

# Mise en place Active Directory

## Introduction :

Lors de ce guide nous allons voir comment mettre en service un Active Directory, un partage de fichier ainsi que la création d'un domaine et de ses utilisateurs, droits et comptes. Pour ce qu'il en est du DHCP il se trouve directement sur le Pare-feu PFsense.

On verra uniquement les parties citées ci-dessus, pour le serveur DNS je vais le rediriger vers un serveur du même réseau.

## Qu'est-ce qu'un Active Directory? :

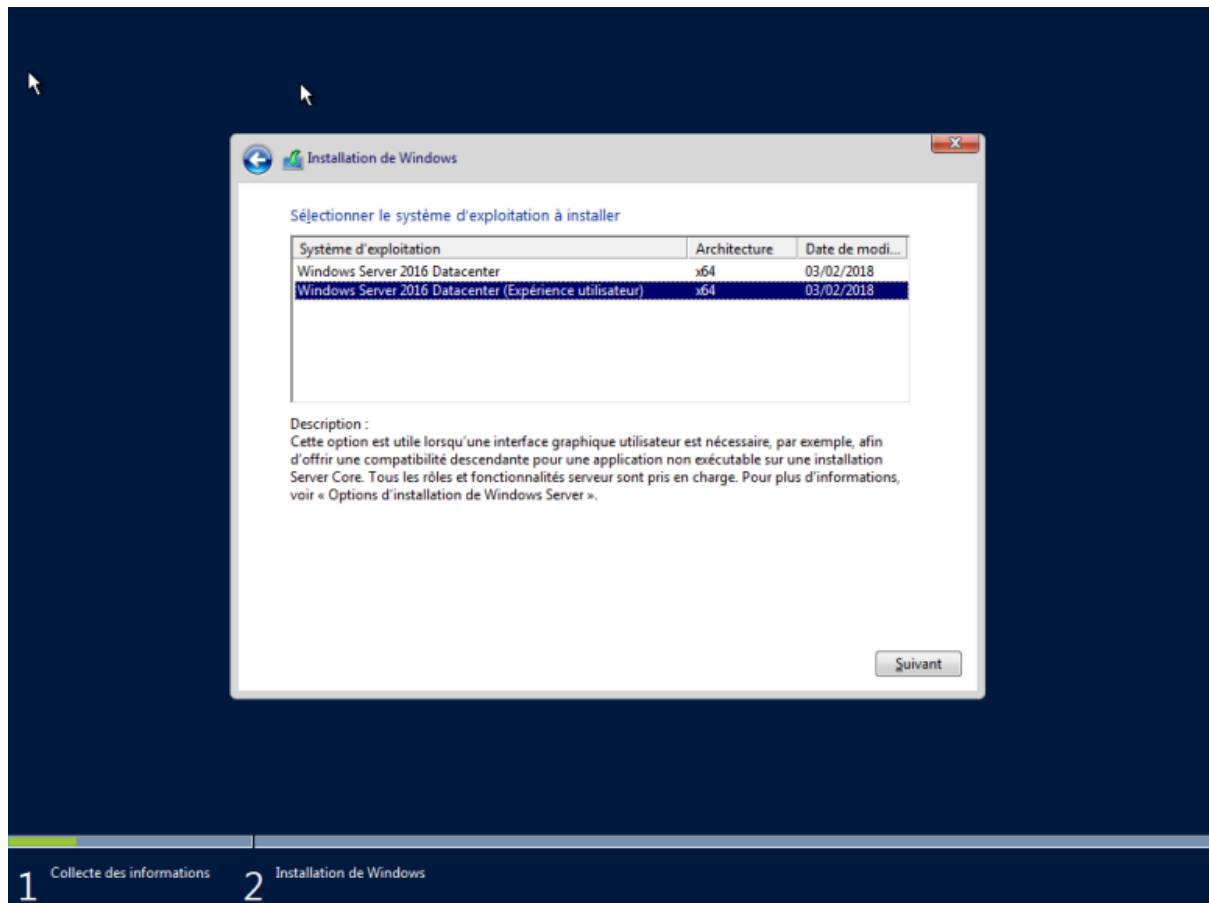
Un Active Directory est un service de répertoire développé par Microsoft. Il est utilisé principalement dans les réseaux Windows pour stocker des informations sur les ressources réseau et permettre leur gestion centralisée, y compris les utilisateurs, les groupes, les ordinateurs et d'autres ressources.

## Pré requis :

*Windows Server 2019 (Expérience de bureau)*  
*Client sous windows 10/11 (En mode graphique)*  
*Connexion internet haut débit*

# 1 - Installation de Windows SRV 2019 [Bureau]

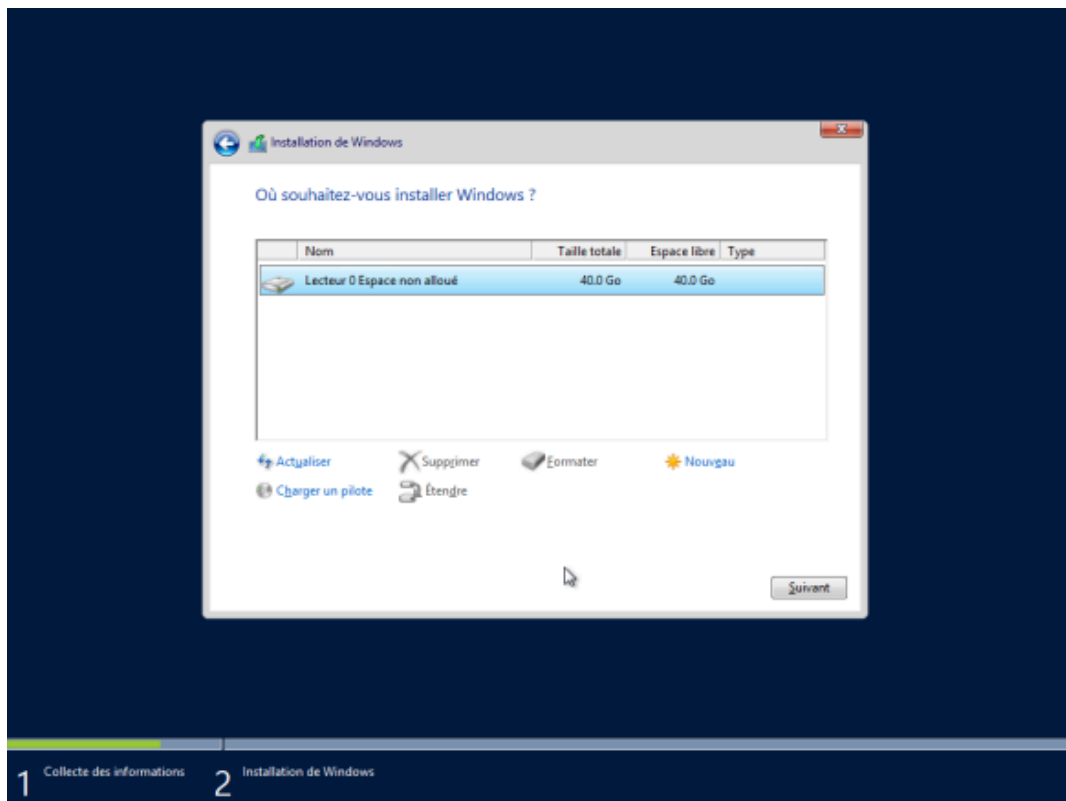
Démarrez votre VM ce qui doit lancer l'installation de Windows Server. Le premier écran notoirement intéressant est celui qui permet de choisir le type de système d'exploitation à installer :



Suivant la version de l'ISO, il y a plus ou moins de choix. Il est vivement conseillé de choisir une version intégrant l'interface graphique ("Expérience Utilisateur") et non "core".

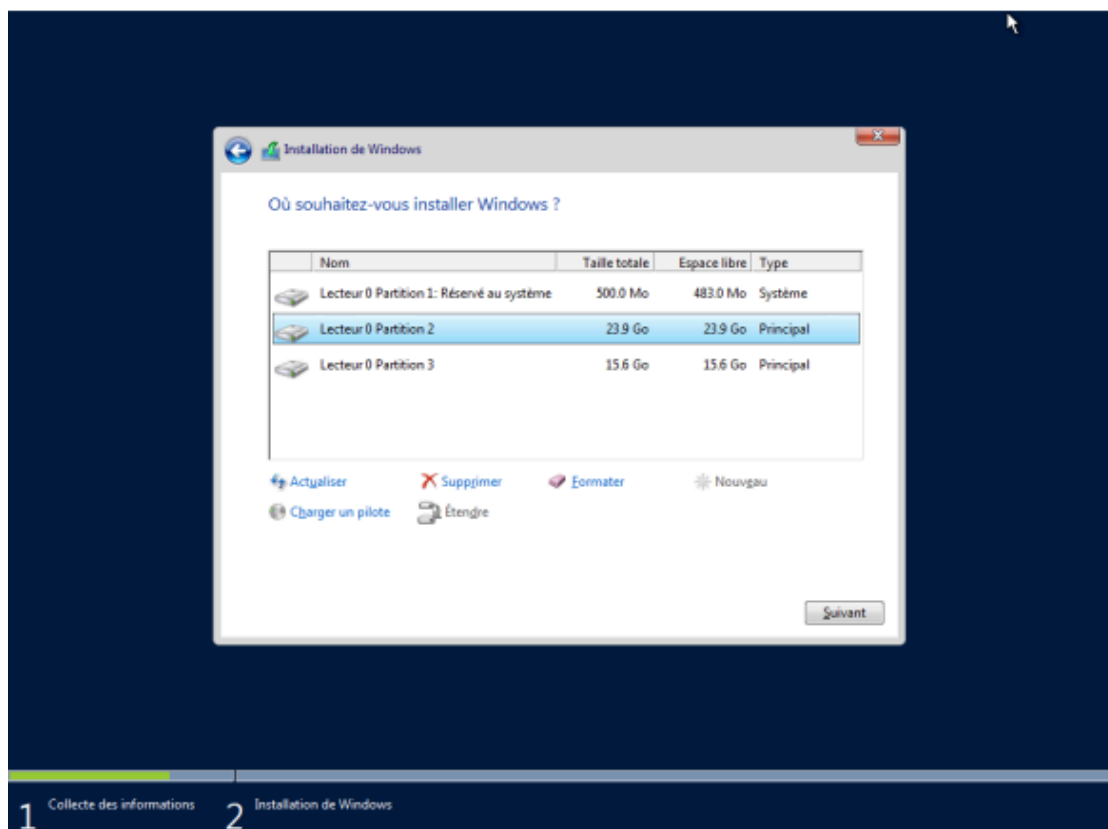
Pour ma part, lors de ce guide nous serons sur une version avec interface graphique.

Ensuite, vient l'écran de partitionnement :



Création ici d'une unique partition de 32GO, nous verrons par la suite si besoin on pourrait rajouter.

On sélectionne donc le disque "lecteur 0" puis on fait le suivant.



Remarque :

Windows crée automatiquement une partition de 500Mo qui contient les outils de boot, diagnostic et récupération : à ne pas modifier !

## 1.2 Mot de passe administrateur

Lors du premier démarrage de Windows Server, vous devez choisir un mot de passe pour l'administrateur. Celui-ci doit respecter des contraintes très précises : faire au moins 7 caractères et faire partie de 3 des 4 catégories suivantes : caractères minuscules, caractères majuscules, nombres, ponctuation.

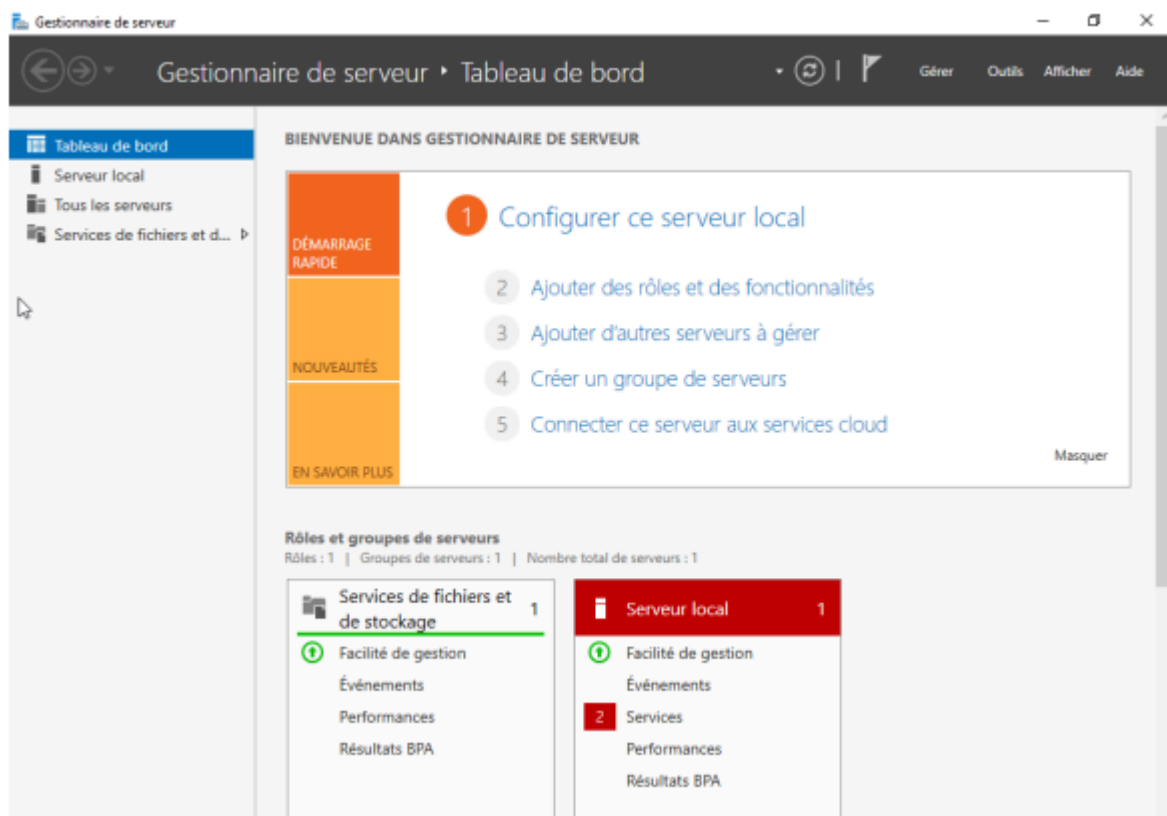
Attention donc à ne pas perdre ce mot de passe, sinon il est impossible de le retrouver car la procédure pour le régénérer est très longue.

## 2 - Configuration du Serveur

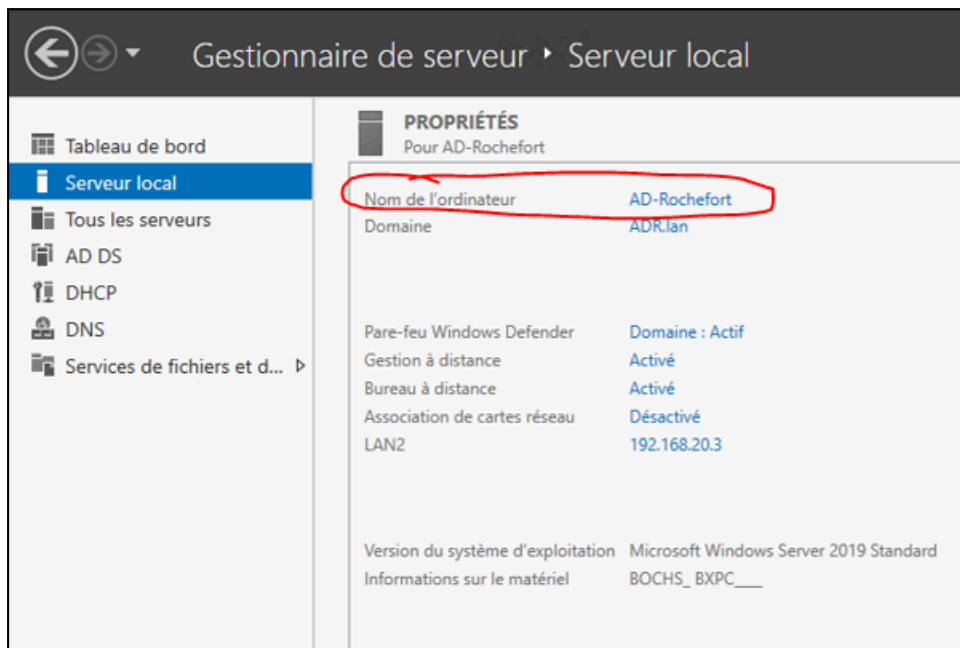
Nous allons le mettre en place pour une situation de labo. Seulement à la fin je changerais les @IP afin de mettre l'AD sur le réseau de production.

### 2.1 Nom du serveur :

Une fois connecté, vous êtes invité à suivre l'étape 1 "Configurer ce serveur local" (ne pas faire les autres pour le moment) pour vérifier ou réaliser les configurations nécessaires :



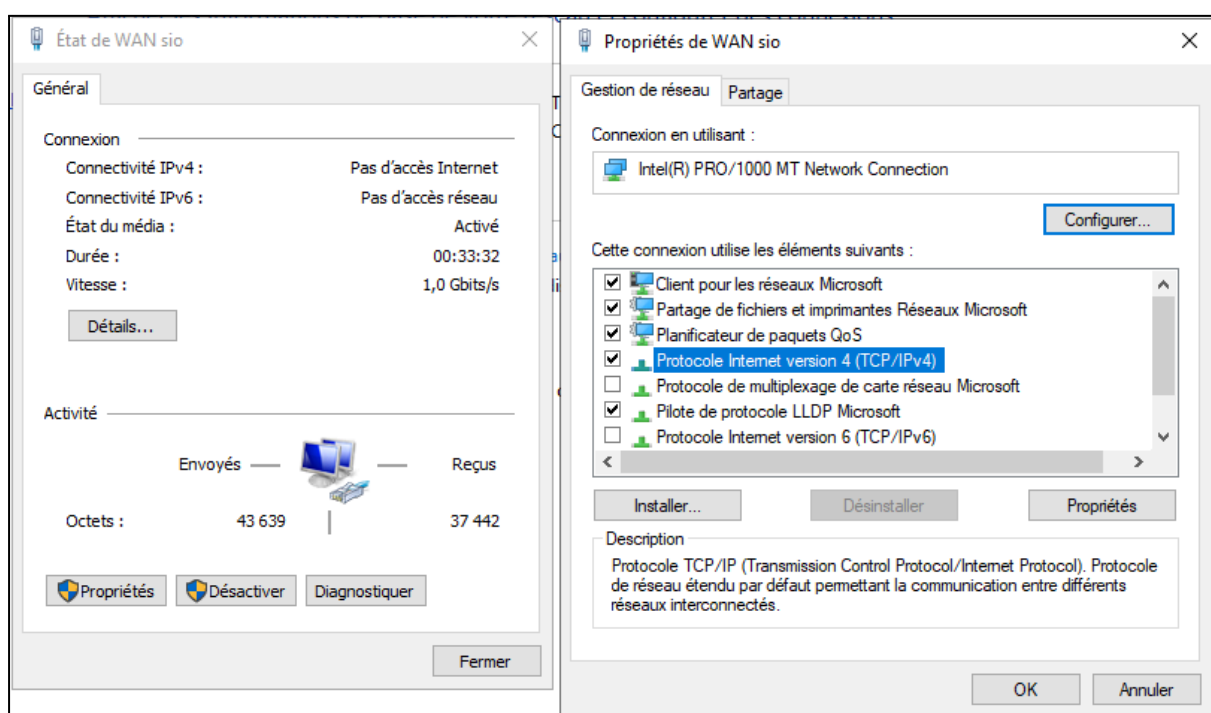
Lors de l'installation, Windows a généré un nom aléatoire mais nous allons définir un nom convenable et significatif.



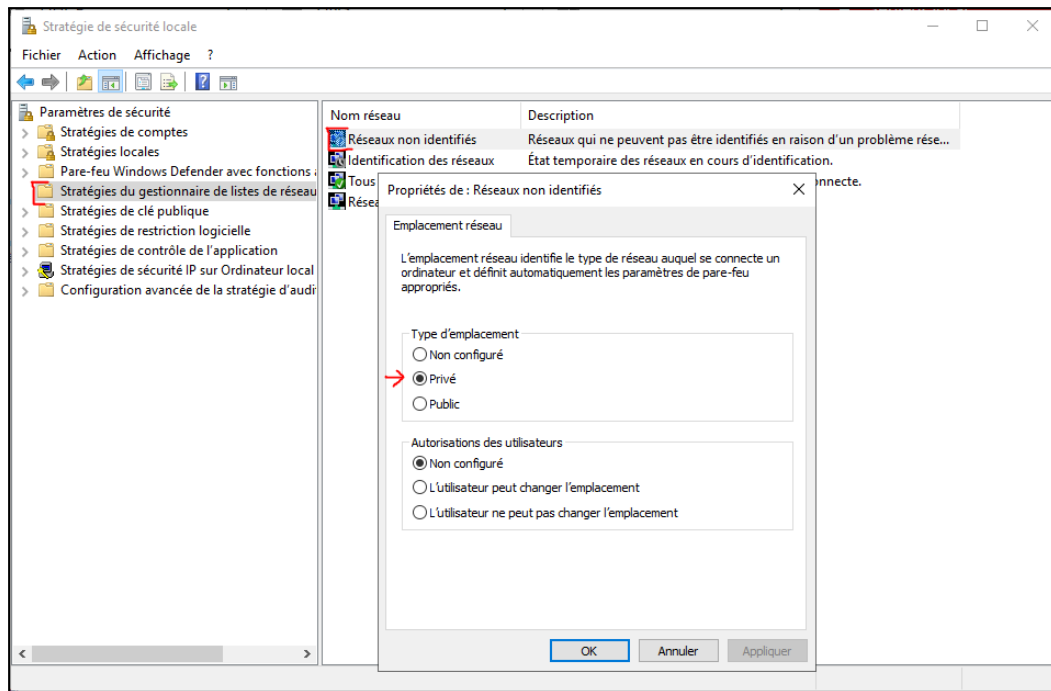
## 2.2 Configuration réseau IP

L'adressage IP dynamique (DHCP) par défaut n'est pas adapté pour un serveur, qui plus est, futur **contrôleur de domaine Windows**.

Vous utiliserez donc une adresse privée **IPv4 statique** qui déterminera les caractéristiques du réseau local de la maquette. Il est aussi conseillé de désactiver IPv6 (à décocher).



Vérifier que le réseau soit privé pour que le pare-feu du serveur autorise les connexions entrantes et le changer en réseau privé si nécessaire (modifiable dans stratégies de sécurité locales → stratégies du gestionnaire de liste de réseaux) - console secpol.msc

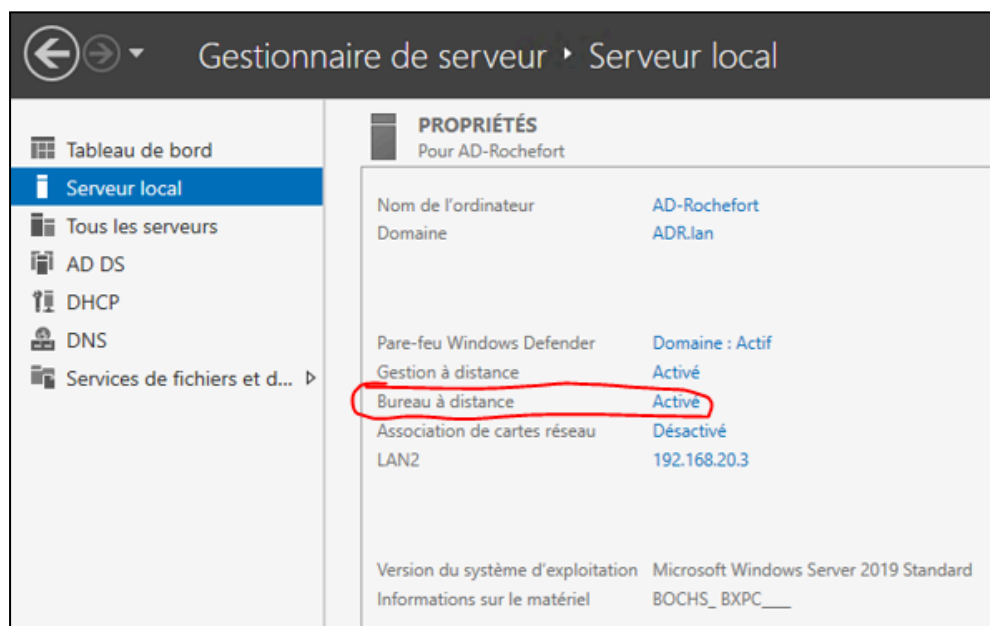


## 2.3 Bureau à distance

L'accès au bureau à distance est indispensable dans le cas d'un serveur de production. Il est nécessaire de l'activer pour pouvoir l'utiliser.

Pour cela depuis le Gestionnaire du serveur rubrique :

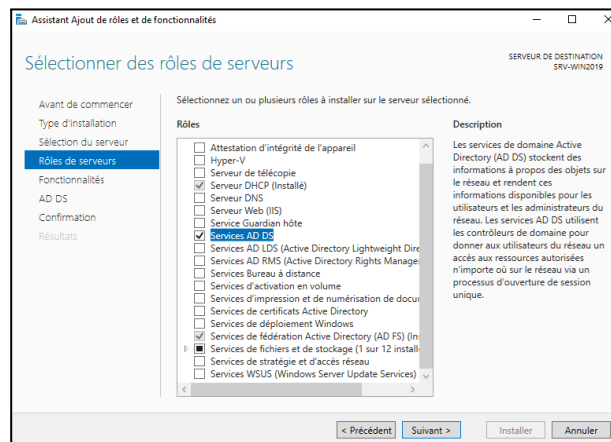
"Bureau à distance" → Autoriser les connexions à distance à cet ordinateur.



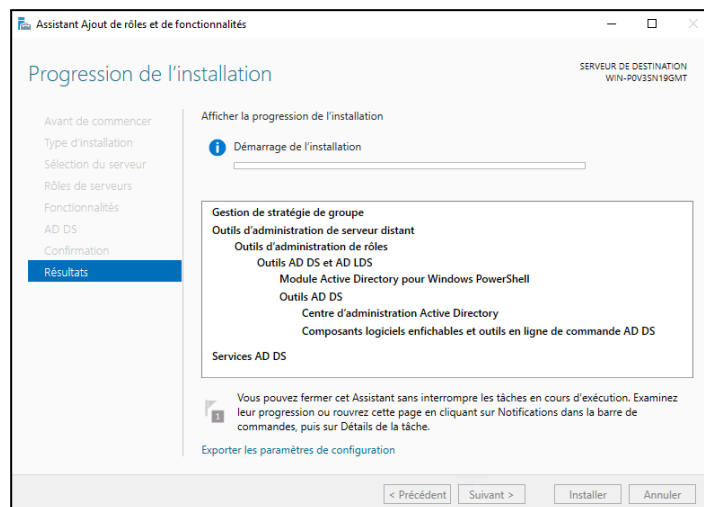
### 3. Ajout du service de Domaine Active Directory

Cliquez sur “Ajouter des rôles et des fonctionnalités”, vous pouvez observer les différents rôles (>20) que peut assurer un Windows Server.

Choisissez le rôle "Services AD DS". Par dépendance, vous devrez aussi installer certaines fonctionnalités requises (notamment le centre d'administration)



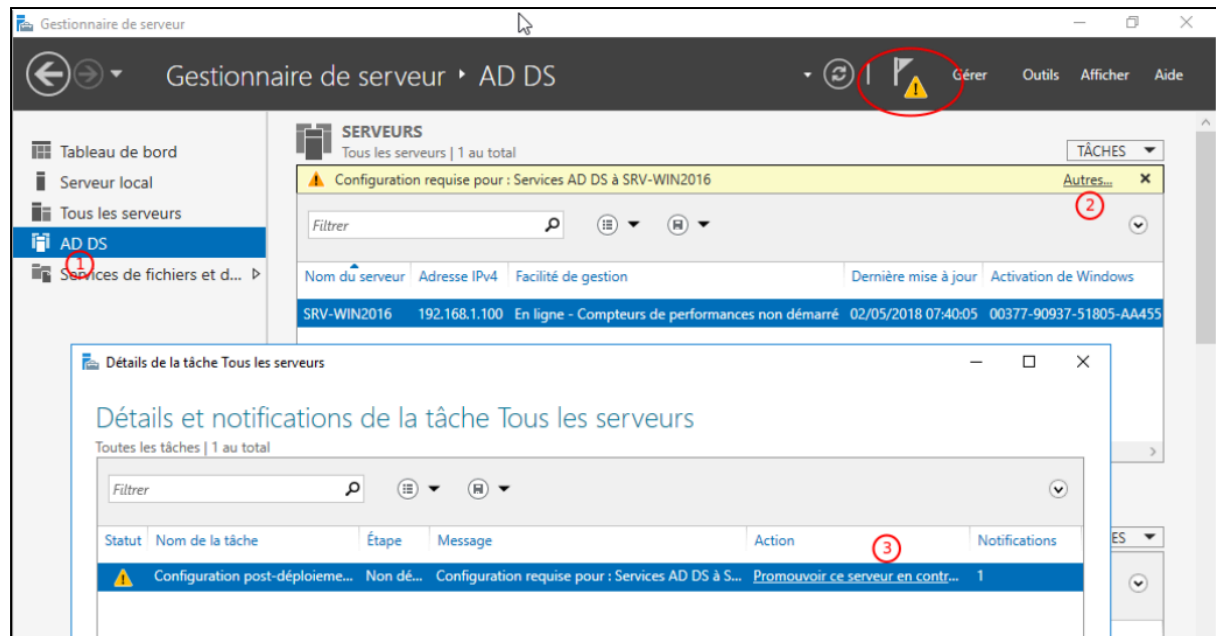
Ensuite faite suivant, et confirmez l'installation.



## 3.1 Promotion du service

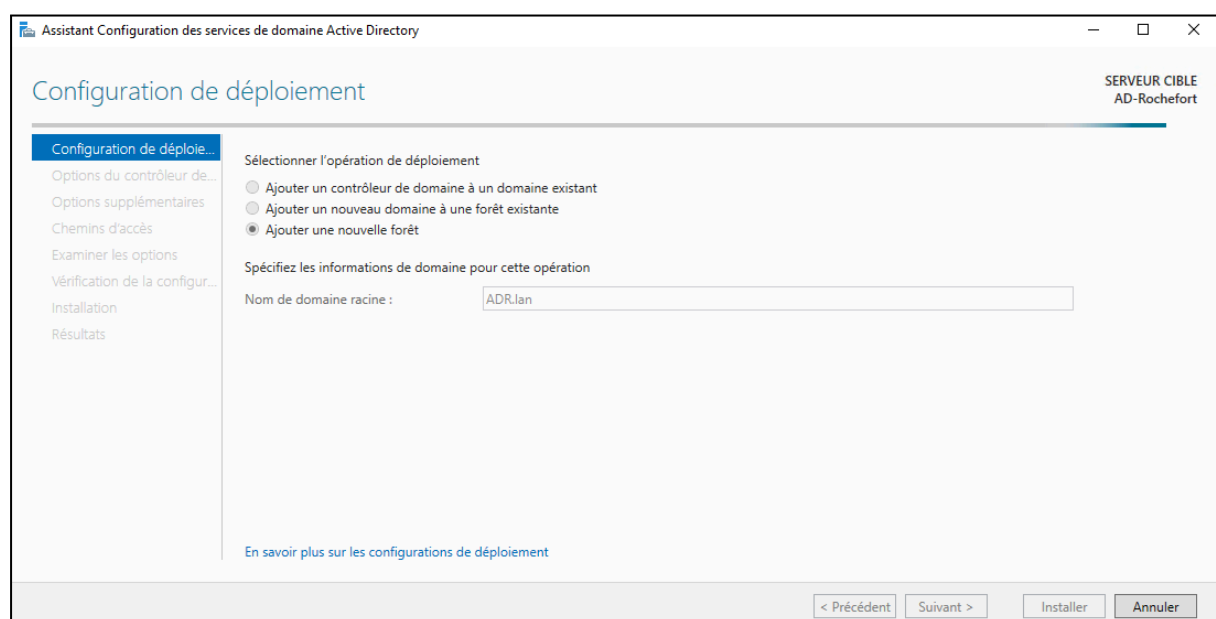
Premièrement, retourner dans le ‘Gestionnaire de serveur’

Puis suivre les étapes ci-après.



## 3.2 Configuration du déploiement

Comme nous installons notre premier serveur, il faut donc “Ajouter une nouvelle forêt”. C’est un ensemble de domaines Windows qui se font confiance (ceci s’applique aux très grandes entreprises).





## Options du contrôleur de domaine

Assistant Configuration des services de domaine Active Directory

Options du contrôleur de domaine

SÉVEUR CIBLE  
AD-Rochefort

Configuration de déploie...  
**Options du contrôleur de...**  
Options DNS  
Options supplémentaires  
Chemins d'accès  
Examiner les options  
Vérification de la configur...  
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 : .....

[En savoir plus sur les options pour le contrôleur de domaine](#)

< Précédent Suivant > Installer Annuler

Niveau fonctionnel : chaque version de Windows apporte ses améliorations. La compatibilité est descendante (Windows 2016 est compatible avec le niveau fonctionnel Windows 2012 mais Windows 2003 n'est pas compatible avec le niveau fonctionnel Windows 2008 R2). Le choix dépend donc de l'existant sur le réseau : ici, on choisit 2016 puisque le serveur est seul.

Surtout on laisse coché "Serveur DNS" qui sera lui aussi installé. Absolument indispensable à AD

Mot de passe pour la restauration de l'annuaire : forcément différent de celui de l'administrateur puisque les données de l'administrateur sont dans l'annuaire

### Options DNS

On laisse le choix par défaut (pas de délégation DNS pour le moment).

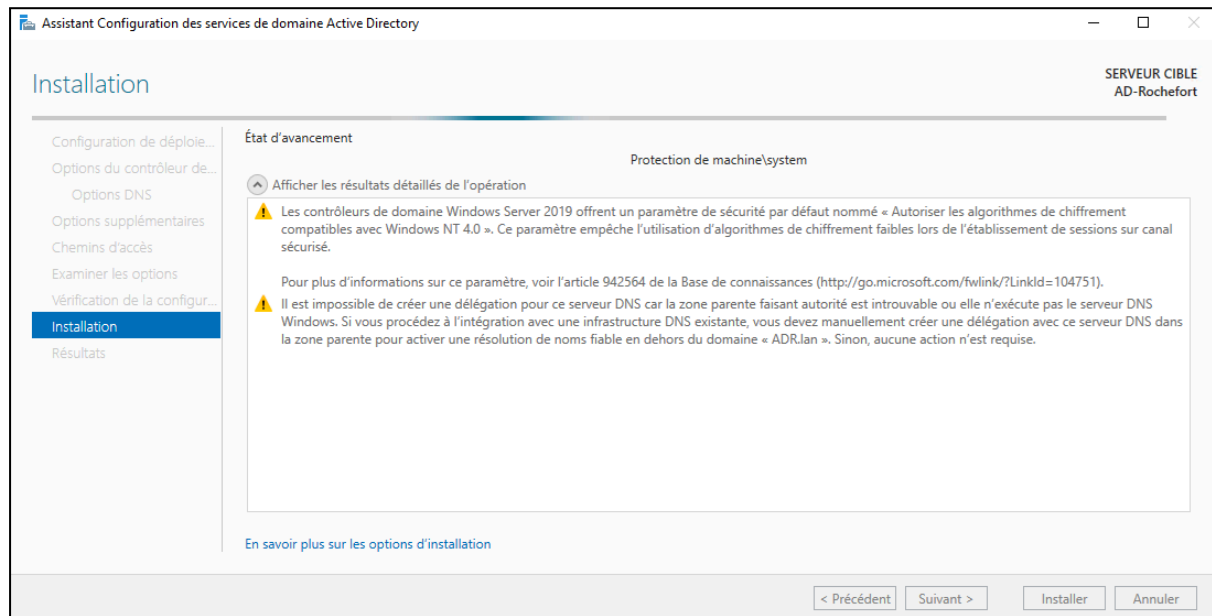
### Options supplémentaires

Nom NetBIOS : le même que le nom de domaine mais sans le .local

### Chemins d'accès

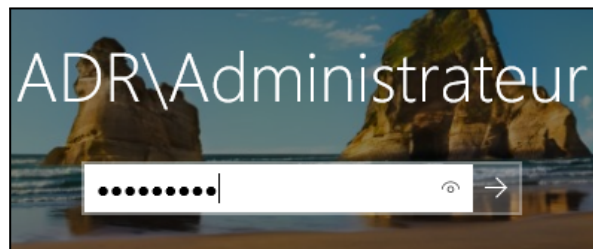
Chemins d'accès pour les fichiers Active Directory : éventuellement stocker sur des disques différents la base de données et les fichiers journaux afin de mieux répartir la charge en lecture/écriture.

Une fois configuré et vérifié on installe donc le tout :

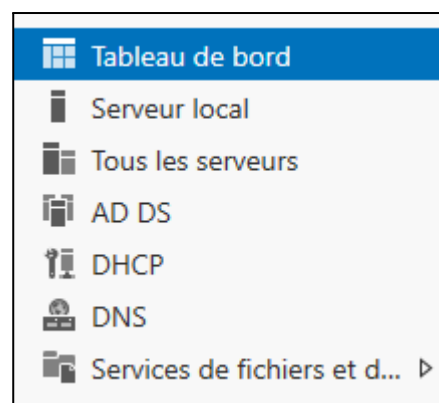


### 3.3 Découverte des services

Après le redémarrage, on peut constater un premier changement sur l'écran de connexion qui fait apparaître le domaine :

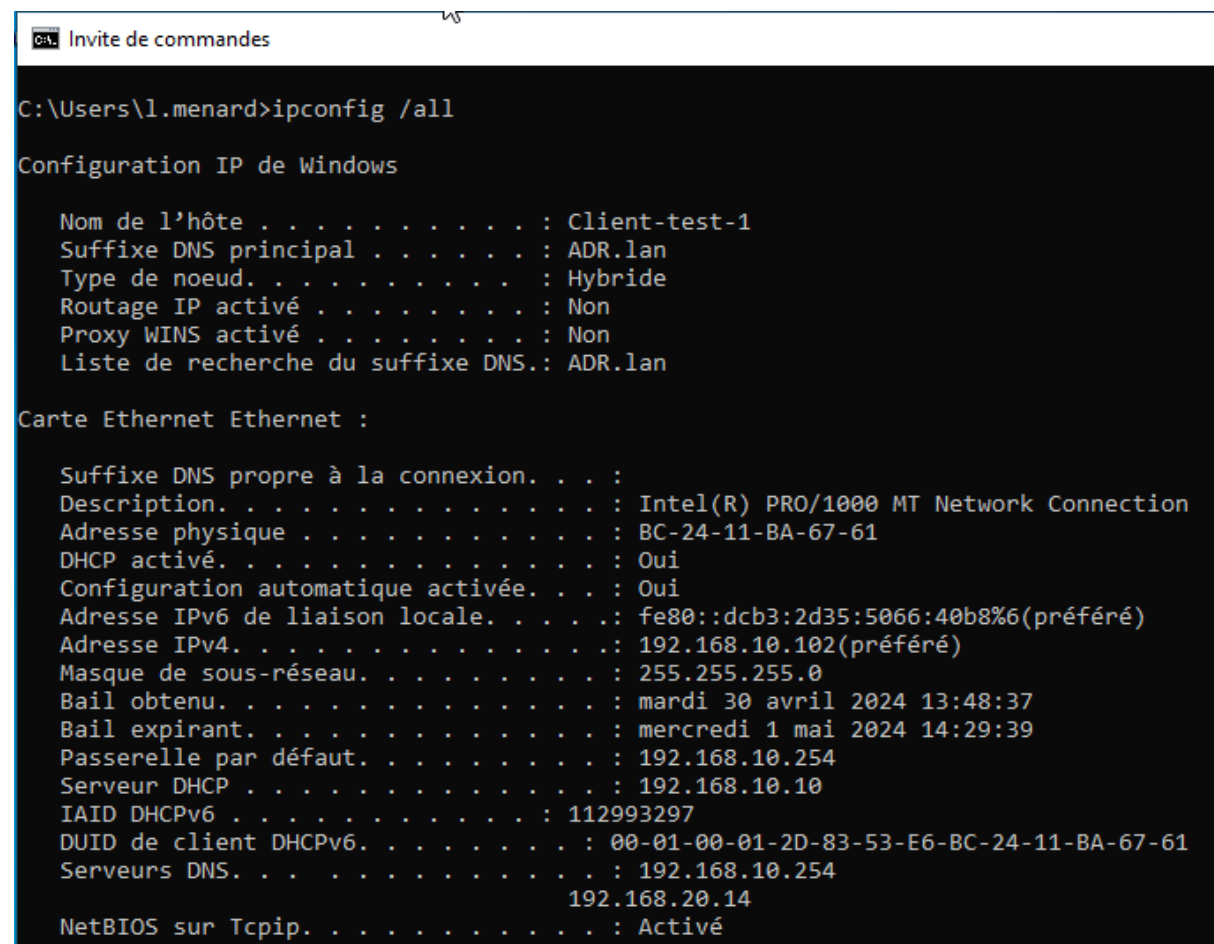
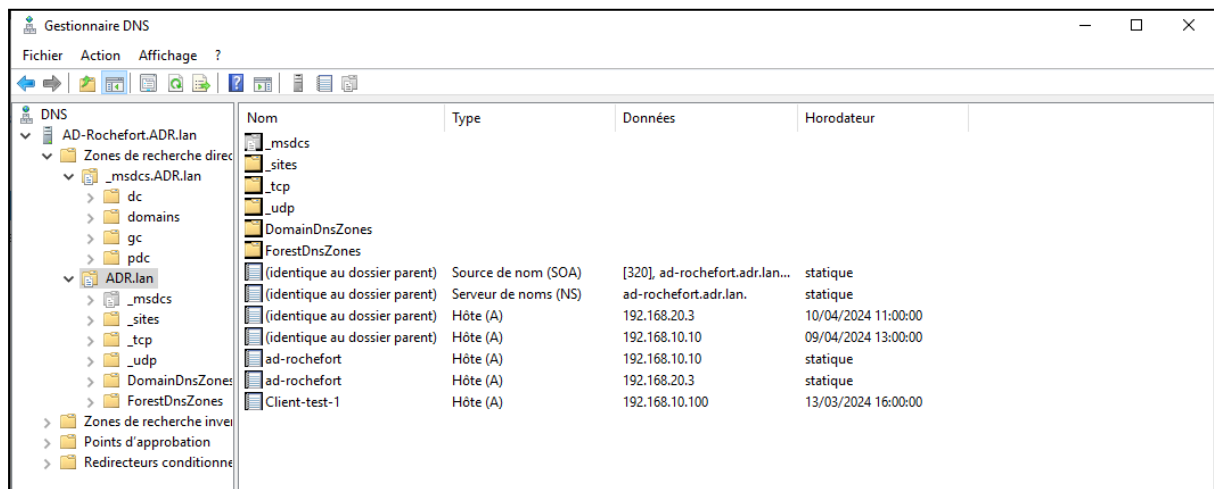


Nous avons maintenant un contrôleur de domaine tout beau tout propre, prêt à accueillir utilisateurs et ordinateurs. Observons les nouveaux outils à notre disposition : (Vous devez avoir sur votre AD plus ou moins cela)



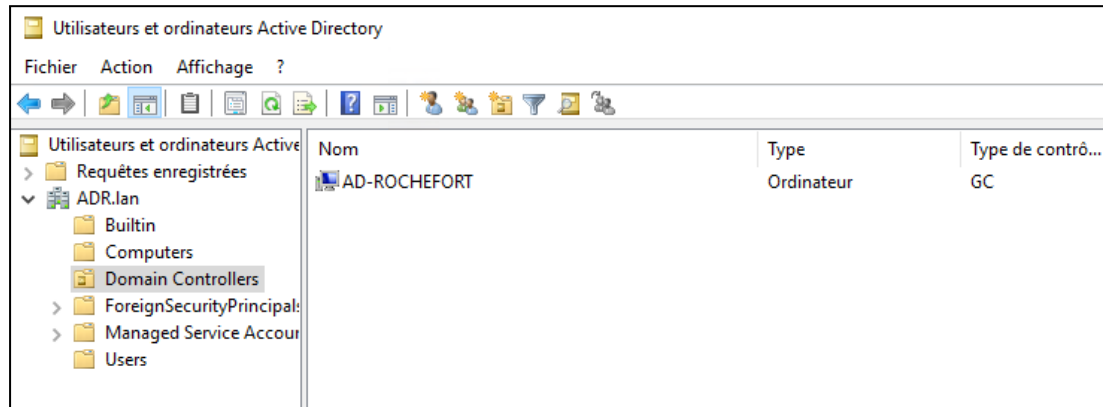
## 3.4 Serveur DNS

Aller dans “Outils \ DNS”, nous pouvons observer ceci :



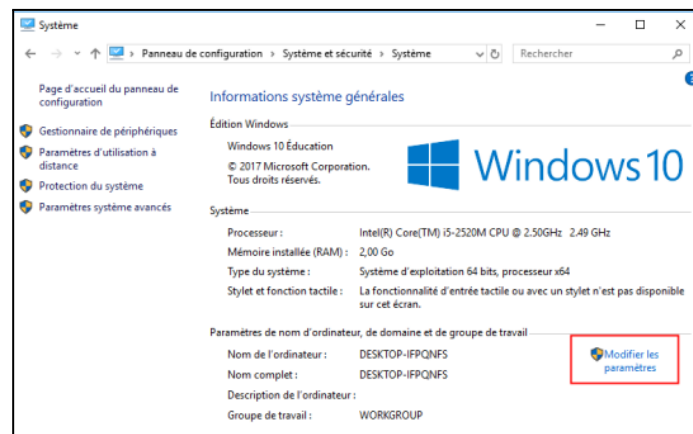
## 3.5 Services AD DS

Allez maintenant dans "Outils\Utilisateurs et Ordinateurs Active Directory". En dépliant l'arborescence, dans "Domain Controllers" nous retrouvons notre serveur :

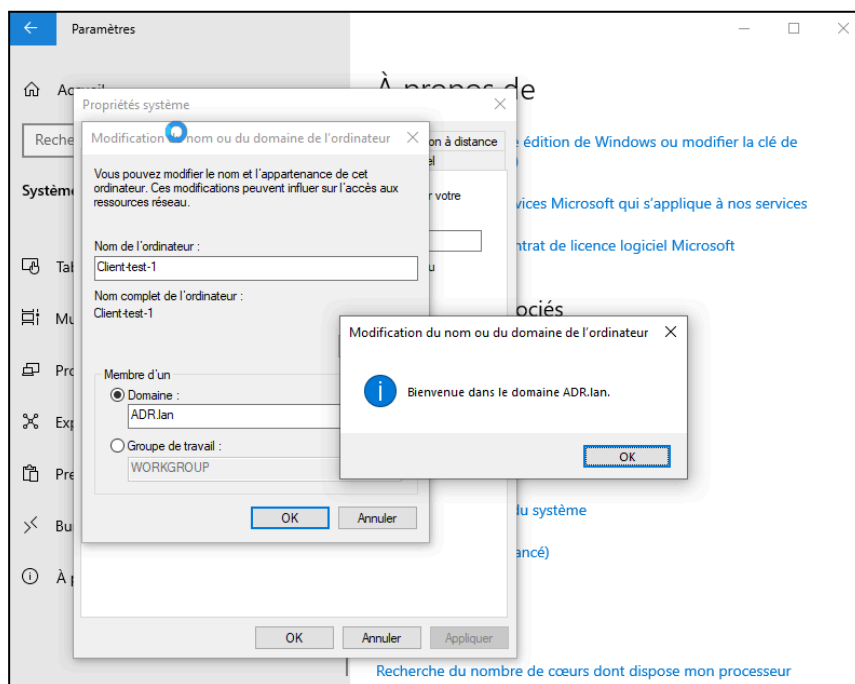


## 4. Joindre le client au domaine Windows

Allez dans "panneau de configuration" / "Système et sécurité" / "Système" :



Cliquez sur "modifier les paramètres" puis indiquez un nom de machine "propre" et le nom de votre domaine :

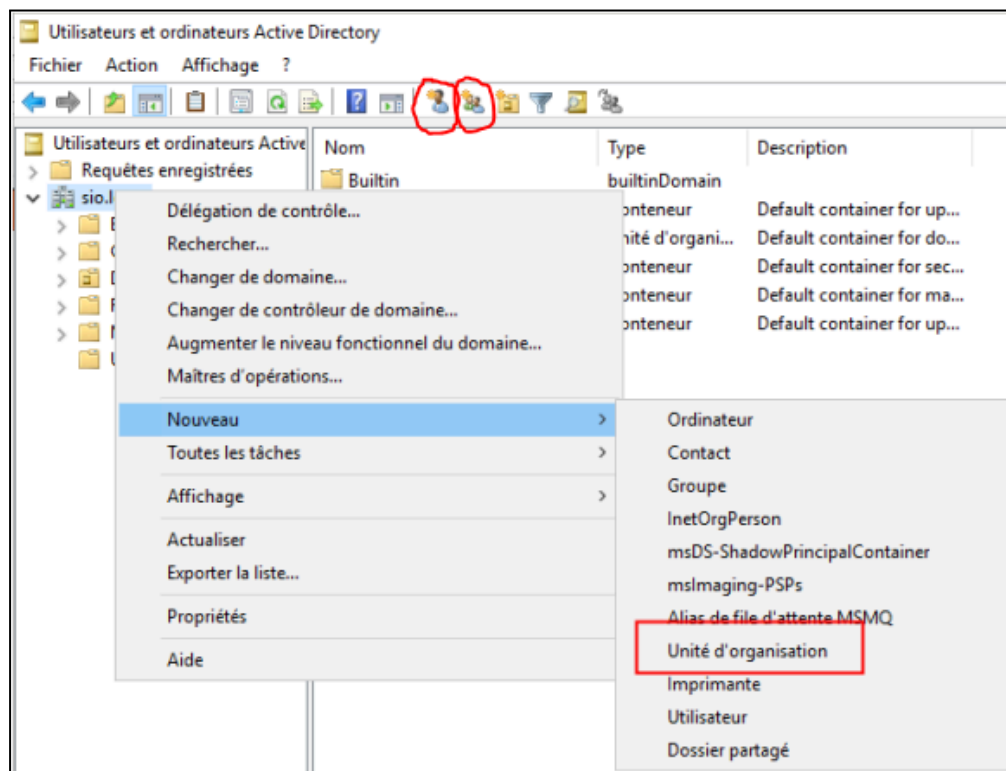


Ensuite, on vous demande un compte autorisé : entrez le compte administrateur de votre domaine.

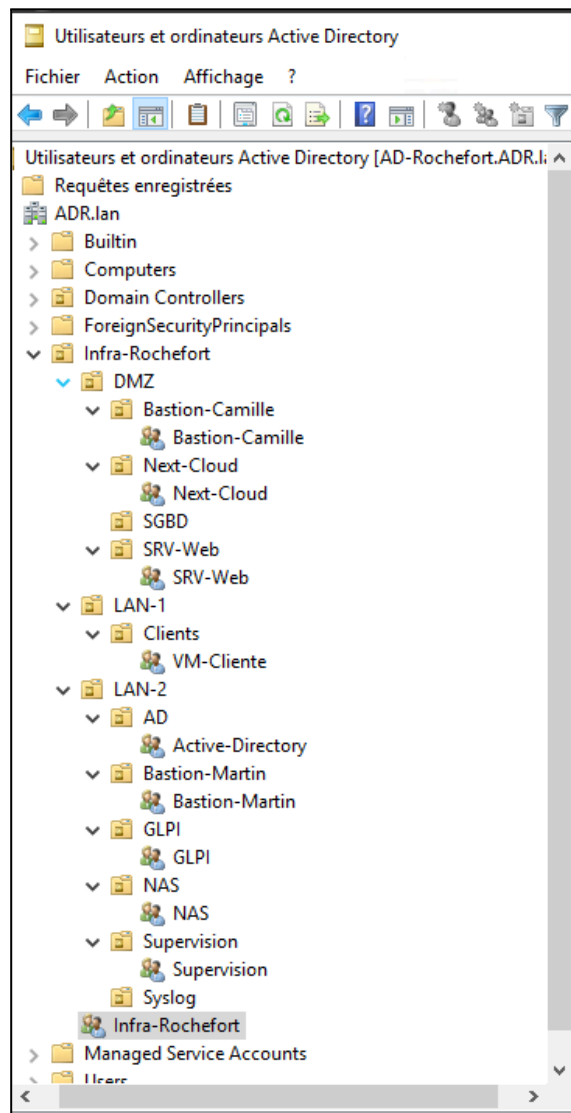
## 5. Gestion des utilisateurs du domaine

### 5.1 Création des unités d'organisation (UO)

En utilisant les boutons en rouge ci-dessous créer votre propre architecture pour cela.



Pour ma part ça vas ressembler à cela :



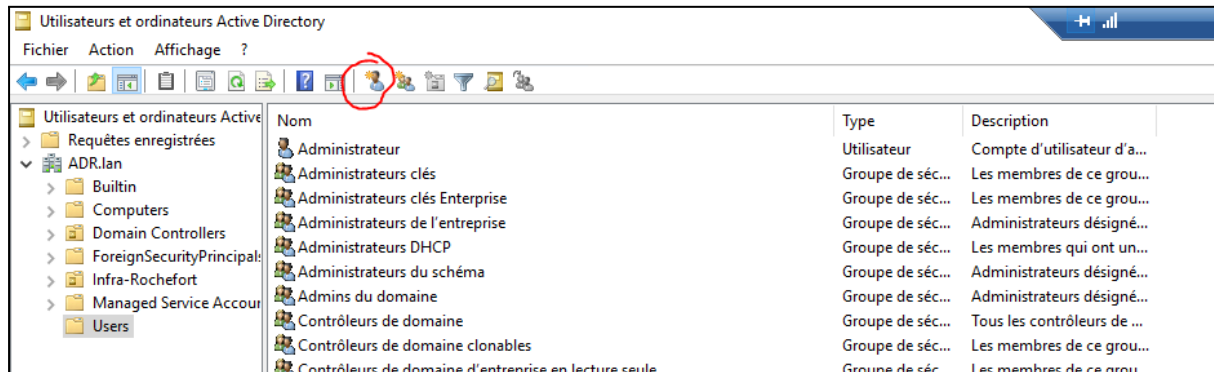
Ensuite il suffit de relier les utilisateurs créés pour les mettre dans les groupes qui leur correspondent.

On sélectionne les utilisateurs puis clique droit et ajoute à un groupe.

Enfin on choisit les groupes auxquels les relier.

## 5.2 Création Utilisateurs

Tout d'abord aller dans l'OU souhaité puis créer un utilisateurs en cliquant sur le boutons entourés en rouge ci-dessous.



Ensuite entrent les informations que vous souhaitez.

Nouvel objet - Utilisateur

Créer dans : ADR.Jan/Users

Prénom :  Initiales :

Nom :

Nom complet :

Nom d'ouverture de session de l'utilisateur :  @ADR.Jan

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

< Précédent Suivant > Annuler

Ensuite entrer le mot de passe avec un type style : azerty! qui seront ensuite changés par l'utilisateur.

Nouvel objet - Utilisateur

Créer dans : ADR.Jan/Users

Mot de passe :

Confirmer le mot de passe :

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

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

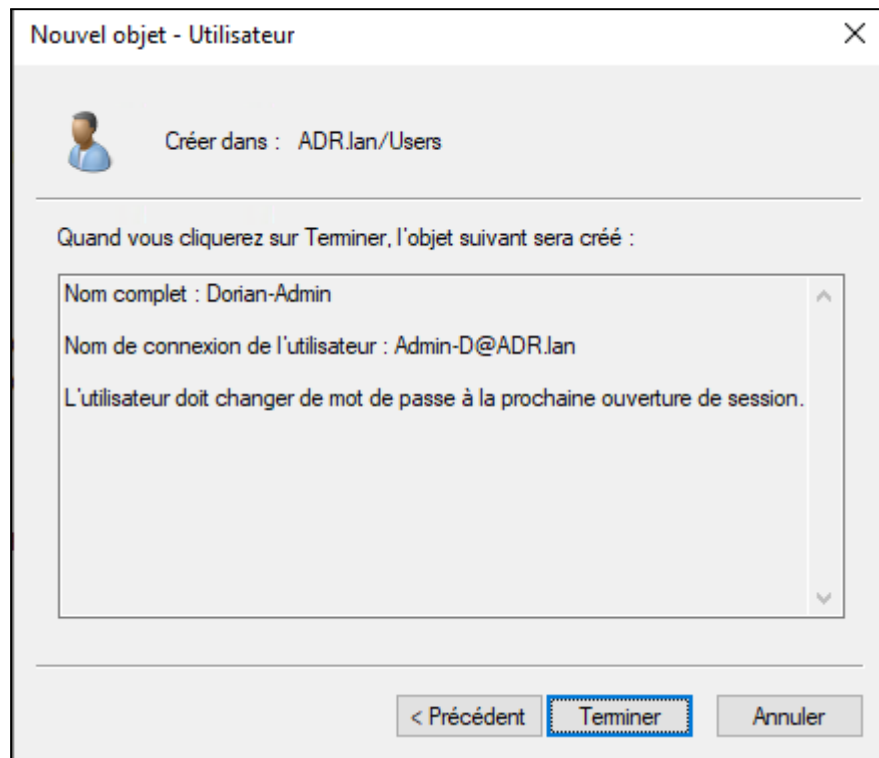
☐ Le mot de passe n'expire jamais

☐ Le compte est désactivé

< Précédent Suivant > Annuler

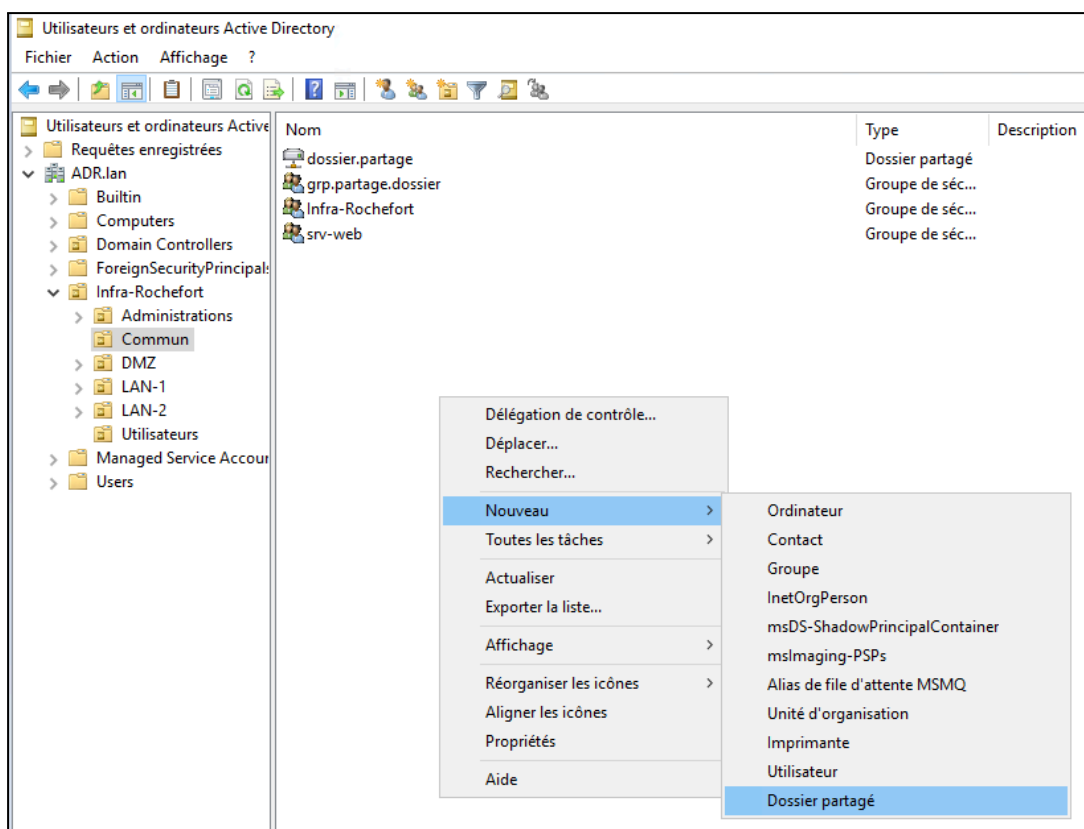


Enfin on vérifie les données entrées et on valide.

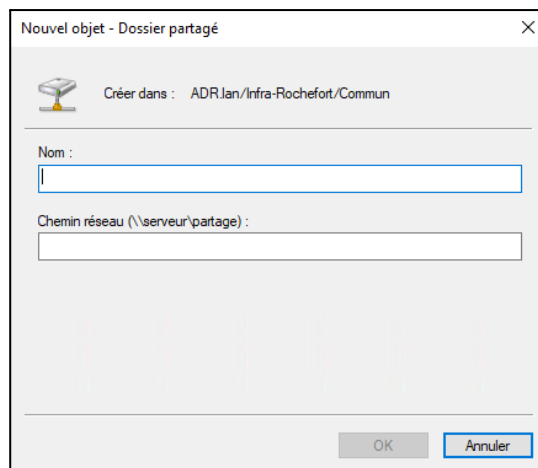


### 5.3 Création d'un dossier partagé.

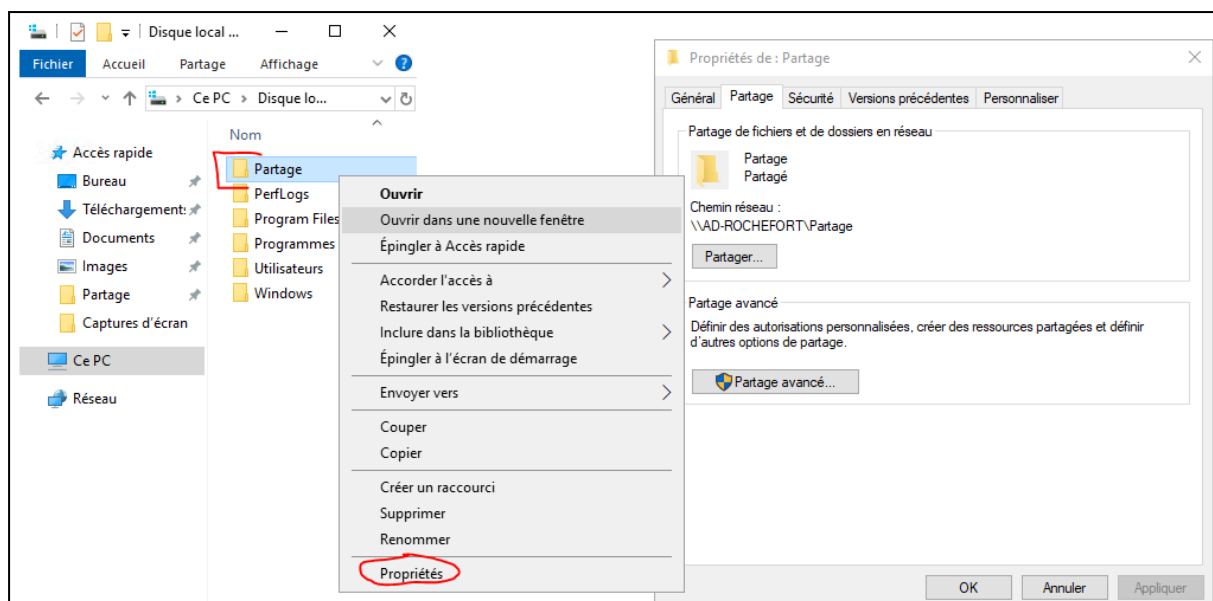
Pour créer ce dossier il faut cliquer droit dans une OU puis faire nouveau et dossier partagé comme ci-dessus.



Ensuite entrer les informations souhaitées et valider cela en faisant OK.



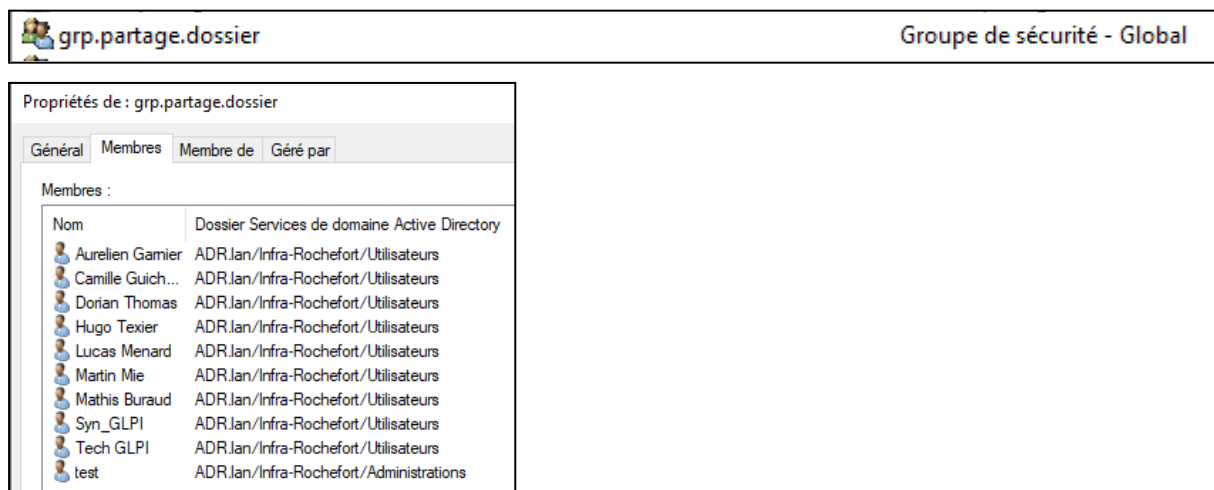
Par la suite, on va donc voir les propriétés du dossier partagés.



On va enfin pouvoir le partager avec les utilisateurs ayant les permissions.

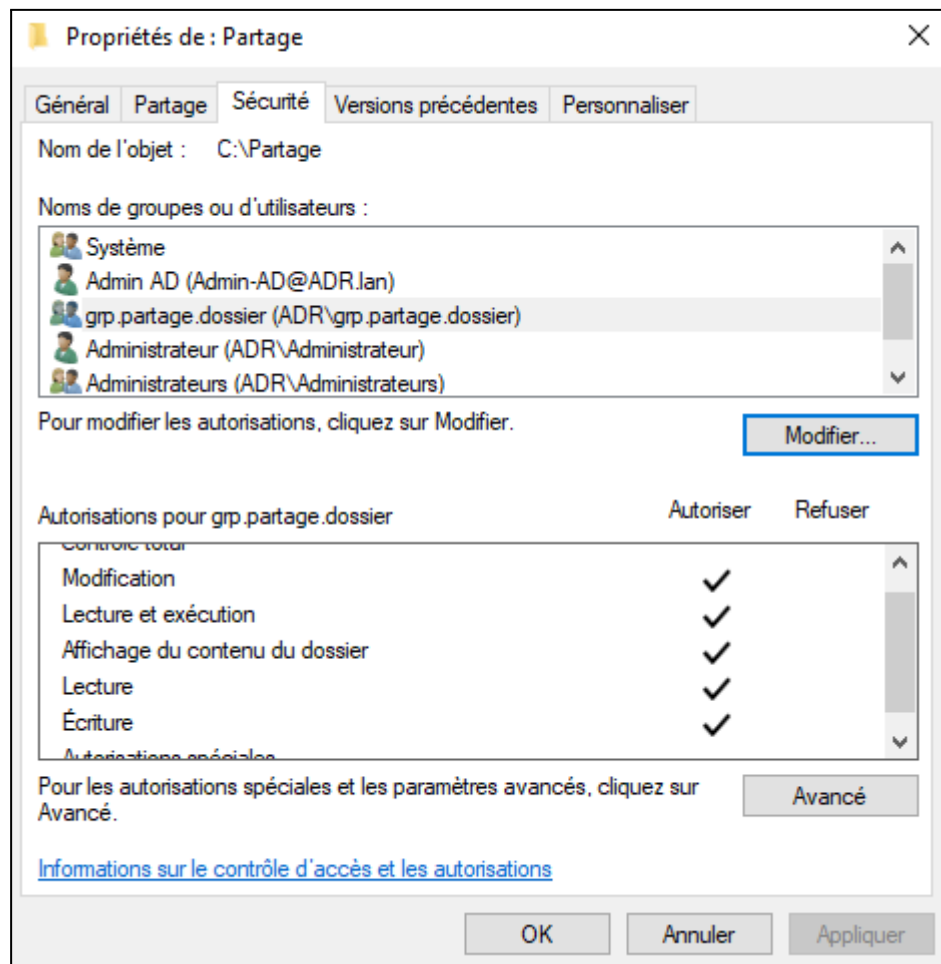
*Au préalable, on crée un groupe dans un onglet "commun" de préférence afin de le rajouter dans le groupe de sécurité du dossier.*

Comme ci-dessous :

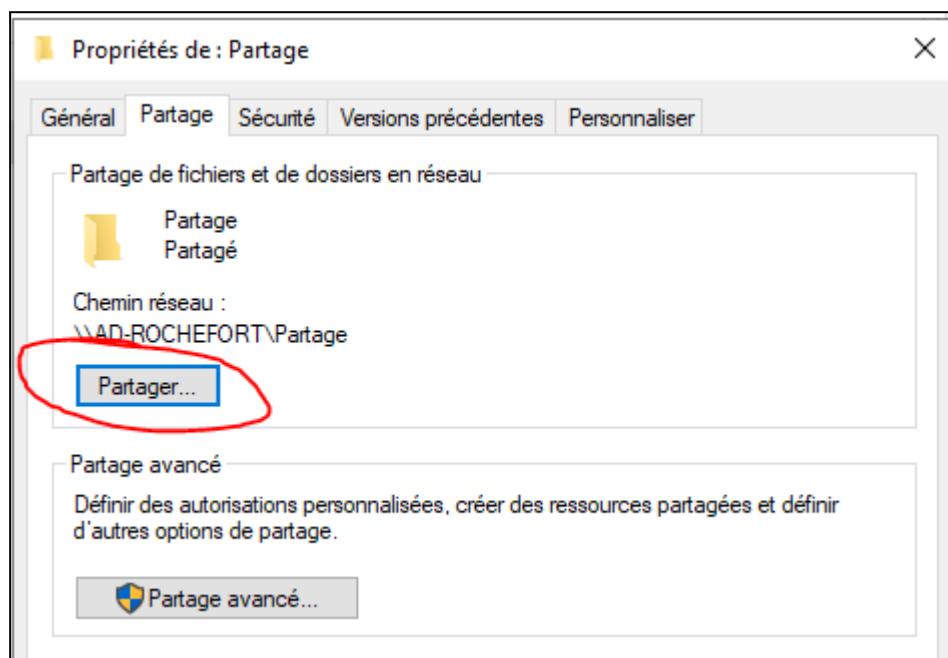


On repasse donc dans l'onglet propriétés :

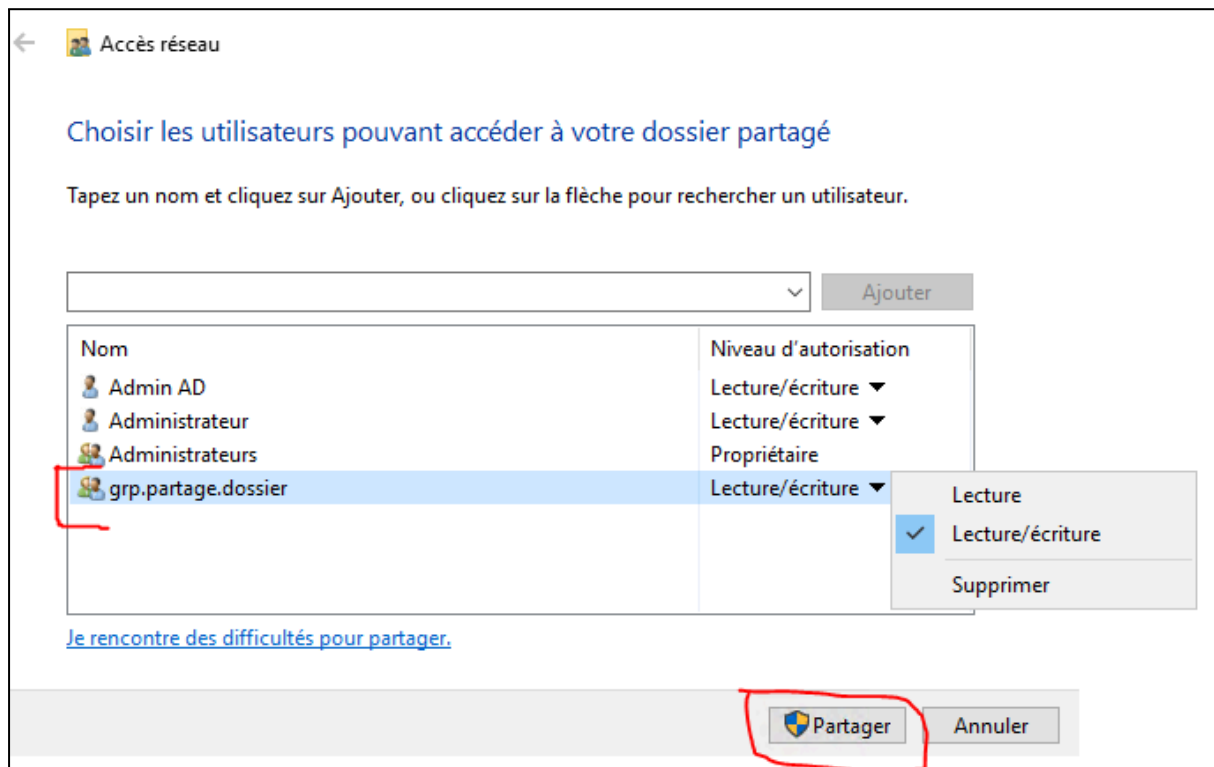
Ajouter le grp créé auparavant avec les users et cliquer sur le boutons modifier afin de leur autoriser tout sauf le contrôle total, possible d'adapter suivant les nécessités.



Enfin retourner en arrière et cliquer sur Partager.



Donner la lecture/écriture et faire partager.

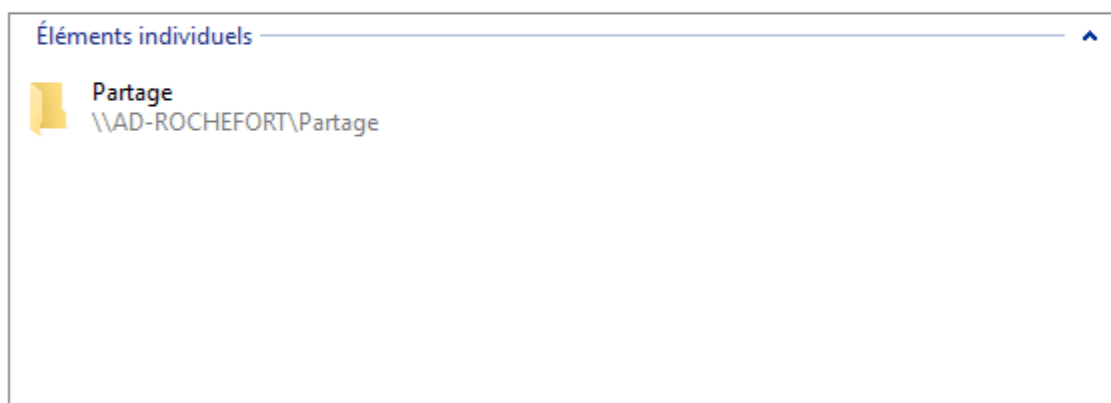


Enfin une fois cela fait on peut donc valider et voir le répertoires du dossier a mettre sur les clients LAN.

Accès réseau

Votre dossier est partagé.

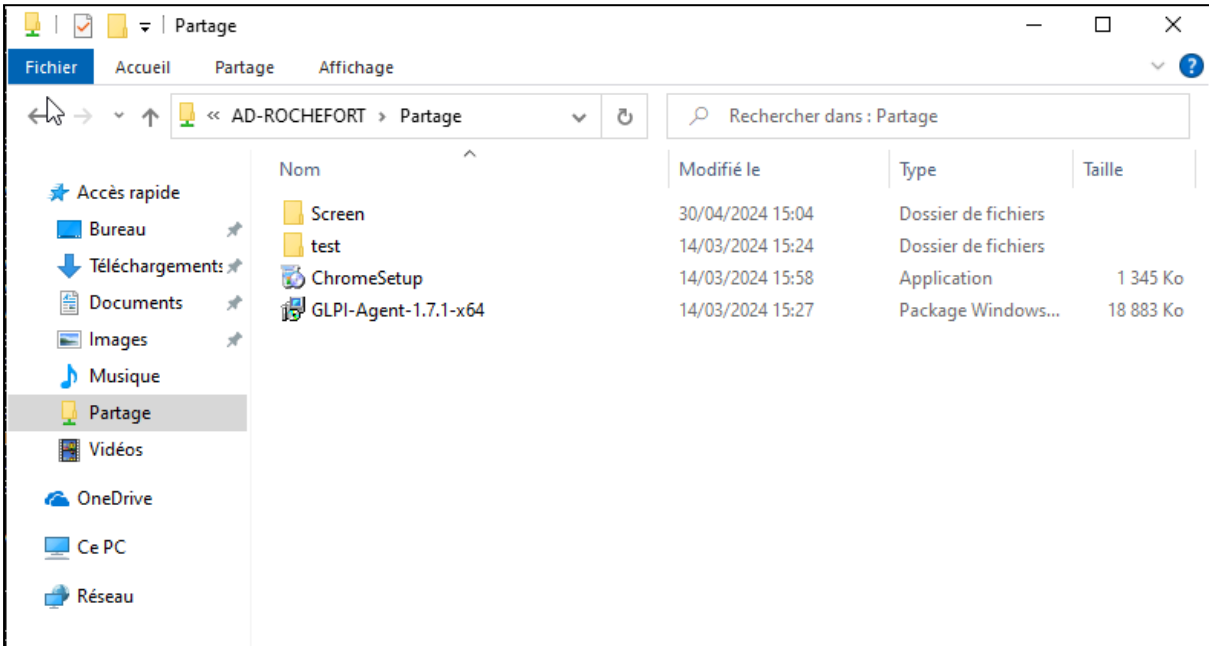
Vous pouvez [envoyer](#) à quelqu'un par courrier électronique ces liens vers des éléments partagés, ou [copier](#) et coller les liens dans une autre application.



[Afficher tous les partages réseau de cet ordinateur.](#)

Terminé

Maintenant on se rend sur la VM-cliente g rer par l'AD et on entre le lien.



## 6 V rification.

Enfin pour valider tout cela on va aller sur le client et lancer une requ te sur internet pour valider l'acc s   internet, pour le reste les autres capture de v rification sont pr sent es   chaque  tape.

