

Installation et mise en place des fonctionnalités de base



Lycée Turgot – BTS SIO – PESCASIO Aaron

Option SISR – Solutions d'infrastructures, Systèmes et Réseaux

Sommaire

Introduction.....	1
Windows Server 2019 & Active Directory	3
Configuration & Installation AD.....	4
Mise en place d'un serveur de fichiers.....	16
Sécurisation AD.....	19

Windows Server 2019

Windows Server 2019 est une version serveur du système d'exploitation Windows, développé par Microsoft, et basé sur l'interface de Windows 10 (NT4). Il permet de mettre en place des services, sur un réseau, avec des fonctionnalités dédiées aux entreprises comme :

- Service d'annuaire (Active Directory, basé sur LDAP) ;
- Attribution d'adresses IP (DHCP) ;
- Résolveur de nom de domaine (DNS) ;
- Service d'impression, etc... ;

Pour procéder à l'installation d'un environnement Windows Server 2019, il faut :

- L'image disque d'installation du système (format disque ou clé USB bootable) ;
- Une machine virtuelle ou un serveur physique.

Active Directory

Un domaine Active Directory est une architecture d'annuaire, basé sur le protocole LDAP, développé par Microsoft. Un domaine Active Directory est géré par un ou plusieurs contrôleurs de domaines disposant des services Active Directory et DNS.

Cet annuaire permet la gestion des utilisateurs et des ordinateurs, en appliquant des permissions, de créer des groupes et d'attribuer des GPO (Group Policy Object : règles de sécurité applicables à un utilisateur ou un ordinateur). Chaque utilisateur enregistré dans l'annuaire pourra se connecter sur les ordinateurs joints au domaine.

Pour procéder à la mise en place d'un domaine Active Directory, il faut :

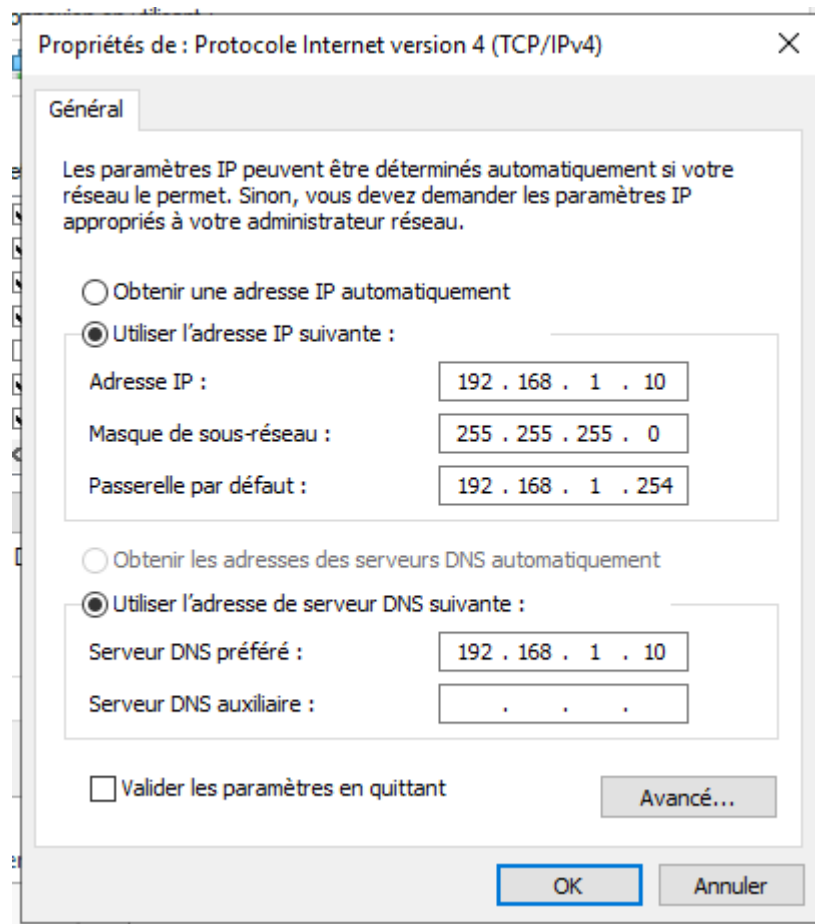
- Un environnement Windows Server 2019 avec :
- Une adresse IP fixe ;
- Un nom d'hôte défini.

Windows serveur 2019

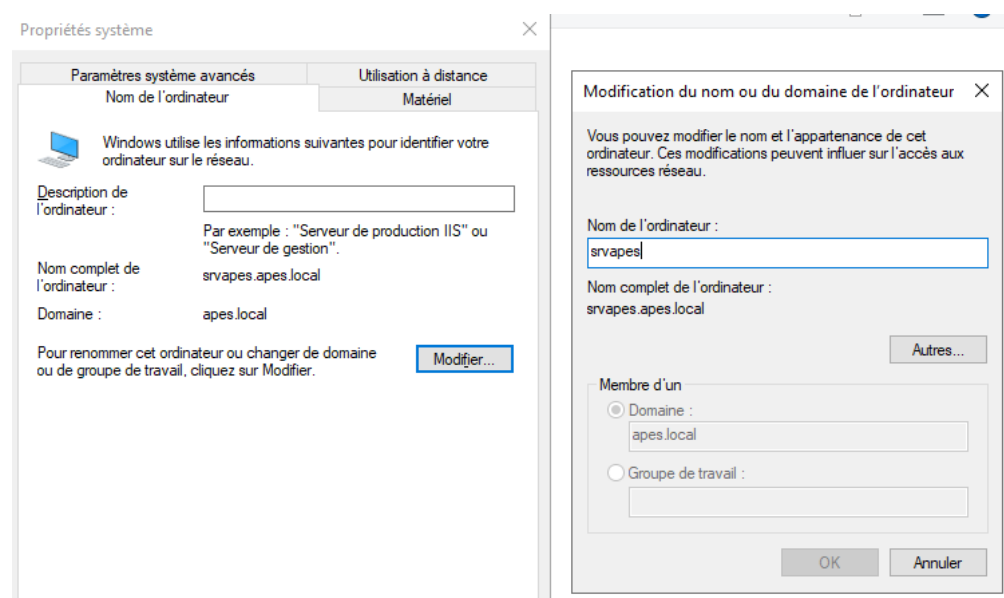
Nous utilisons une machine virtuelle Windows serveur 2019, dans lequel rien n'a été installé, il faut que l'Active Directory soit la première installation sur la machine. Il faut bien être connecté en administrateur sur la machine.

Dans un premier temps, il faut configurer une @IP statique sur le serveur, lui renseigner la passerelle du Firewall/Routeur, ainsi que son DNS local, car il doit être capable de résoudre lui-même son nom de domaine

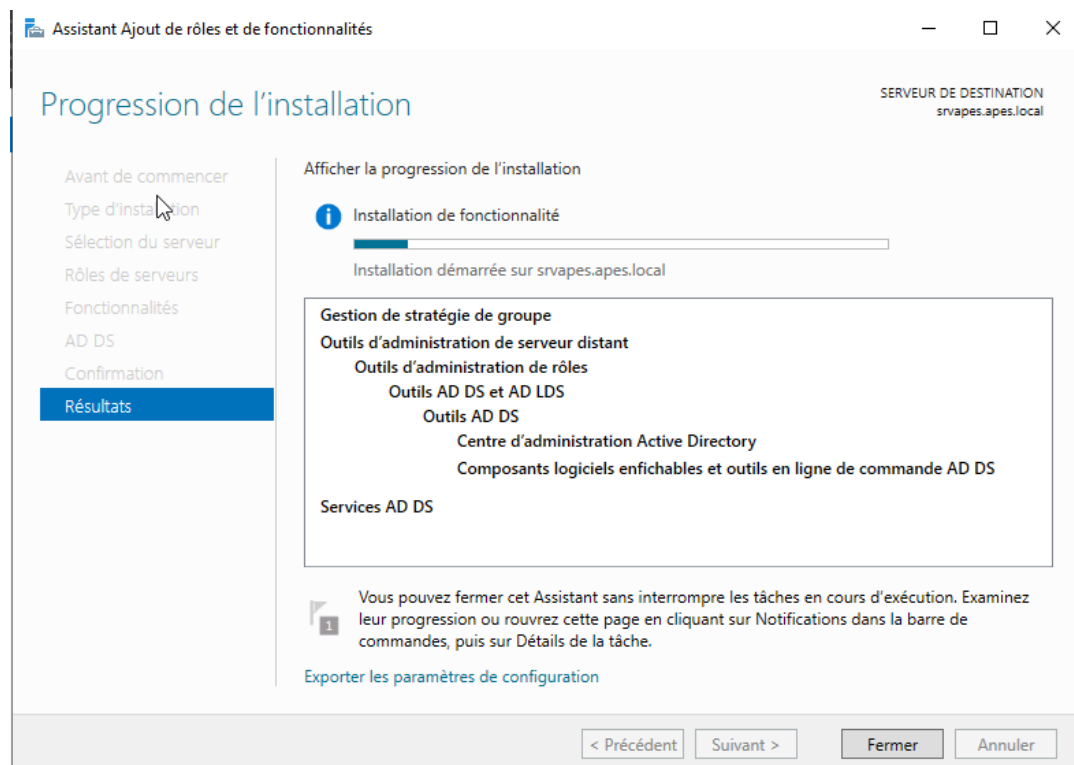
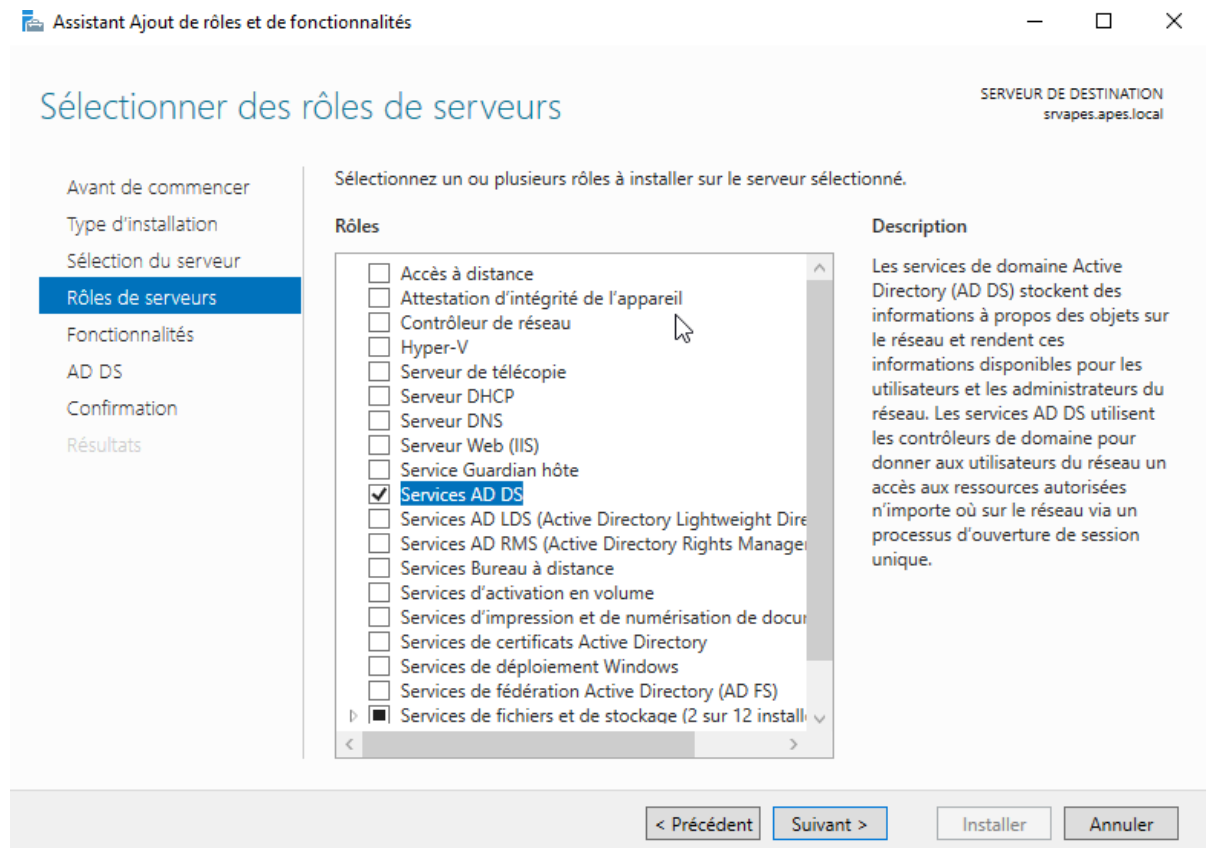
Propriétés de : Protocole Internet version 4 (TCP/IPv4)



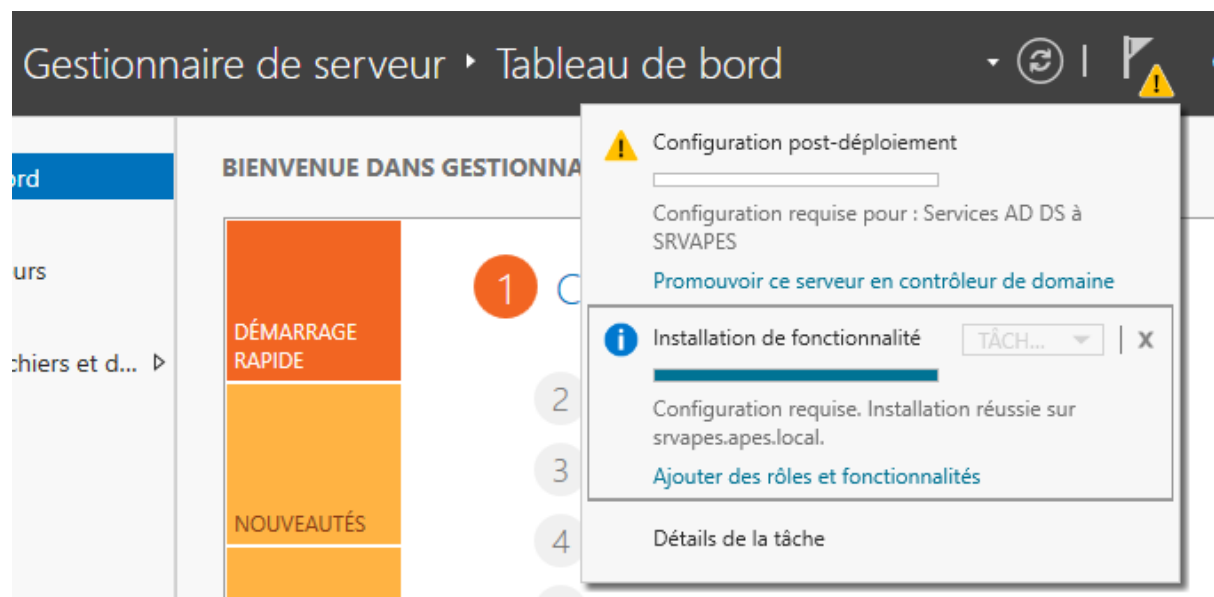
On peut changer en suite le nom du serveur pour mieux se visualiser et puis on redémarre la machine virtuelle pour l'actualiser



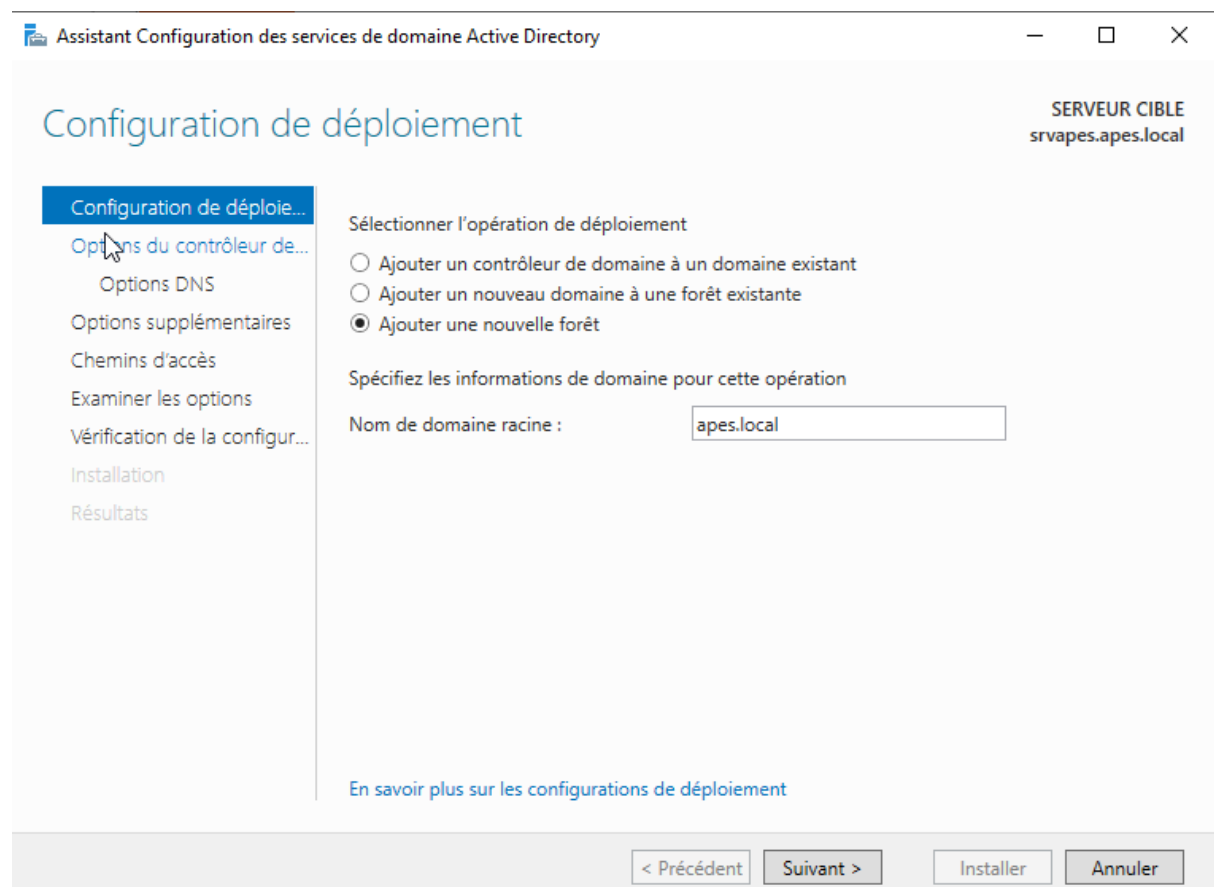
On peut ensuite installer le service AD DS depuis le gestionnaire de serveur (Gérer -> Ajouter des rôles et fonctionnalités)



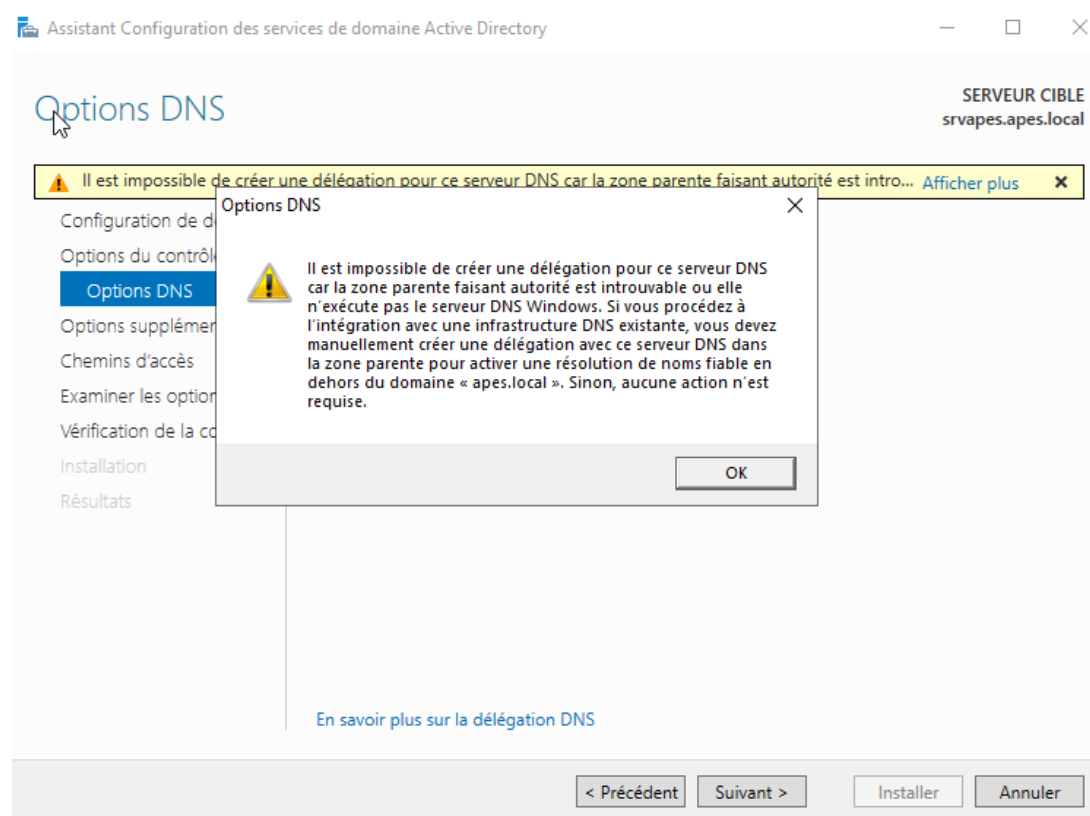
Ensuite, il faut promouvoir le serveur en contrôleur de domaine



On choisira « Ajouter une nouvelle forêt » puis on met le nom de domaine.

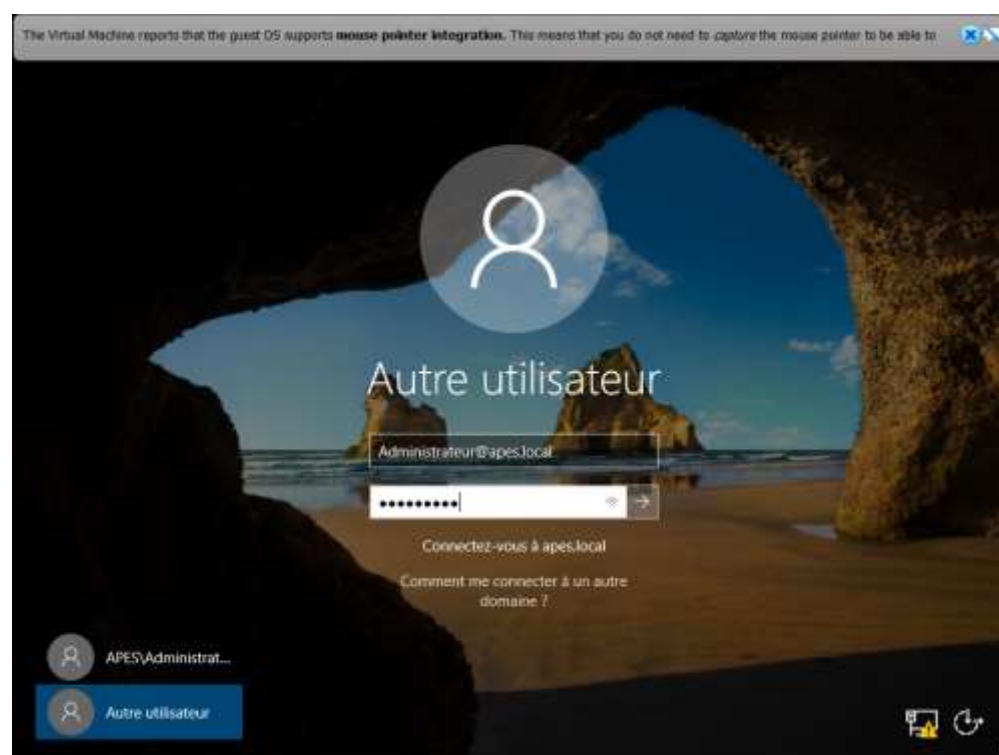


Cliquer sur suivant, vu que notre serveur fera office de parent DNS, cette erreur est normale

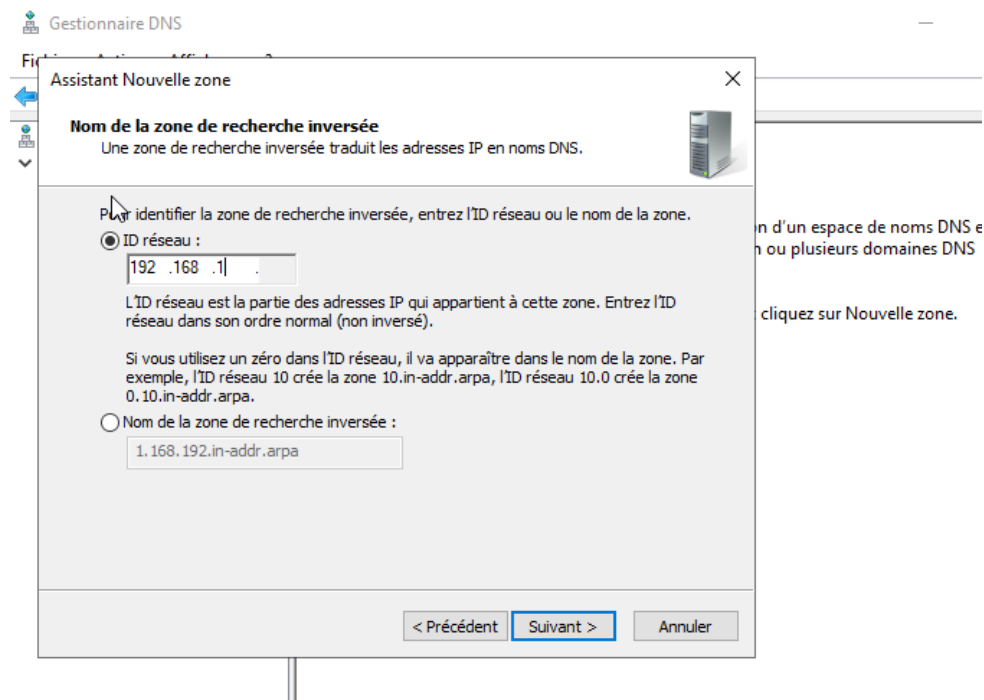


Après la configuration du serveur, on redémarre la machine virtuelle et l'installation des services va se faire tout seul. (Cela prendra plusieurs minutes)

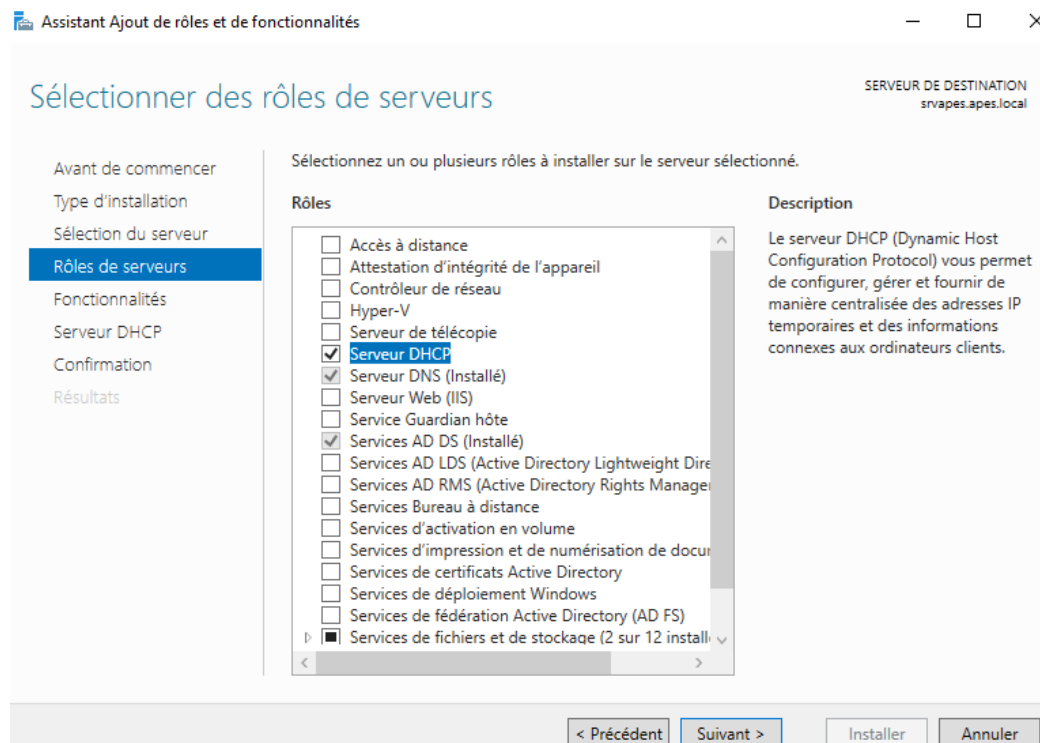
Le domaine apes.local est créé, il est donc nécessaire de se logger au serveur en admin via le domaine. « Administrateur@apes.local » pour se logger en admin.

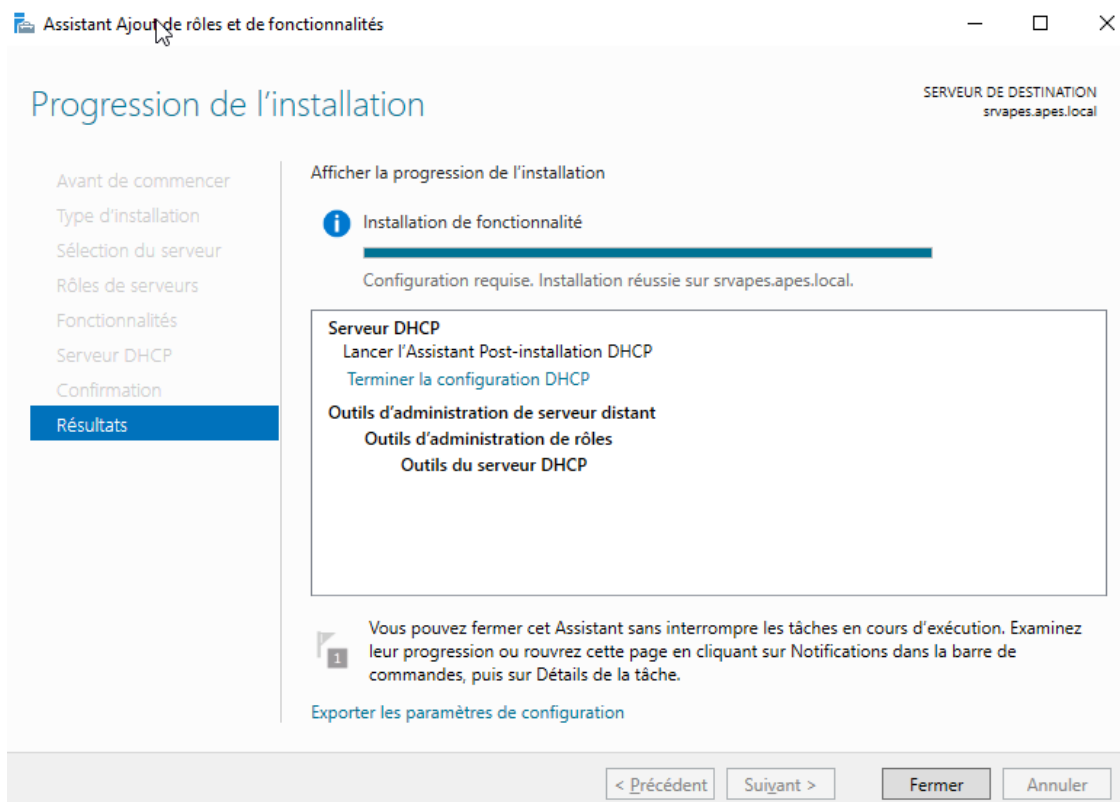


Nous pouvons maintenant finir de configurer le serveur DNS dans le gestionnaire DNS en ajoutant une nouvelle zone de recherche inversée

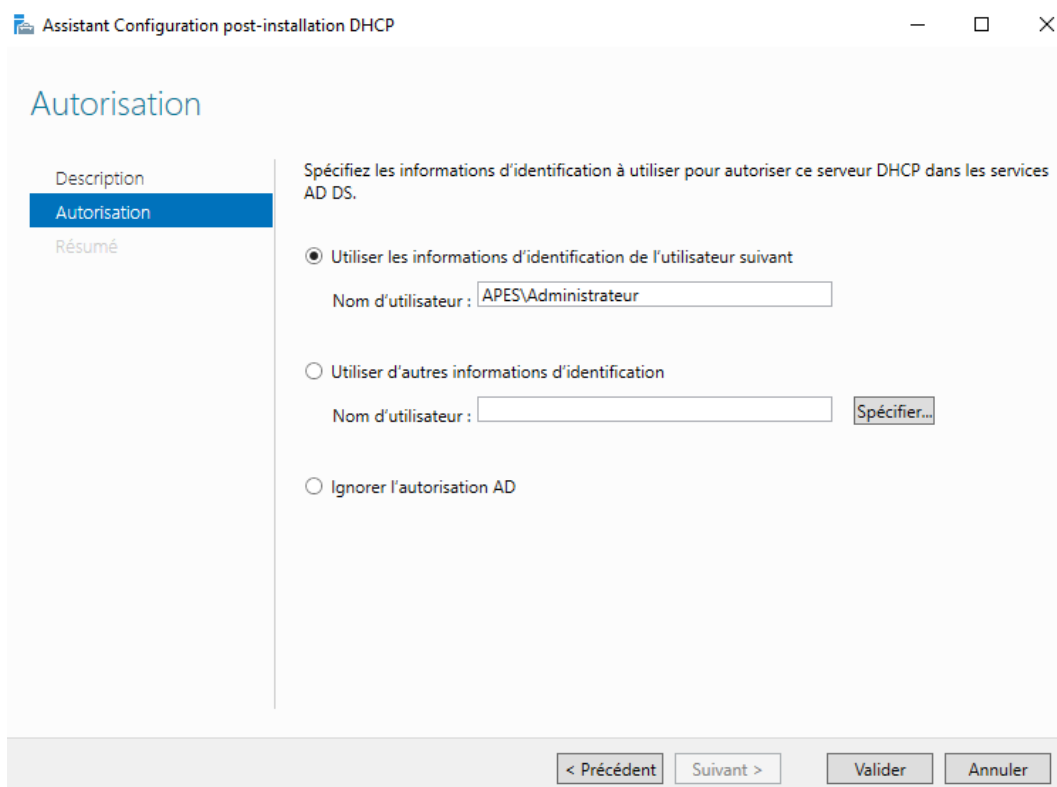


On installe ensuite le serveur DHCP



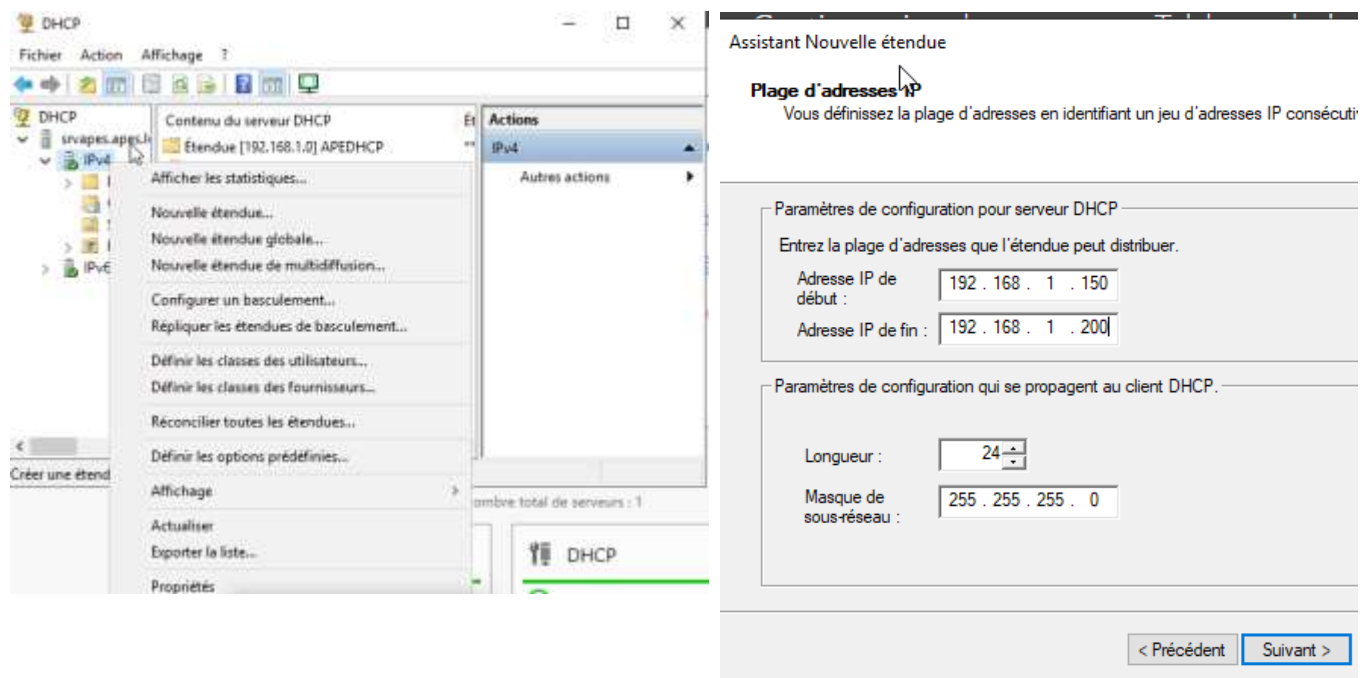


On cliquera après sur « Terminer la configuration DHCP »



Puis « Valider ».

Il faut ensuite créer une nouvelle étendue dans le gestionnaire DHCP



Assistant Nouvelle étendue

Configuration des paramètres DHCP

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



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

DHCP

< Précédent

Suivant >

Annuler

Assistant Nouvelle étendue



Routeur (passerelle par défaut)

Vous pouvez spécifier les routeurs, ou les passerelles par défaut, qui doivent être distribués par cette étendue.



Pour ajouter une adresse IP pour qu'un routeur soit utilisé par les clients, entrez l'adresse ci-dessous.

Adresse IP :

Ajouter

192.168.1.254

Supprimer

Monter

Descendre

< Précédent

Suivant >

Annuler

Assistant Nouvelle étendue

Nom de domaine et serveurs DNS

DNS (Domain Name System) mappe et traduit les noms de domaines utilisés par les clients sur le réseau.



Vous pouvez spécifier le domaine parent à utiliser par les ordinateurs clients sur le réseau pour la résolution de noms DNS.

Domaine parent :

Pour configurer les clients d'étendue pour qu'ils utilisent les serveurs DNS sur le réseau, entrez les adresses IP pour ces serveurs.

Nom du serveur :

Résoudre

Adresse IP :

Ajouter

192.168.1.10

Supprimer

Monter

Descendre

< Précédent

Suivant >

Annuler

Assistant Nouvelle étendue

Activer l'étendue

Les clients ne peuvent obtenir des baux d'adresses que si une étendue est activée.



Voulez-vous activer cette étendue maintenant ?

☒ Oui, je veux activer cette étendue maintenant

☐ Non, j'activerai cette étendue ultérieurement


< Précédent Suivant > Annuler

Notre serveur DHCP pourra distribuer des adresses IP de 192.168.1.150 jusqu'à 192.168.1.200 aux machines clients qui se trouvent dans le domaine.

Nous allons ensuite créer un utilisateur dans notre AD pour qu'on puisse se connecter avec cet utilisateur dans le domaine.

Nouvel objet - Utilisateur



 Créer dans : apes.local/Users

Prénom : Initiales :

Nom :

Nom complet :

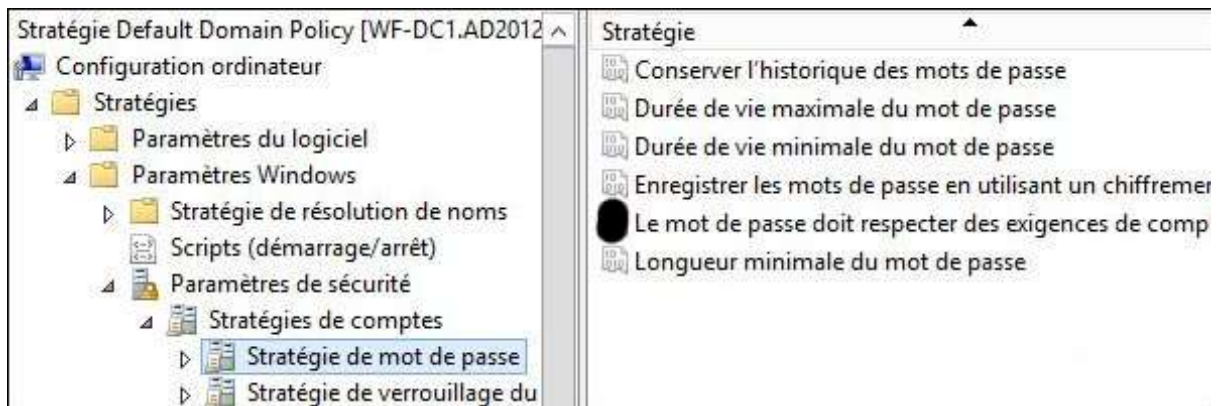
Nom d'ouverture de session de l'utilisateur :

@apes.local

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

< Précédent Suivant > Annuler

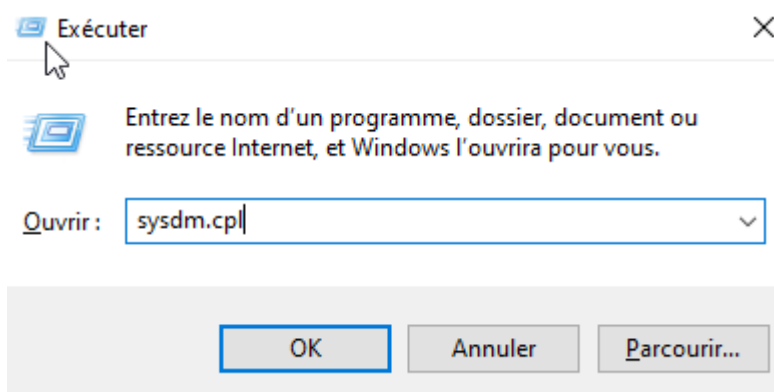
Pour ajuster les conditions de créations de mots de passe, il faut se rendre dans Outil > Gestion de stratégies de groupe > Forêt > Domaines > apes.local > Clic droit sur « Default Domain Policy » puis Config Ordinateur > Stratégies > Paramètres windows > Paramètres de sécurité > Stratégie de compte > Stratégie de mot de passe



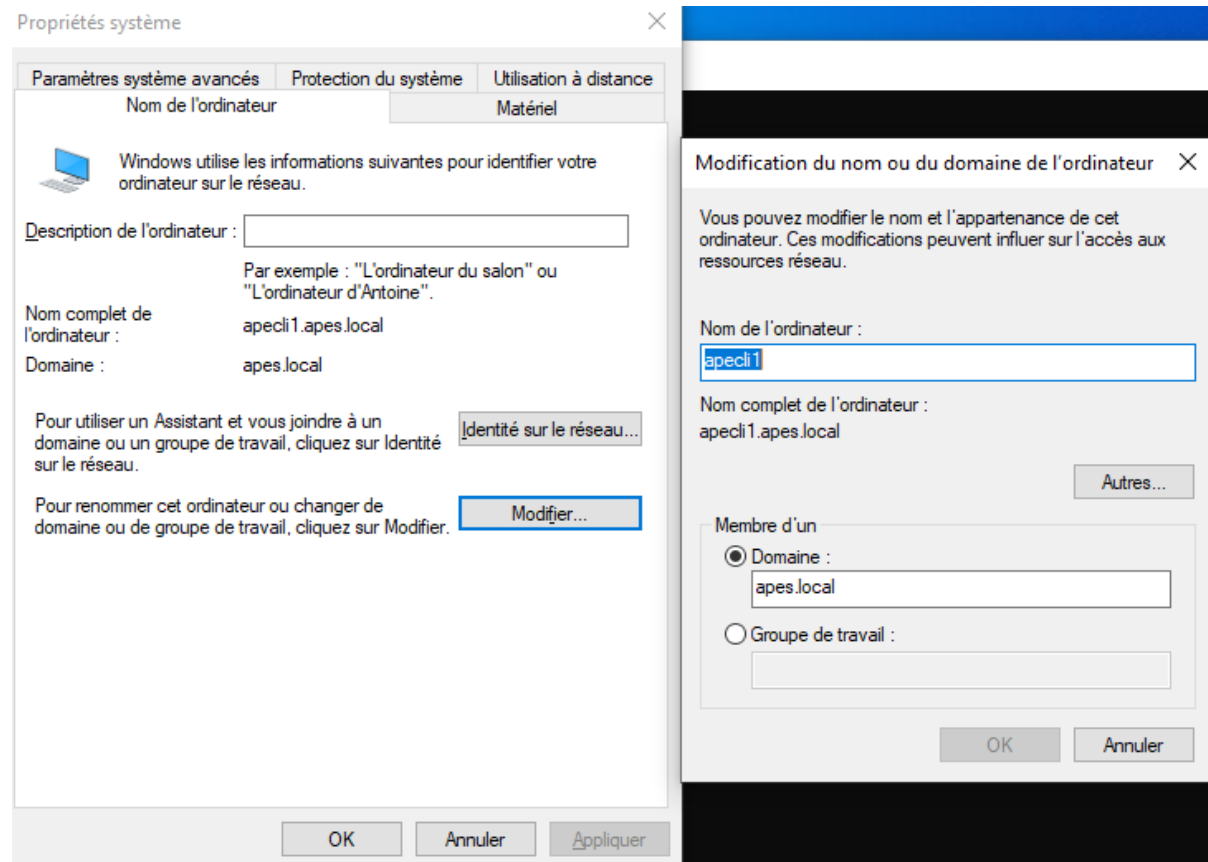
Ensuite, il faut taper la commande gpupdate /force pour appliquer les modifications de stratégie GPO

```
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.
```

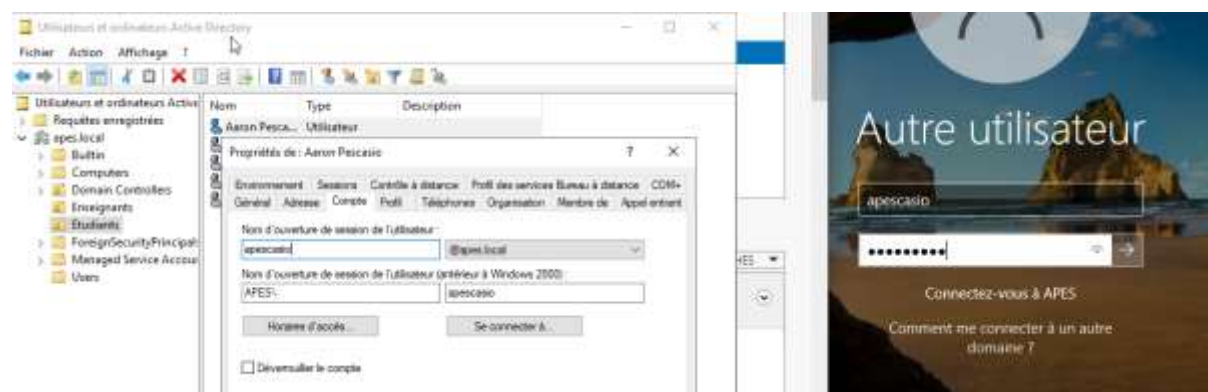
On peut joindre notre PC Client WINDOWS 10 à notre domaine en allant sur sysdm.cpl



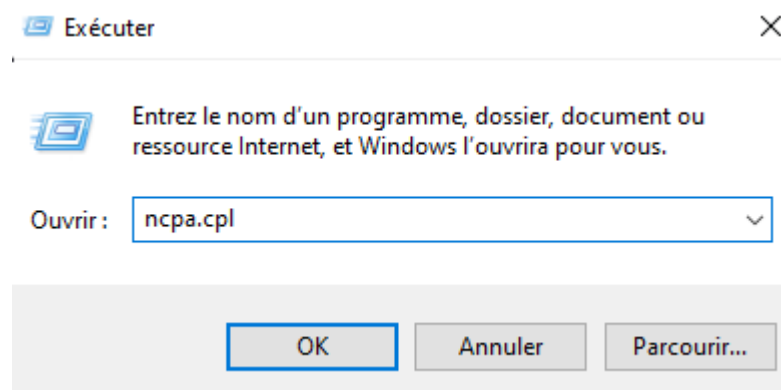
On mets le nom de notre domaine dans «Domaine : » : « apes.local » et on modifie le nom de l'ordinateur, ensuite on redémarre la machine virtuelle pour l'actualiser



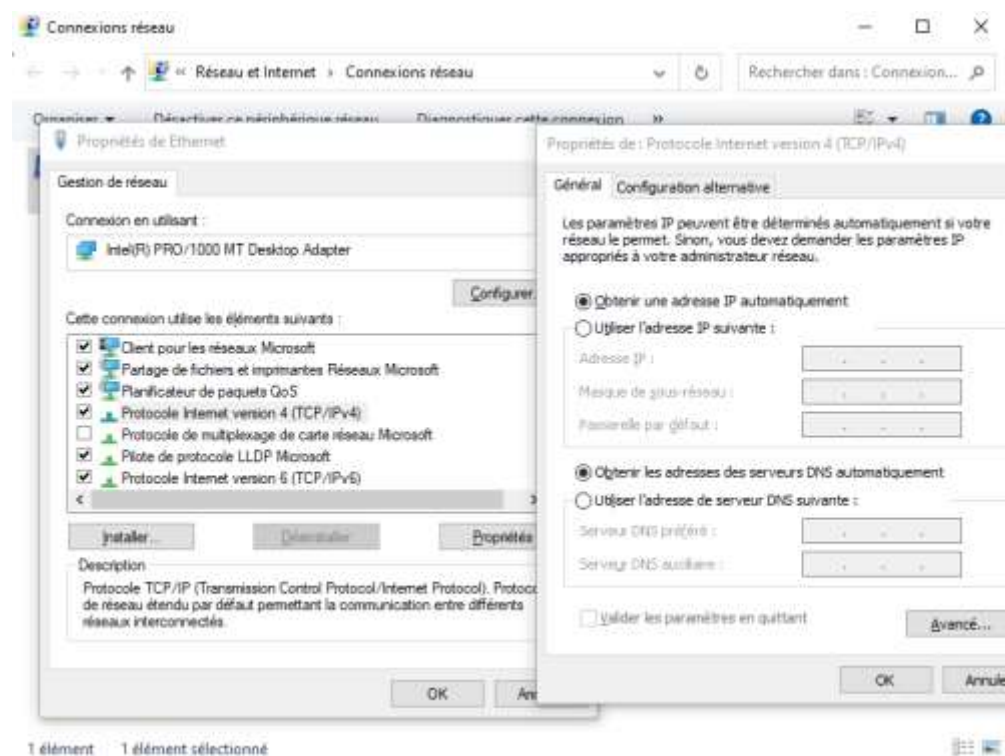
On pourra se connecter avec l'utilisateur qu'on a créé dans notre AD DS, sur le PC Client WINDOWS 10.



Ensuite pour qu'on puisse recevoir automatiquement une adresse IP sur le PC Client WINDOWS 10, il faudra qu'on aille dans « ncpa.cpl »



On coche « Obtenir une adresse IP automatiquement »



Pour voir si le DHCP a bien fonctionné, on fait un ipconfig/all

```
C:\Users\apescasio>ipconfig /All

Configuration IP de Windows

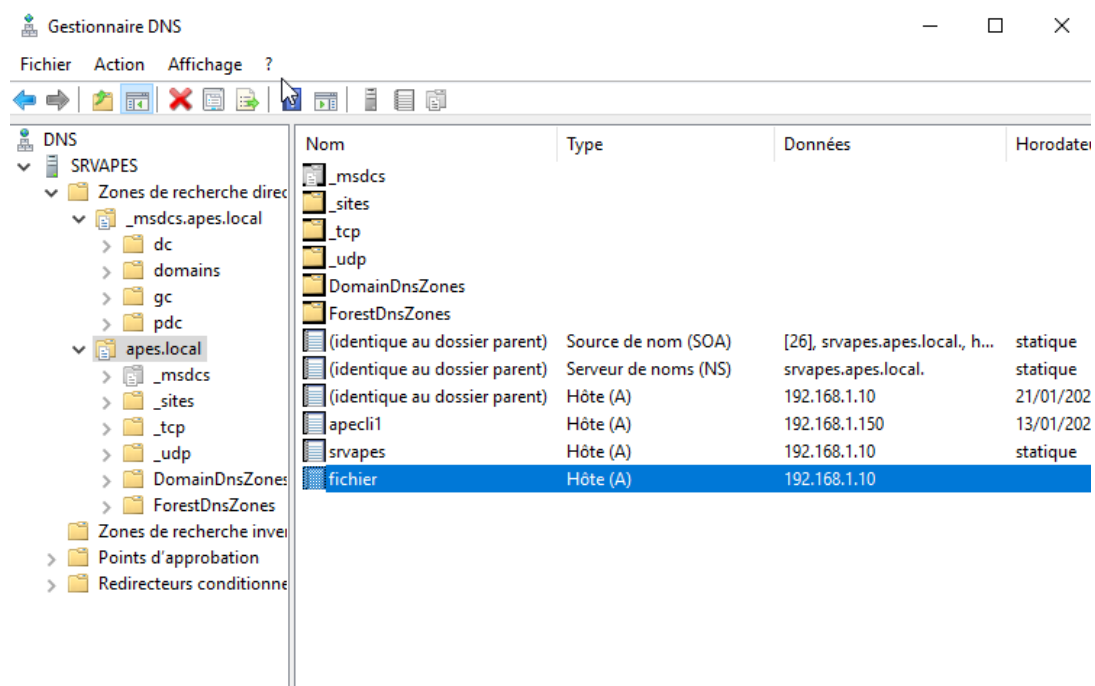
    Nom de l'hôte . . . . . : apecli1
    Suffixe DNS principal . . . . . : apes.local
    Type de noeud . . . . . : Hybride
    Routage IP activé . . . . . : Non
    Proxy WINS activé . . . . . : Non
    Liste de recherche du suffixe DNS.: apes.local

Carte Ethernet Ethernet :

    Suffixe DNS propre à la connexion. . . : apes.local
    Description. . . . . : Intel(R) PRO/1000 MT Desktop Adapter
    Adresse physique . . . . . : 08-00-27-54-43-0A
    DHCP activé. . . . . : Oui
    Configuration automatique activée. . . : Oui
    Adresse IPv6 de liaison locale. . . . : fe80::64fc:b06b:2071:2ca6%3(préfééré)
    Adresse IPv4. . . . . : 192.168.1.150(préfééré)
    Masque de sous-réseau. . . . . : 255.255.255.0
    Bail obtenu. . . . . : mardi 18 janvier 2022 14:06:25
    Bail expirant. . . . . : mercredi 26 janvier 2022 14:06:25
    Passerelle par défaut. . . . . : 192.168.1.254
    Serveur DHCP . . . . . : 192.168.1.10
    IAID DHCPv6 . . . . . : 101187623
    DUID de client DHCPv6. . . . . : 00-01-00-01-29-72-48-8E-08-00-27-54-43-0A
    Serveurs DNS. . . . . : 192.168.1.10
    NetBIOS sur Tcpiip. . . . . : Activé
```

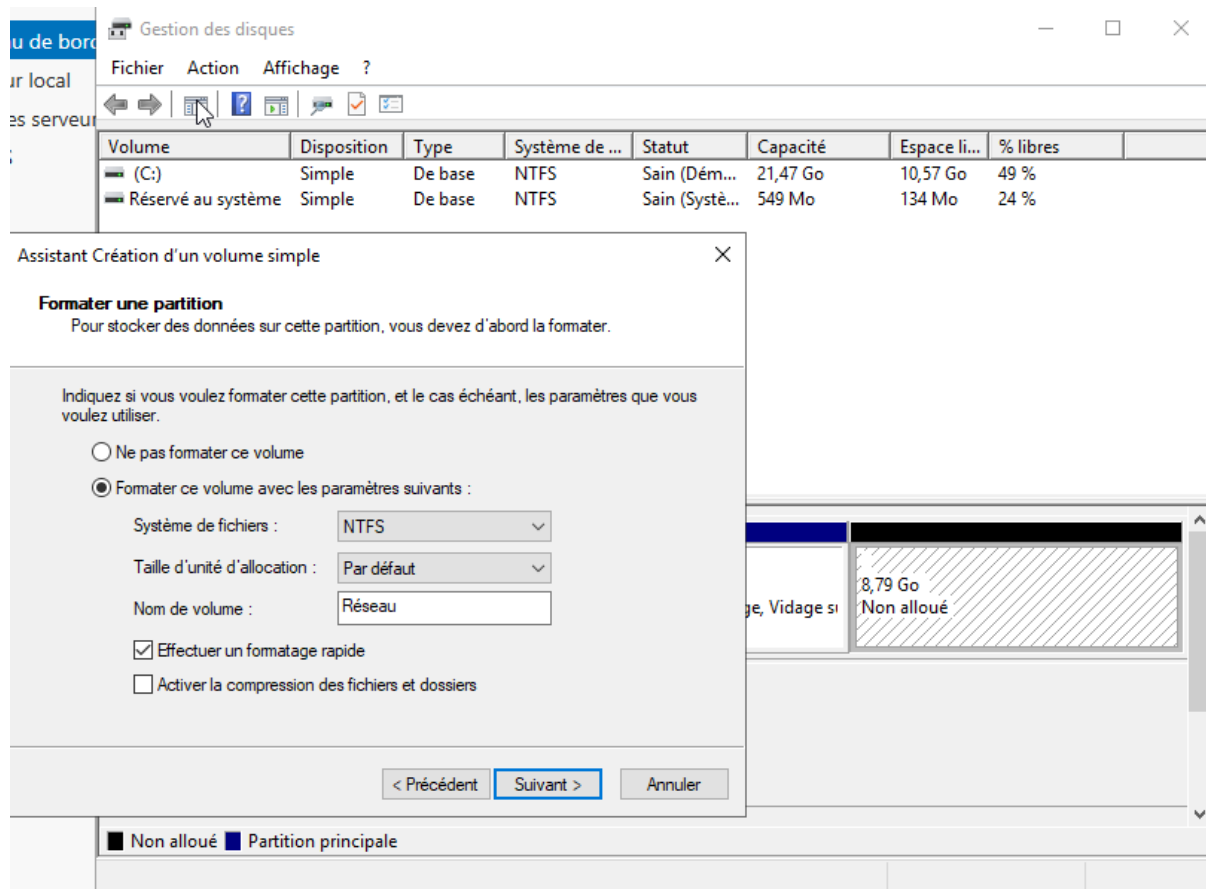
192.168.1.150 fait bien partie de notre étendue DHCP donc on voit bien que le serveur DHCP fonctionne.

Mise en place d'un serveur de fichiers

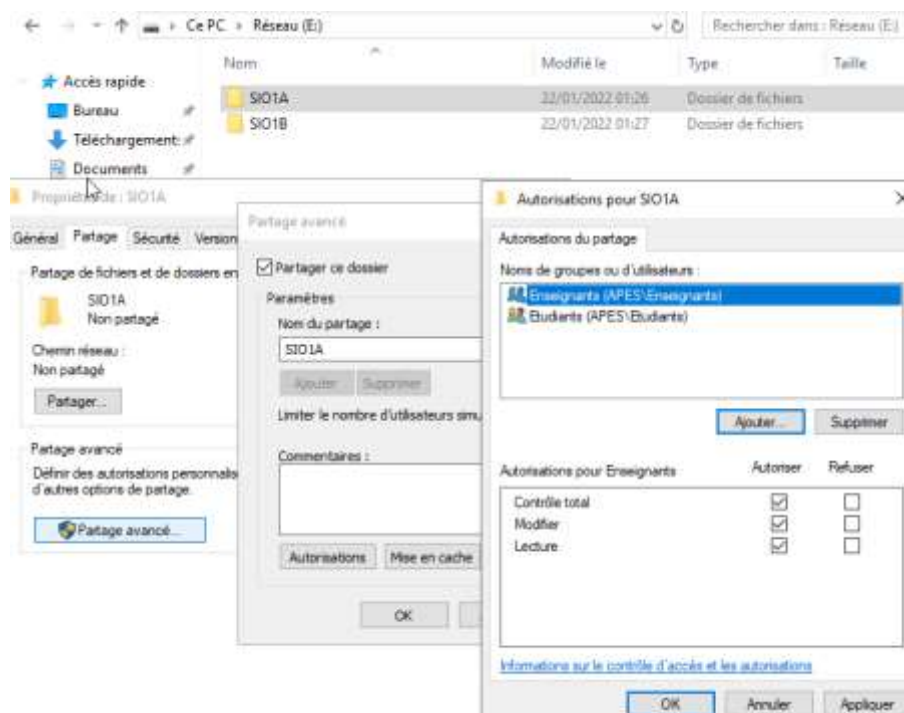


On ajoutera un enregistrement DNS pour pouvoir taper uniquement « files » au lieu du domaine entier ou de son adresse IP. L'enregistrement DNS est bien du type A car on utilise l'IPv4.

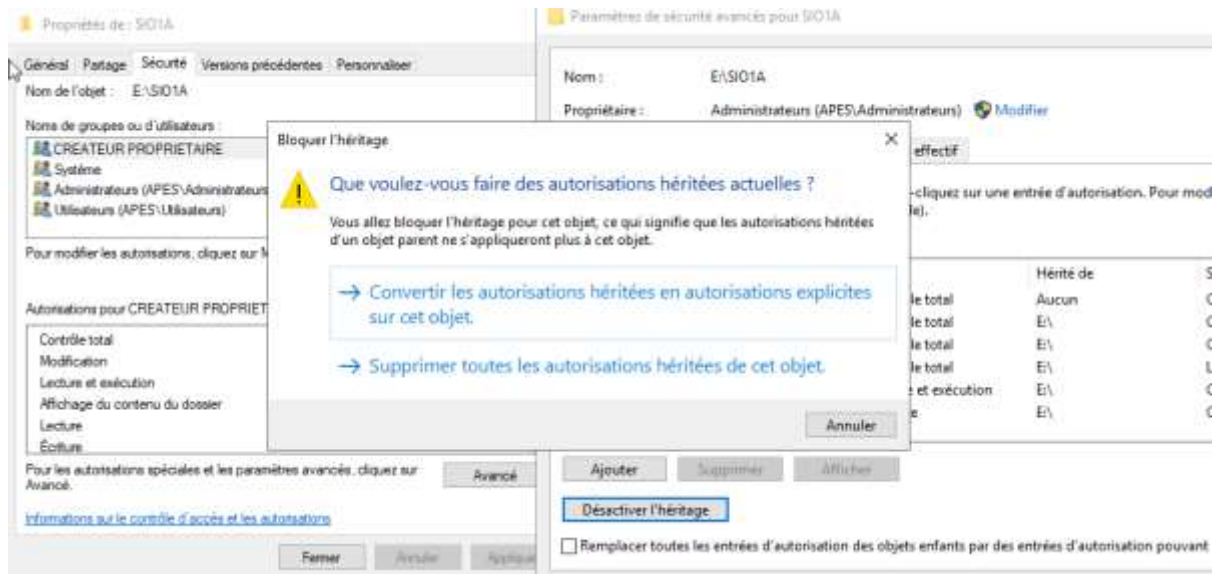
Tout d'abord, il est nécessaire de créer un volume dédié au stockage des dossiers et des fichiers formatés en NTFS car on est dans un environnement Windows. Il faut bien réduire le volume de disque C puis avec la partition non allouée, nous créerons le volume dédié.



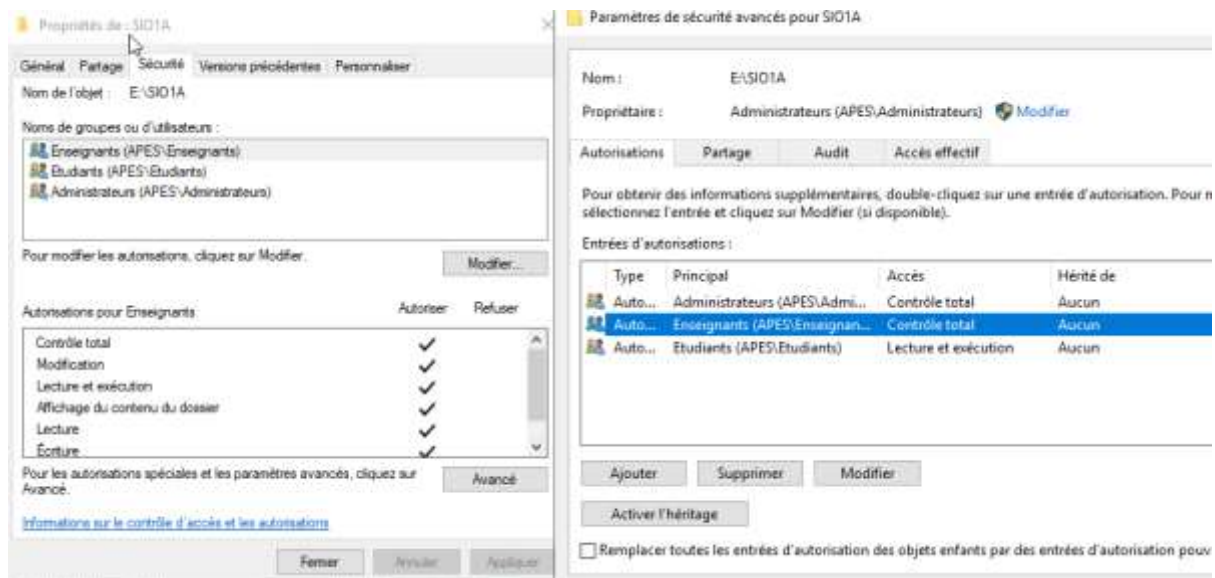
Après la création des dossiers, on va autoriser le partage des dossiers sur le réseau aux utilisateurs du domaine. Il faut bien supprimer « Tout le monde » qui a par défaut le contrôle total des dossiers.



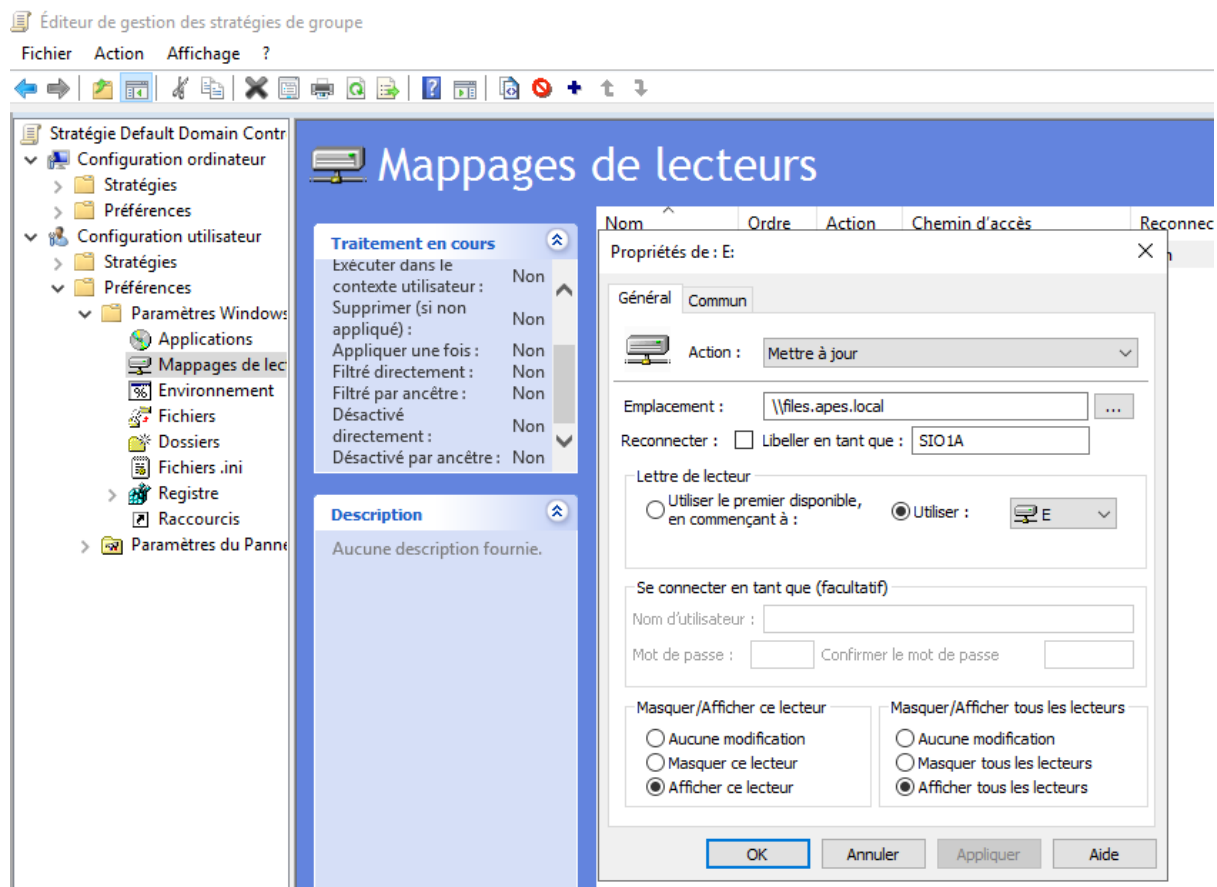
Il faut également désactiver l'héritage des autorisations (Sécurité > Paramètres avancés > Supprimer toutes)



Nous pouvons ajouter maintenant le groupe qui peut avoir le contrôle total au dossier et le groupe qui n'a pas le contrôle total. Il faut savoir que l'administrateur n'est pas supposé d'avoir accès, d'avoir le contrôle total des dossiers des autres services.

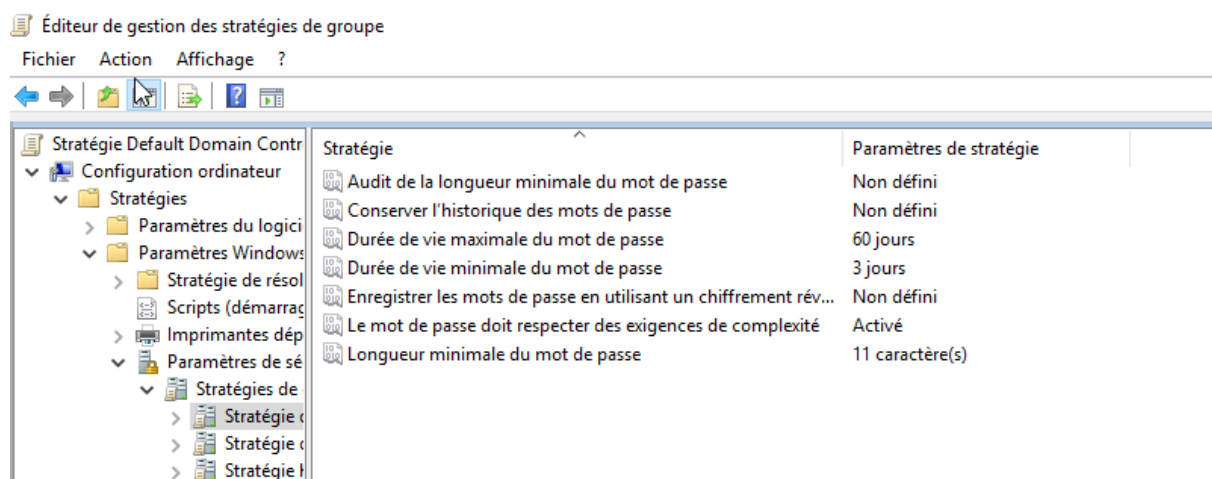


On va ensuite mapper le lecteur réseau sur le dossier voulu. Il faut d'abord créer une stratégie de groupe dans l'arborescence AD et puis faire un clic droit modifier pour accéder à l'éditeur de gestion des stratégies de groupes. Puis on ajoute un nouveau lecteur mappé dans la « Configuration utilisateur » > Préférences > Paramètres Windows > Mappages de lecteurs.



Sécurisation AD

Nous allons définir des stratégies de mots de passe pour mieux sécuriser notre AD maintenant.



On fait un gpupdate /force pour actualiser les modifications

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [version 10.0.17763.1879]
(c) 2018 Microsoft Corporation. Tous droits réservés.

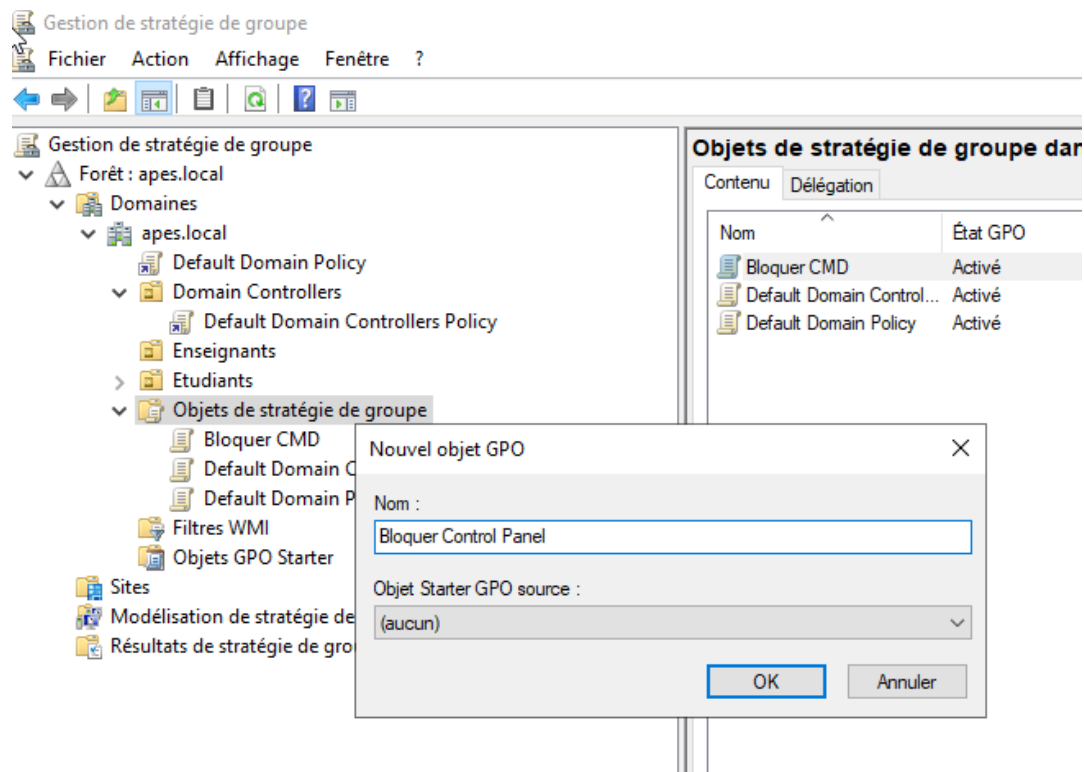
C:\Users\Administrateur>gpupdate /force
Mise à jour de la stratégie...

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.

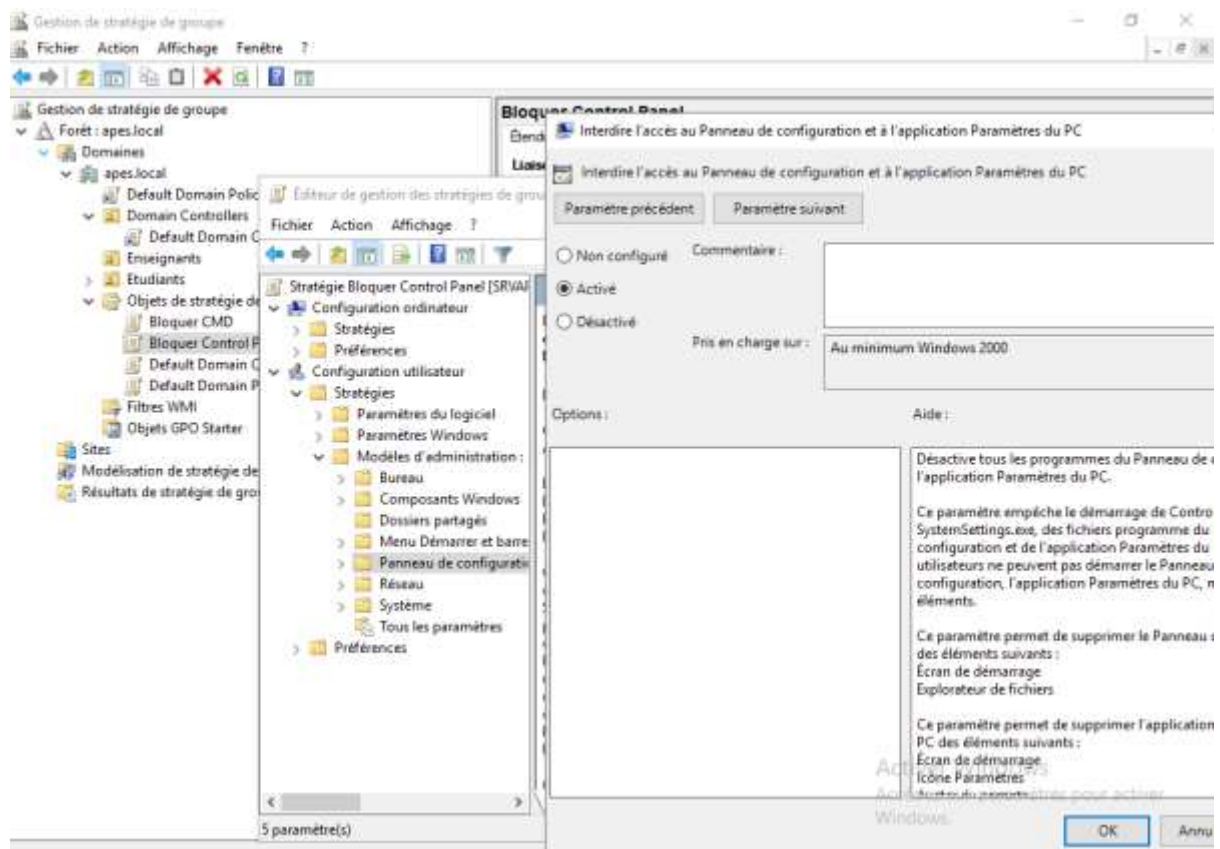
C:\Users\Administrateur>
```

Création d'une GPO qui permettra de bloquer l'accès au panneau de configuration

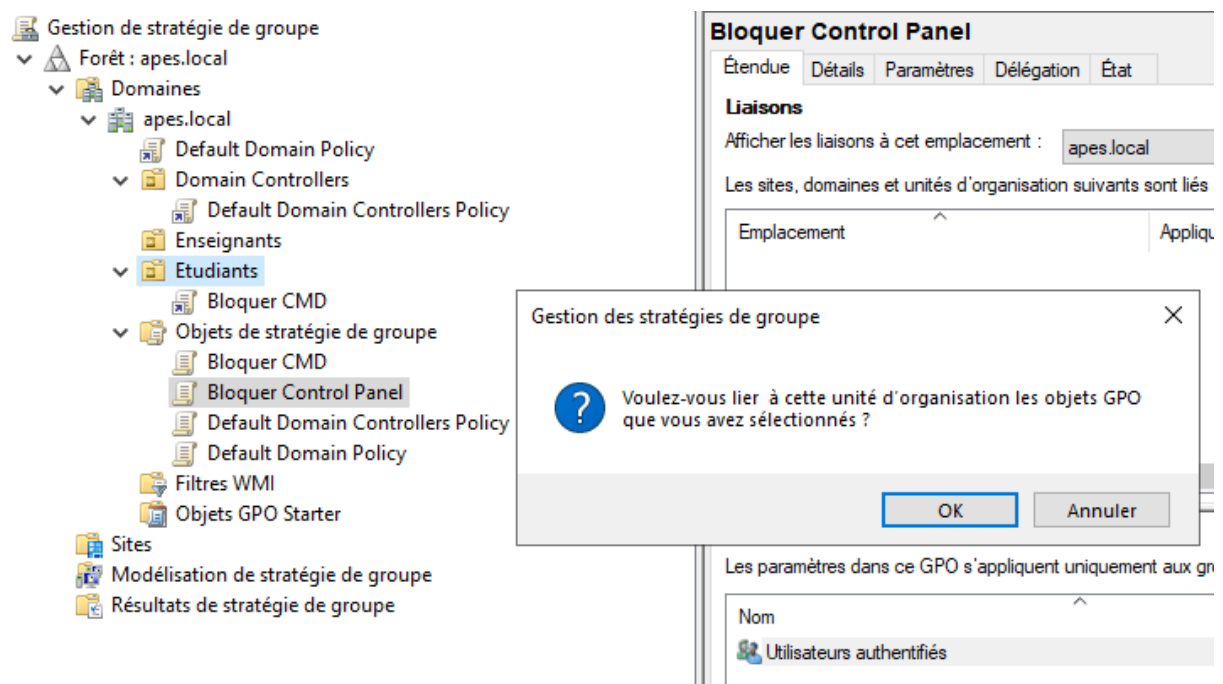
On crée un nouvel objet GPO en premier



Puis on configure la GPO



Après la création de la GPO, il faut lier la GPO à l'OU de votre choix. Par exemple ici, les étudiants ne pourront plus accéder au panneau de configuration.



On fait un gpupdate /force pour faire la mise à jour des GPO.

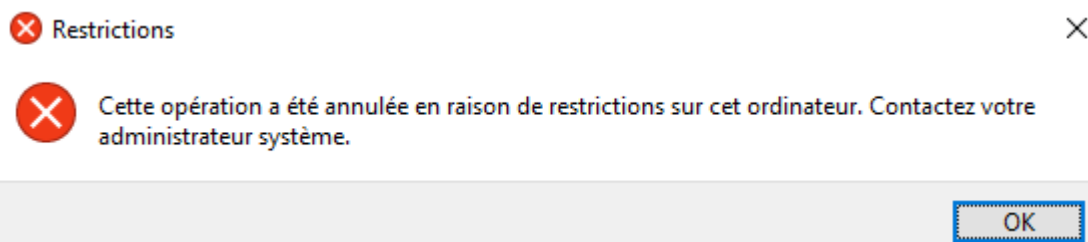
```
Microsoft Windows [version 10.0.17763.1879]
(c) 2018 Microsoft Corporation. Tous droits réservés.

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>
```

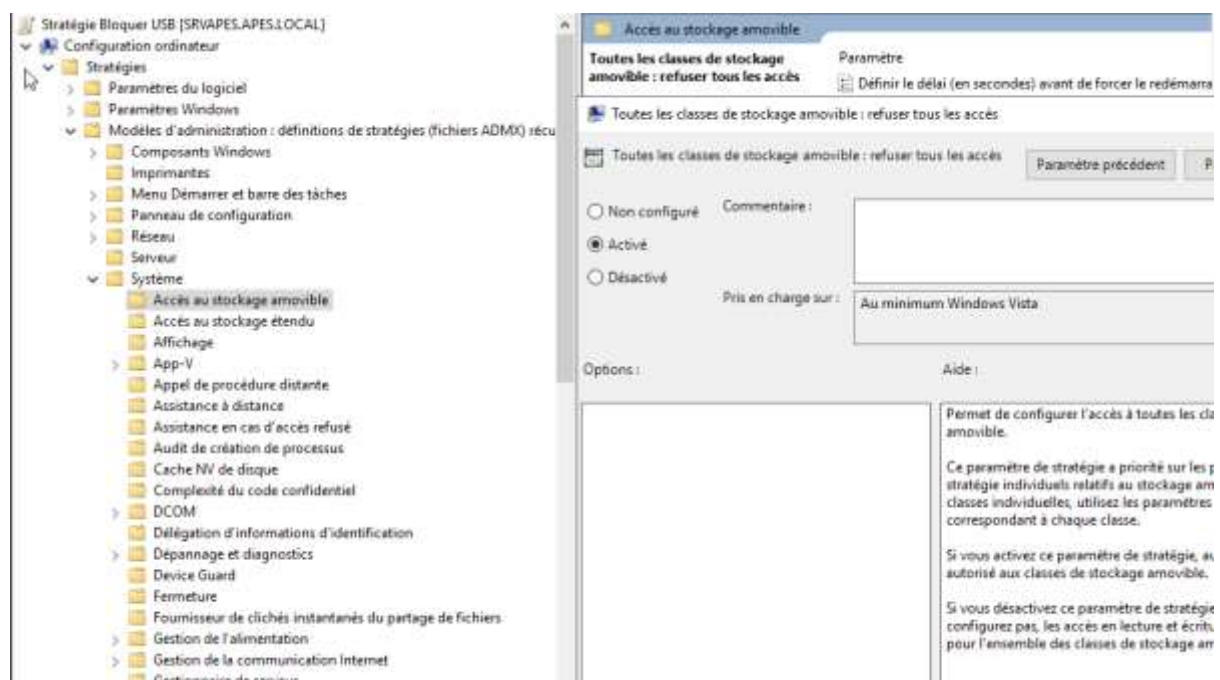
Les étudiants n'ont plus accès au panneau de configuration après un redémarrage de la machine.



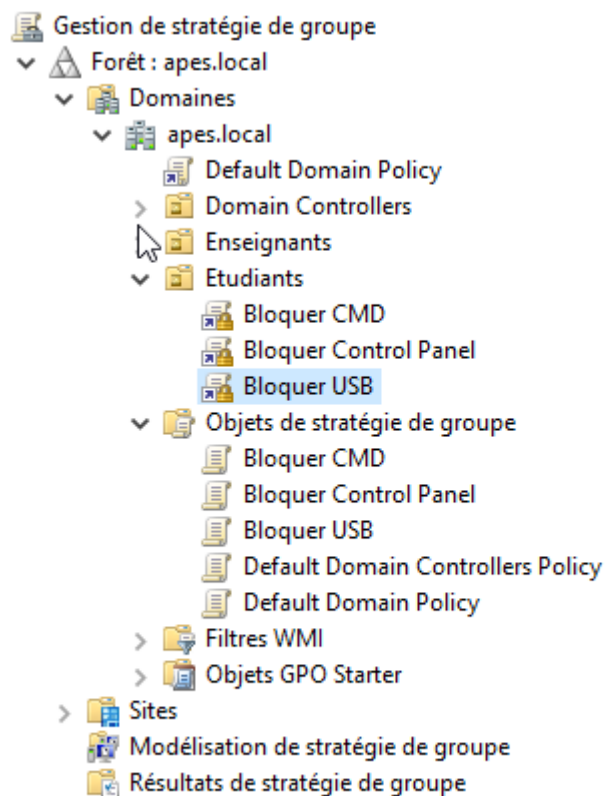
La GPO Bloquer Control Panel va empêcher complètement l'utilisateur de modifier les paramètres de l'ordinateur, même la plus simple modification. Le seul moyen d'ouvrir le panneau de config est de se connecter à l'aide d'un autre compte d'utilisateur qui n'est pas affecté par la stratégie.

Création d'une GPO qui permettra de bloquer les USB

On crée la GPO et on coche « Active » puis on clique sur OK.



On fait le lien ensuite



On fait un gpupdate /force pour faire la mise à jour des GPO.

```
Microsoft Windows [version 10.0.17763.1879]
(c) 2018 Microsoft Corporation. Tous droits réservés.

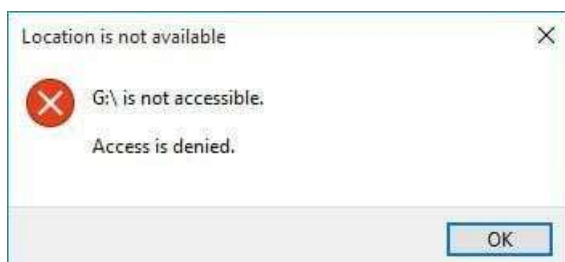
C:\Users\Administrateur>gpupdate /force
Mise à jour de la stratégie...

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>_
```

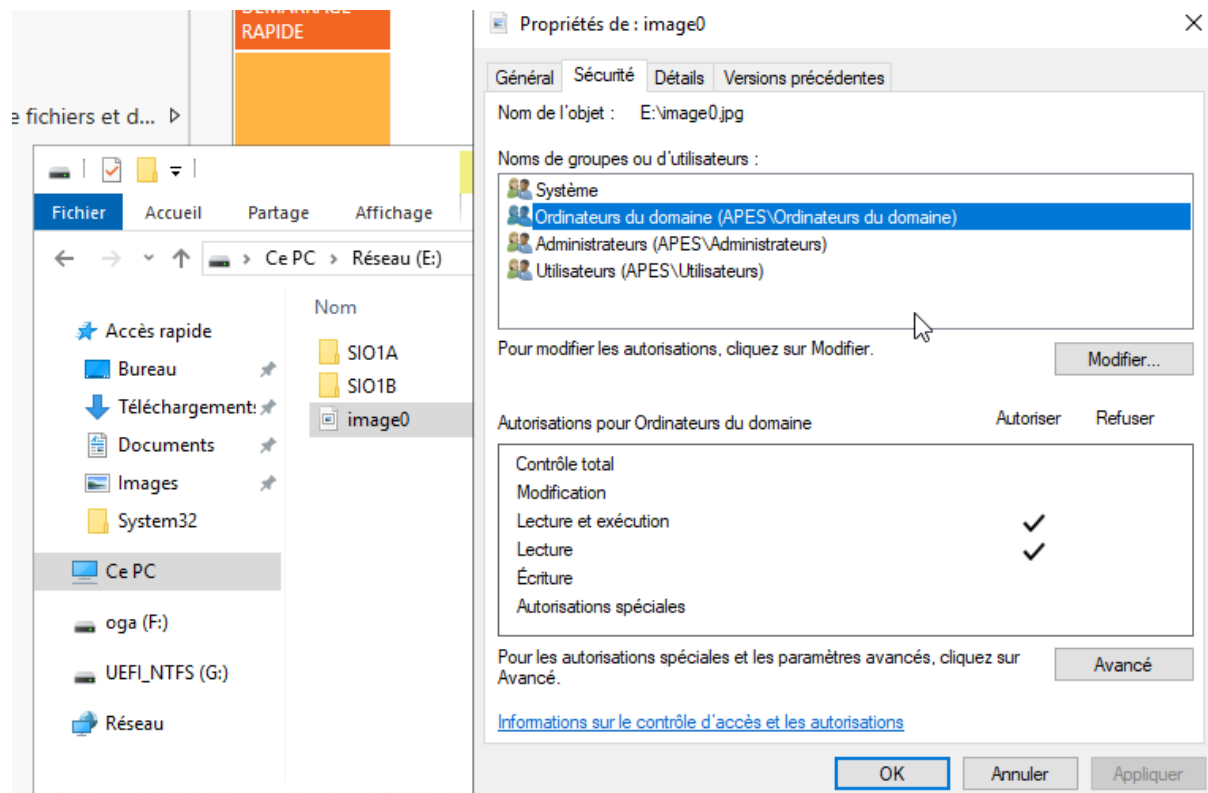
Les étudiants n'ont plus le droit d'utiliser des clés USB.

Il faut faire attention quand on applique la GPO car il n'y aura pas le même effet applicatif sur l'utilisateur et sur l'ordinateur

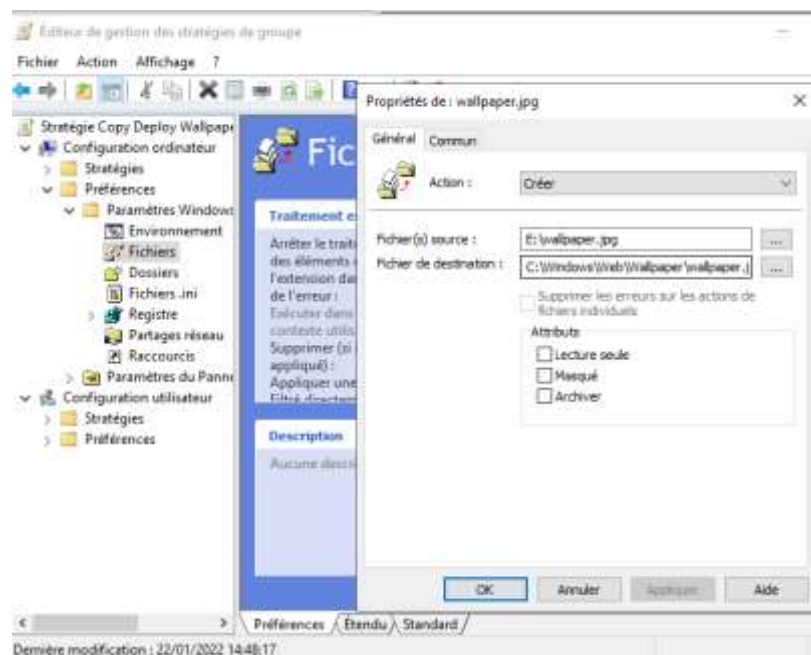


Fond d'écrans des clients Windows

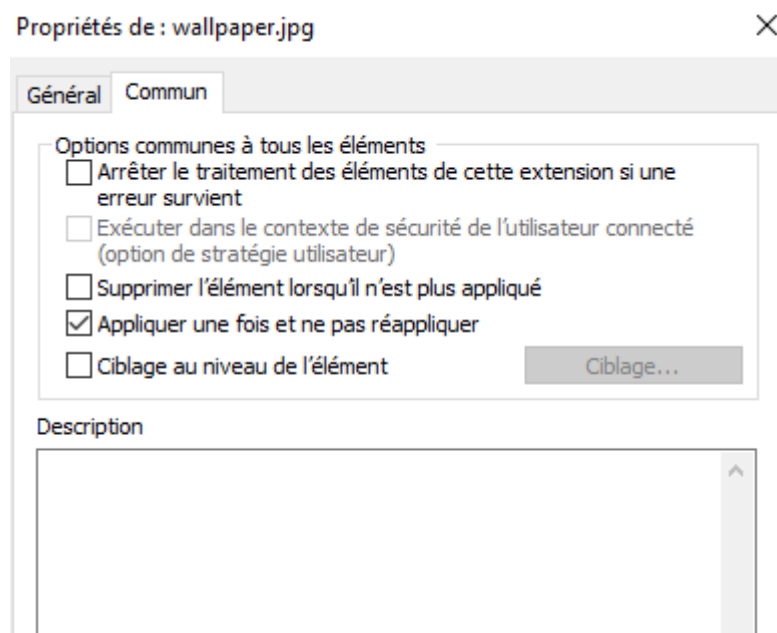
On commence par créer un partage pour héberger le fichier du fond d'écran, il faut qu'il soit accessible par le réseau par les postes clients.



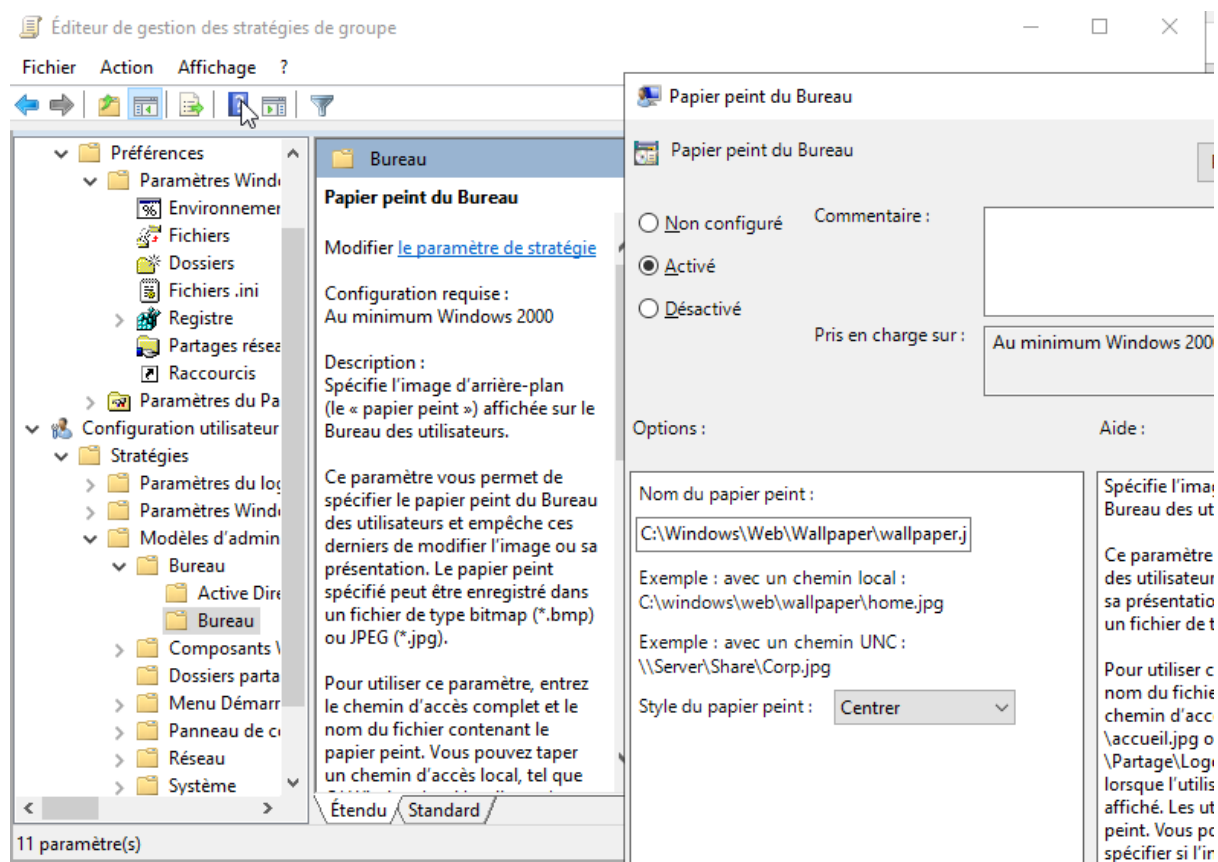
Ensuite, on crée une nouvelle GPO et on va créer un paramètre de préférence pour que le fichier image du fond d'écran soit copié sur les ordinateurs distants dans « Config ordi », « Préférences », « Paramètres Windows » et « Fichiers ».



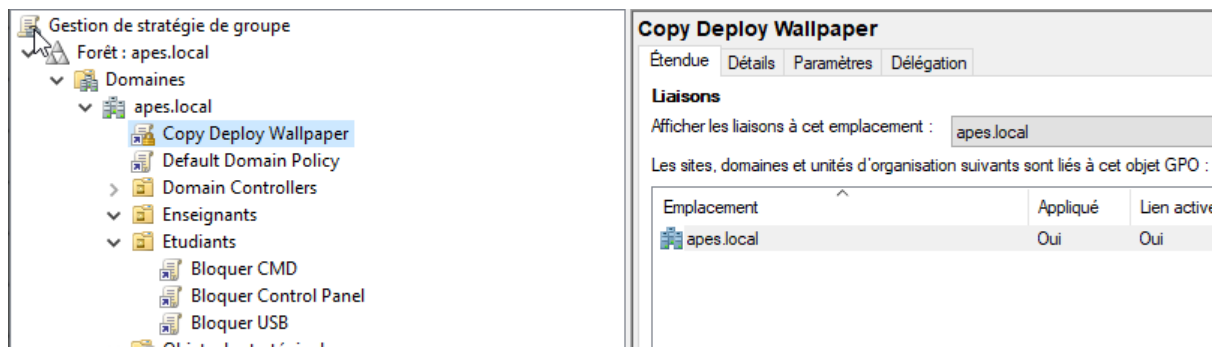
Puis dans l'onglet « Commun », on cochera « Appliquer une fois » pour ne pas copier le fond d'écran à chaque fois.



Après, il faut activer le « papier peint du bureau » dans « Config utilisateur, Modèles d'admin, Bureau, Bureau »



Enfin, il suffit de lier la GPO à notre domaine et puis faire un gpupdate /force

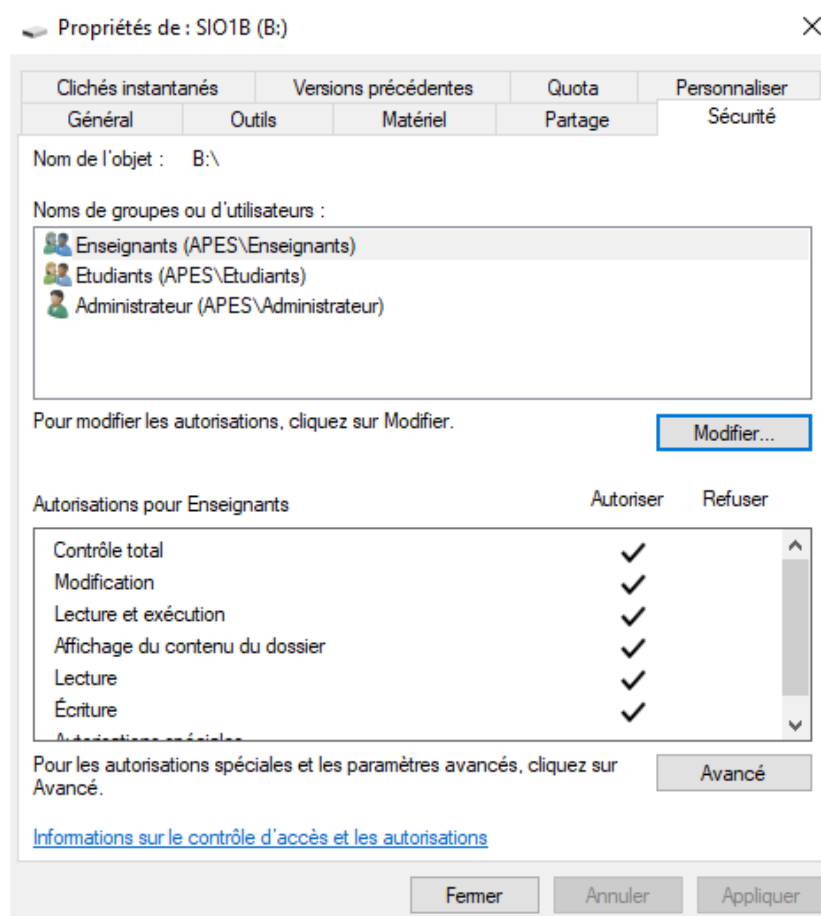
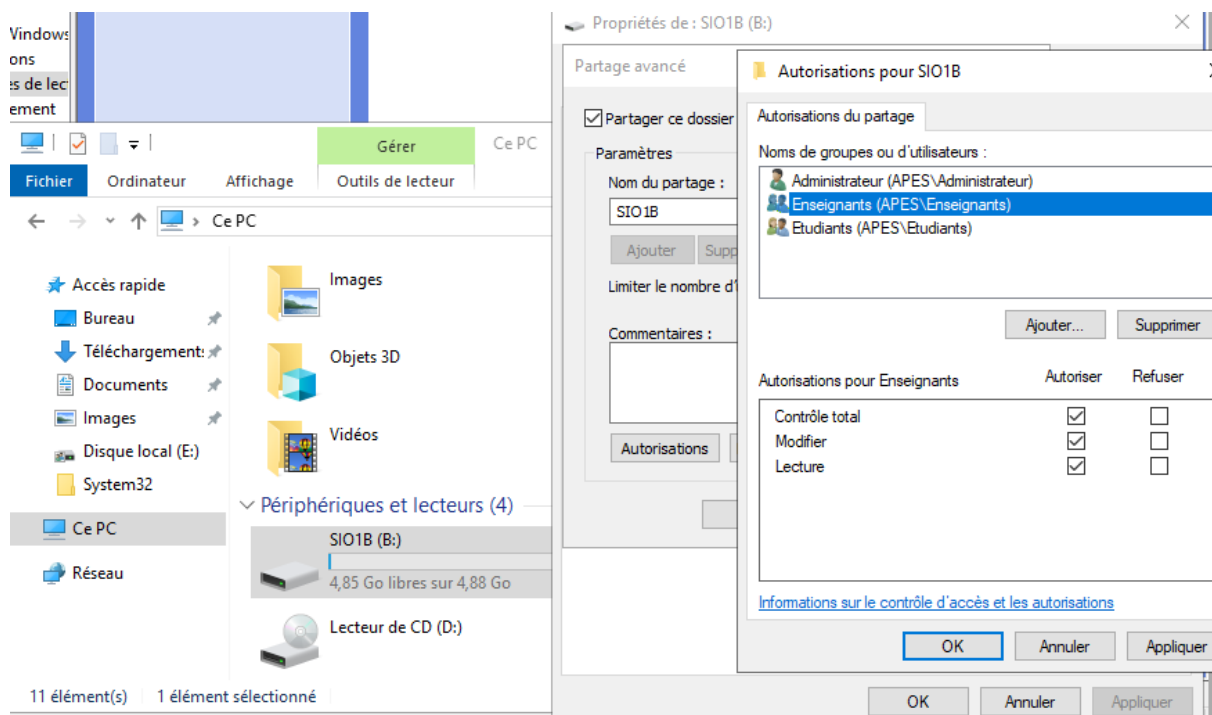


On redémarre la machine et on obtient normalement le fond d'écran

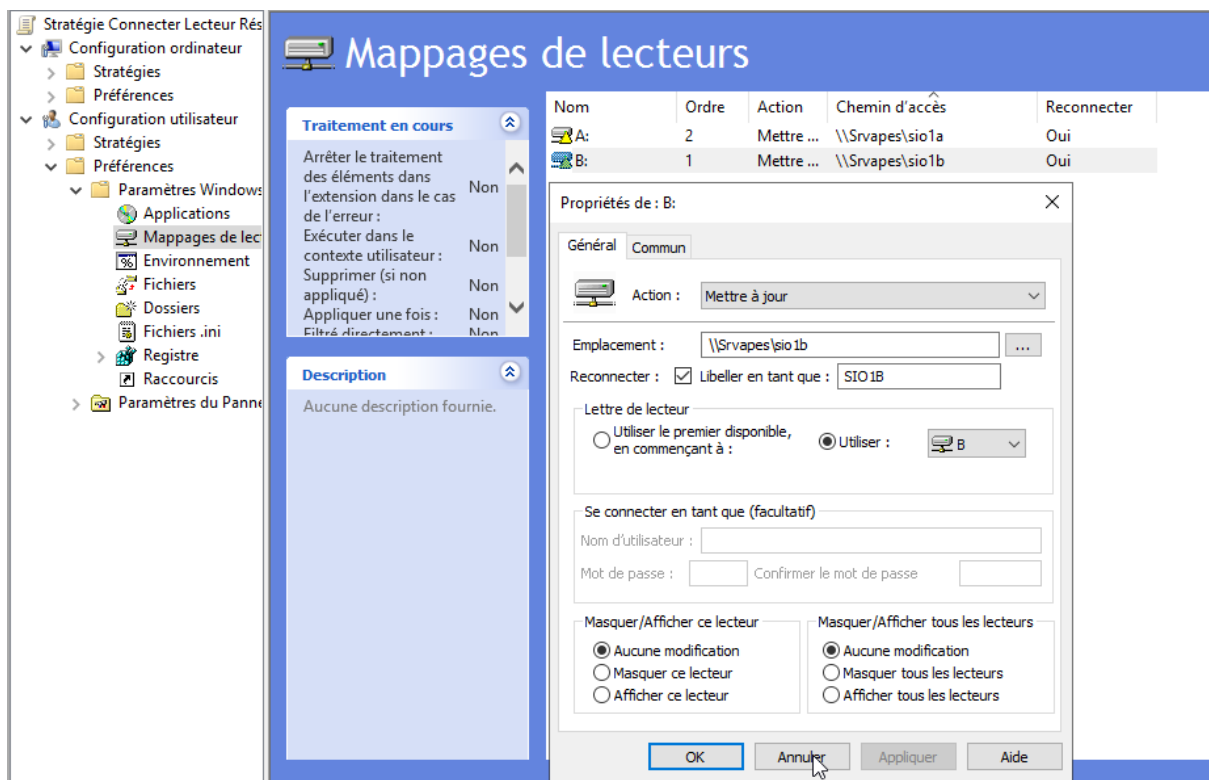


Mapper un lecteur réseau par GPO

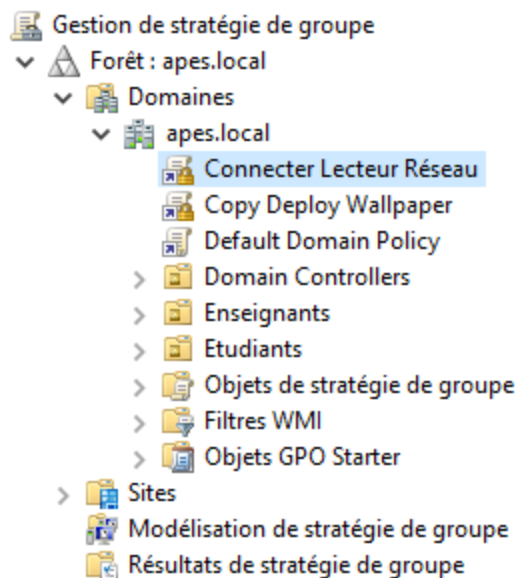
On crée un volume dédié au partage des fichiers et puis on met les autorisations qu'on veut pour les groupes



Ensuite, on crée un nouveau lecteur mappé dans « Config util », « Préférences », « Paramètres Windows », « Mappages de lecteur ». Il faut mettre l'action « Mettre à jour » et puis préciser l'emplacement du disque qu'on veut partager.



Il faut également lier la GPO qu'on a crée au domaine pour que tous les utilisateurs qui se trouvent dans le domaine puissent accéder aux lecteurs réseau



On fait un gpupdate /force pour actualiser

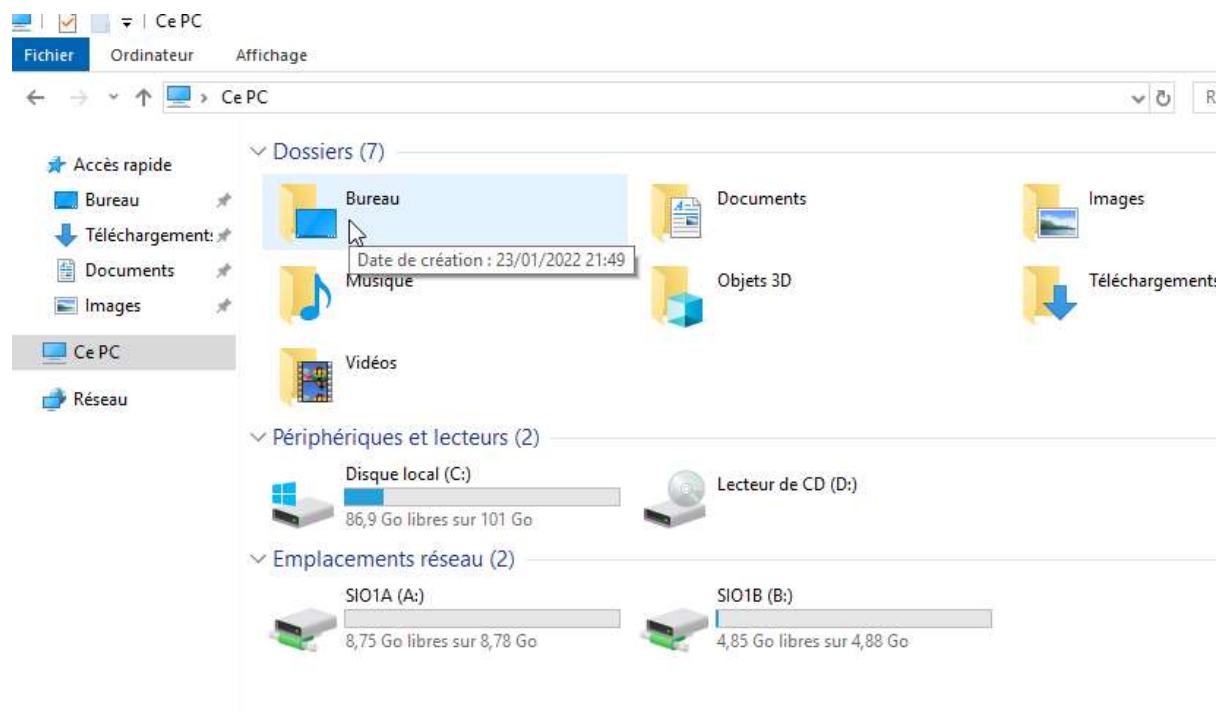
```
Microsoft Windows [version 10.0.17763.1879]
(c) 2018 Microsoft Corporation. Tous droits réservés.

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>
```

Ensuite, on redémarre le PC Client WINDOWS 10 et on voit bien les lecteurs réseaux « SIO1A » et « SIO1B ».



S'ils s'affichent avec une croix rouge, il suffit de double cliquer sur les lecteurs réseaux pour les actualiser.