



Lycée Générale et Technologie Baimbride
Brevet Technicien Supérieur
Services informatiques aux Organisations



Planification de rôles pour des services d'une infrastructure Windows

Compte rendu

TP1 bloc2



Réalisé par ROSIER Matthias BTS SIO 2A

Sommaire

Compte rendu TPn°1_Bloc_n°2_SISR	3
Introduction.....	3
A) Contexte du TP	3
B) objectifs et enjeux.....	3
Etape 1 : Planification d'AD et du DC :.....	3
A) Interface réseau du serveur :	4
B) Modification nom serveur et description :	4
C) Installation Active directory et contrôleur domaine :	5
Etape 2 : Planification du DNS :.....	6
A) installation DNS :.....	6
B) Création zone de recherche direct :	6
C) Ajout nouvel hôte :	8
D) Création zone de recherche indirect :	9
E) Ajout nouveau pointeur :	9
F) Teste du bon fonctionnement du dns :	10
Etape 3 : Planification du DHCP :	11
A) Installation DHCP :	11
B) CONFIGURATION DES Paramètres dhcp :	11
C) Test du bon fonctionnement du dhcp :	13
Etape n°4 : Crédation des utilisateurs, groupes et unités d'organisation :	14
A) Procédure création utilisateurs :	14
B) Mise en place stratégie pour les mdp :	14
C) Procédure création de groupe :	15
D) Procédure création unités d'unité d'organisation :	15
E) Procédure déplacement utilisateurs dans un groupe :	16
Etape n°5 : Intégration de postes de travail au domaine :	16
A) Démarche à suivre :	16
B) vérification de l'intégration :	17
Etape n°6 : Elaboration de stratégies de groupe (GPO) :	18
A) Désactiver le pare-feu des postes de travail :	18
B) Désactiver l'accès au panneau de configuration :	20
C) Définir un papier par défaut pour les utilisateurs en fonction de l'UO à laquelle ils appartiennent :	22
D) Désactiver l'accès la commande « exécuter » :	25
E) Désactiver la configuration réseau :	26
F) Créer et monter automatiquement des lecteurs réseaux en fonction des UO :	28
Etape n°7 : Déploiement de logiciels par GPO :	30
Etape n°8 : Réalisation de profils itinérants :	32
Conclusion :	34
Fin du TP :	34

COMPTE RENDU TPN°1_BLOC_N°2_SISR

INTRODUCTION

A) CONTEXTE DU TP

Ce TP traite de l'installation et de la configuration des services **Active Directory** et des rôles associés, tels que **DHCP** et **DNS**, pour répondre aux besoins de la mairie de la ville des Abymes. Dans un contexte de centralisation et de gestion simplifiée, ce projet vise à mettre en place une infrastructure permettant de **centraliser la gestion des comptes utilisateurs, des ressources**, ainsi que des **droits d'accès**. Sous la supervision de M. Laurent, l'objectif est d'offrir une meilleure **sécurisation du réseau**, tout en facilitant le **déploiement d'applications à distance** et en centralisant le **stockage des données utilisateurs**. Cette digitalisation est un atout majeur pour moderniser la gestion des systèmes informatiques de la mairie et améliorer leur efficacité

B) OBJECTIFS ET ENJEUX

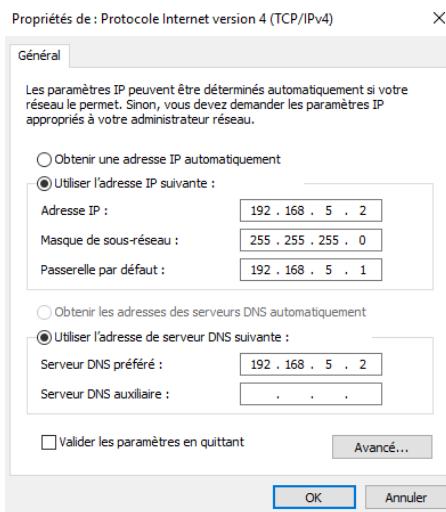
Acquérir et mettre en application les compétences suivantes :

- * Installer et configurer des éléments d'infrastructure
- *Déployer une solution d'infrastructure
- *Administrer un système
- *Administtrer sur site et à distance des éléments d'une infrastructure
- *Automatiser des tâches d'administration
- *Tester l'intégration et l'acceptation d'une solution d'infrastructure
- *Rédiger ou mettre à jour la documentation technique et utilisateur d'une solution d'infrastructure

Condition de travail : Individuel

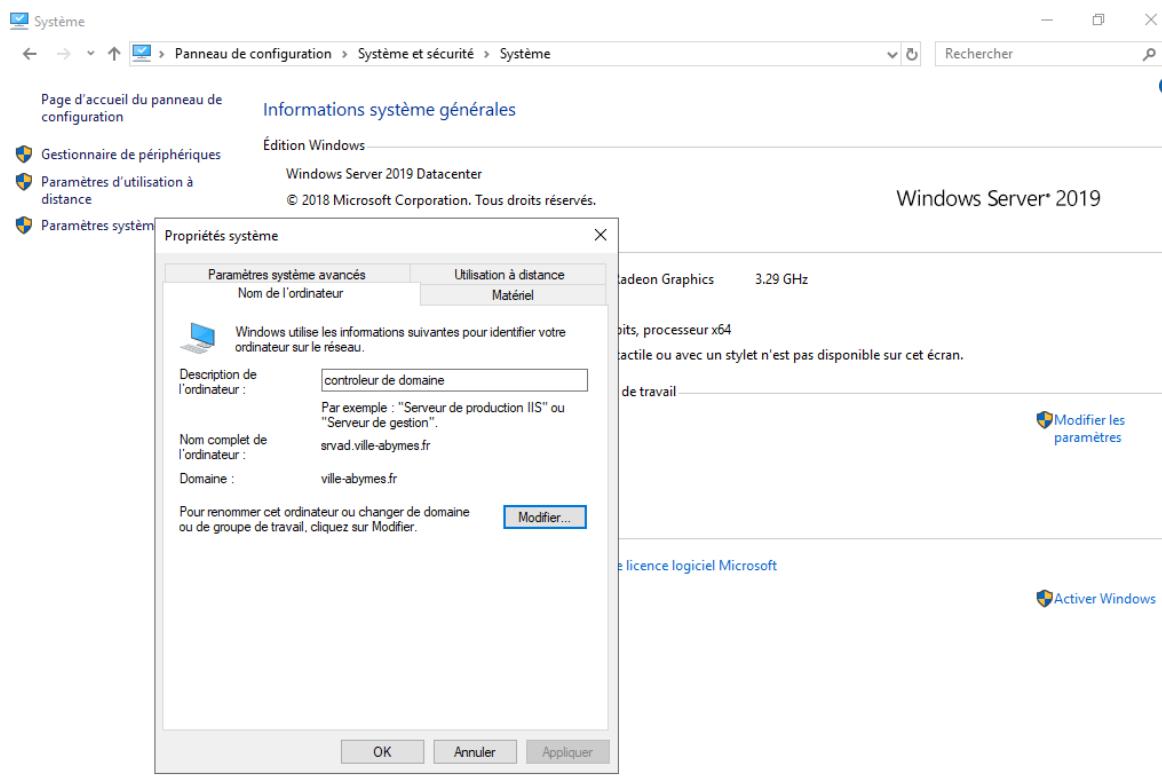
ETAPE 1 : PLANIFICATION D'AD ET DU DC :

A) INTERFACE RÉSEAU DU SERVEUR :

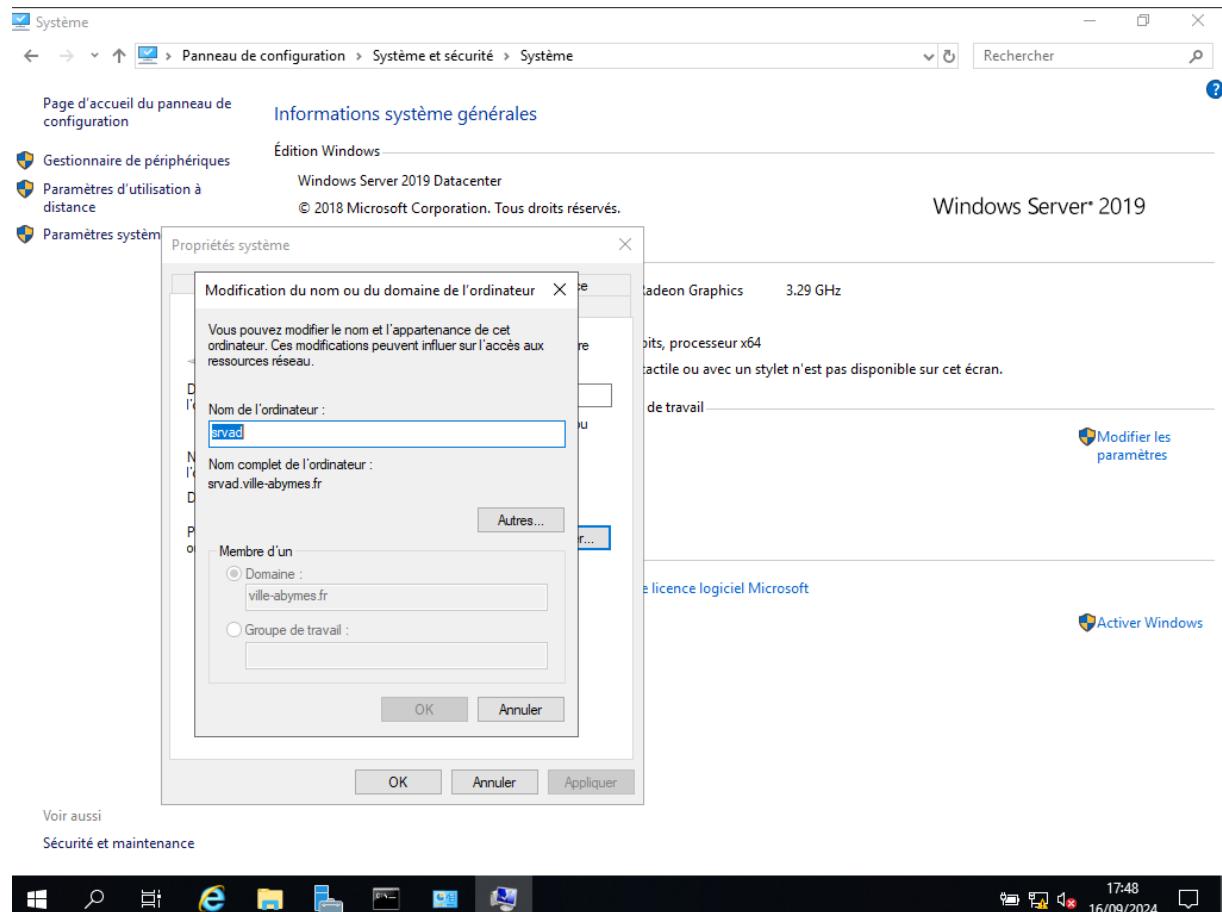


B) MODIFICATION NOM SERVEUR ET DESCRIPTION :

- On peut taper et ouvrir dans la barre de recherche le Panneau de configuration puis Sécurité et Systèmes ensuite Systèmes. Dans la nouvelle fenêtre cliquez sur Modifier les paramètres :



- Il est maintenant possible de changer la description. Et pour donner un nouveau nom au pc cliquez encore sur **Modifier** puis **OK** par rapport à la fenêtre qui va s'ouvrir et l'accès au changement de nom du pc sera possible.



C) INSTALLATION ACTIVE DIRECTORY ET CONTRÔLEUR DOMAINE :

- Il faut aller dans **Démarrer** → **Gestionnaire de serveur** → **Tableau de bord**

- Cliquez sur **Ajouter des rôles et fonctionnalités** → **Suivant (3fois)** → **Suivant** → **Suivant**
- Dans **Rôles de serveurs** cochez **Service AD DS** ensuite cliquez sur **Ajouter des fonctionnalités** et une fois de plus **Suivant (3fois)** → **Suivant** → **Suivant** → **Installer**.
- Maintenant une alerte avec  à coté de Gérer en dessous d'un drapeau pour **Promouvoir ce serveur en contrôleur de domaine** cliquez dessus. Une fois dans **Configuration de déploiement** → **Ajouter une nouvelle forêt** → **Spécifiez le nom de domaine (ville-abymes.fr)** → **Niveau fonctionnel** (Windows Serveur 2016 le plus récent) → **Mot de passe (@admin&2425@)**. Faire **Suivant** jusqu'au récapitulatif d'installation en laissant les valeurs par défauts. **Redémarrer** obligatoirement le serveur.

ETAPE 2 : PLANIFICATION DU DNS :

A) INSTALLATION DNS :

Pour commencer la configuration du **service DNS**, il suffit de suivre les étapes suivantes un peu comme l'installation de l'AD DS:

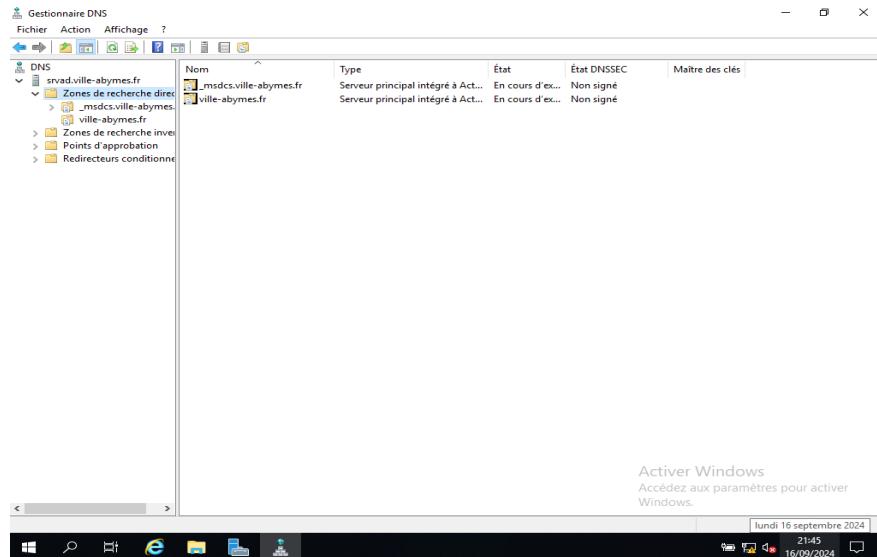
- Depuis le **Gestionnaire de serveur**, cliquez sur **Ajouter des rôles et des fonctionnalités**.
- Avancez en cliquant sur **Suivant** jusqu'à l'étape **Rôles de serveurs**.
- Dans cette étape, j'ai coché l'option **Service DNS** et validé l'ajout des fonctionnalités nécessaires en cliquant sur **Ajouter des fonctionnalités**, puis sur **Suivant**.
- Après avoir confirmé l'installation, le rôle **DNS** a été installé avec succès.

Une fois le rôle installé, l'icône **DNS** est apparue dans le **Gestionnaire de serveur** sur la gauche de la fenêtre.

B) CRÉATION ZONE DE RECHERCHE DIRECT :

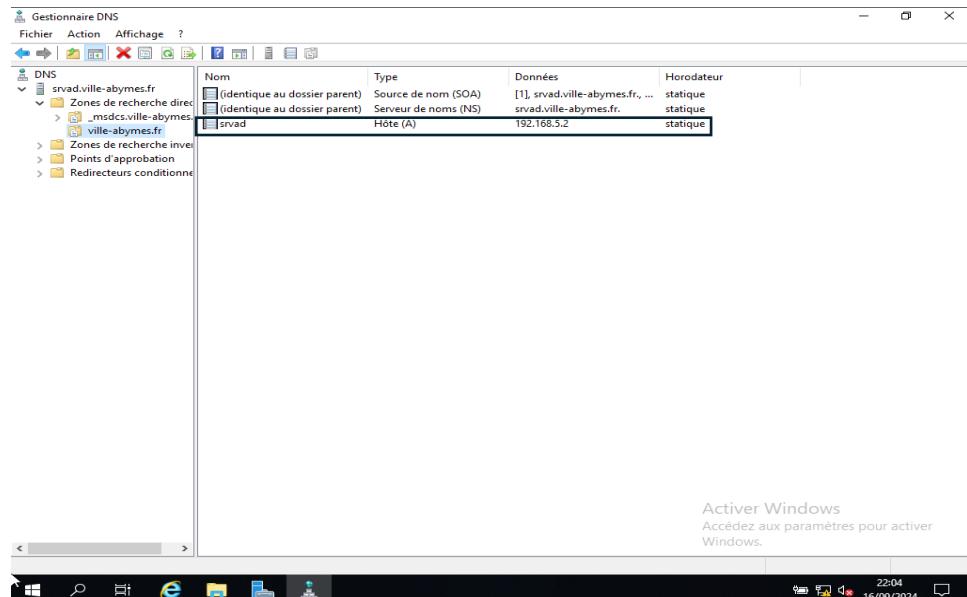
Dans le **Gestionnaire de serveur** :

- Cliquez sur l'icône **DNS** et dans la fenêtre centrale, localisé le serveur **srvad**.
 - Un clic droit sur **srvad** permet de lancer le **Gestionnaire DNS** pour commencer la configuration du service.
-
- Ensuite il faut faire un clique droit sur **Zone de recherche directe**, puis sélectionner **Nouvelle zone**.
 - Dans l'assistant faire **Suivant**, choisir **Zone principale**, puis cliquer sur **Suivant → Suivant** une deuxième fois.
 - Ensuite, entrez le **nom de la zone**, ici **ville-abymes.fr**, puis cliquer sur **Suivant**.
 - À l'étape suivante, il est important de **désactiver les mises à jour dynamiques**.
 - Après cela, cliquer sur **Suivant** et **Terminer** la création de la zone.



C) AJOUT NOUVEL HÔTE :

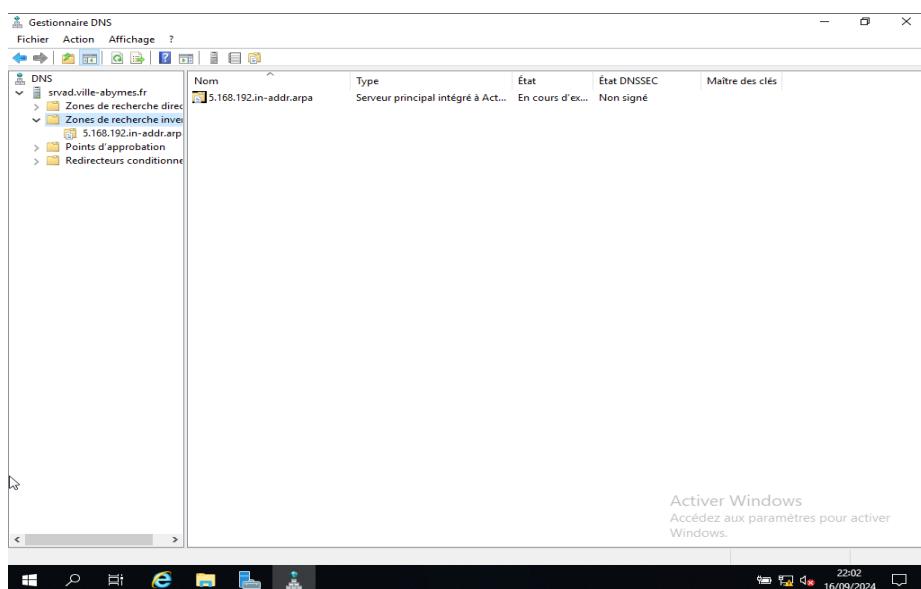
- Une fois la zone de recherche directe créée, il faut **entrer dans cette zone** en cliquant dessus.
- Ensuite, cliquer droit sur la zone et choisir **Nouvel hôte (A ou AAAA)**.
- Dans le formulaire, entrer le **nom de l'hôte (svad)** et l'**adresse IP** du serveur (pour ma part **192.168.5.2**), puis cliquer sur **Ajouter un hôte**.



D) CRÉATION ZONE DE RECHERCHE INDIRECT :

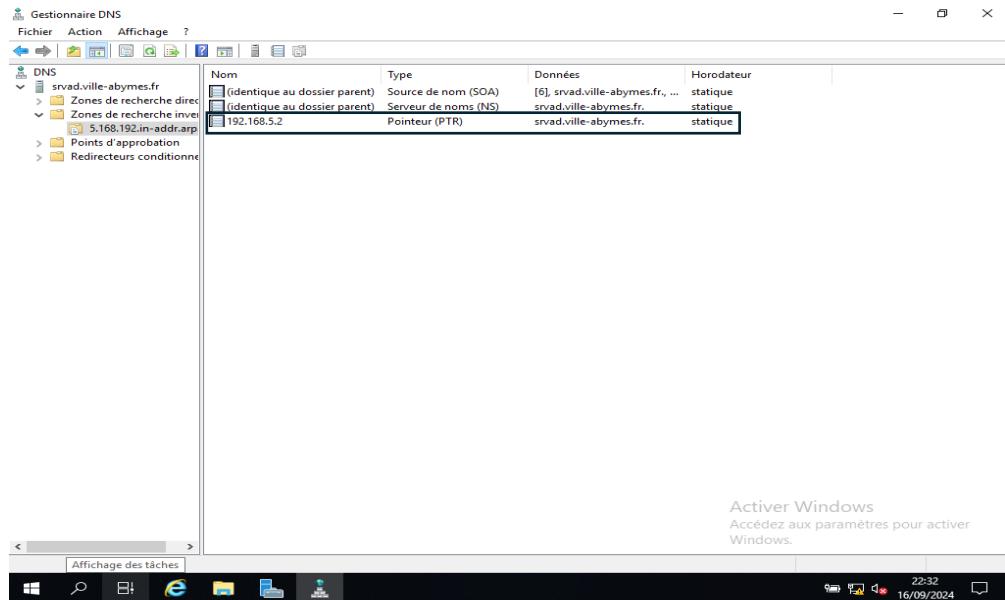
Dans le **Gestionnaire DNS**:

- Cette fois clique droit sur **Zone de recherche inversée**, puis choisir **Nouvelle zone**.
- Dans l'assistant faire **Suivant**, choisir **Zone principale**, puis cliquer sur **Suivant → Suivant** une deuxième fois → **Suivant** une troisième fois.
- Saisir le **réseau** (pour ma part, **192.168.5.0**), puis cliquer sur **Suivant**.
- À l'étape suivante, il est important de **désactiver les mises à jour dynamiques**.
- Après cela, cliquer sur **Suivant et Terminer** la création de la zone.



E) AJOUT NOUVEAU POINTEUR :

- Une fois la zone de recherche inversée créée, il faut **entrer dans cette zone**.
- Cliquer droit sur la zone et choisir **Nouvel enregistrement de pointeur (PTR)**.
- Dans le formulaire, entrer l'**adresse IP** du serveur (**192.168.5.2**) et le **nom de l'hôte** associé (**svravd**), puis cliquer sur **OK**



F) TESTE DU BON FONCTIONNEMENT DU DNS :

- On peut utiliser la commande **nslookup** qui permet de vérifier le bon fonctionnement du service DNS en testant la résolution directe (conversion d'un nom de domaine en adresse IP) et la résolution inversée (conversion d'une adresse IP en nom de domaine). Cet outil est essentiel pour s'assurer que le serveur DNS est correctement configuré et que la communication réseau se déroule sans erreurs de résolution.

Testes effectués sur le Poste client virtuel :

```

poste1_ad [En fonction] - Oracle VM VirtualBox
C:\Windows\system32\cmd.exe
C:\Users\User>nslookup ville-abymes.fr
Serveur :   srvad.ville-abymes.fr
Address: 192.168.5.2
Nom :   ville-abymes.fr
          ↓
          Recherche directe

C:\Users\User>nslookup 192.168.5.2
Serveur :   srvad.ville-abymes.fr
Address: 192.168.5.2
Nom :   srvad.ville-abymes.fr
Address: 192.168.5.2
          ↓
          Recherche inversée
  
```

The screenshot shows a Windows command prompt window titled 'poste1_ad [En fonction] - Oracle VM VirtualBox'. It contains two 'nslookup' commands. The first command, 'nslookup ville-abymes.fr', shows the server as 'srvad.ville-abymes.fr' and the address as '192.168.5.2', with the name 'ville-abymes.fr' highlighted. The second command, 'nslookup 192.168.5.2', shows the server as 'srvad.ville-abymes.fr' and the address as '192.168.5.2', with the name 'srvad.ville-abymes.fr' highlighted. Two blue arrows point from the highlighted names to boxes labeled 'Recherche directe' and 'Recherche inversée' respectively. The taskbar at the bottom shows the date and time as '16/09/2024 23:02'.

- Cette capture ci-dessus confirme que le service DNS est opérationnel, avec une résolution correcte du nom de domaine en adresses IP ainsi que de l'adresses IP en noms de domaine, validant ainsi la configuration DNS effectuée.

ETAPE 3 : PLANIFICATION DU DHCP :

A) INSTALLATION DHCP :

Pour commencer la configuration du **service DHCP**, il suffit de suivre les étapes suivantes un peu comme l'installation du **DNS** :

- Depuis le **Gestionnaire de serveur**, cliquez sur **Ajouter des rôles et des fonctionnalités**.
- Avancez en cliquant sur **Suivant** jusqu'à l'étape **Rôles de serveurs**.
- Dans cette étape, j'ai coché l'option **Service DHCP** et validé l'ajout des fonctionnalités nécessaires en cliquant sur **Ajouter des fonctionnalités**, puis sur **Suivant**.
- Après avoir confirmé l'installation, le rôle **DHCP** a été installé avec succès.

Une fois le rôle installé, l'icône **DHCP** est apparue dans le **Gestionnaire de serveur** sur la gauche de la fenêtre.

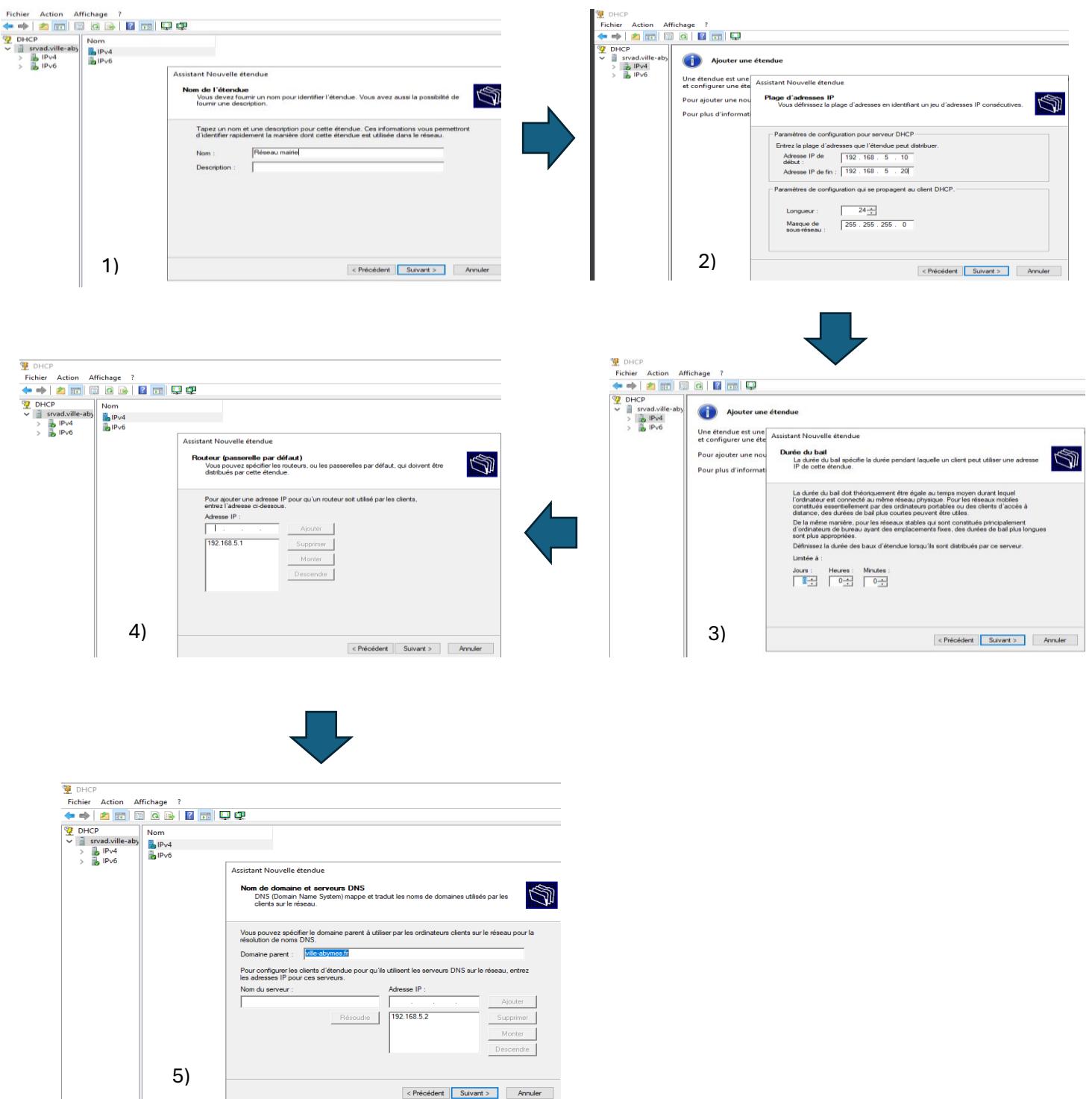
Après installation une alerte avec  à coté de Gérer en dessous d'un drapeau apparaît pour **Terminer la configuration DHCP**. Il suffit de faire **Suivant (3fois)** dont la première fois autorisez le serveur DHCP dans Active Directory.

B) CONFIGURATION DES PARAMÈTRES DHCP :

Dans le **Gestionnaire de serveur** :

- Cliquez sur l'icône **DHCP** et dans la fenêtre centrale, localisé le serveur **srvad**.
- Un clic droit sur **srvad** permet de lancer le **Gestionnaire DHCP** pour commencer la configuration du service.

- Ensuite il faut cliquer sur le **serveur** (srvad.ville-abymes.fr), puis clique droit sur **IPV4** ensuite choisir **Nouvelle étendue**.
- Commencez par nommer l'étendue **1) Réseau mairie**. Ensuite, configurez la **2) plage d'adresses IP** de 192.168.5.10 à 192.168.5.20 sans exclude d'adresses. Définissez la **3) durée du bail** à 8 jours. Ajoutez la **4) passerelle** (192.168.5.1), puis le **5) nom de domaine** (ville-abymes.fr) et le **DNS** (192.168.5.2). Enfin, n'oublier sélectionnez **Oui** pour configurer et activer l'étendue immédiatement.



C) TEST DU BON FONCTIONNEMENT DU DHCP :

- Pour vérifier si le service DHCP fonctionne correctement, il faut s'assurer que le client a bien reçu une adresse IP dynamique venant du serveur en utilisant la commande **ipconfig /all**

```
pose1.ad [En fonction] - Oracle VM VirtualBox
C:\Windows\system32\cmd.exe
C:\Users\User>ipconfig /all
Configuration IP de Windows

Nom de l'hôte . . . . . : DESKTOP-547TK70
Suffisage DNS principal . . . . . : ville-abymes.fr
Type de nœud . . . . . : Hybride
Partage IP activé . . . . . : Non
Proxy WINS activé . . . . . : Non
Liste de recherche du suffixe DNS . . . . . : ville-abymes.fr

Carte Ethernet Ethernet :

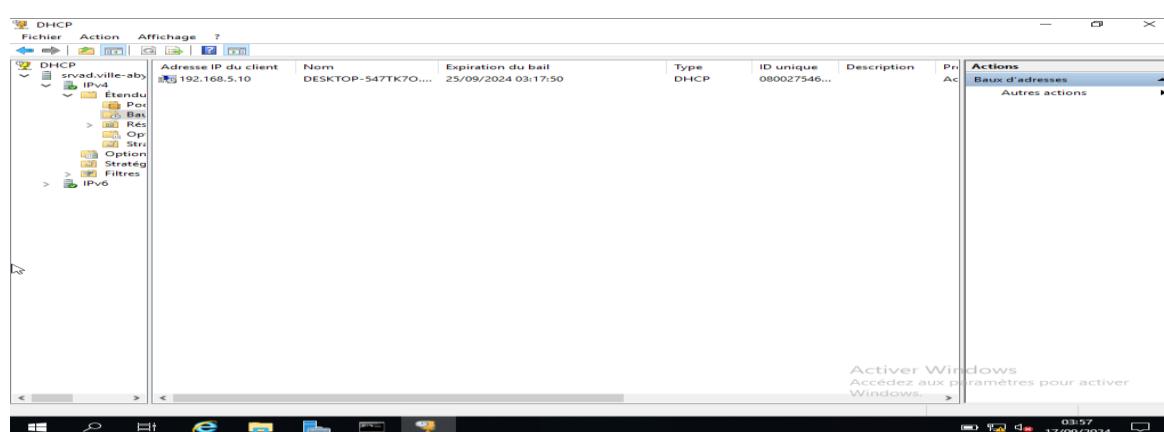
Suffisage DNS propre à la connexion . . . . . : ville-abymes.fr
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Adresse physique . . . . . : 08-00-27-54-66-58
DHCP activé . . . . . : Oui
Configuration automatique activée . . . . . : Oui
Adresse IPv6 de liaison locale . . . . . : fe80::2418:7ff5:298:8152%6(préféré)
Adresse IPv4 . . . . . :
  Masque de sous-réseau . . . . . : 255.255.0.0
  Bail obtenu . . . . . : mardi 17 septembre 2024 03:16:44
  Bail expirant . . . . . : mercredi 25 septembre 2024 03:16:43
  Passerelle par défaut . . . . . : 192.168.5.1
  Serveur DHCP . . . . . : 192.168.5.2
  IAID DHCPv6 . . . . . : 34078759
  DUID de client DHCPv6 . . . . . : 00-01-00-01-2E-70-C6-66-08-00-27-54-66-58
  Serveurs DNS . . . . . : 192.168.5.2
  NetBIOS sur Tcpip . . . . . : Activé

Carte Tunnel isatap.ville-abymes.fr :

Statut du média . . . . . : Média déconnecté
Suffisage DNS propre à la connexion . . . . . : ville-abymes.fr
Description . . . . . : Microsoft ISATAP Adapter #3
Adresse physique . . . . . : 00-00-00-00-00-00-E0
DHCP activé . . . . . : Non
Configuration automatique activée . . . . . : Oui

C:\Users\User>
```

- Ensuite, vérifier que le serveur affiche l'adresse IP du client dans les baux d'adresses du Gestionnaire DHCP.



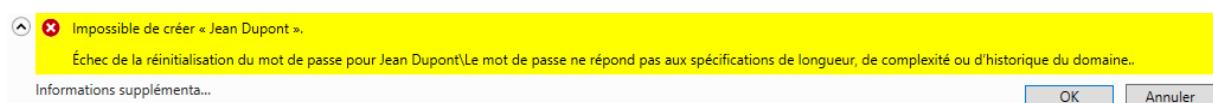
- Comme on peut le voir, ces conditions sont remplies, le service DHCP fonctionne bien.

ETAPE N°4 : CRÉATION DES UTILISATEURS, GROUPES ET UNITÉS D'ORGANISATION :

A) PROCÉDURE CRÉATION UTILISATEURS :

- On peut se diriger dans le **Gestionnaire de Serveur** aller dans **Outils → Centre d'administration Active Directory** → cliquez ici sur **ville-abymes (local)** → ensuite dans le volet de droite **Tâche** → vers le bas avec **Users** → faire **Nouveau** → **Utilisateur**

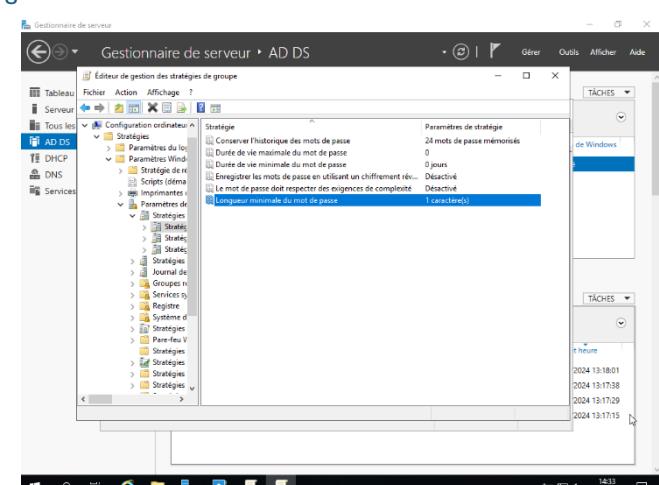
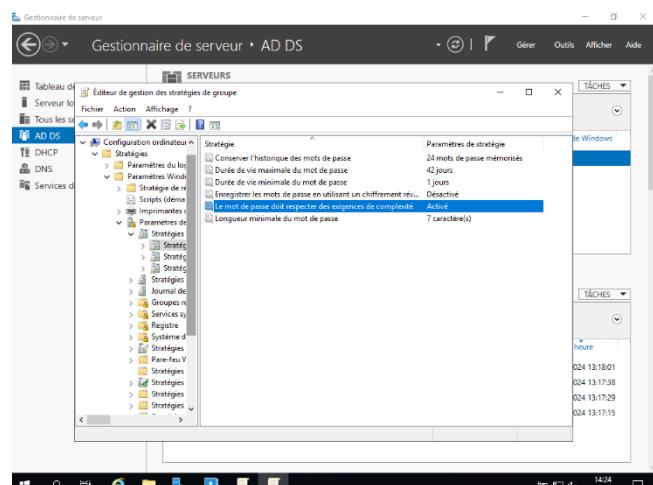
B) MISE EN PLACE STRATÉGIE POUR LES MDP :



- On constate lors de l'essai de la création du premier utilisateur ce message d'erreur, disant que le mot de passe ne répond pas aux critères de complexité et on ne peut pas créer l'utilisateur.

Alors, pour modifier la stratégie de mot de passe, voici les étapes.

- D'abord, il faut aller dans le **Gestionnaire de serveur** → ensuite dans **Outils → Gestion des stratégies de groupe** → **Forêt (ville-abymes.fr)** → **Domaines (ville-abymes.fr)** → **Objet de stratégie de groupe** (en haut de la fenêtre de droite à côté d'Etat) → vous verrez **Default Domain Policy** (C'est la stratégie qui est appliquée au domaine par défaut)
- Une fois sélectionné, faites un **clic droit** dessus, puis choisissez **Modifier**. Ensuite, naviguez dans **Configuration de l'ordinateur → Paramètres Windows → Paramètres de sécurité → Stratégies de compte → Stratégie de mot de passe** C'est ici que l'on désactive la stratégie **Le mot de passe doit respecter les exigences de complexité**.
- On peut désactiver aussi les options de durée de vie minimale et maximale (mettre à 0) de mot de passe ainsi que le nombre minimal de caractères à 7 et le mettre à 1. Car on souhaite que le mot de passe n'expire jamais et qu'il puisse être modifié par les utilisateurs



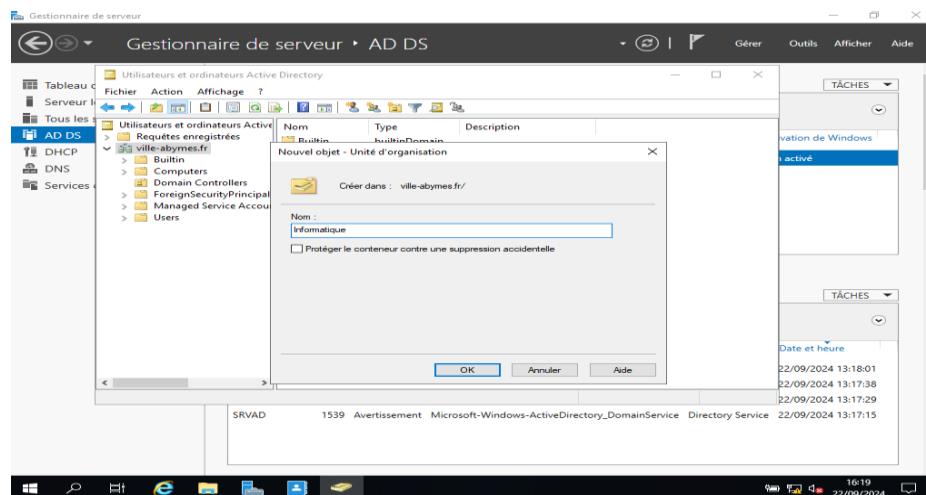
C) PROCÉDURE CRÉATION DE GROUPE :

- **Méthode 1 :** On peut se diriger dans le **Gestionnaire de Serveur** aller dans **Outils** → **Centre d'administration Active Directory** → cliquez ici sur **ville-abymes (local)** → ensuite dans le volet de droite **Tâche** → vers le bas avec **Users** → faire **Nouveau** → **Groupe**

Note : Il faudra ensuite les déplacer dans les unités d'organisation. Vous apprendrez à le faire dans le petit E). C'est la même procédure que pour mettre des utilisateurs dans un groupe.

D) PROCÉDURE CRÉATION UNITÉS D'UNITÉ D'ORGANISATION :

- D'abord, dans le **Gestionnaire de serveur** → allez dans **Outils** → puis **Utilisateurs et ordinateurs Active Directory** → dans l'annuaire **ville-abymes.fr** faites un clic droit et sélectionne **Nouveau** → **Unité d'organisation**. Saisis le nom de l'unité d'organisation, puis décoche l'option **Protéger contre la suppression accidentelle** (au cas où on souhaitez pouvoir déplacer l'objet facilement). Enfin, clique sur **OK** pour valider la création.



- **Méthode 2 :** On peut aussi créer les groupes directement dans l'unité d'organisation. Pour cela on peut faire un clic droit sur l'UO nouvellement créée, puis sélectionne **Nouveau > Groupe**. Entre le nom du groupe, définir l'**étendue** et le **type de groupe** et **OK** pour finir la création du groupe.

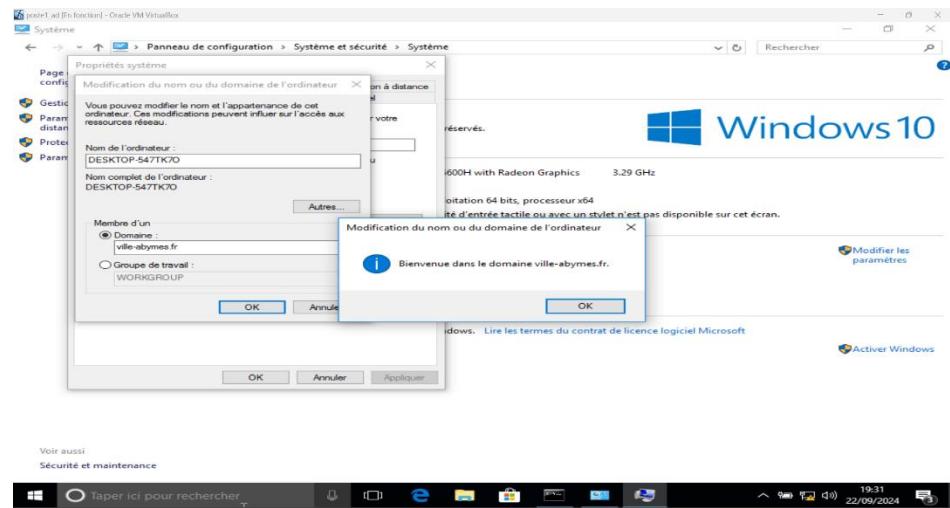
E) PROCÉDURE DÉPLACEMENT UTILISATEURS DANS UN GROUPE :

- Dans un premier temps j'ai créé dans chaque UO, 1 groupe Admin suivie du nom de l'UO (exemple Admin Informatique) et 1 groupe utilisateur de la même manière (exemple Utilisateur Informatique).
 - Pour les **groupes Administrateurs**, l'étendue est globale car elle permet de gérer les ressources sur tout le domaine, assurant aux administrateurs les droits nécessaires sur l'ensemble du domaine.
 - Pour les **groupes Utilisateurs**, l'étendue est locale car elle restreint l'accès aux ressources spécifiques au domaine local, convenant aux utilisateurs ayant des permissions limitées.
 - Le type de groupe est défini en sécurité pour les deux, car il permet de gérer les autorisations d'accès aux ressources dans l'environnement réseau.
-
- Pour déplacer un utilisateur dans la bonne UO allez dans **Utilisateurs et ordinateurs Active Directory** → domaine **ville-abymes.fr** → dans le dossier **Users**, faites un clic droit sur l'utilisateur souhaité → **Déplacer**. Ensuite, naviguez dans l'arborescence pour sélectionner la bonne **Unité d'organisation (UO)**.
 - Une fois l'utilisateur dans la bonne UO, cliquez sur ce même utilisateur **Ajouter à un groupe**, puis cliquez sur **Avancé** (permet d'effectuer une recherche dans l'active Directory) → Rechercher (ce qui fait apparaître la liste des différents groupes) → sélectionnez le bon groupe et faites **OK (2fois)** → **OK**.

ETAPE N°5 : INTÉGRATION DE POSTES DE TRAVAIL AU DOMAINE :

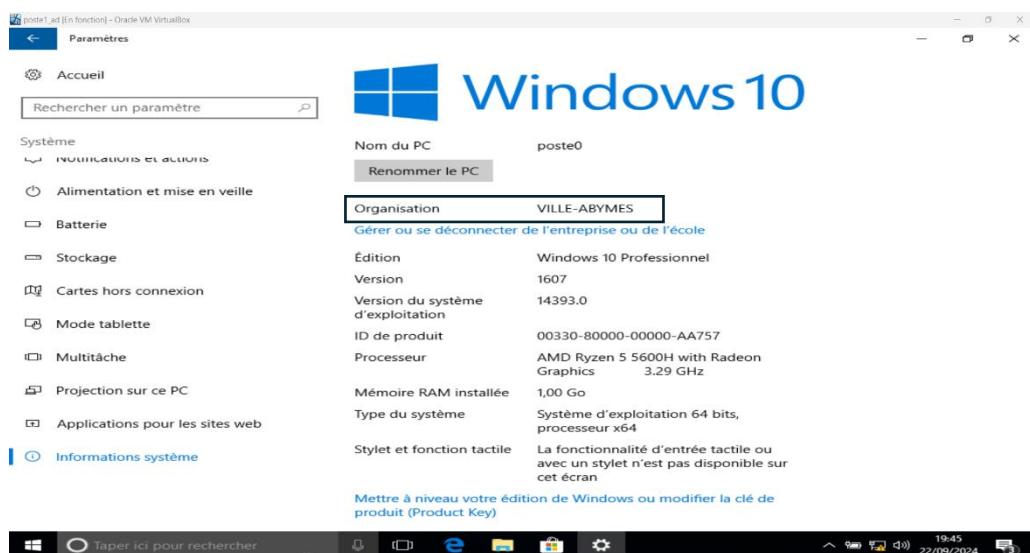
A) DÉMARCHE À SUIVRE :

- Dans un premier temps il faut se connecter au poste client, la manipulation s'effectue sur celui-ci / !\ . Dirigez-vous dans la barre de recherche **Panneau de configuration** → **Système et sécurité** → **Système** → **Modifier les paramètres** → **Modifier** → **Domaine (ville-abymes.fr)**
- Il faut se connecter en tant que **administrateur du domaine** (Administrateur et @admin&2425@) . Puis un message de bienvenu apparaît et faites **OK (2fois)** → **OK** et **Redémarrer l'ordinateur** (pour que le changement soit effectif) .

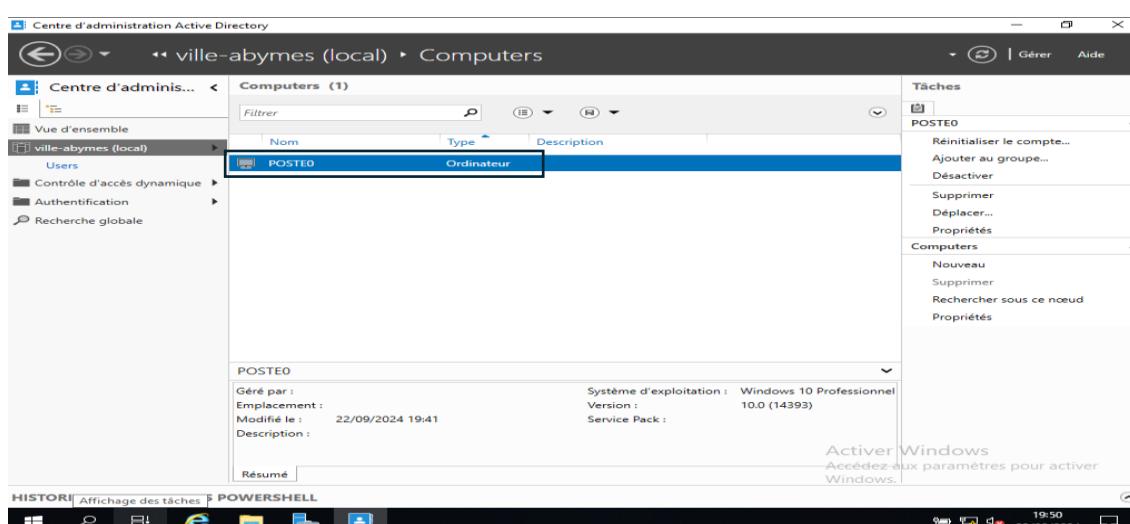


B) VÉRIFICATION DE L'INTÉGRATION :

- Côté client : On peut aller dans **Paramètre → Systèmes → Informations système → dans Organisation** → doit apparaître le nom de domaine **VILLE-ABYMES**.



- Côté serveur : On peut aller dans **le Gestionnaire de Serveur → Outils → Centre d'administration Active Directory** → dans **ville-abymes.fr (local) → Computers** doit apparaître le nom du pc renommé **POSTE0**.



ETAPE N°6 : ELABORATION DE STRATÉGIES DE GROUPE (GPO) :

A) DÉSACTIVER LE PARE-FEU DES POSTES DE TRAVAIL :

- D'abord, il faut aller dans le **Gestionnaire de serveur** → ensuite **dans Outils** → puis dans **Gestion des stratégies de groupe**.
- Dans la fenêtre de Gestion des stratégies de groupe, naviguez dans **Forêt (ville-abymes.fr)** → **Domaines (ville-abymes.fr)** → cliquez sur **Créer un objet de stratégie de groupe dans ce domaine et le lier ici**.
- Une fois l'objet créé, nommez la stratégie (par exemple, **Désactivation parefeu**), puis faites un **clic droit** sur la stratégie nouvellement créée et choisissez **Modifier**.
- Naviguez ensuite dans **Configuration de l'ordinateur** → **Stratégies** → **Paramètres Windows** → **Paramètres de sécurité > Pare-feu Windows Defender avec sécurité avancée** → **Propriété du Pare-Feu Windows Defender**.
- Sélectionnez les profils que vous souhaitez **désactiver** : **Profil Domaine**, **Profil Privé**, et **Profil Public**.
- Sur chacun de ces profils définissez le **Pare-feu sur Désactivé**.
- Validez en cliquant sur **Appliquer** → **OK** pour chaque profil.
- Enfin, la stratégie étant déjà liée à l'ensemble du domaine (puisque'elle a été créée au niveau du domaine), elle s'appliquera automatiquement à tous les ordinateurs du domaine sans avoir besoin de la lier à chaque unité d'organisation (OU) individuellement.

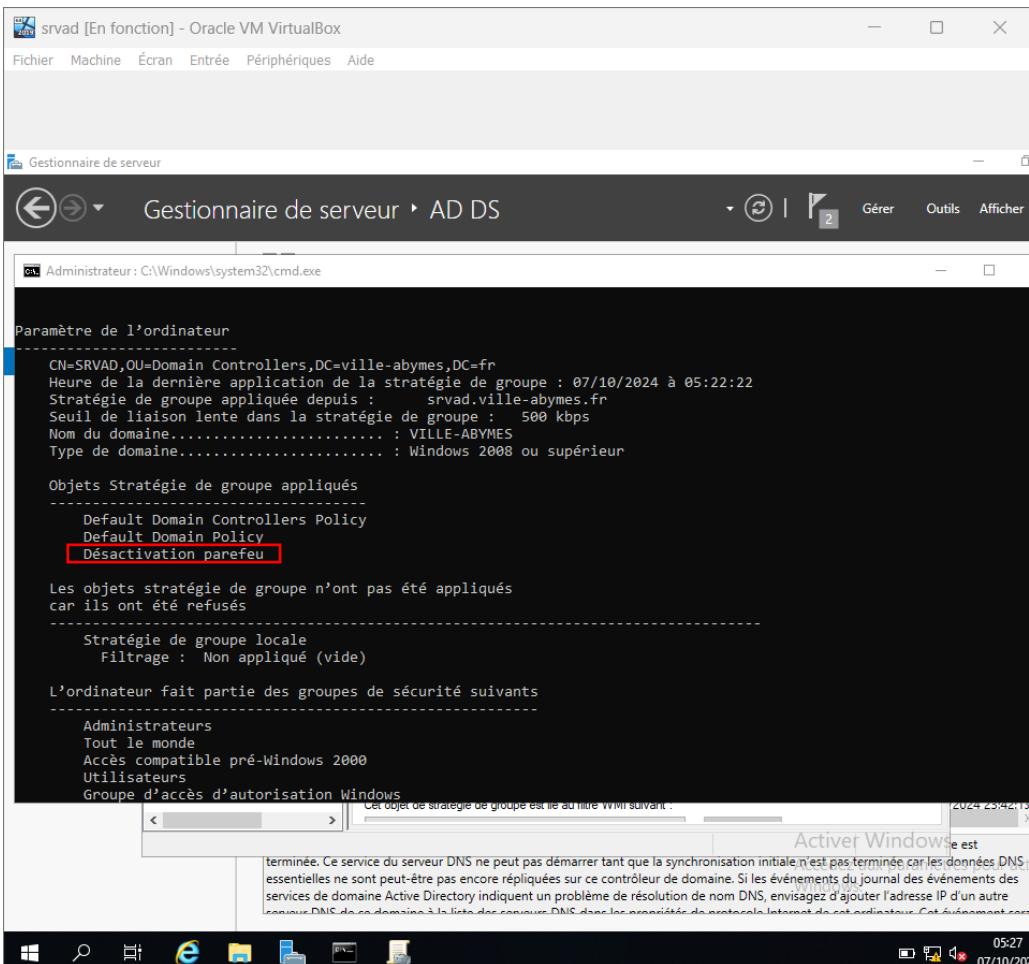
Lier la stratégie à une Unité d'Organisation (OU) spécifique : (Facultatif)

- Si vous souhaitez appliquer la stratégie uniquement à une OU spécifique (par exemple : **Compta_finance**), faites un **clic droit** sur l'**OU Compta_finance** puis sélectionnez **Lier un objet de stratégie de groupe existant**.
- Sélectionnez la stratégie que vous avez créée (par exemple : **Désactivation parefeu**) dans la liste des stratégies disponibles.
- Cliquez sur **OK** pour finaliser le lien.

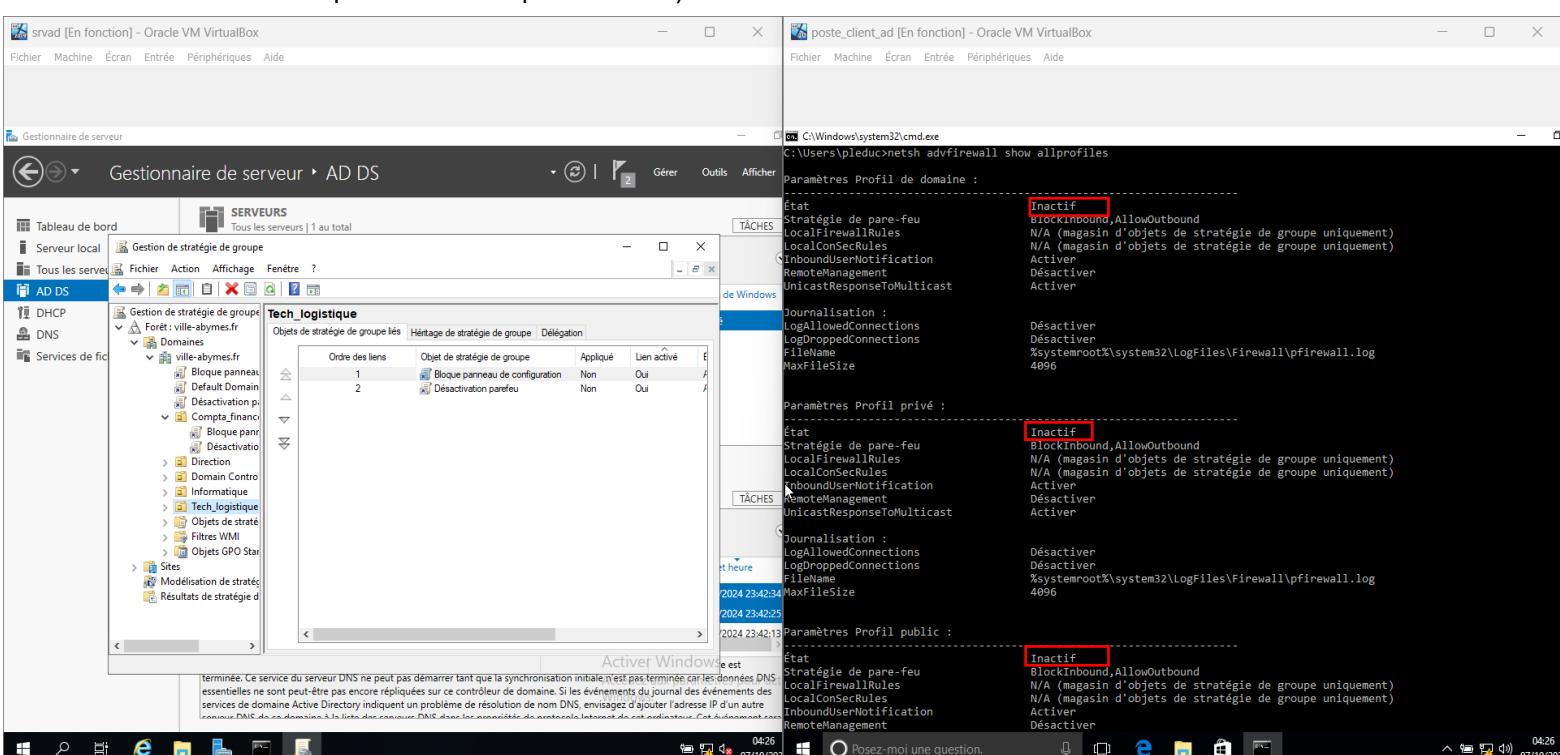
Forcer l'application de la stratégie :

- Pour forcer l'application de la stratégie immédiatement, exécutez la commande suivante sur le poste client : **<< gpupdate /force >>**

Teste << gpresult /r >> côté serveur :



Teste << netsh advfirewall show allprofiles >> (Si la stratégie fonctionne, l'état du pare-feu pour les profils Domaine, Privé, et Public sera **inactif**, ce qui signifie que la stratégie a bien désactivé le pare-feu sur le poste client) :



Remarque : N/A (magasin d'objets de stratégie de groupe uniquement), cela signifie que le pare-feu est contrôlé uniquement par la stratégie de groupe (GPO), et que toute modification locale des paramètres du pare-feu est bloquée ou ignorée.

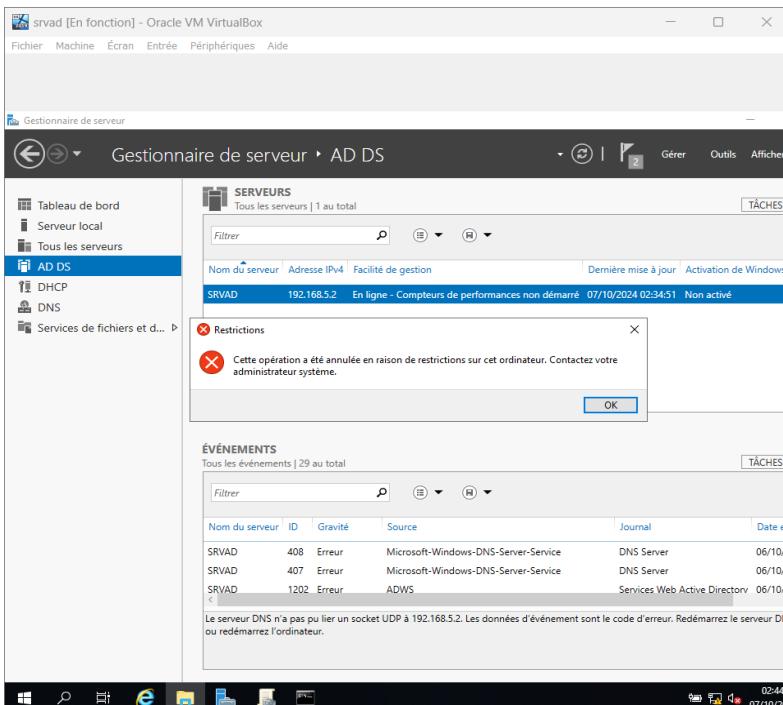
B) DÉSACTIVER L'ACCÈS AU PANNEAU DE CONFIGURATION :

- D'abord, il faut aller dans le **Gestionnaire de serveur** → ensuite dans **Outils** → puis dans **Gestion des stratégies de groupe**.
- Dans la fenêtre de Gestion des stratégies de groupe, naviguez dans **Forêt (ville-abymes.fr)** → **Domaines (ville-abymes.fr)** → cliquez sur **Créer un objet de stratégie de groupe dans ce domaine et le lier ici**
- Une fois l'objet créé, nommez la stratégie (par exemple : **Blocage panneau de configuration**), puis faites un **clic droit** sur la stratégie nouvellement créée et choisissez **Modifier**.
- Naviguez ensuite dans **Configuration utilisateur** → **Stratégies** → **Modèles d'administration** → **Panneau de configuration**.
- Sélectionnez le paramètre **Interdire l'accès au Panneau de configuration et aux Paramètres PC**, faites un **clic droit** dessus et choisissez **Modifier**. Activez cette stratégie en sélectionnant **Activé**, puis cliquez sur **OK**.
- Enfin, la stratégie étant déjà liée à l'ensemble du domaine (puisque elle a été créée au niveau du domaine), elle s'appliquera automatiquement à tous les utilisateurs du domaine sans avoir besoin de la lier à chaque unité d'organisation (OU) individuellement.

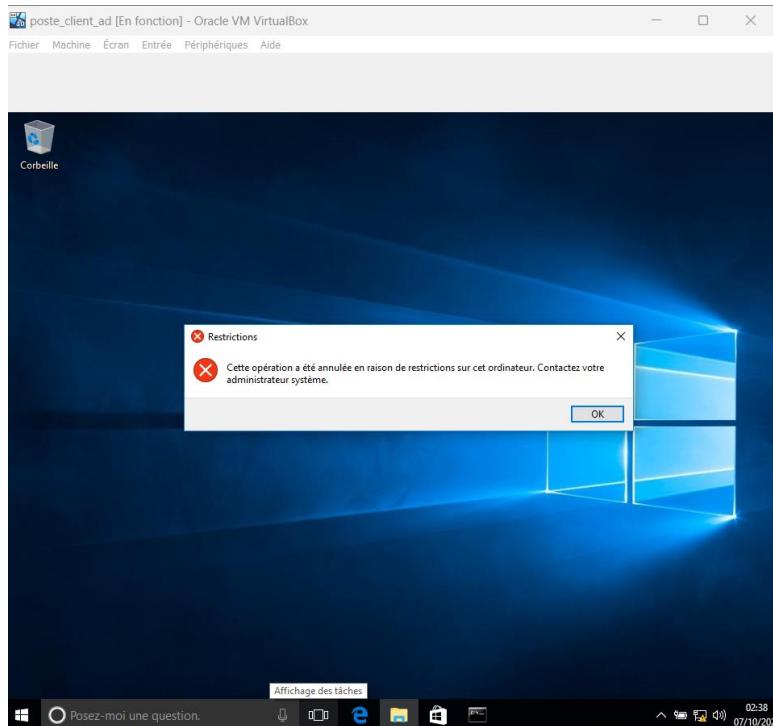
- Pour lier une stratégie à une unité (exemple : **Direction**), faites un **clic droit** sur l'OU **Direction**, puis sélectionnez **Lier un objet de stratégie de groupe existant**.
- Sélectionnez la stratégie que vous avez créée (par exemple, **Blocage Panneau de configuration**) dans la liste des stratégies disponibles.
- Cliquez sur **OK** pour finaliser le lien

- Pour **forcer l'application de la stratégie immédiatement**, exécutez la commande suivante sur le poste client : << **gpupdate /force** >>
- Après avoir redémarré le **poste client**, connectez-vous avec **un utilisateur du domaine** et essayez d'accéder au panneau de configuration et sur le serveur elle est censée déjà fonctionner. Si la stratégie fonctionne, un message de restriction apparaîtra, indiquant que l'accès au panneau de configuration est bloqué.

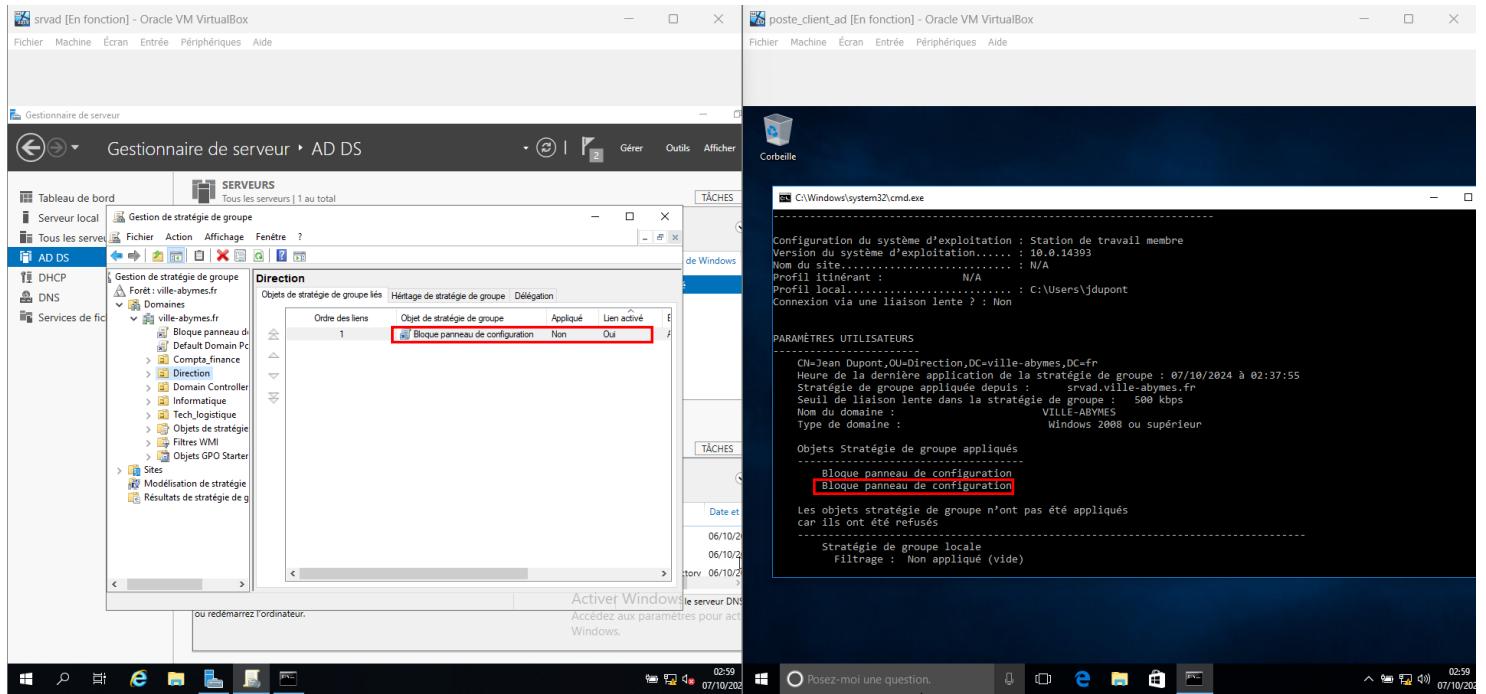
Teste d'accès panneau de configuration côté serveur :



Teste d'accès panneau de configuration côté client :



Teste <>gpresult /r>> côté client (ce qui montre que le client a bien reçu la stratégie venant du serveur) :



C) DÉFINIR UN PAPIER PAR DÉFAUT POUR LES UTILISATEURS EN FONCTION DE L'UO À LAQUELLE ILS APPARTIENNENT :

Création d'un dossier partagé pour stocker les papiers peints

- J'ai commencé par créer un **dossier partagé** sur le serveur **srvad (partition 10Go Données)** afin de **stocker les différents papiers peints** que j'ai sélectionnés pour chaque Unité d'Organisation (Direction, Compta_financial, Tech_logistique, Informatique). Ce dossier, nommé **papier_peint**, est accessible via le chemin réseau **\SRVAD\papier_peint**. J'ai configuré les permissions pour que **tous les utilisateurs** puissent accéder à ces images en lecture seule.
- Pour chaque UO, j'ai téléchargé des papiers peints de manières personnalisées sur **Pexels** et les ai renommés en utilisant le préfixe "f" suivi du domaine métier correspondant, par exemple **fdirection** pour la **Direction**. Ces images sont ainsi stockées dans le dossier partagé accessible aux clients, prêtes à être déployées via les GPO pour chaque service.
- Maintenant pour chaque Unité d'Organisation (UO), il est nécessaire de **créer une stratégie à l'intérieur de l'OU elle-même**. Nous allons illustrer cette procédure en prenant **l'exemple de la création pour l'OU Direction**, et il suffira ensuite de **reproduire** les mêmes étapes en **modifiant les paramètres en fonction des autres UO**.

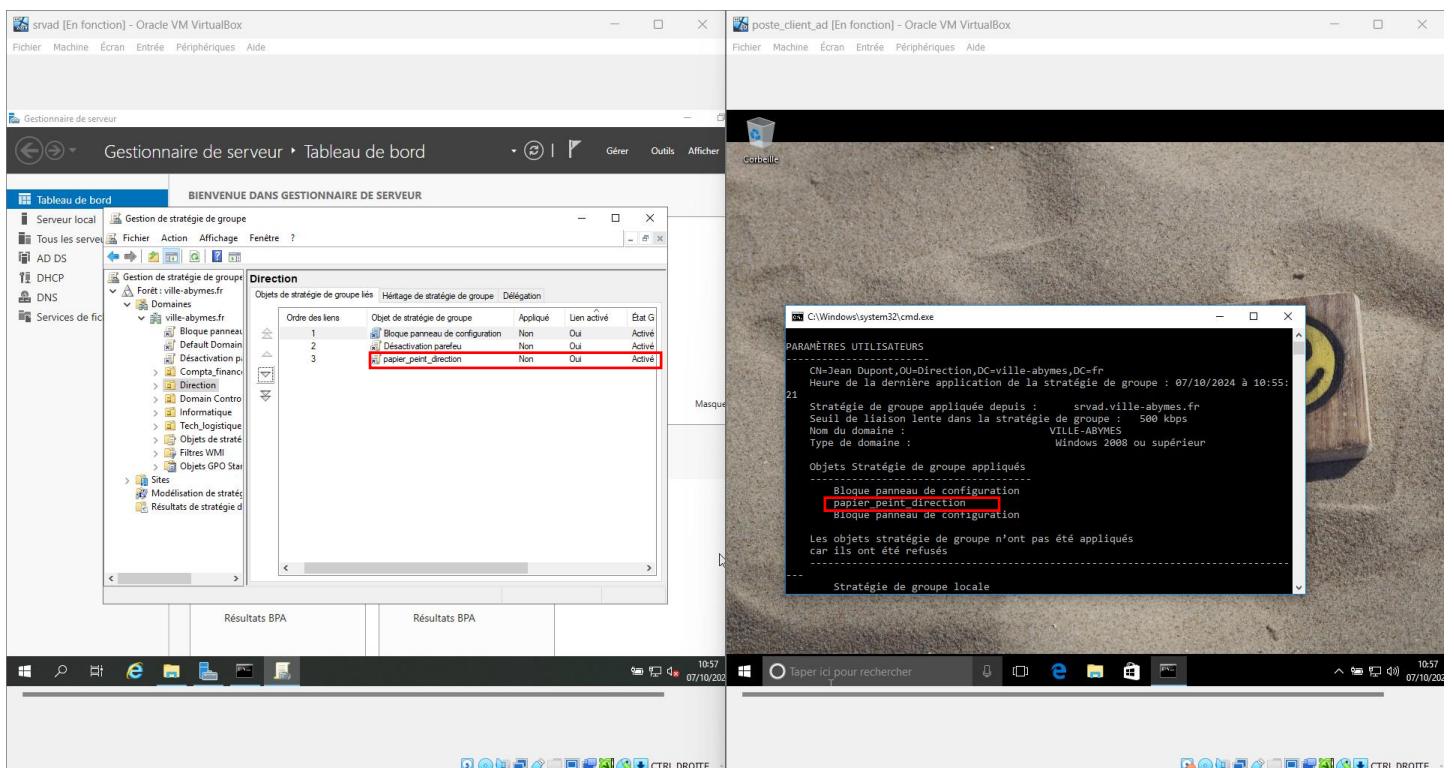
Création de la stratégie de groupe pour l'OU Direction

- Ouvrez le **Gestionnaire de serveur** → puis **Outils** → ensuite **Gestion des stratégies de groupe**.
- Dans la fenêtre de Gestion des stratégies de groupe, naviguez dans **Forêt (ville-abymes.fr)** → **Domaines (ville-abymes.fr)** → dans l'arborescence naviguez vers l'**OU Direction** (au lieu de créer la GPO au niveau du domaine).
- Faites un **clic droit sur Direction** → sélectionnez **Créer un objet de stratégie de groupe dans ce domaine et le lier ici**
- Nommez la stratégie (par exemple : **papier_peint_direction**) pour plus de clarté.

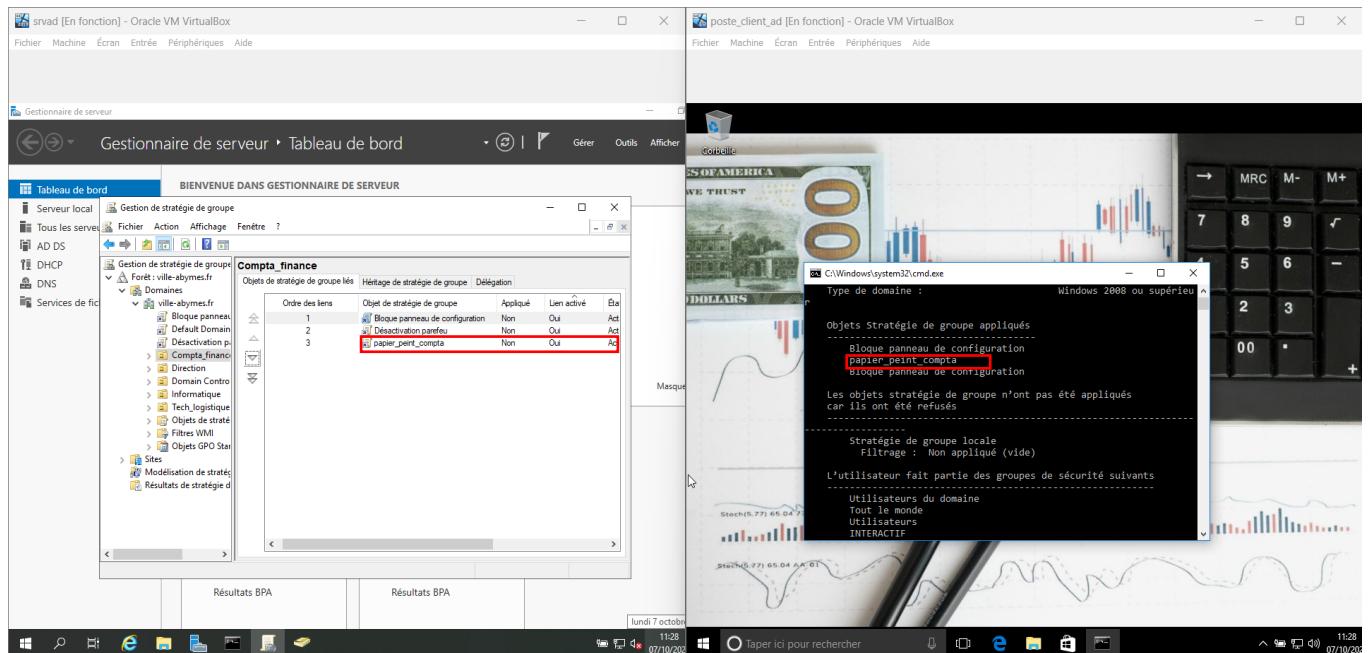
Configuration du papier peint

- Une fois la stratégie créée, faites un **clic droit sur la stratégie** créée et sélectionnez **Modifier**.
- Naviguez dans **Configuration utilisateur** → puis **Stratégies** → ensuite **Modèles d'administration** → 2 fois de suite **Bureau** → **Bureau** → enfin **Papier peint du Bureau**
- Cliquer en haut à gauche sur **Activé**
- Dans le champ **Nom du fichier du papier peint**, entrer le chemin du fond d'écran spécifique à l'OU : << \\sravad\\papier_peint\\fdirection.jpg >>
! Ne pas oublier le type de l'image << .jpeg et >>
- Valider en cliquant sur **Appliquer** → puis **OK**

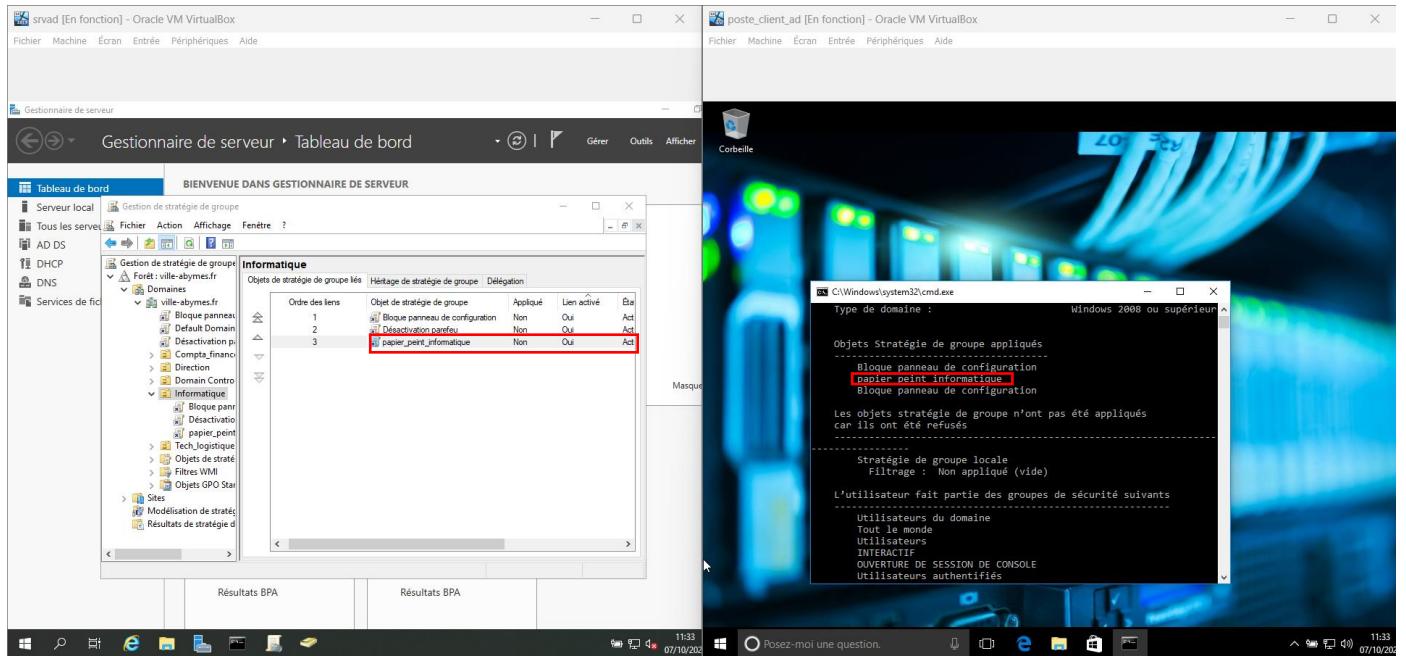
Teste de connexion au compte jdupont appartenant à l'OU Direction côté client :



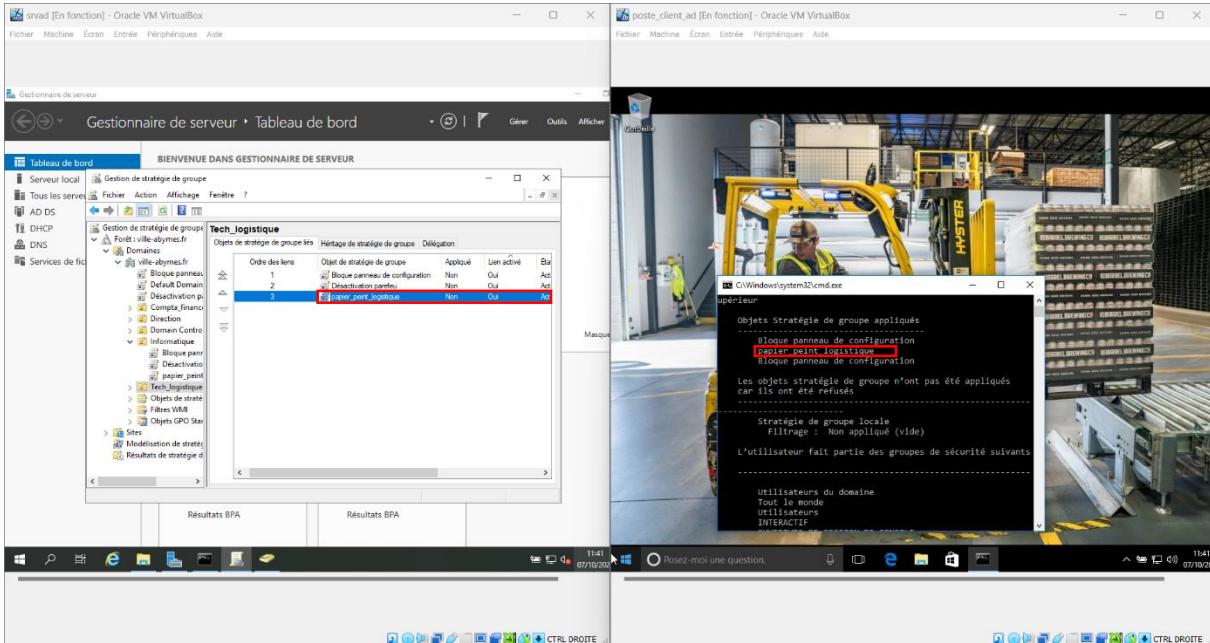
Teste de connexion au compte pleduc appartenant à l'UO Compta_finance côté client :



Teste de connexion au compte dlaurent appartenant à l'UO Informatique côté client :



Teste de connexion au compte clemarchal appartenant à l'UO Tech_logistique côté client :



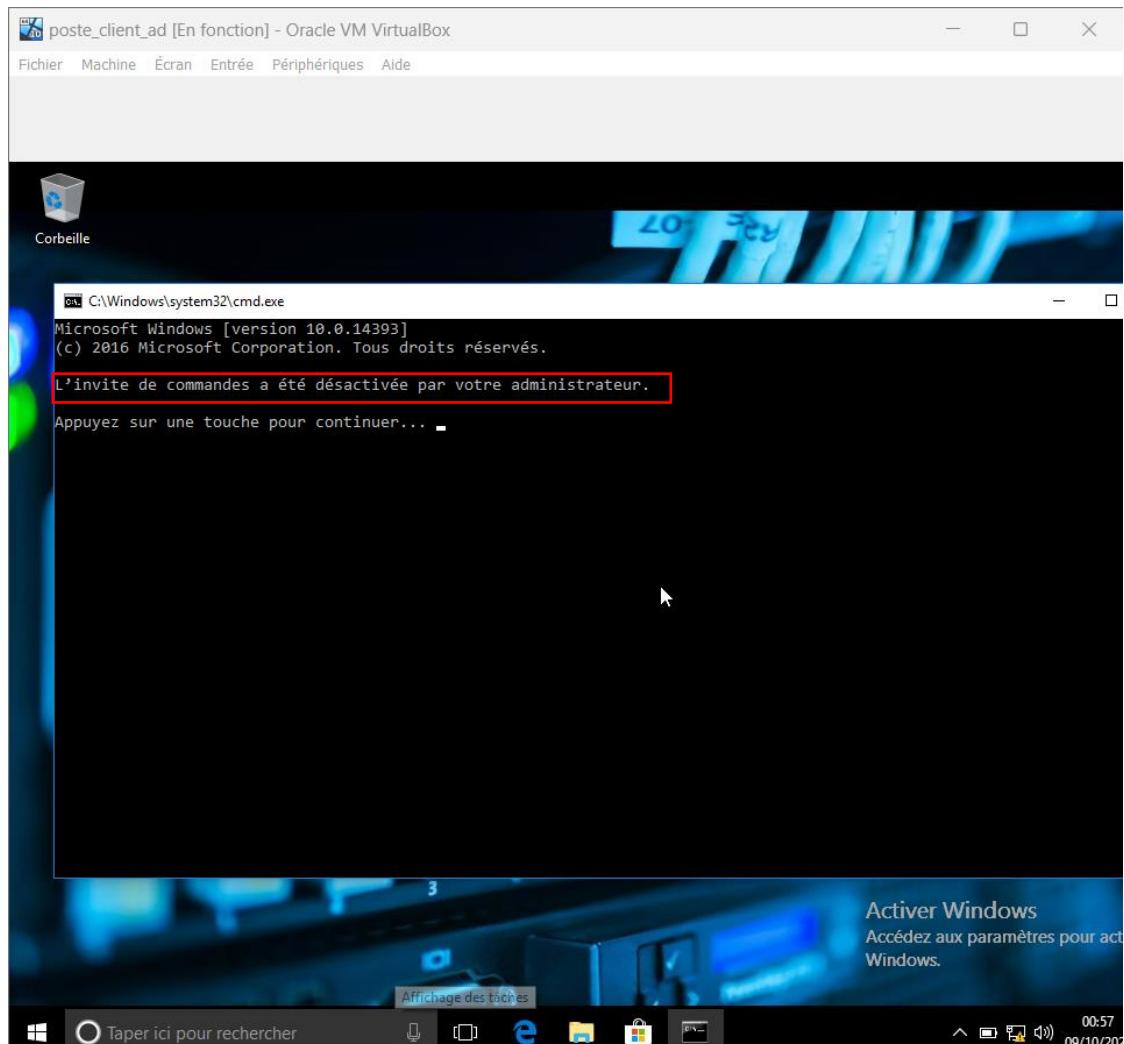
D) DÉSACTIVER L'ACCÈS À LA COMMANDE « EXÉCUTER » :

- D'abord, il faut aller dans le **Gestionnaire de serveur** → ensuite dans **Outils** → puis dans **Gestion des stratégies de groupe**.
- Dans la fenêtre de Gestion des stratégies de groupe, naviguez dans **Forêt (ville-abymes.fr)** → **Domaines (ville-abymes.fr)** → dans l'arborescence naviguez vers l'**OU Informatique** par exemple (au lieu de créer la GPO au niveau du domaine) → cliquez sur **Créer un objet de stratégie de groupe dans ce domaine et le lier ici**
- Une fois l'objet créé, nommez la stratégie (par exemple, **Désactive commande exécuter**), puis faites un **clic droit** sur la stratégie nouvellement créée et choisissez **Modifier**.
- Naviguez ensuite dans **Configuration Utilisateur** → **Stratégies** → **Modèles d'administration** → **Système** → **Désactiver l'accès à l'invite de commandes** → Activez cette stratégie en sélectionnant **Activé**, puis cliquez sur **OK**.
- Validez en cliquant sur **Appliquer** → **OK**

Forcer l'application de la stratégie :

- Pour forcer l'application de la stratégie immédiatement, exécutez la commande suivante sur le poste client : <> **gpupdate /force** >>

Teste d'accès à l'invite de commande sur le compte d'administrateur de l'UO Informatique :



Observation : On a un message qui confirme l'application de la stratégie en disant que l'invite de commande et par conséquent la commande exécuté à été désactivée.

E) DÉSACTIVER LA CONFIGURATION RÉSEAU :

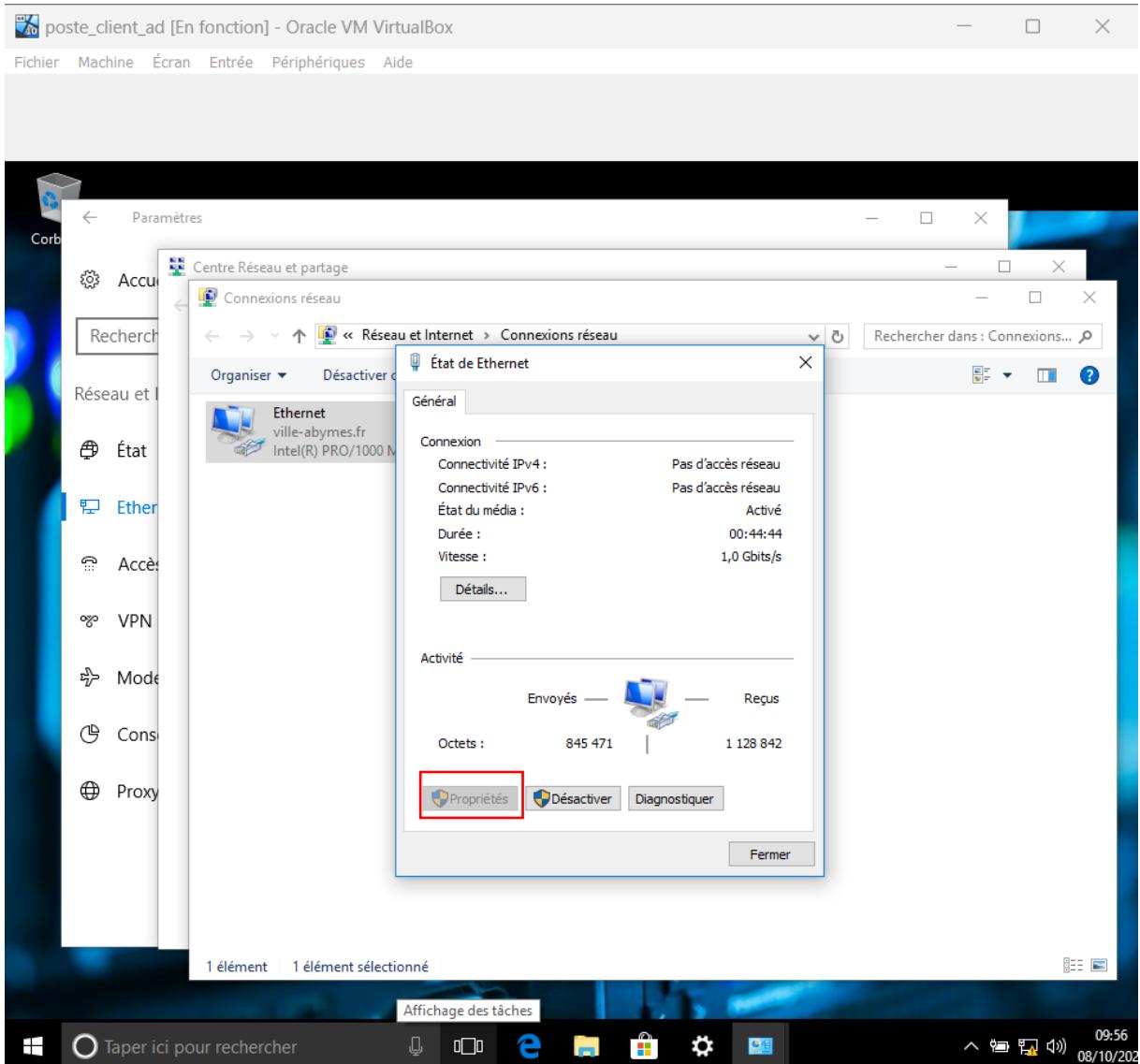
- D'abord, il faut aller dans le **Gestionnaire de serveur** → ensuite dans **Outils** → puis dans **Gestion des stratégies de groupe**.
- Dans la fenêtre de Gestion des stratégies de groupe, naviguez dans **Forêt (ville-abymes.fr)** → **Domaines (ville-abymes.fr)** → cliquez sur **Créer un objet de stratégie de groupe dans ce domaine et le lier ici**.
- Une fois l'objet créé, nommez la stratégie (par exemple, **Désactivation configuration réseaux**), puis faites un **clic droit** sur la stratégie nouvellement créée et choisissez **Modifier**.
- Naviguez ensuite dans **Configuration Utilisateur** → **Stratégies** → **Modèles d'administration** → **Réseau** → **Connexions réseau** → **Interdire l'accès aux propriétés d'une connexion local**
- Validez en cliquant sur **Appliquer** → **OK**

- Enfin, la stratégie étant déjà liée à l'ensemble du domaine (puisque'elle a été créée au niveau du domaine), elle s'appliquera automatiquement à tous les ordinateurs du domaine sans avoir besoin de la lier à chaque unité d'organisation (OU) individuellement.

Forcer l'application de la stratégie :

- Pour forcer l'application de la stratégie immédiatement, exécutez la commande suivante sur le poste client : <> gpupdate /force >>

Teste d'accès à la configuration réseaux sur le compte d'administrateur de l'UO Informatique :



Remarque : Après la mise en place de la stratégie **Désactivation configuration réseaux**, on constate que la case **Propriétés** dans les **Connexions réseau** est désormais grisée et inaccessible. Cela signifie qu'on ne peut plus accéder ni modifier les paramètres de configuration réseau (comme l'adresse IP, les DNS, etc.). Par conséquent, cette stratégie répond bien à la consigne de désactiver la configuration réseau, car elle empêche toute modification manuelle des paramètres réseau.

F) CRÉER ET MONTER AUTOMATIQUEMENT DES LECTEURS RÉSEAUX EN FONCTION DES UO :

Création du dossier de partage et attribution des droits d'accès (contrôle total)

- Dans un premier temps, il faut créer les dossiers partagés de chaque UO dans la partition de 10 Go réservée aux Données. Lors du partage, pour donner un contrôle total à l'UO à qui appartient le dossier, faites **clic droit** sur le dossier (ici : **Tech_logistique**) → puis **Propriétés** → en haut à gauche **Partage** → **Partage avancé** → cochez **Partager ce dossier** → cliquez sur **Autorisations** → **Supprimer** le groupe par défaut donnant accès à **Tout le monde** → **Ajouter** l'UO (ici :**Tech_logistique**) associée au dossier en question en faisant → **Avancé** → **Rechercher** → une fois trouvé **OK** → **OK** → cocher maintenant dans **Autoriser** → **Contrôle total** → **Appliquer** → enfin **OK**.
- Maintenant **pour chaque Unité d'Organisation (UO)**, il est nécessaire de **créer une stratégie à l'intérieur de l'OU elle-même**. Nous allons illustrer cette procédure en prenant **l'exemple de la création pour l'OU Tech_logistique**, et il suffira ensuite de reproduire les mêmes étapes en **modifiant les paramètres en fonction des autres UO**.

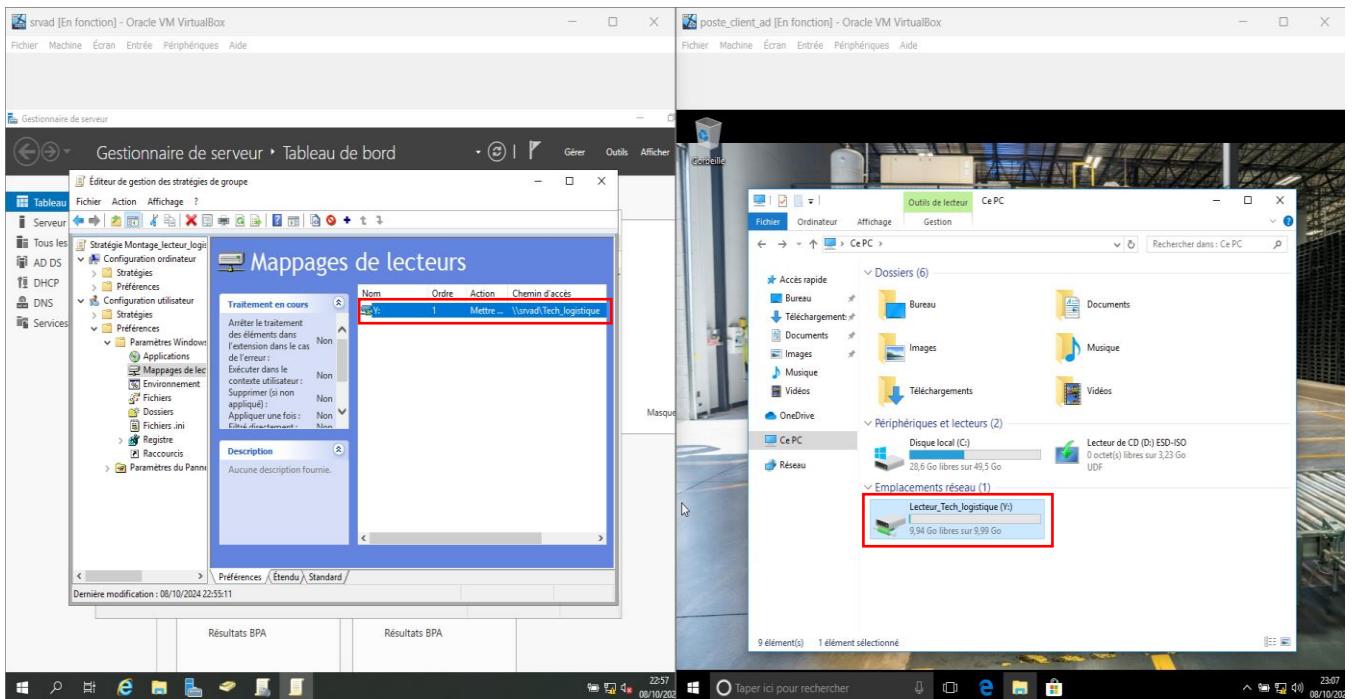
Création de la stratégie de groupe pour l'OU Tech_logistique

- Ouvrez le **Gestionnaire de serveur** → puis **Outils** → ensuite **Gestion des stratégies de groupe**.
- Dans la fenêtre de Gestion des stratégies de groupe, naviguez dans **Forêt (ville-abymes.fr)** → **Domaines (ville-abymes.fr)** → dans l'arborescence naviguez vers l'**OU Tech_logistique** (au lieu de créer la GPO au niveau du domaine).
- Faîtes un **clic droit** sur **Tech_logistique** → sélectionnez **Créer un objet de stratégie de groupe dans ce domaine et le lier ici**
- Nommez la stratégie (par exemple : **Montage_lecteur_logistique**) pour plus de clarté.

Configuration du papier peint

- Une fois la stratégie créée, faîtes un **clic droit sur la stratégie** crée et sélectionnez **Modifier**.
- Naviguez dans **Configuration utilisateur** → puis **Préférences** → ensuite **Paramètres Windows** → **Mappages de lecteurs** → **clic droit Nouveau** → enfin **Lecteur mappé**
- Une fois dans la fenêtre de configuration du lecteur mappé ; remplissez sont **Emplacement** (ici : **\\\srval\Tech_logistique**); cochez **Reconnecter**, **Afficher ce lecteur**, **Afficher tous les lecteurs** et enfin de pas oublier à coté de **Utiliser faire défiler le menu déroulant pour choisir la lettre** du lecteur (ici : **Y**)
- Valider en cliquant sur **Appliquer** → puis **OK** , faîtes **<>gpupdate /force>>** dans cmd

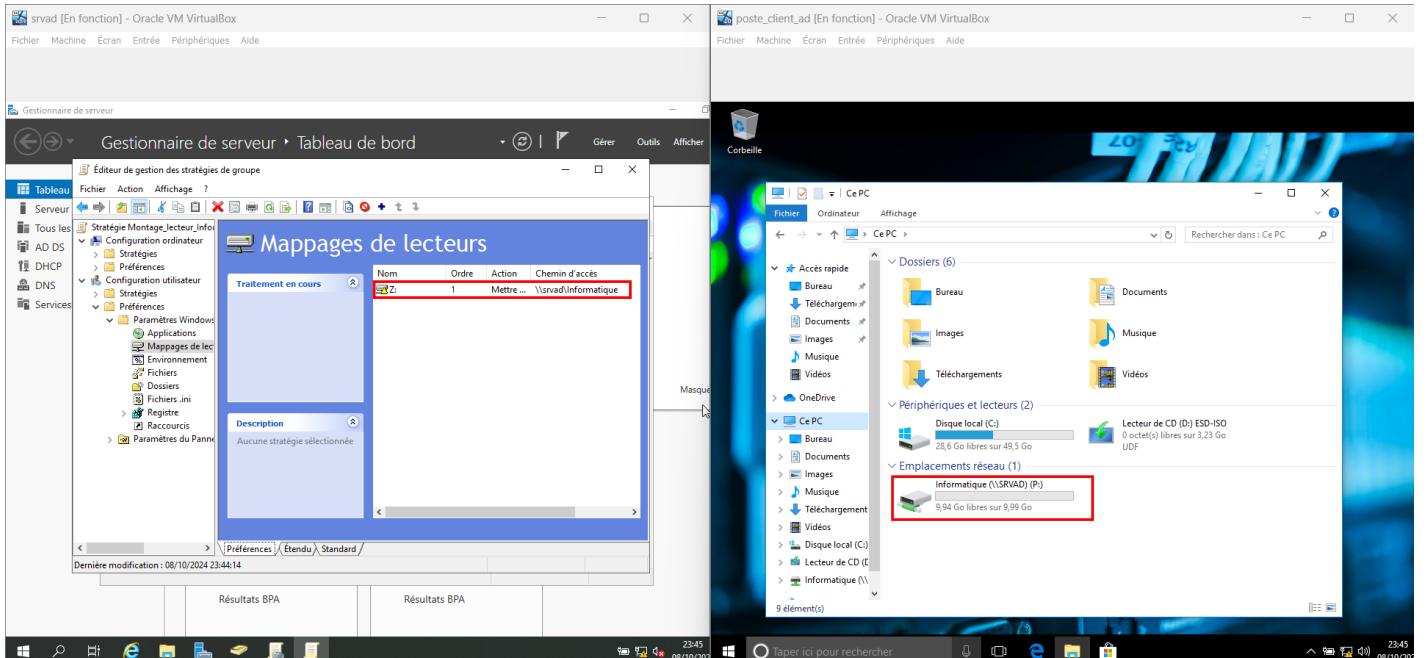
Teste d'accès à l'explorateur de fichier du compte clemarchal de l'UO Tech_logistique :



Observation : Lorsque l'on va dans ce **CePC**, on constate que le lecteur créé et appliquer automatiquement dans la stratégie est en effet déjà monter et est accessible par l'utilisateur.

Dans mappage de lecteurs, on voit que lecteur Y: a été correctement configuré et assigné à l'OU **Tech_logistique**.

Teste d'accès à l'explorateur de fichier du compte dlaurent de l'UO Informatique :



ETAPE N°7 : DÉPLOIEMENT DE LOGICIELS PAR GPO :

- Dans un premier temps il faut, **télécharger** les logiciels ici pour **Notepad++** et **Firefox** en <<.msi>>
- Une fois les logiciels téléchargés, créez un **dossier partagé** sur le serveur **srvad** afin de les **stocker** et rendre **accessibles** pour le **déploiement**. Ce dossier est nommé **Logiciels** et se trouve dans la partition dédiée aux données avec le chemin réseau suivant : << \\srvad\\Logiciels >>
- Ajoutez le groupe **Ordinateurs du domaine** dans les permissions de sécurité du dossier partagé.
- Donc faites un clic droit sur le dossier **Logiciel** → puis **Propriétés** → **Sécurité** → **Modifier**.
- Ensuite, j'ai cliqué sur **Ajouter**, puis **Avancé** → **Rechercher** et j'ai sélectionné le groupe **Ordinateurs du domaine**.
- J'ai coché dans **Autorisations** → **Lecture** → **Affichage du contenu du dossier** → **Lecture et exécution** (cela va permettre aux ordinateurs de pouvoir récupérer les logiciels)
- Valider en cliquant sur **Appliquer** → puis **OK**
- **PS** : Pour éviter un problème d'accès au dossier partagé, j'ai ajouté toutes les UO concernées et le groupe "Ordinateurs du domaine" dans les permissions de sécurité, avec des droits de lecture, exécution et contrôle total pour permettre l'accès aux logiciels. J'ai aussi mit le poste client dans en tant que membre dans chaque groupe de chaque UO. Et pour rappel Tout le monde à accès en lecture au dossier partagé !

Création de la stratégie GPO pour le déploiement des logiciels :

- J'ai ouvert le **Gestionnaire de serveur** → **Outils** → **Gestion des stratégies de groupe**.
- Ensuite, j'ai navigué dans **Forêt (ville-abymes.fr)** → **Domaines (ville-abymes.fr)**.
- J'ai fait un **clic droit** sur le domaine ville-abymes.fr, puis j'ai sélectionné **Créer un objet de stratégie de groupe dans ce domaine et le lier ici**.
- J'ai nommé cette stratégie **Déploiement_npp** → puis **clic droit** → **Modifier**
- Allez dans **Configuration de l'ordinateur** → **Stratégies** → **Paramètres du logiciel** → **Installation du logiciel** → ensuite **clic droit** et sélectionné **Nouveau** → **Package**
- Naviguez jusqu'au chemin résa du dossier partagé où sont stockés les logiciels :

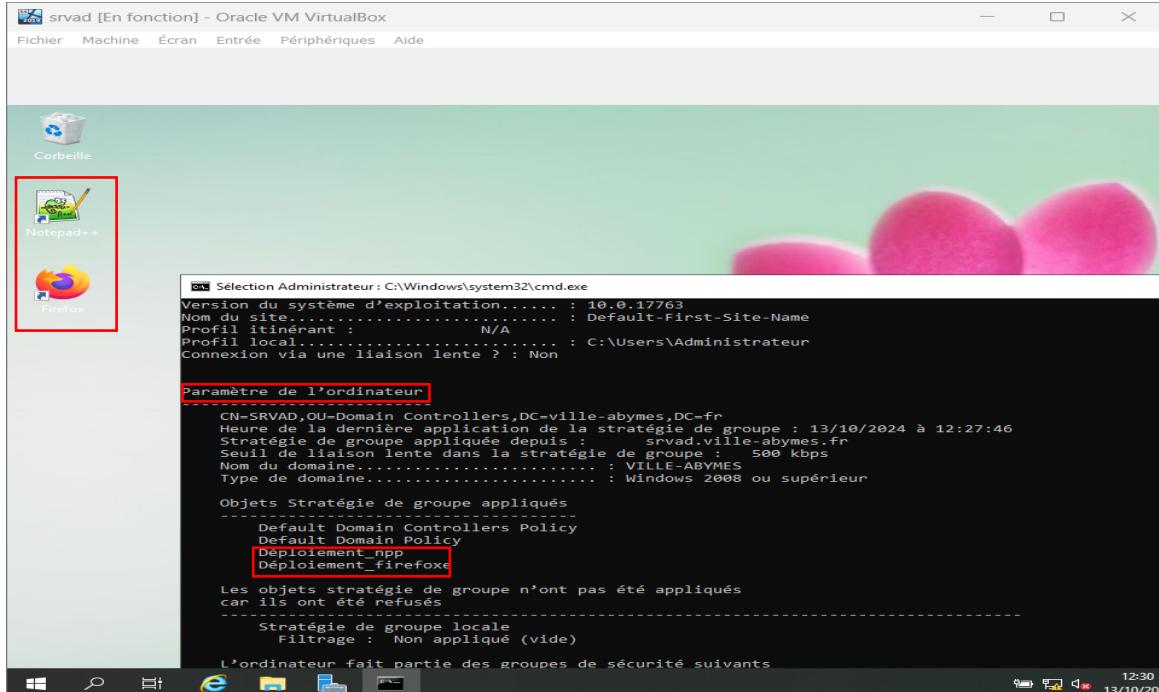
<< \\srvad\\Logiciels\\Notepadpp v8.6.4.msi >>
- Ensuite, j'ai sélectionné **Ouvrir** → **Oui** → type de déploiement **Attribué** → **OK**.

Forcer l'application de la stratégie :

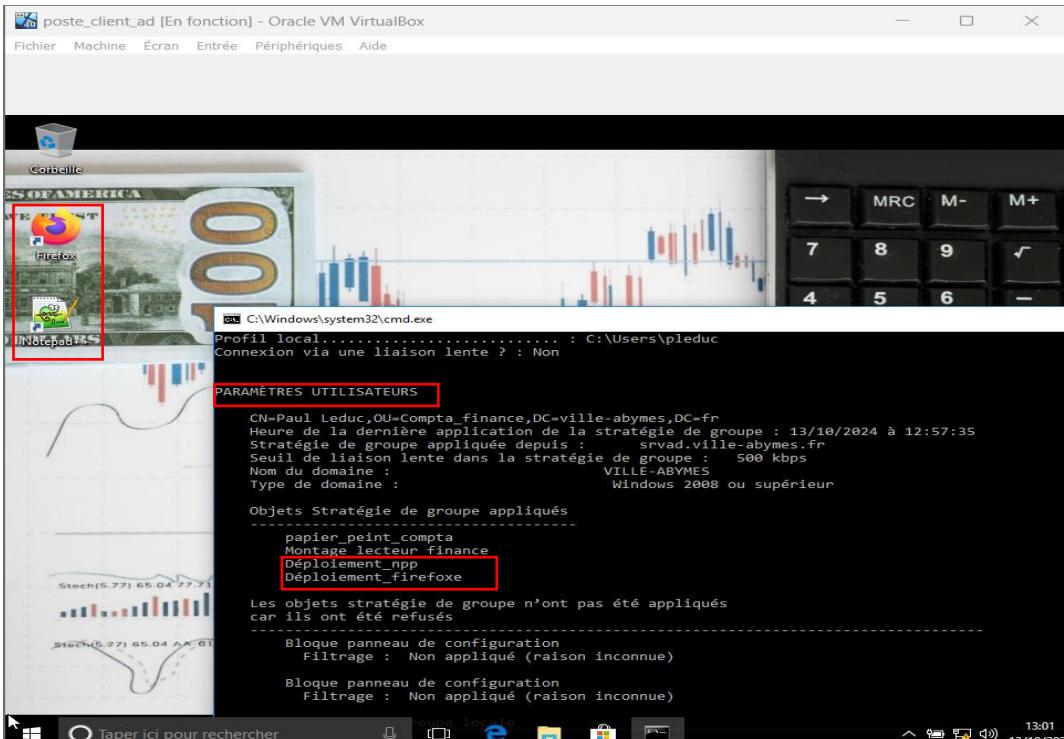
- Pour forcer l'application de la stratégie immédiatement, exécutez la commande suivante sur le poste client : << **gpupdate /force** >> → Il va falloir entrez la lettre **O (OUI)** pour accepter le redémarrage de l'ordinateur et le téléchargement va se faire juste avant la fin du redémarrage
- Pour déployer Firefox il suffit de refaire une autre stratégie en suivant la procédure ci-dessus et de choisir le fichier MSI de Firefox.

PS : la stratégie pour déployer les logiciels en mode configuration de logiciel s'appliquait bien au serveur mais le client même après redémarrage n'installait pas les logiciels or il a accès aux dossier partagé. Donc j'ai mis en la stratégie en **Paramètre Utilisateur** pour que le **client** et il l'a installé.

Teste de la stratégie de déploiement logiciel côté serveur :



Teste de la stratégie de déploiement logiciel côté client :

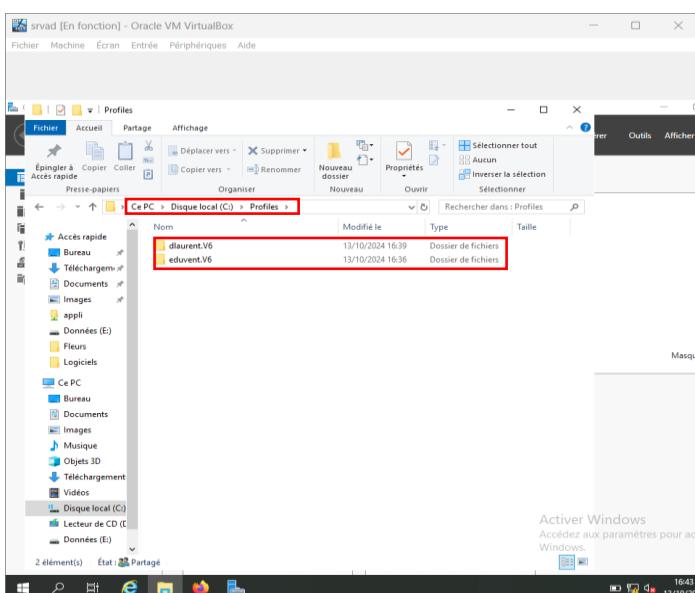


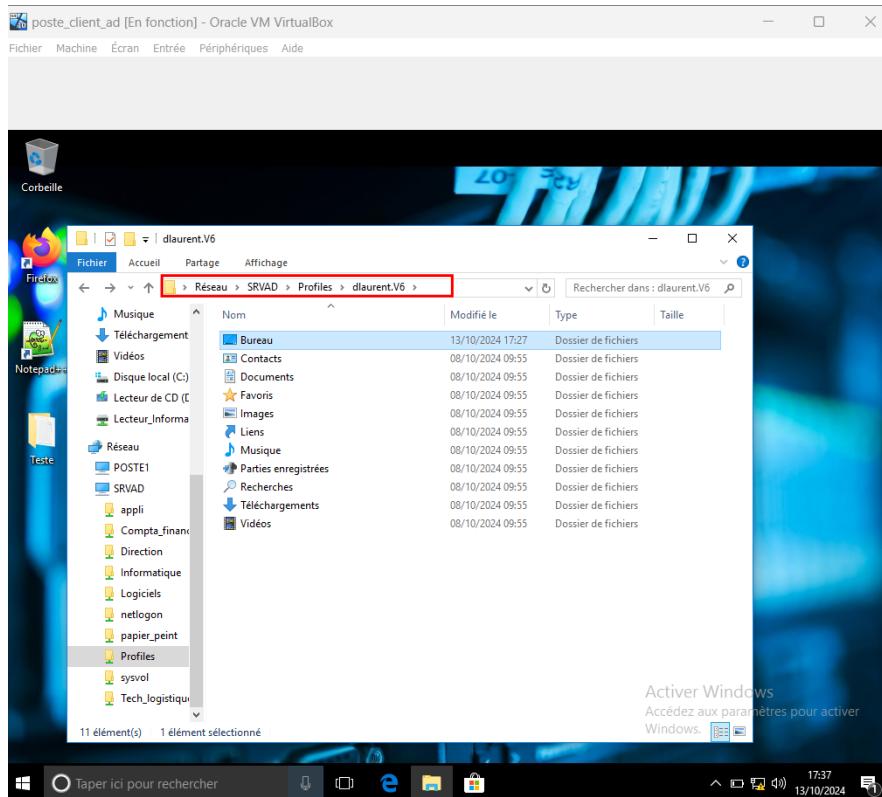
ETAPE N°8 : RÉALISATION DE PROFILS ITINÉRANTS :

- **Création d'un dossier partagé sur le serveur** pour stocker les profils itinérants des utilisateurs avec pour emplacement << C:\Profiles >> sur le serveur.
- Faîtes un clic sur le dossier → Propriétés → Partage → Partage avancé → Partager ce dossier → Autorisations
- Maintenant Supprimer Tout le monde → Ajouter les utilisateurs **David Laurent et Etienne Duvent** avec les permissions Lecture et Modifier → Appliquer → OK
- Maintenant dans Sécurité → Ajouter les utilisateurs **David Laurent et Etienne Duvent** avec les permissions de Contrôle total
- **Configuration des chemins des profils itinérants** dans Active Directory pour cela on va dans Utilisateurs et Ordinateurs Active Directory → UO Informatique → clic droit sur un utilisateur concerné (d'abord par exemple : **David Laurent**) → Propriétés → Profil → dans le champ **Chemin du profil**, saisis le chemin ici pour David Laurent : << \srvad\Profiles\%username% >>
- **Création stratégies pour limiter la taille à 5go pour les profils itinérants :**
- J'ai ouvert le Gestionnaire de serveur → Outils → Gestion des stratégies de groupe.
- Ensuite, j'ai navigué dans Forêt (ville-abymes.fr) → Domaines (ville-abymes.fr) → UO Informatique
- J'ai fait un **clic droit** sur l'UO Informatique fr, puis j'ai sélectionné **Créer un objet de stratégie de groupe dans ce domaine et le lier ici**.
- J'ai nommé cette stratégie **Limite_taille_5go** → puis **clic droit** → **Modifier**
- Allez dans Configuration utilisateur → Stratégies → Modèles d'administration → Système → Profils utilisateur → Activé le paramètre **Limiter la taille du profil** → dans Taille maximale du profil (ko) mettez 5 000 000 ko → **Appliquer** → **OK**
-

Teste de vérification de l'itinérance des profils pour David Laurent et Etienne Duvent :

Méthode : Il faut se connecter sur le poste client aux comptes ici de David Laurent (dlaurent) et Etienne Duvent (eduven) puis se déconnecter. Ensuite se connecter sur le serveur en tant qu'admin du domaine aller dans le dossier partagé profiles et voir qu'il y a des dossiers qui se sont créer pour chacun des profils itinérants.

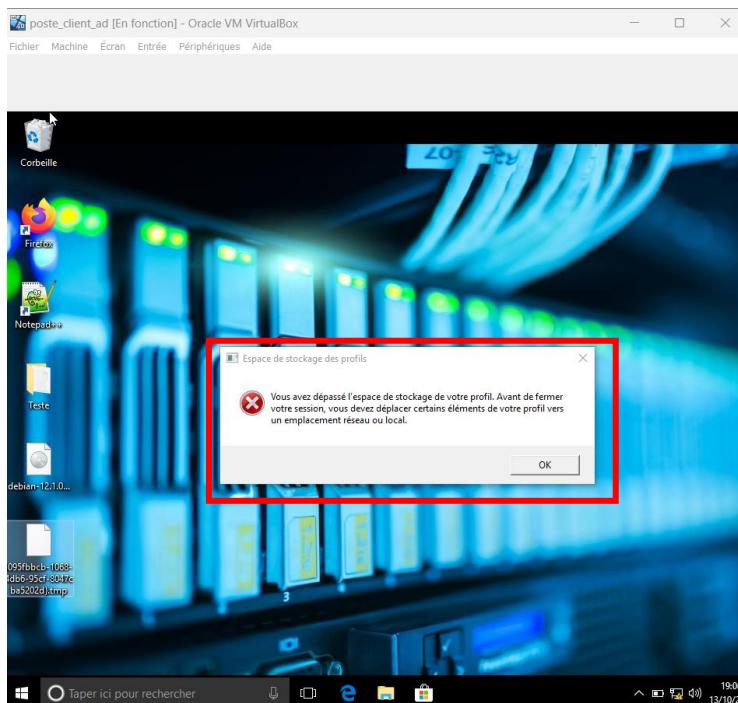




Une fois dans le dossier qui s'est créé automatiquement pour le profile itinérant on retrouve bien tous les éléments appartenant à un utilisateur « normal » comme on peut le voir dont le Bureau etc.

Teste de la limite de 5Go des profils itinérants :

Méthode : J'ai monté sur VirtuelBox un clé usb accessible par la machine virtuelle cliente avec un iso debian de 4Go que j'ai essayé de copier 2 fois sur le bureau. La première fois la copie a réussi et la deuxième fois comme on dépasse les 5go. Un message d'erreur apparaît disant que l'on a atteint la limite de stockage du profil.



CONCLUSION :

Cette expérience pratique sur la configuration d'Active Directory a été une plongée enrichissante dans la gestion des environnements Windows Server. La mise en place d'un domaine, la création et la gestion d'objets, d'unités d'organisation, et de groupes ont permis de comprendre les fondements essentiels de l'administration de serveurs. Ces compétences, que nous avons développées en déployant diverses fonctionnalités, constituent la base de toute infrastructure réseau moderne. Elles ne changent que très peu au fil du temps, ce qui fait de cette expérience un acquis durable pour les futures missions professionnelles. La satisfaction d'avoir manipulé avec succès l'Active Directory, tout en assurant une gestion cohérente des utilisateurs et des ressources, confirme l'importance de cette maîtrise pour un administrateur système en devenir.

FIN DU TP :

