . . . . : samedi 16 mars 2024 09:40:19
   Bail expirant. . . . . . . . . . . . . : dimanche 24 mars 2024 09:40:19
   Passerelle par défaut. . . . . . . . . :
   Serveur DHCP . . . . . . . . . . . . . : 192.168.10.10
   Serveurs DNS. . .  . . . . . . . . . . : 192.168.10.10
   NetBIOS sur Tcpip. . . . . . . . . . . : Activé
```

On peut voir que le DHCP est correctement attribué et que nous sommes bien dans le domaine.local

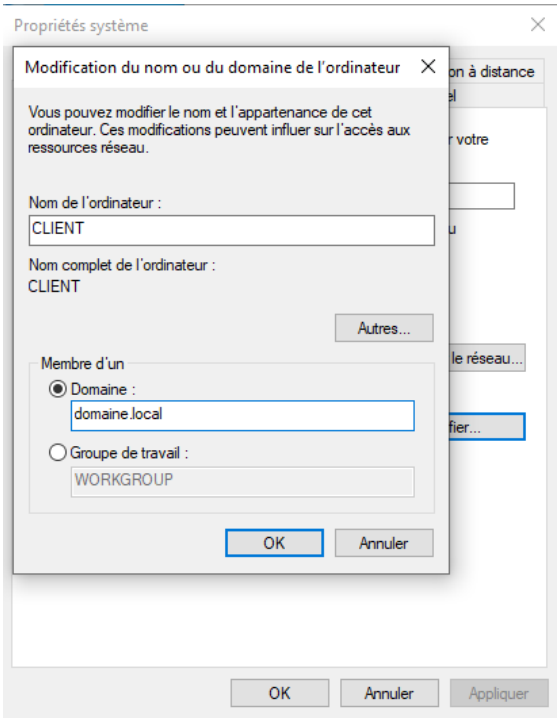
Maintenant il faut changer le nom de l'ordinateur pour cela aller dans système → paramètre avancé du système → nom de l'ordinateur → Modifier → puis renommer le en client.




Une fois le pc renommer, il faut redémarrer le pc.

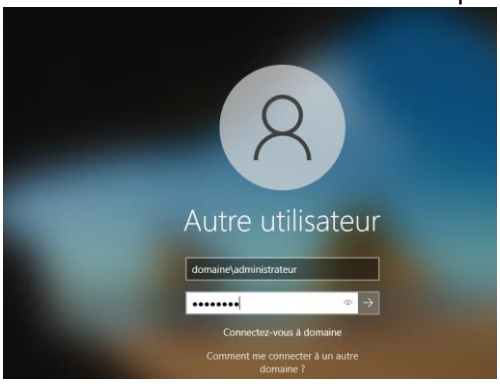
Maintenant il faut joindre le pc au domaine.

Pour cela aller dans les paramètres avancés du système, nom de l'ordinateur modifier et cocher domaine puis dite lui de rejoindre domaine.local

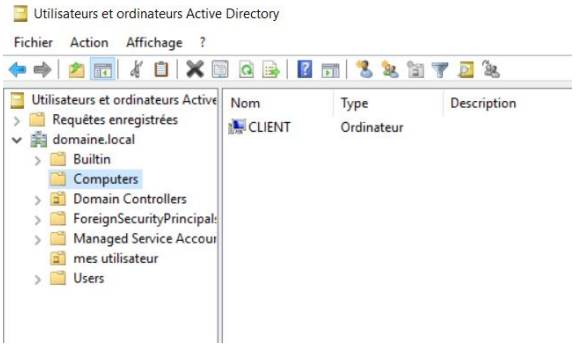



Il vous demandera d'entrer le compte administrateur de la machine dc01 une fois cela fait il faudra redémarrer l'ordinateur.

Maintenant il faut se connecter sur le pc CLIENT avec le compte administrateur du domaine



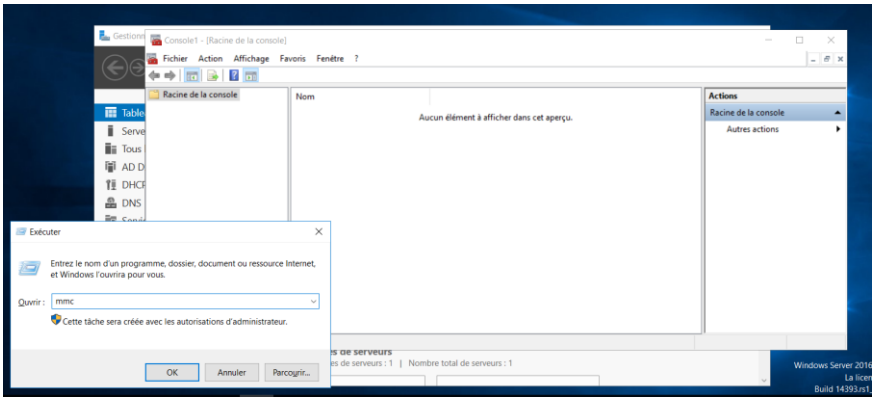

Pour vérifier que le pc a bien rejoint le domaine, aller dans la machine DC01, outils, utilisateur active directory, computer



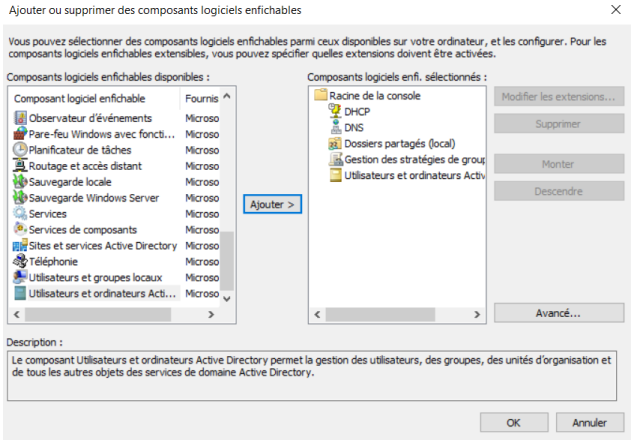

Voilà, on voit bien que le pc CLIENT à rejoint le domaine.

## VII-Création des USERS

Pour commencer nous allons personnaliser une console mmc pour sélectionner les éléments importants et ce dont on n'aura besoin pour cela exécuter une commande mmc, cela vous ouvrira une console, puis dans fichier cliquer sur ajouter des composants



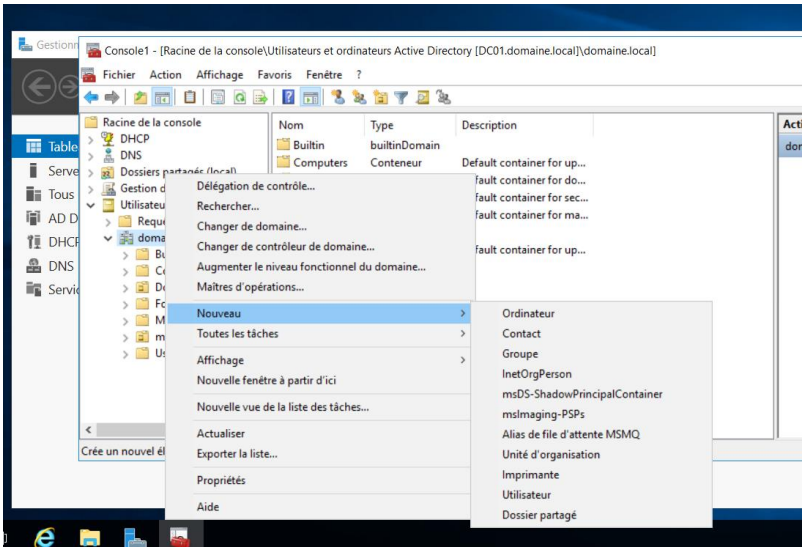

Voici les composants dont on aura besoin :




Enregistré la sur le bureau pour ne pas la perdre et pouvoir la fermer.

## A-Création des Unités Organisationnelles (UO)

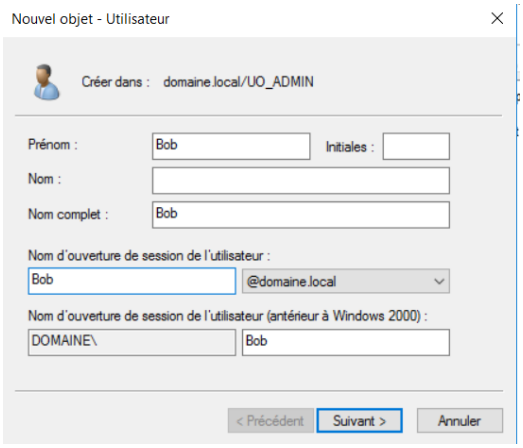
Nous allons créée plusieurs unité organisationnels pour cela :
Aller dans utilisateur active directory → domaine.local → clic droit → nouveau → UO




Répéter cette étape a trois reprise pour créer les UO : UO_ADMIN, UO_Paris, UO_Lyon.
Créer aussi un groupe dans l'UO_Admin, nommer le GROUPE_ADMIN, un groupe dans l'UO_Paris « GROUPE_PARIS »

## B-Création des utilisateurs dans chaque UO

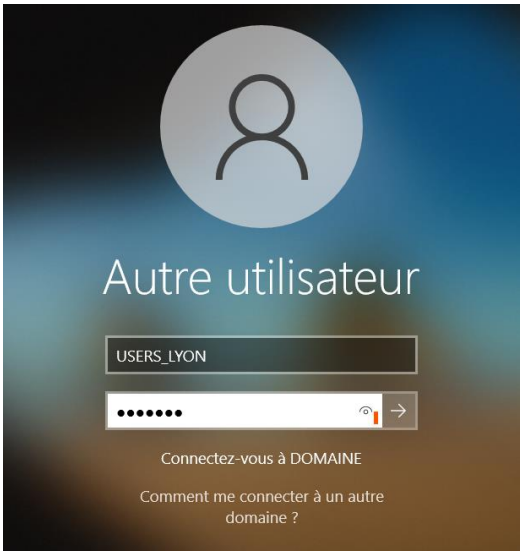
Pour créer les utilisateurs dans chaque UO cela ressemble à la pratique de la création des UO sauf que le clic droit est fait sur L'UO
Placer vous sur uo_admin → clic droit → nouveau → utilisateur




Puis entrer un mot de passe.
Créer un utilisateur Stef dans le groupe Admin

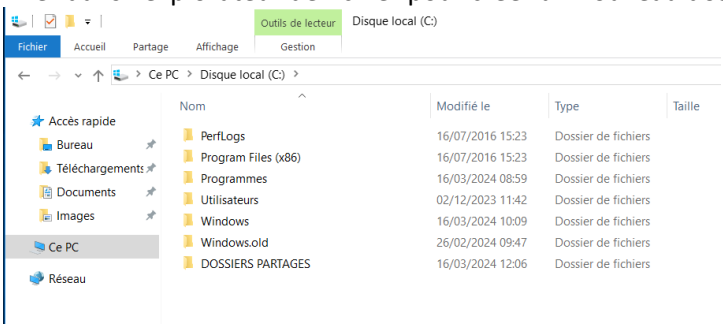
Ajouter Bob et Stef dans le groupe Admin faite double clic sur le groupe, aller dans membre de, enfin ajouter les deux utilisateur.
Ensuite ajouter l'utilisateur USERS_PARIS dans l'UO_Paris, puis ajouter le dans le groupe_paris.
Enfin ajouter l'utilisateur USERS_LYON dans l'UO_Lyon, puis ajouter le dans le groupe_lyon.

Pour vérifier que tout a bien été pris en compte connecter vous avec un compte de n'importe quel utilisateurs crée sur le pc



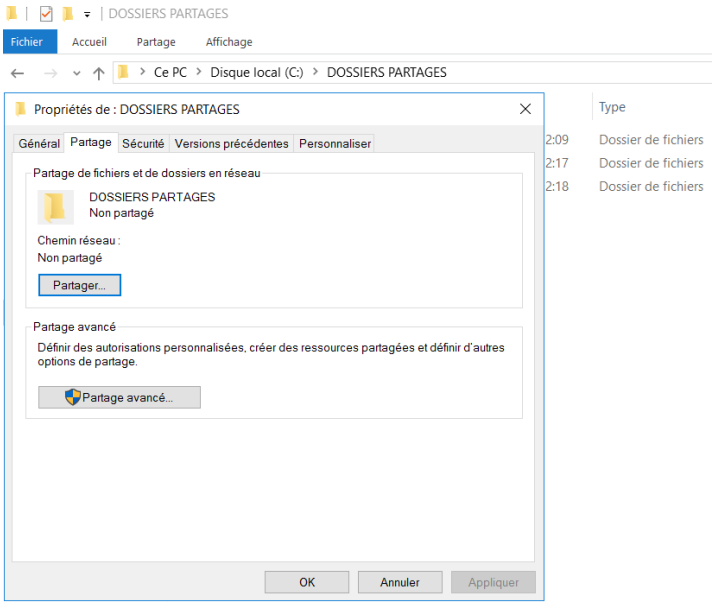

## VIII-Dossier partagés

Aller dans l'explorateur de fichier pour créer un nouveau dossier sur le disque local C :

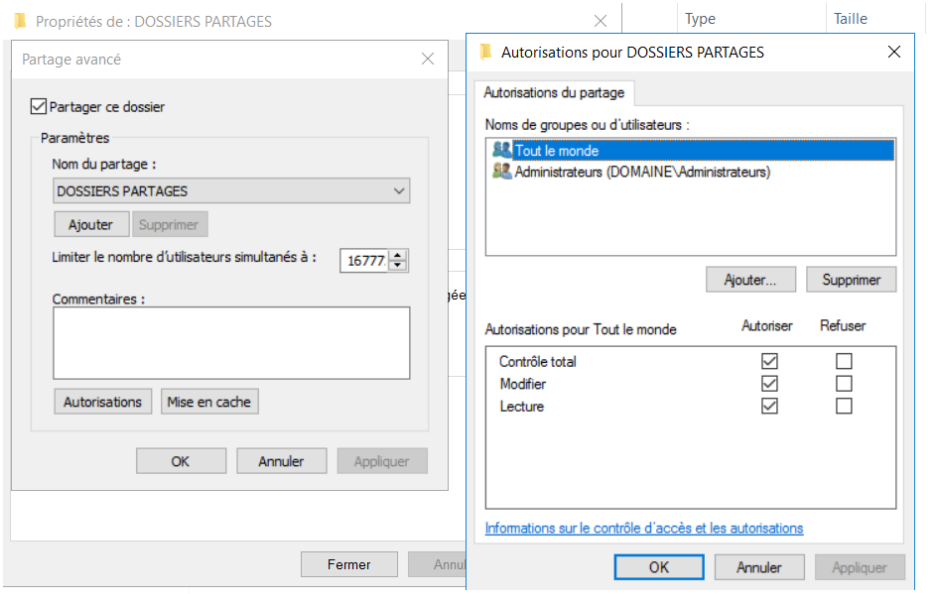



A l'intérieur de ce dossier créer trois dossier « ADMIN », « APPLICATIONS »
et « PARTAGES » dans le dossier Partage créer aussi deux dossier « Lyon » et « Paris ».

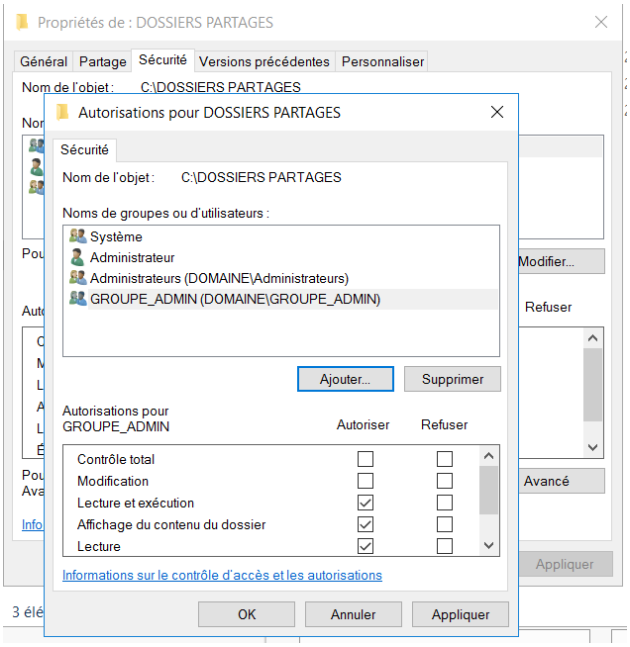
On commence par le dossier Admin faite clic droit sur le dossier Admin, aller dans propriétés, partage



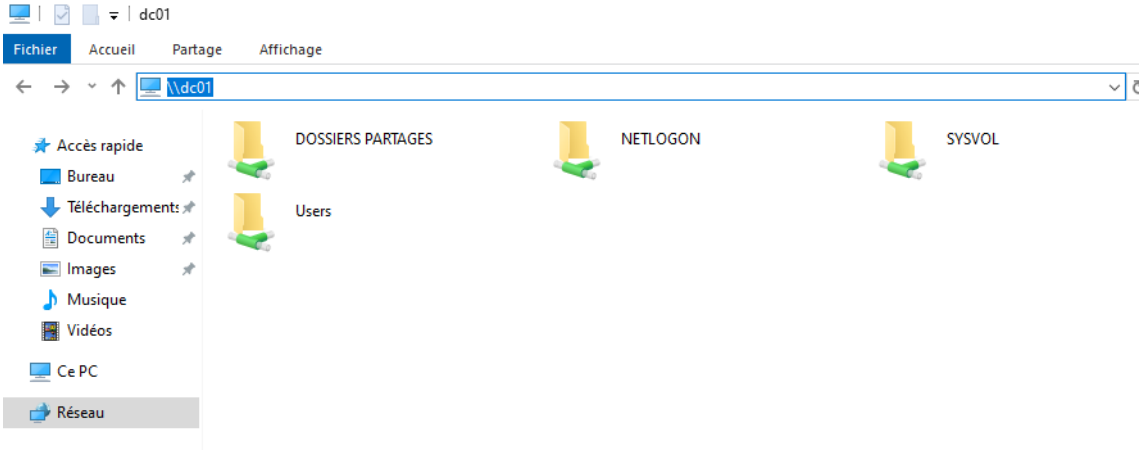

Cliquer sur partager, ensuite une fenêtre vas s'ouvrir cliquer encore sur partager et terminer, puis aller dans partage avancé, autorisation puis supprimer le nom de groupe tout le monde pour le dossier admin et ajouter le groupe_admin




Donner le contrôle total pour les administrateurs. Ensuite aller dans l'onglet sécurité et ajouter le groupe admin.



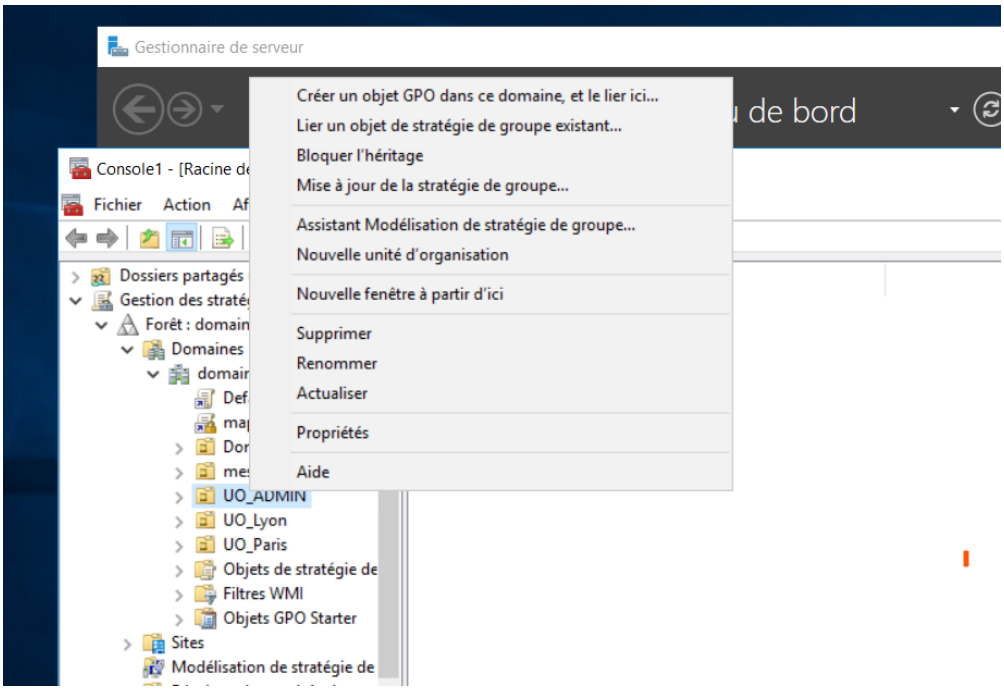

On peut vérifier que les paramètres ont bien été pris en compte en se connectant sur le pc CLIENT avec l'utilisateur Bob.
Puis aller dans l'explorateur de fichiers et taper dans la fenêtre d'accès \\dc01



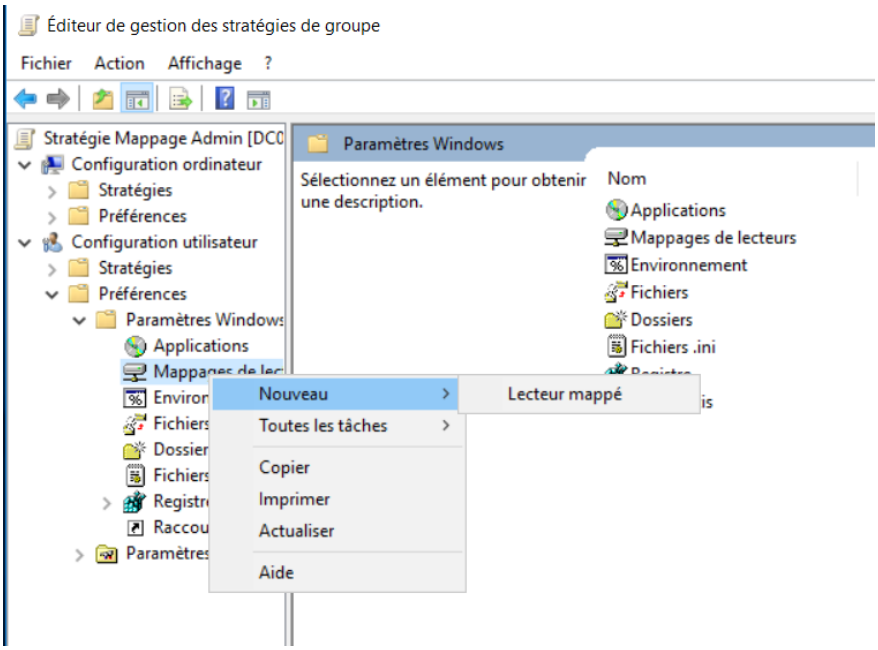

Pour le dossier applications donner l'accès a tout le monde, pour le dossier paris seulement aux groupe paris et aux administrateur et pareil pour lyon.

## IX- Création de GPO et mappage de lecteur

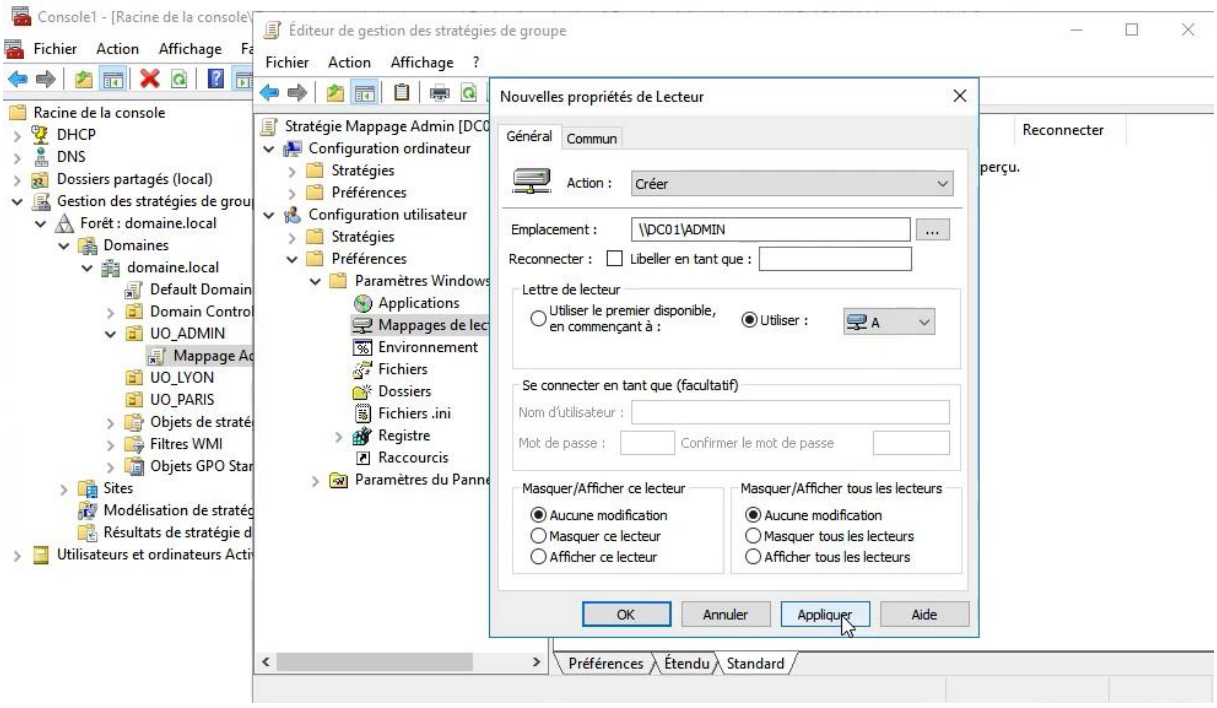
Aller sur gestion des stratégies de groupe ensuite domaine.local puis sur le dossier Admin faites clic droit et cliquer sur « Créer un objet GPO dans ce domaine … »




Une fois cette gpo créer faite clique droit sur son emplacement modifier, puis cliquer sur préférence, paramètre windows puis cliquer sur mappage de lecteur, puis faite clique droit nouveau lecteur mappé




Une fenêtre s'ouvrira puis changer l'action par créer et puis mettez le chemin de l'emplacement du dossier admin




Pour vérifier que le lecteur a correctement été mapper, connectez vous sur l'utilisateur Bob, vous aurez un dossier dans l'emplacement réseau.