Naimi Abdelaadim

Lahdi Bilel

BTS SIO 1

Document de validation de compétences

AP1 - NetworkSI

1. Présentation du contexte d'entreprise

Besoins de l'entreprise :

La **Maison des Ligues** est en pleine expansion et doit faire face à une augmentation constante du nombre de collaborateurs et de postes de travail. Afin d'accompagner cette croissance et d'optimiser la gestion de son infrastructure informatique, elle a fait appel à **NetworkSI**, une société de services en ingénierie informatique (SSII).

En tant qu'employé de **NetworkSI**, notre mission consiste à proposer et déployer une solution réseau efficace pour simplifier l'administration du parc informatique et assurer une gestion centralisée des utilisateurs et des ressources.

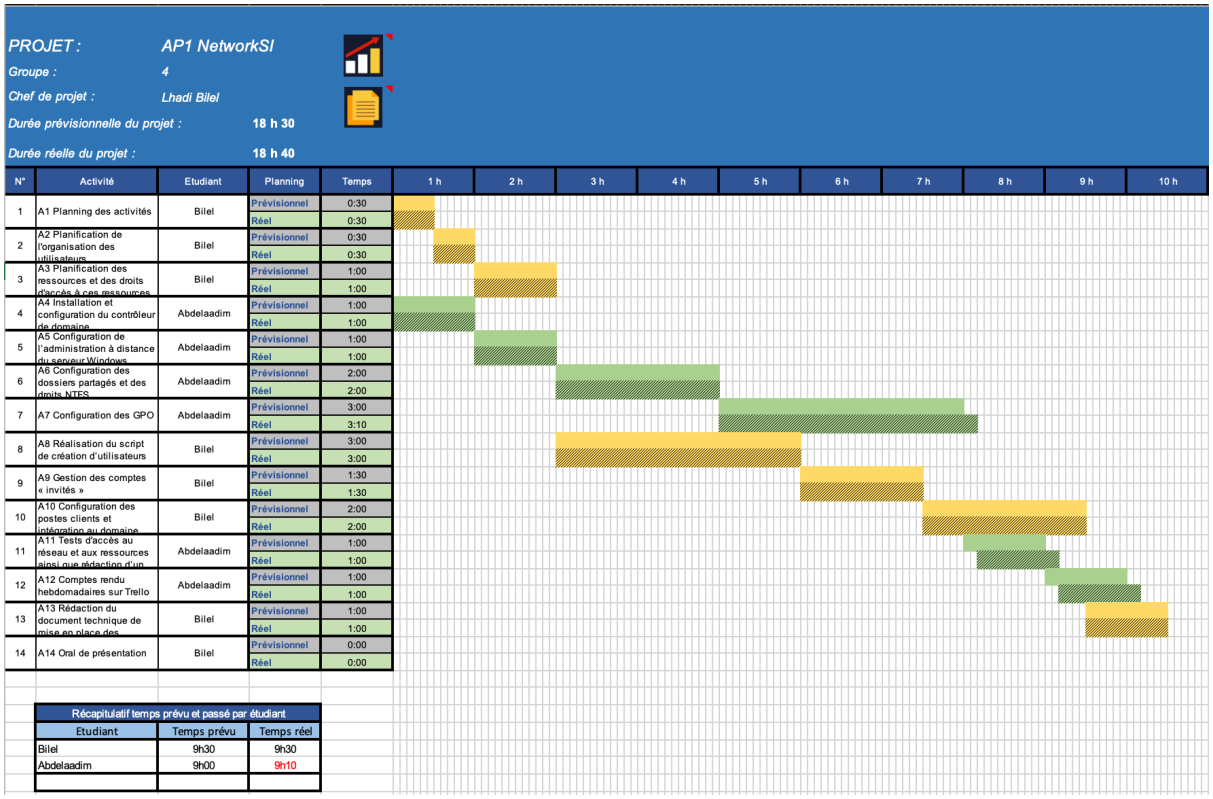
Les contraintes techniques :

- Le serveur sera un contrôleur de domaine Windows Server 2022
- Les administrateurs du domaine devront pouvoir administrer le serveur AD DS + DNS à distance
- Les OS clients seront de 2 au minimum avec systèmes Windows différents W11 et W10
- La règle de nommage des comptes sera la suivante : 7 premières lettres du nom + 1 ère lettre du prénom
- Les utilisateurs et les ressources seront organisés de manière structurée dans un domaine nommé MDL.LOCAL
- Les utilisateurs auront accès à un répertoire personnel « P:/ Dossier personnel » ou ils disposeront de tous les droits et personne d'autre ne devra y accéder à part les admins du domaine, et à un répertoire « Q:/ Outils service » ou ils n'auront que le droit de lecture en fonction du service dans lequel ils travaillent. Ces lecteurs devront se monter à la connexion de l'utilisateur de manière automatisée dans « Ce PC ».
- Les droits d'accès à ces répertoires seront configurés de manière à ce que la confidentialité soit respectée.
- Les profils des utilisateurs seront configurés de manière à ce que les utilisateurs retrouvent le même environnement de travail, quel que soit le poste sur lequel ils se connectent. Ils ne pourront pas ajouter/supprimer des programmes et ne pourrons pas changer le fond d'écran qui sera imposé
- Les utilisateurs temporaires (invités, stagiaires, visiteurs...) auront accès à un environnement standard non modifiable restreint, et n'auront accès à aucune ressource réseau. Ils pourront uniquement naviguer sur internet et utiliser les outils bureautiques sans accéder aux paramètres des PC.
- Le navigateur Mozilla Firefox et le lecteur multimédia VLC seront déployés de manière automatisée sur les postes clients
- Mettre en place un système de création d'utilisateurs avec un script pour simplifier la gestion quotidienne

2. Objectifs attendus

- Installation et configuration du contrôleur de domaine
- Configuration de l'administration à distance du serveur Windows
- Configuration des dossiers partagés et des droits NTFS
- Configuration des stratégies de groupe (GPO)
- Réalisation du script de création d'utilisateurs
- Gestion des comptes « invités »
- Configuration des postes clients et intégration au domaine

3. Plan de travail



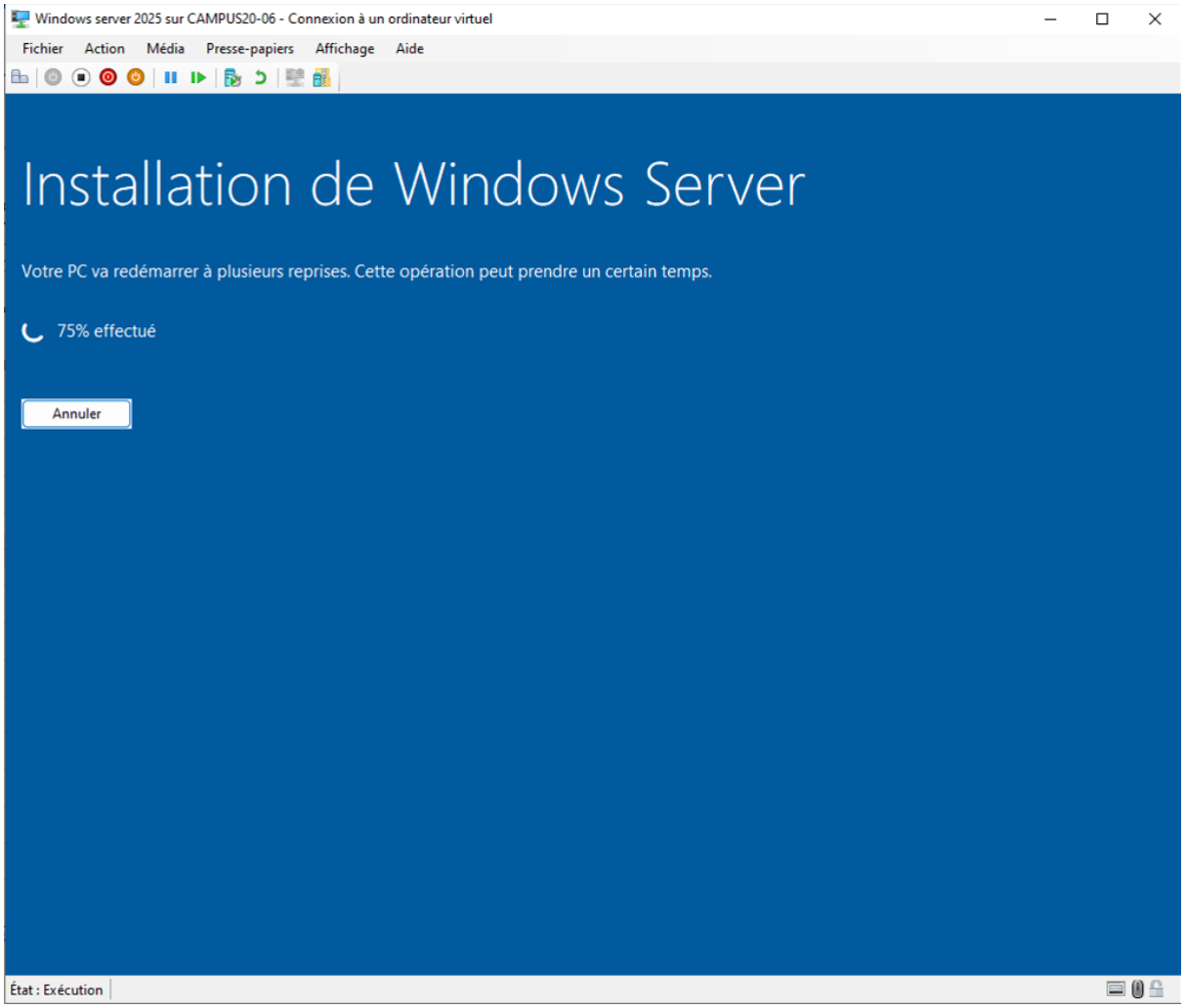
PROJET : *AP1 NetworkSI*
Groupe : *4*
Chef de projet : *Lhadi Bilel*
Durée prévisionnelle du projet : **18 h 30**
Durée réelle du projet : **18 h 40**

N°	Activité	Etudiant	Planning	Temps
1	A1 Planning des activités	Bilel	Prévisionnel	0:30
			Réel	0:30
2	A2 Planification de l'organisation des utilisateurs	Bilel	Prévisionnel	0:30
			Réel	0:30
3	A3 Planification des ressources et des droits d'accès à ces ressources	Bilel	Prévisionnel	1:00
			Réel	1:00
4	A4 Installation et configuration du contrôleur de domaine	Abdelaadim	Prévisionnel	1:00
			Réel	1:00
5	A5 Configuration de l'administration à distance du serveur Windows	Abdelaadim	Prévisionnel	1:00
			Réel	1:00
6	A6 Configuration des dossiers partagés et des droits NTFS	Abdelaadim	Prévisionnel	2:00
			Réel	2:00
7	A7 Configuration des GPO	Abdelaadim	Prévisionnel	3:00
			Réel	3:10
8	A8 Réalisation du script de création d'utilisateurs	Bilel	Prévisionnel	3:00
			Réel	3:00
9	A9 Gestion des comptes « invités »	Bilel	Prévisionnel	1:30
			Réel	1:30
10	A10 Configuration des postes clients et intégration au domaine	Bilel	Prévisionnel	2:00
			Réel	2:00
11	A11 Tests d'accès au réseau et aux ressources ainsi que rédaction d'un	Abdelaadim	Prévisionnel	1:00
			Réel	1:00
12	A12 Comptes rendu hebdomadaires sur Trello	Abdelaadim	Prévisionnel	1:00
			Réel	1:00
13	A13 Rédaction du document technique de mise en place des	Bilel	Prévisionnel	1:00
			Réel	1:00
14	A14 Oral de présentation	Bilel	Prévisionnel	0:00
			Réel	0:00

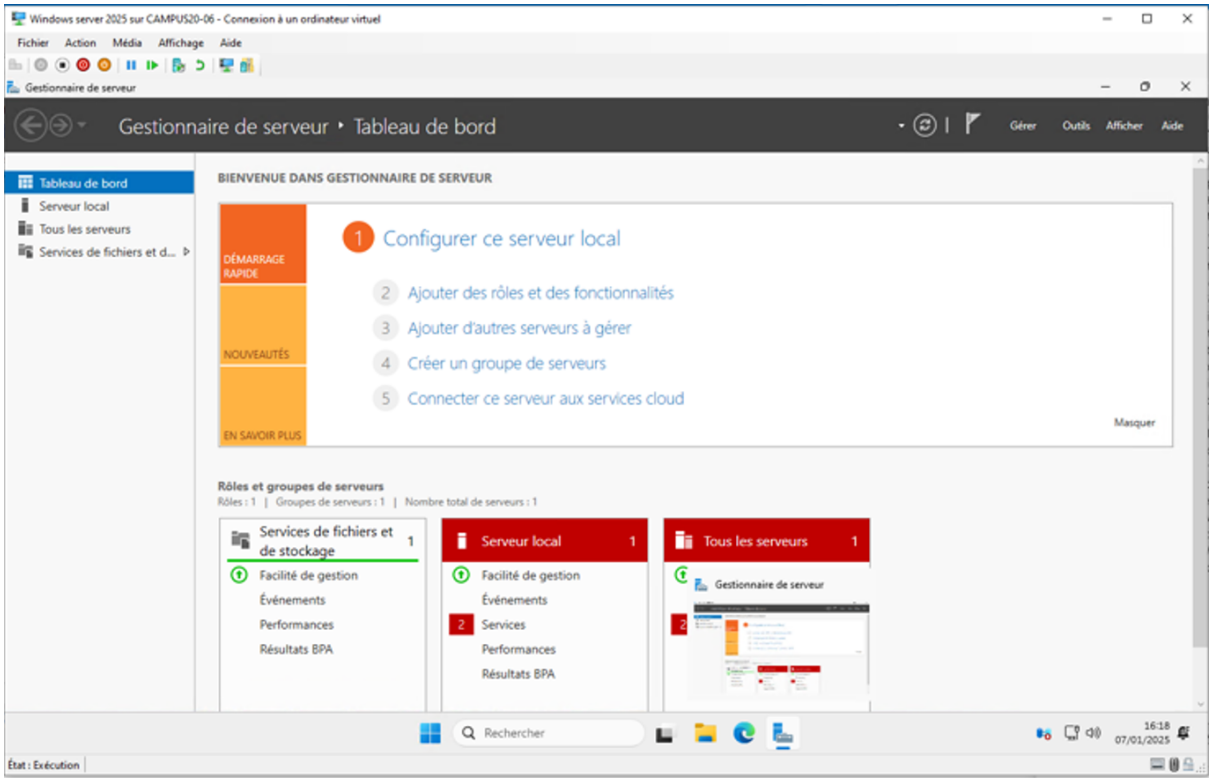
Récapitulatif temps prévu et passé par étudiant		
Etudiant	Temps prévu	Temps réel
Bilel	9h30	9h30
Abdelaadim	9h00	9h10

4. Réalisation

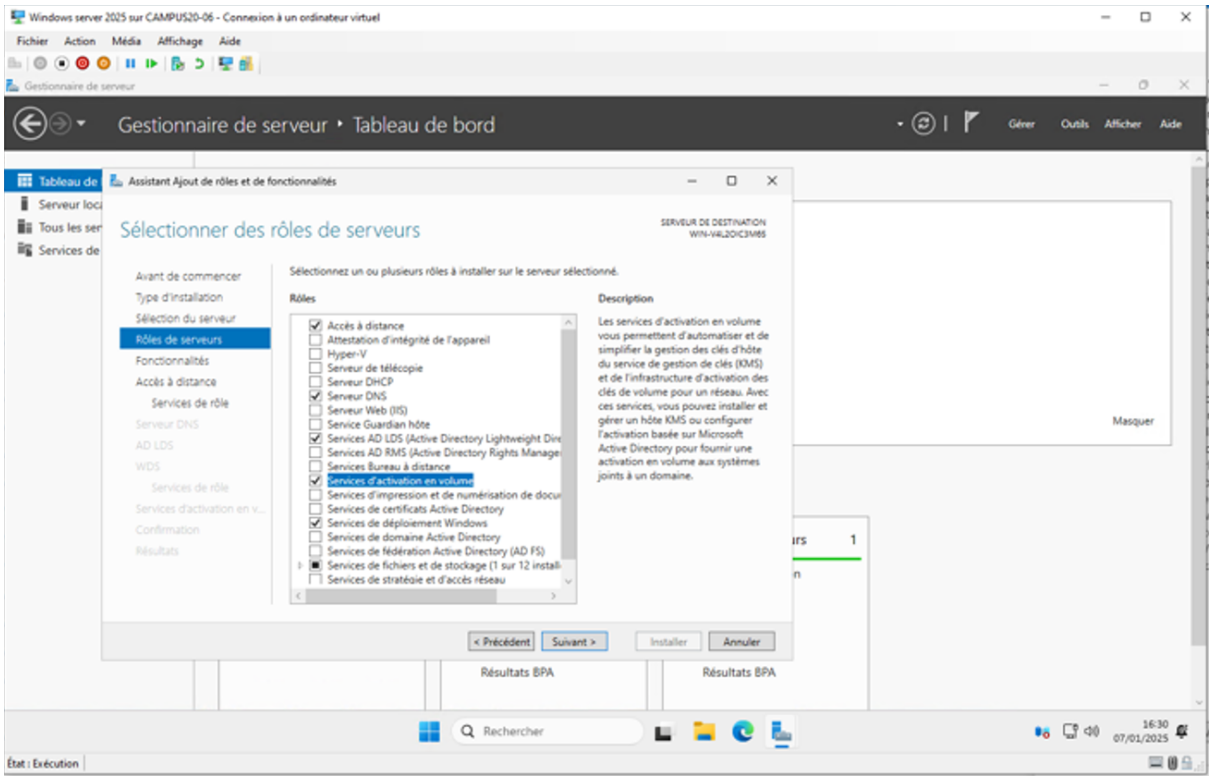
Installation et configuration du contrôleur de domaine :



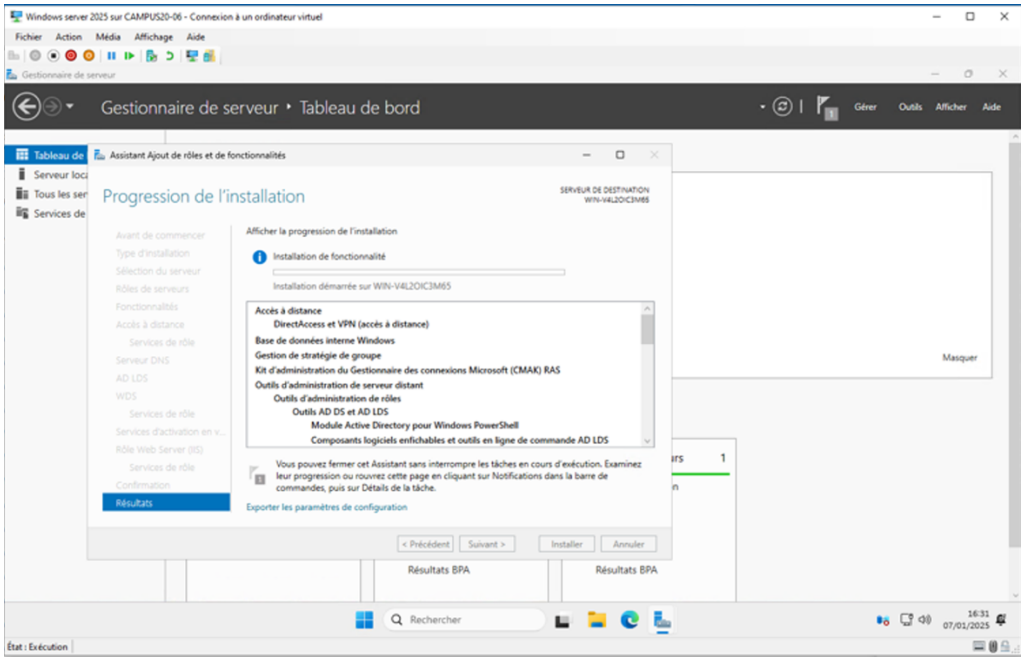
Nous avons installé **Windows Server 2022** sur une machine virtuelle sous **Hyper-V** afin de déployer une infrastructure réseau centralisée, optimisant ainsi la gestion des utilisateurs, des ressources et des services réseau.



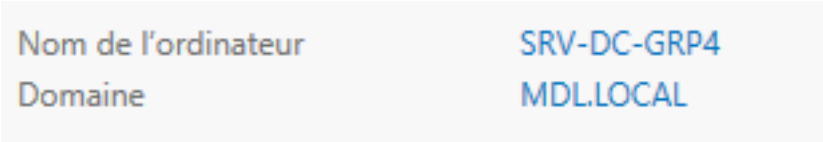
Voici l'environnement de base au premier lancement. À partir de là, nous devons ajouter les rôles qui nous serviront, changer l'adresse IP et enfin changer le nom du serveur en vue de **l'intégrer au domaine et configurer les services nécessaires à la gestion du réseau**.



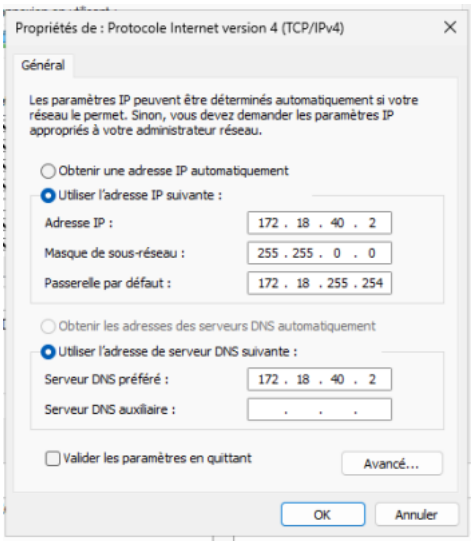
Nous ajoutons notamment les rôles Active Directory Domain Services (AD DS) pour la gestion des utilisateurs et des ressources, DNS pour la résolution des noms de domaine, ainsi que Bureau à distance pour l'administration à distance du serveur.



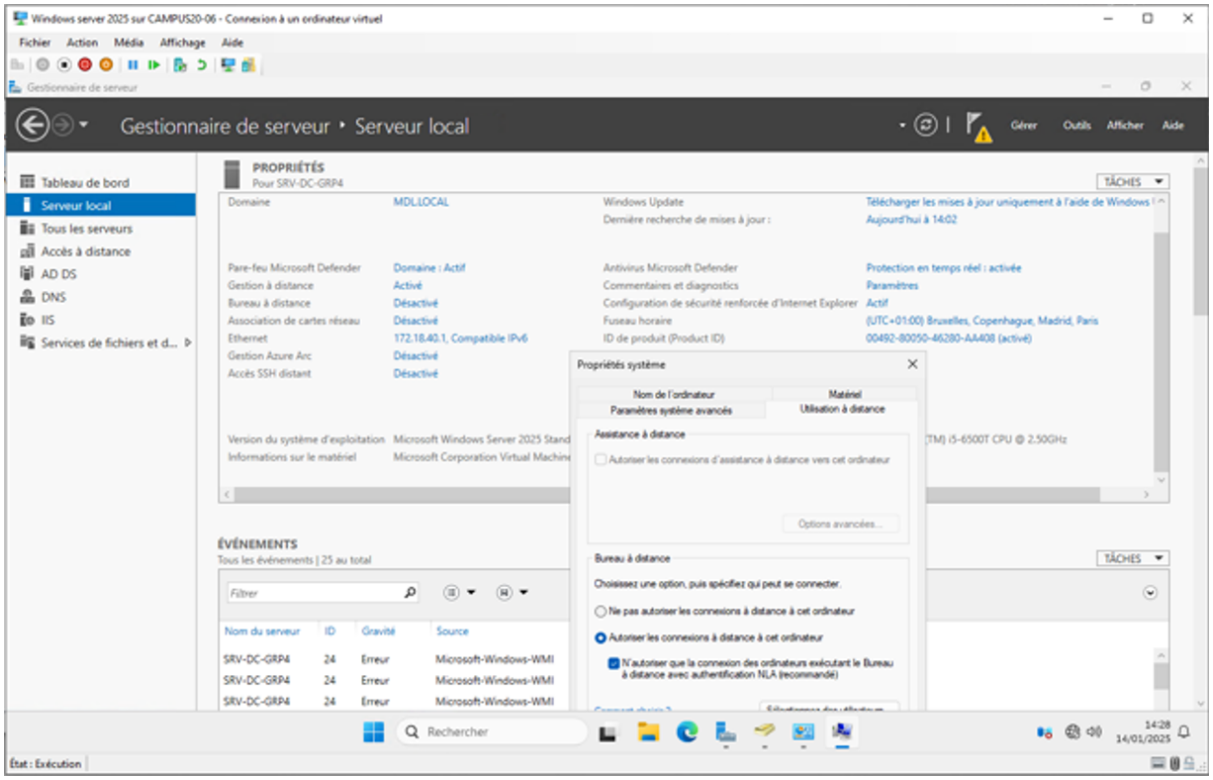
On vérifie que l'on a bien tous les rôles qui nous serviront par la suite



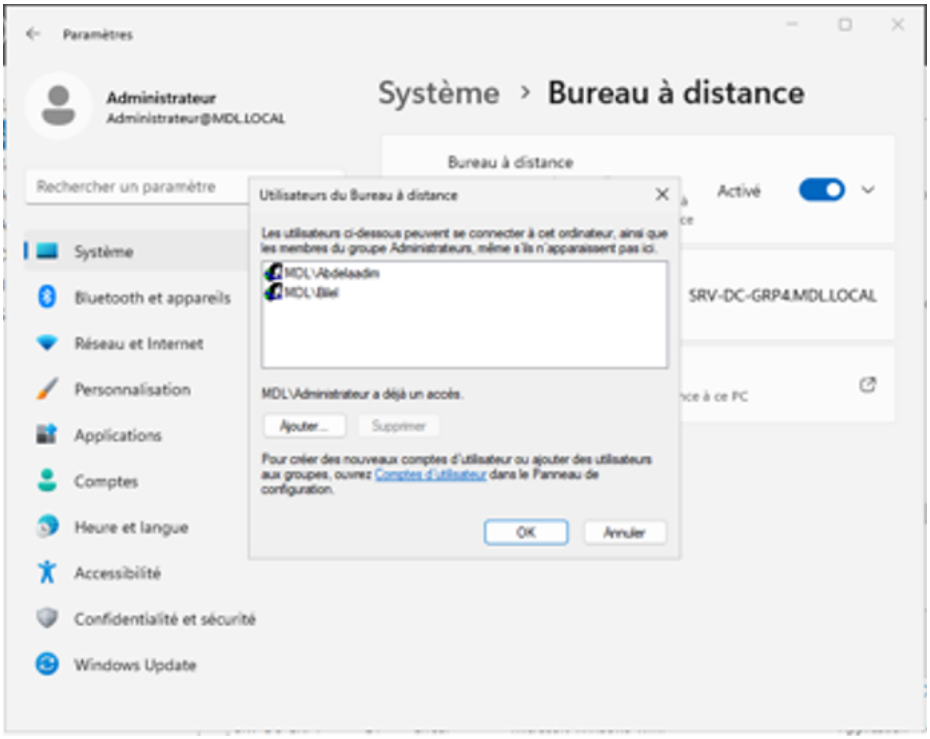
On renomme le serveur SRV-DC-GRP4 et on vérifie qu'il est bien dans le domaine souhaité



Configuration de l’administration à distance du serveur Windows :

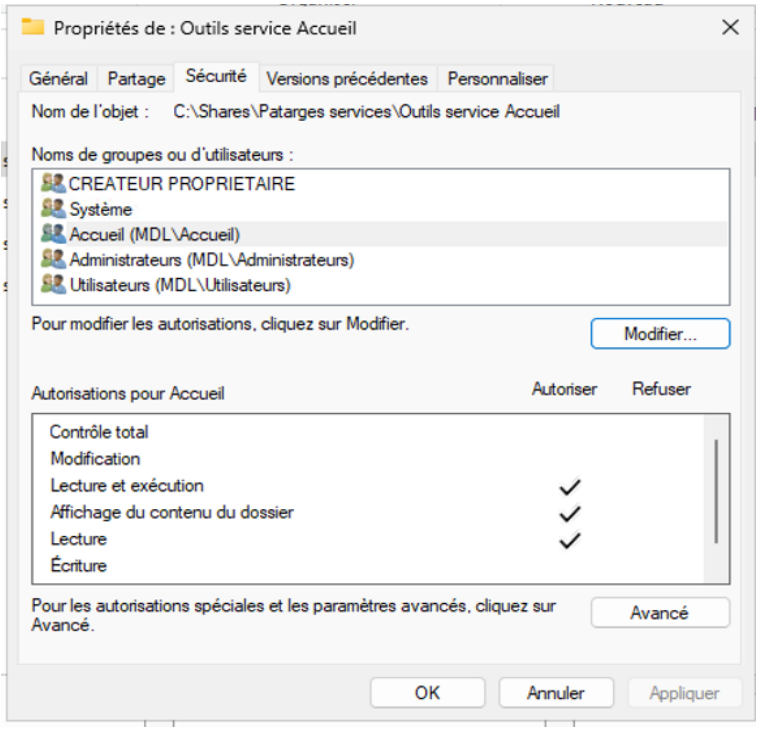


Nous activons ensuite l’option **Bureau à distance** afin de permettre une administration plus flexible du serveur. Cette fonctionnalité nous permet de travailler simultanément sur la même machine, sans avoir besoin d’un accès physique direct. Grâce à **Remote Desktop Protocol (RDP)**, nous pouvons nous connecter à distance, effectuer des configurations, gérer les rôles et assurer la maintenance du serveur de manière plus efficace.



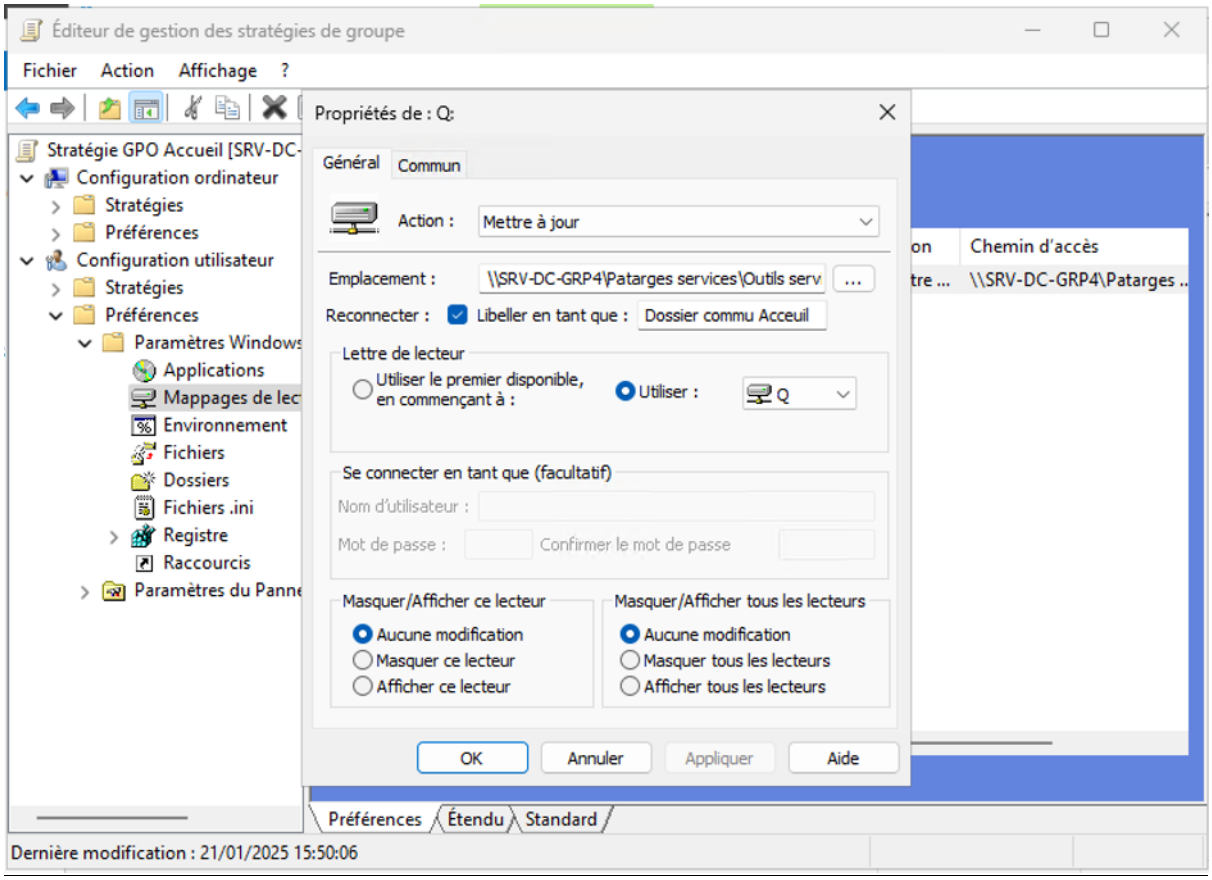
Nous créons ensuite un compte utilisateur pour chaque membre de l'équipe, afin de permettre une connexion individuelle via **Bureau à distance**. Chaque compte est configuré avec les droits nécessaires pour accéder aux ressources et effectuer les tâches d'administration en toute sécurité.

Configuration des dossiers partagés et des droits NTFS :

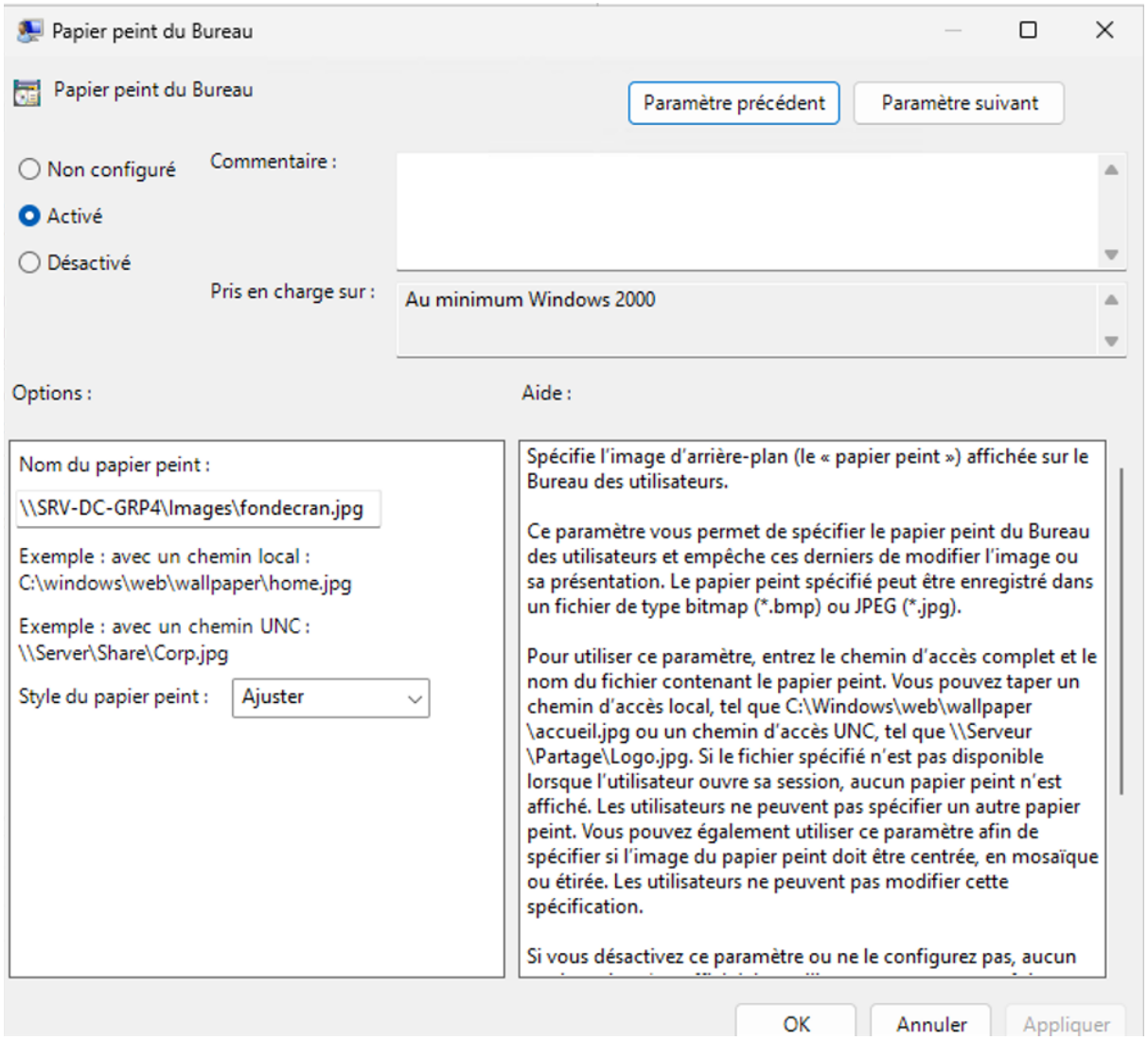


Nous attribuons à chaque département un **dossier partagé** spécifique, en appliquant des droits d'accès restreints afin de garantir la sécurité et la confidentialité des données. Ces restrictions sont définies à l'aide des **permissions NTFS** et des **partages réseau**, permettant ainsi aux utilisateurs d'accéder uniquement aux fichiers et dossiers correspondant à leur service. Cette configuration assure une gestion efficace des ressources tout en limitant les accès non autorisés.

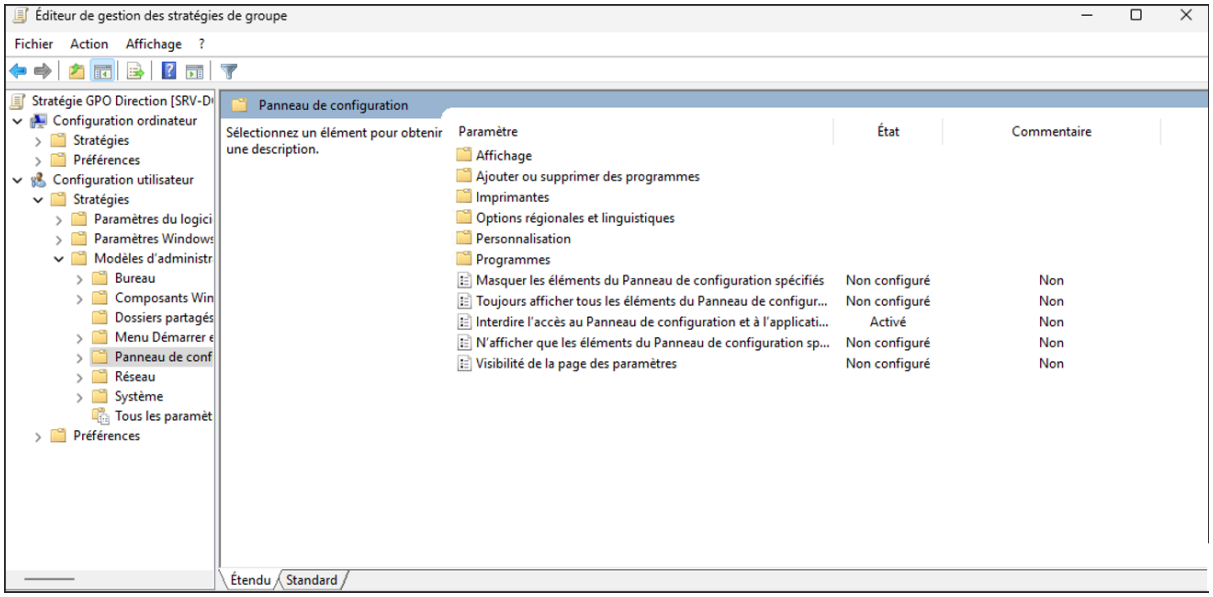
Configuration des GPO :



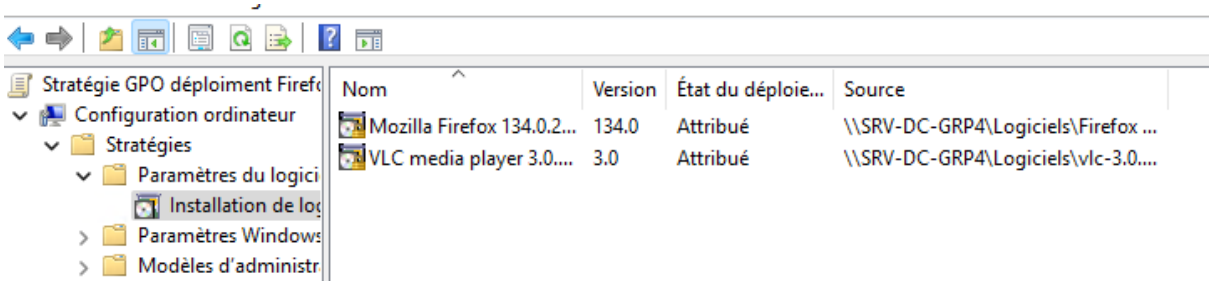
Nous procédons ensuite au mappage **des lecteurs** pour permettre aux membres de chaque département d'accéder facilement à leur dossier commun créé en amont. Cela se fait à l'aide d'une **stratégie de groupe (GPO)**, qui permet de lier automatiquement les lecteurs réseau aux postes de travail des utilisateurs en fonction de leur département. Cette méthode garantit que chaque utilisateur ait un accès transparent et sécurisé à son dossier partagé, sans avoir à configurer manuellement les connexions réseau.



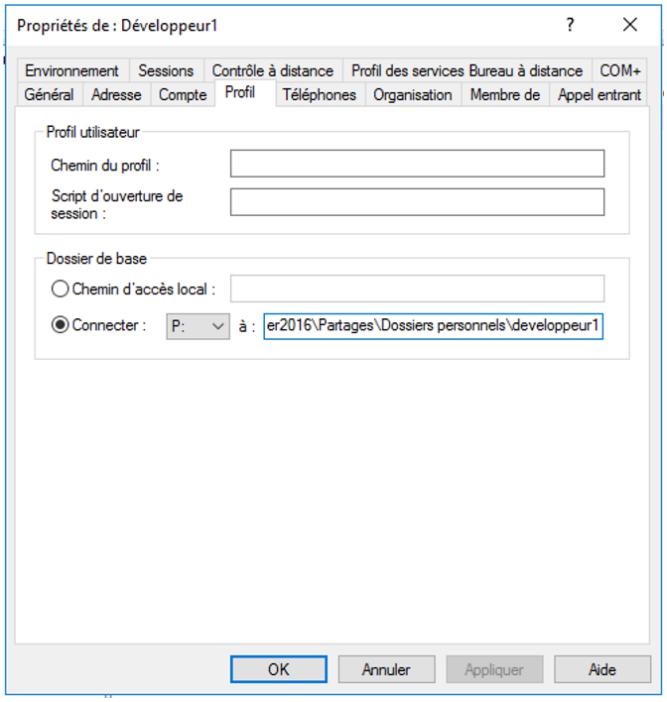
Nous déployons également un **fond d'écran** pour tous les utilisateurs à l'aide d'une autre **GPO**. Cette configuration permet de personnaliser l'environnement de travail de manière uniforme, en appliquant automatiquement un fond d'écran sur tous les postes de travail des utilisateurs, quel que soit leur département.



Nous bloquons l'accès au **Panneau de configuration** pour les utilisateurs non habilités en utilisant une autre **stratégie de groupe (GPO)**. Cette restriction permet de renforcer la sécurité en empêchant les utilisateurs non autorisés de modifier les paramètres système, les configurations réseau, ou d'autres options sensibles. En appliquant cette GPO, nous nous assurons que seuls les administrateurs ou les utilisateurs ayant des privilèges spécifiques puissent accéder à ces fonctionnalités, garantissant ainsi un contrôle plus strict sur l'environnement informatique.



Nous avons déployé les logiciels **VLC** et **Mozilla Firefox** sur tous les postes de l'entreprise en utilisant des fichiers d'installation **.msi** et une **stratégie de groupe (GPO)**. Cette méthode permet d'automatiser l'installation des logiciels sur les machines des utilisateurs, sans intervention manuelle. Grâce à la GPO, les logiciels sont déployés de manière uniforme et centralisée, garantissant ainsi que tous les postes disposent des mêmes versions des applications, tout en simplifiant leur gestion et mise à jour à l'échelle de l'entreprise.

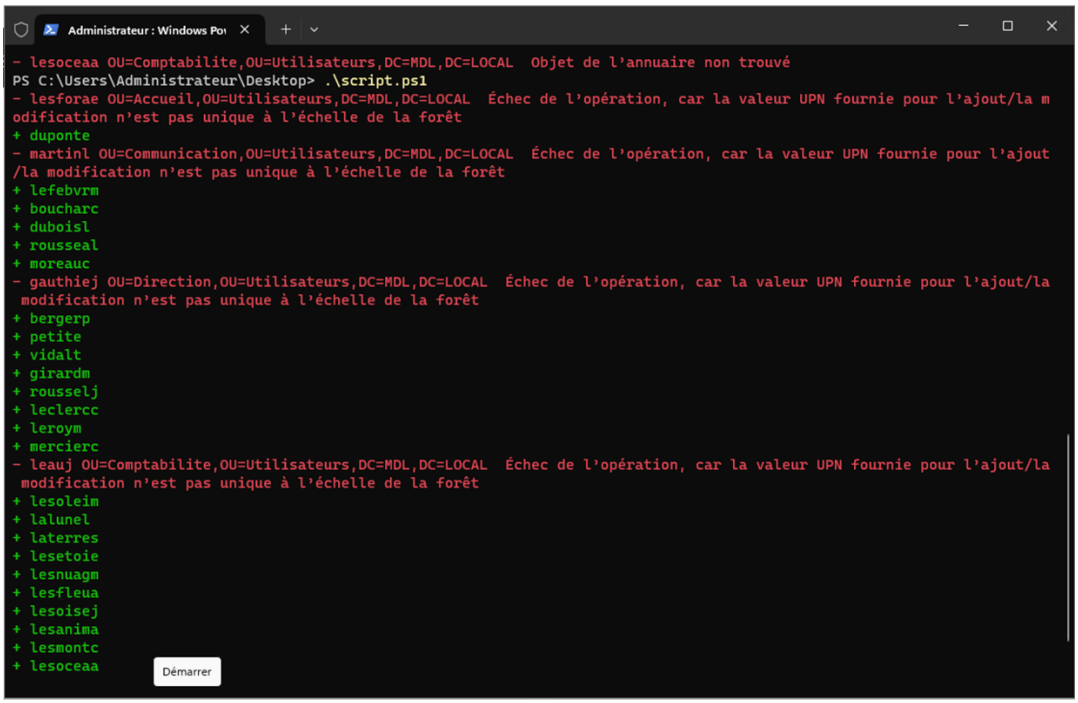


Pour le **mappage du disque personnel** sur le réseau, nous utilisons l'onglet **Profil** lors de la création de l'utilisateur dans **Active Directory**. Dans cet onglet, nous spécifions le chemin du **dossier personnel** de l'utilisateur, qui sera automatiquement mappé lors de la connexion. Cela permet à chaque utilisateur d'avoir un espace de stockage personnel accessible depuis n'importe quel poste connecté au domaine. Ce mappage facilite l'accès aux fichiers de l'utilisateur et garantit que ses données sont stockées de manière centralisée et sécurisée sur le réseau.

Réalisation du script de création d'utilisateurs :

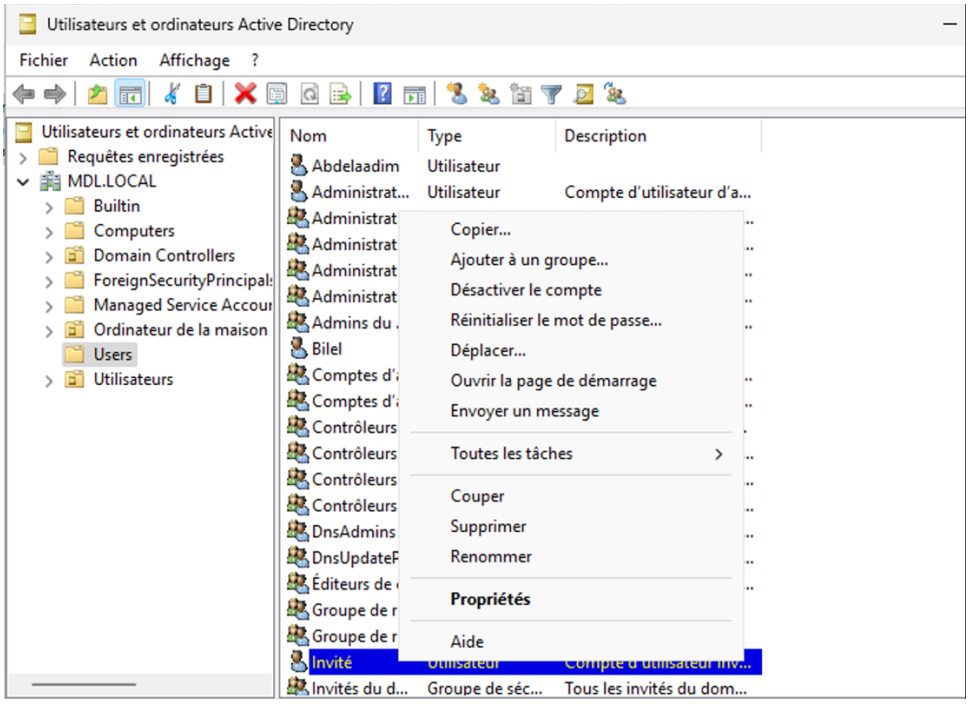
```powershell
$users = Import-Csv -Path "AdUsers.csv" -Delimiter ";"

foreach ($user in $users) {

    $user_params = @{
        SamAccountName = $user.username
        UserPrincipalName = "$($user.username)@MDL.LOCAL"
        Name = "$($user.firstname) $($user.lastname)"
        GivenName = $user.firstname
        Surname = $user.lastname
        DisplayName = "$($user.firstname) $($user.lastname)"
        EmailAddress = $user.email
        Path = $user.ou
        AccountPassword = (ConvertTo-SecureString $user.password -AsPlainText -Force)
        Enabled = $true
    }

    try {
        New-ADUser @user_params
        Write-Host "+ $($user.username)" -ForegroundColor Green
    } catch {
        Write-Host "- $($user.username) $($user.ou)  $_" -ForegroundColor Red
    }
}
```

Nous avons écrit un **script PowerShell** permettant d'automatiser la création des comptes utilisateurs. Ce script simplifie et accélère le processus d'ajout de nouveaux utilisateurs dans **Active Directory** en définissant les paramètres essentiels tels que le nom, le mot de passe, le département et les groupes d'appartenance. Grâce à cette automatisation, nous minimisons les erreurs humaines et rapide des comptes utilisateurs



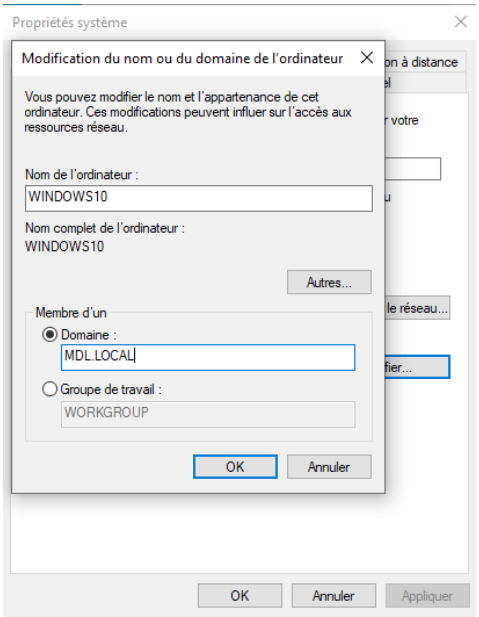
On peut voir ici la bonne exécution du script

Gestion des comptes « invités » :

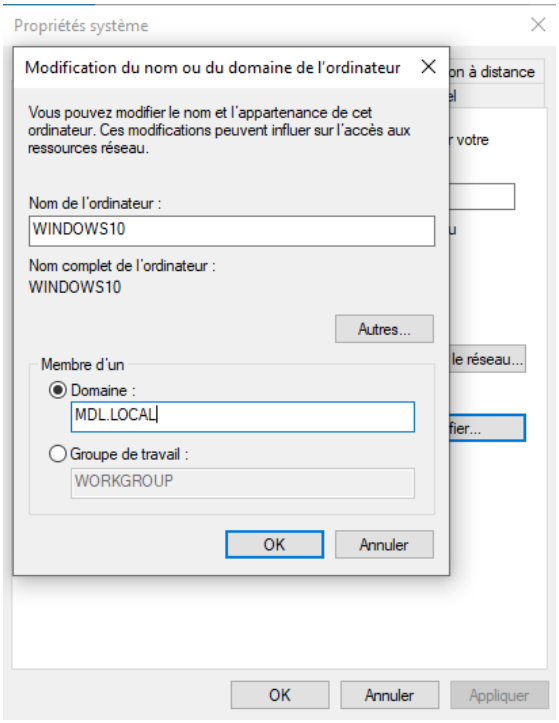


Nous activons le **compte invité** dans le but de permettre à des personnes extérieures d'accéder temporairement à la machine, tout en limitant leurs privilèges. Ce compte est configuré avec des droits d'accès très restreints afin que les utilisateurs externes puissent uniquement effectuer les actions nécessaires, sans compromettre la sécurité du réseau ou des données internes. L'activation de ce compte permet une gestion efficace des accès temporaires, tout en maintenant un contrôle strict sur les ressources de l'entreprise.

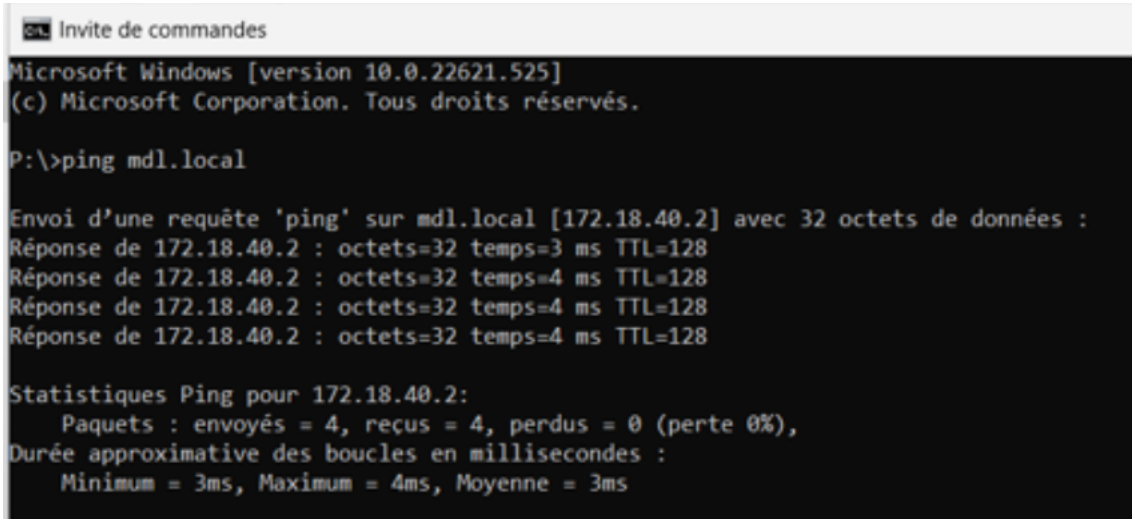
<u>Configuration des postes clients et intégration au domaine :</u>



Une fois sur un PC de l'entreprise, nous devons lui attribuer une **adresse IP** dans le même réseau que celui du serveur afin de permettre son **intégration au domaine**. Cela garantit que le poste de travail pourra communiquer correctement avec le serveur, notamment pour l'authentification des utilisateurs et l'accès aux ressources partagées. Une fois l'adresse IP configurée, le PC pourra rejoindre le domaine en utilisant le nom du contrôleur de domaine, ce qui permettra à l'utilisateur de se connecter avec son compte Active Directory et d'accéder aux ressources du réseau de manière sécurisée.

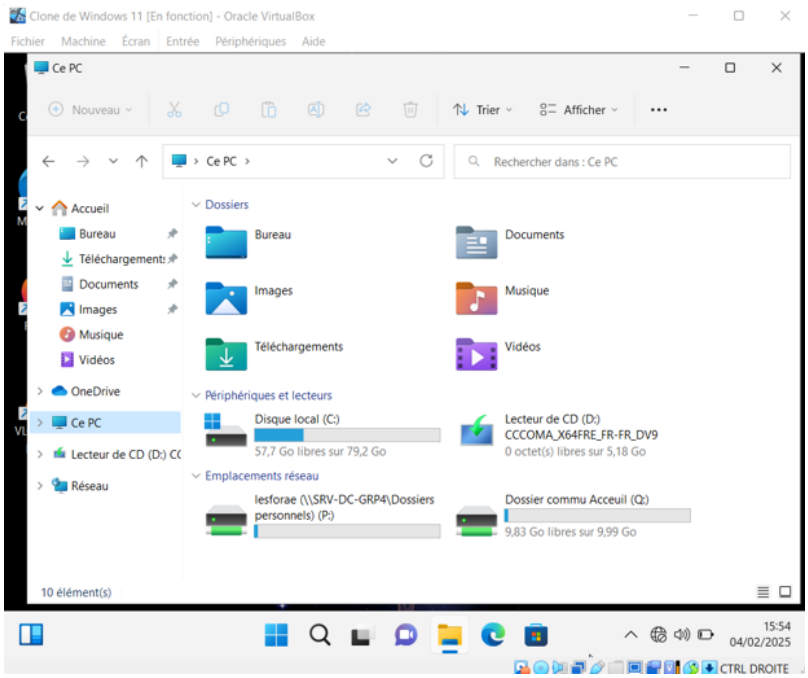


Tests d'accès au réseau et aux ressources :



Nous effectuons un **ping** du serveur depuis un ordinateur afin de valider la **communication réseau** entre les deux machines. Cette étape permet de vérifier que l'ordinateur est bien connecté au réseau et qu'il peut communiquer avec le serveur, ce

qui est essentiel pour l'intégration au domaine. Si le ping répond correctement, cela confirme que le PC peut atteindre le serveur.



Nous vérifions ensuite sur un **compte utilisateur** si l'accès aux différentes **ressources** est bien fonctionnel, en fonction du département de l'utilisateur. Cette étape permet de confirmer que les **droits d'accès** sont correctement appliqués, et que l'utilisateur peut accéder uniquement aux ressources auxquelles il est autorisé, comme les dossiers partagés, les applications ou les imprimantes. Cela garantit que la gestion des permissions fonctionne comme prévu, en offrant un accès sécurisé et ciblé aux ressources du réseau.