Document de validation de compétences

AP1 - SISR

Installer et configurer un réseau centralisé autour d'un contrôleur de domaine

Dates du projet :
Début le 09/01/2026
Fin le 30/01/2026

Equipe 4
Bardet Arthur
Vallée Estéban

Sommaire

Présentation du contexte de l'entreprise

Nous sommes les employés fictifs de l'entreprise *NetworkSI* qui a pour vocation d'aider les entreprises à réaliser ou améliorer leur parc informatique.
L'entreprise de la maison des ligues fait appel à notre expertise en tant qu'employés de *NetworkSI* afin d'améliorer leur parc existant, qui était jusque là un parc en "poste par poste", car celui-ci s'agrandit par le recrutements de plus en plus importants et le nombre de postes croissant. Il nous faut donc mettre en place une solution réseau optimisée pour répondre aux demandes de notre client.

La maison des ligues dispose de plusieurs services qu'il faudra donc administrer, ces services comprennent diverses postes et peuvent être représentés comme-ci :

- L'accueil (3 postes)
- La comptabilité (20 postes)
- La communication (20 postes)
- La direction (7 postes)

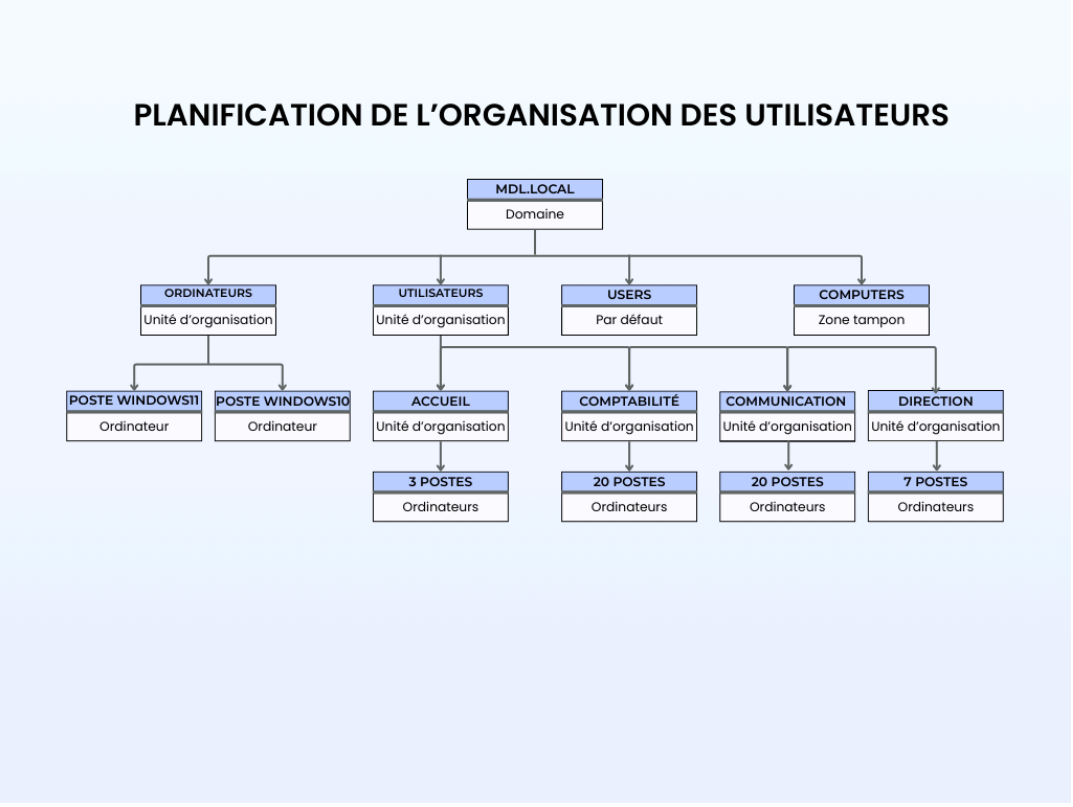


Schéma de la planification de l'organisation des utilisateurs

L’ensemble de ces services, compartimentés en groupe, doivent avoir différents droits d’accès à des ressources à la fois personnelles mais aussi collectives. Cette planification devrait donner un ensemble ressemblant à celui de nos tableaux ci-dessous :

Tableau des différents lecteurs mappés et des ressources NTFS/partageés

Ressources	**Emplacement**	**Utilisation**	**Lecteur**
Dossiers personnels	Serveur de fichiers	Stockage privé par utilisateur, sauf pour les comptes invités	Q
Dossiers de service	Serveur de fichiers	Stockage partagé par groupe avec accès aux outils par service	Z

Tableau des groupes par service de l’Active Directory

Services	**Groupes de l’Active Directory associés**	**Nombre de postes**
Accueil	accueil	3 postes
Comptabilité	comptabilite	20 postes
Communication	communication	20 postes
Direction	direction	7 postes

Droits d’accès aux dossiers partagés et privés

Groupes	**Dossiers**	**Droits**	**Lecteurs**
Accueil	- Personnel - Outils Accueil	- Contrôle total - Lecture/Ecriture	- Q - Z
Comptabilité	- Personnel - Outils Comptabilité	- Contrôle total - Lecture/Ecriture	- Q - Z
Communication	- Personnel - Outils Communication	- Contrôle total - Lecture/Ecriture	- Q - Z
Direction	- Personnel - Outils Direction	- Contrôle total - Lecture/Ecriture	- Q - Z
Administrateur (2 postes)	- L’ensemble des dossiers du domaine	- Contrôle total	
Invité	- Aucun		

Les conditions de la réalisation de ce nouvel environnement passent par un contrôleur de domaine Windows Server hébergé par un hyperviseur de type 1 ainsi que deux machines test, dîtes clientes, que nous ajouterons au domaine MDL.LOCAL et qui seront respectivement une machine Windows 10 et une machine Windows 11 en hypervision de type 2 via Oracle VirtualBox.

Il nous faut également mettre en œuvre des profils utilisateurs générés par un script, ceux-ci doivent respecter une règle de nommage précise que nous repréciserons par la suite, rendre l’environnement de travail coordonnées non pas aux postes mais bien aux utilisateurs afin que ceux-ci retrouvent leur données sur n’importe quel poste après identification.

Les postes de la société doivent avoir un déploiement automatisé et généralisé des applications Mozilla Firefox et VLC, et les utilisateurs ne doivent pas disposer du droit d’ajouter ou de supprimer des programmes et de changer le fond d’écran déployé par la maison des ligues sur les postes.

Il nous faut également paramétrer des utilisateurs temporaires, via les comptes invités, qui auront un accès à un environnement standard qui ne peut être modifié, aucun accès aux ressources et seulement la fonctionnalité de surfer sur Internet et utiliser les outils bureautiques à leur disposition. Les postes ne doivent pas sauvegarder leur session qui est réinitialisée à chaque déconnexion.

Le tout en veillant bien évidemment à respecter la confidentialité attendue par l'entreprise ainsi que leur cahier des charges.

Les objectifs attendus

A travers cet Atelier Professionnel, nous allons apprendre à travailler en commun et s'organiser professionnellement afin de concevoir, déployer et documenter une infrastructure réseau tournée autour d'un serveur servant d'Active Directory sous Windows Server 2022, tout en respectant un cahier des charges fictif exigeant.

De manière plus détaillé, nous devrions pouvoir analyser le cahier des charges afin d'identifier les spécificités de la structure que nous mettrons en place. Ces objectifs passent également par une maîtrise générale de l'OS Windows Server afin de configurer un contrôleur de domaine compétent et structuré, par des groupes, des utilisateurs et des unités d'organisation.

La sécurité de cette infrastructure est également prioritaire, avec un respect strict de la confidentialité et des permissions entre groupes, utilisateurs et ressources partagées.

L'administration et le déploiement de services généralisés afin de faciliter la mise en place des postes et des utilisateurs sur le domaine sont également centraux, avec la gestion de GPO, de profils itinérants, de restrictions utilisateurs et de script permettant la création en grand nombre de manière quasiment automatisé de ces mêmes utilisateurs.

Enfin, nos compétences d'organisation avec la rédaction de ce document technique et de rapports de test, couplés avec le travail collaboratif en binôme dans un environnement partagé avec un travail de répartition des tâches et de suivi (Trello) nous permet également de vérifier nos compétences dans un environnement quasi-professionnel.

Veuillez trouver ci-dessous, la liste précise des différents points à réaliser :

A.1 Planning des activités

A.2 Planification de l'organisation des utilisateurs

A.3 Planification des ressources et des droits d'accès à ces ressources

A.4 Installation et configuration du contrôleur de domaine

A.5 Configuration de l'administration à distance du serveur Windows

A.6 Configuration des dossiers partagés et des droits NTFS

A.7 Configuration des GPO

A.8 Réalisation du script de création d'utilisateurs

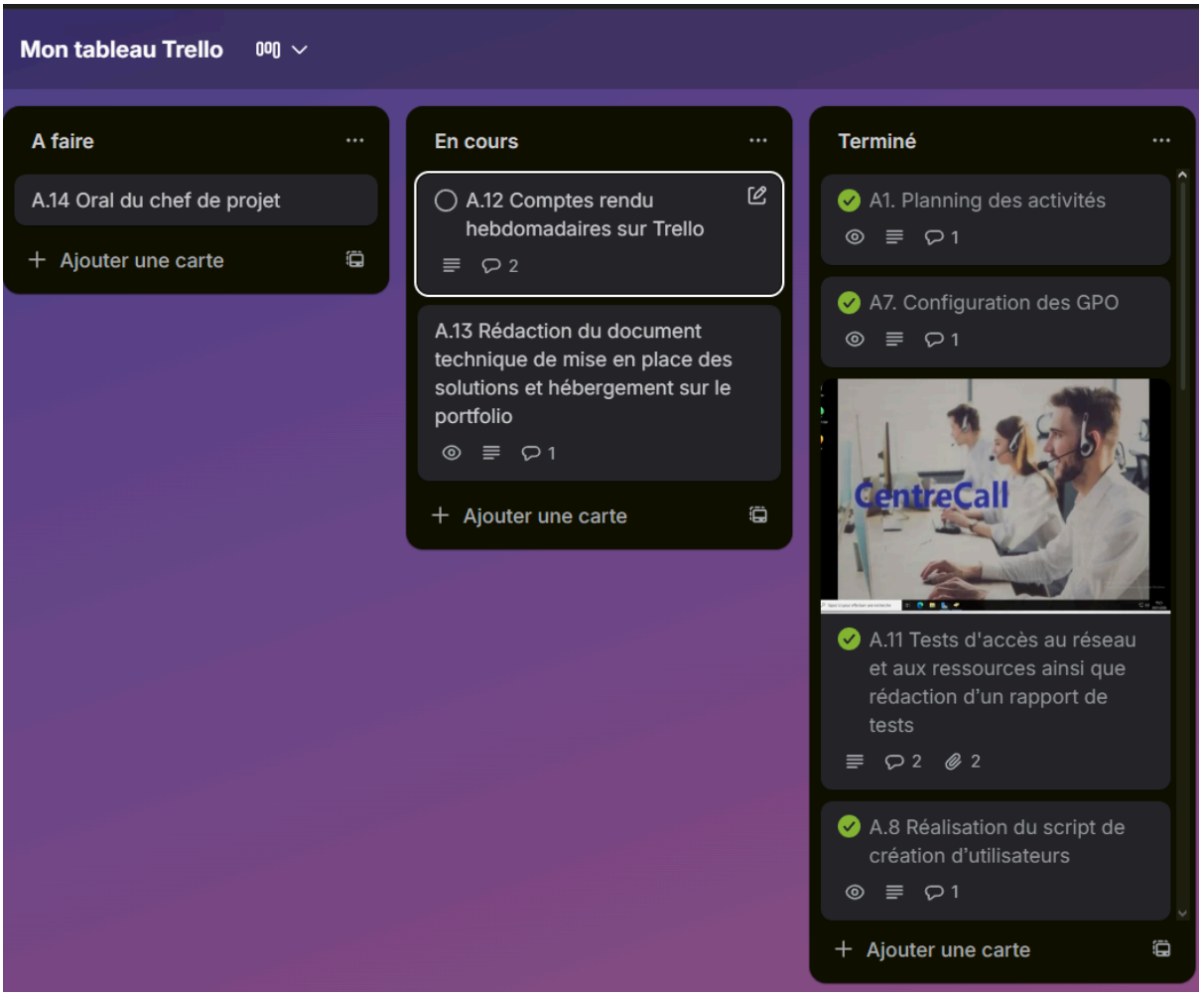
A.9 Gestion des comptes « invités »

A.10 Configuration des postes clients et intégration au domaine

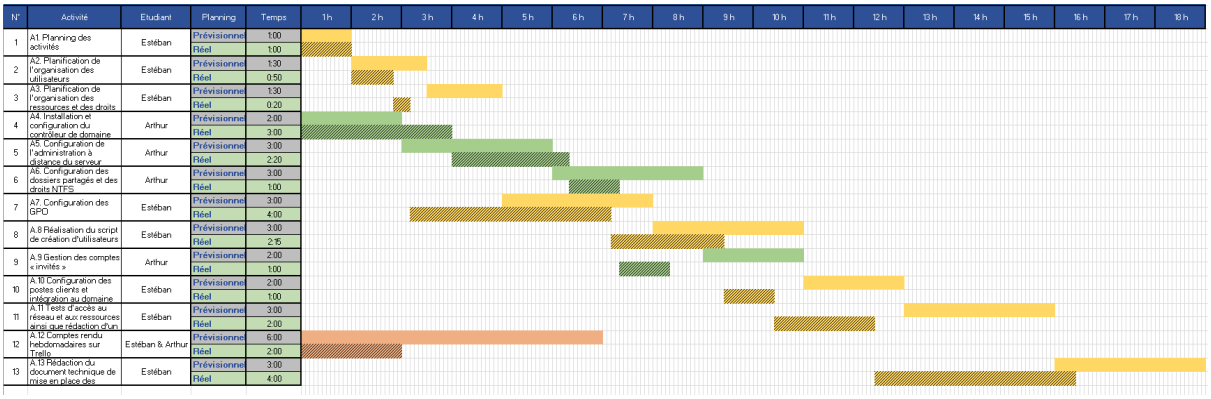
A.11 Tests d'accès au réseau et aux ressources ainsi que rédaction d'un rapport de tests

Plan de travail

Nous avons décidés de nous répartir les tâches de manière équitable, chacun ayant autour de 16 heures de tâches préalablement estimées à réaliser, en choisissant également les tâches où nous étions le plus à l'aise :



Capture d'écran de notre Trello, regroupant les diverses activités attribuées lors de la première séance.



N°	Activité	Etudiant	Planning	Temps
1	A1 Planning des activités	Estéban	Prévisionnel	1:00
			Réel	1:00
2	A2 Planification de l'organisation des utilisateurs	Estéban	Prévisionnel	1:30
			Réel	0:50
3	A3 Planification de l'organisation des ressources et des droits	Estéban	Prévisionnel	1:30
			Réel	0:20
4	A4 Installation et configuration du contrôleur de domaine	Arthur	Prévisionnel	2:00
			Réel	3:00
5	A5 Configuration de l'administration à distance du serveur	Arthur	Prévisionnel	3:00
			Réel	2:20
6	A6 Configuration des dossiers partagés et des droits NTFS	Arthur	Prévisionnel	3:00
			Réel	1:00
7	A7 Configuration des GPO	Estéban	Prévisionnel	3:00
			Réel	4:00
8	A 8 Réalisation du script de création d'utilisateurs	Estéban	Prévisionnel	3:00
			Réel	2:15
9	A 9 Gestion des comptes « invités »	Arthur	Prévisionnel	2:00
			Réel	1:00
10	A 10 Configuration des postes clients et intégration au domaine	Estéban	Prévisionnel	2:00
			Réel	1:00
11	A 11 Tests d'accès au réseau et aux ressources ainsi que rédaction d'un	Estéban	Prévisionnel	3:00
			Réel	2:00
12	A 12 Comptes rendu hebdomadaires sur Trello	Estéban & Arthur	Prévisionnel	6:00
			Réel	2:00
13	A 13 Rédaction du document technique de mise en place des	Estéban	Prévisionnel	3:00
			Réel	4:00

Capture d'écran de notre diagramme de Gantt, représentant le nombre d'heures passées par élèves et par tâches sur chaque activité.

Les horaires initialement prévues ont été, pour la plupart, respectées, il est à noter un écart dans l'activité 4 qui stipule de configurer notre contrôleur de domaine suite à une impossibilité de changer les options de la carte réseau dans la dernière version de Windows Server 2025, nous poussant donc à revoir notre installation.

Réalisation :

Nous allons dans cette section reprendre point par point la réalisation des diverses activités demandés, par ordre de la liste d'activité donnée précédemment.

Activité 1. Planning des activités (Estéban).

Le planning des activités a pour objectif de s'organiser et d'accorder aux membres du binôme l'ensemble des tâches nécessaires et listées dans l'énoncé de l'Atelier Professionnel afin de mener à bien le projet dans le strict respect du cahier des charges.

A travers ce planning nous avons pu structurer le projet en amont sur un ensemble de 16 heures estimées par personne, répartir les tâches de manière équitable au sein du binôme, et assurer le suivi de l'avancement du projet notamment grâce à Trello que nous traiterons dans une différente partie.

Cette planification a été réalisée de manière logique, par exemple nous avons déduit que le plus important était l'installation du contrôleur du domaine et l'activation du bureau à distance sur celui-ci afin d'être apte le plus rapidement possible à travailler à deux sur celui-ci.

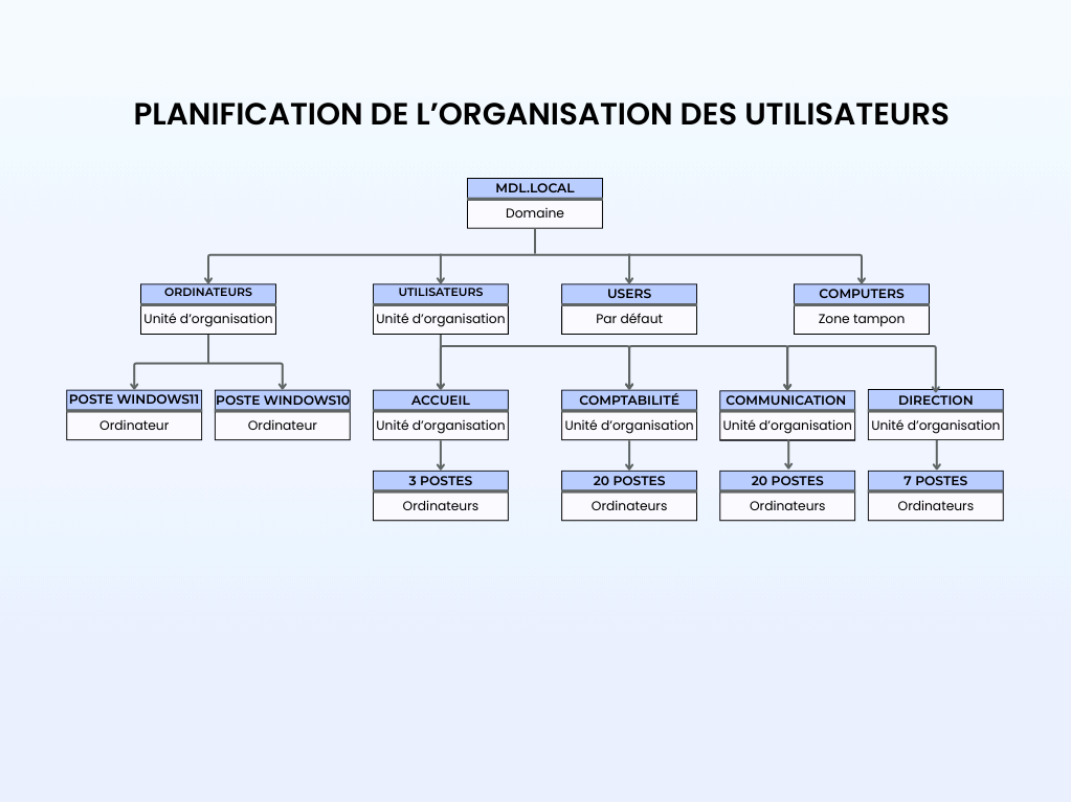
Ainsi, nous avons décidés de réaliser les activités dans l'ordre suivant et par élève :

Estéban	Arthur
- Planning des activités - Planification de l'organisation des utilisateurs - Planification des ressources et des droits d'accès à ces ressources - Gestion des comptes « invités - Configuration des GPO - Tests d'accès au réseau et aux ressources ainsi que rédaction d'un rapport de tests - Rédaction du document technique	- Installation et configuration du contrôleur de domaine - Configuration des postes clients et intégration au domaine - Configuration de l'administration à distance du serveur Windows - Configuration des dossiers partagés et des droits NTFS - Gestion des comptes « invités » - Tests d'accès au réseau et aux ressources ainsi que rédaction d'un rapport de tests

L’ensemble de ces tâches réalisées en binôme a été planifié par le chef du projet et proposé par la suite au second membre du binôme, il nous a également permi de se répartir les différents tests à réaliser par la suite, nous avons notamment décidé que le membre du binôme qui testera un des points clefs de l’activité sera celui qui n’aura pas travaillé dessus afin de valider promptement celui-ci à travers une vision globale.

Activité 2. Planification de l'organisation des utilisateurs (Estéban)

La planification de l'organisation des utilisateurs va nous permettre de mieux schématiser et comprendre comment le réseau doit être organisé autour de ces mêmes utilisateurs. On a décidé d'effectuer un organigramme synthétique permettant de mieux visualiser les droits accordés à chaque groupe d'utilisateurs, le nombre de ceux-ci par groupe et également le nombre de postes de ceux-ci.
Pour ce faire, nous nous sommes aidés d'exemple trouvés en ligne afin de réaliser ce schéma :



Il faut donc comprendre, avec celui-ci, que les utilisateurs sont, entre eux, cloisonnés et différents. Que ceux-ci appartiennent à des groupes avec des droits et accès partagés et qu'ils ne peuvent notamment pas ajouter ou supprimer de programme par exemple, en dehors des administrateurs du domaine, les membres du binôme que nous composons.
Nous avons également décidés de représenter les comptes invités (invités sur le réseau, stagiaires…) qui ne disposent pas de session personnelle mais bien d'une session partagée qui se réinitialisera à chaque fermeture, ne disposant que d'un navigateur internet et quelques outils et ne permettant pas de modifier quoi que ce soit sur le réseau.

Activité 3. Planification des ressources et des droits d'accès à ces ressources (Estéban).

La planification des ressources et les droits d'accès à ceux-ci fonctionnent de la même manière que l'activité précédente, nous avons décidé de réaliser diverses tableaux représentants chaque groupes d'utilisateurs, leurs ressources et les droits d'accès à ceux-ci comme représenté ci-dessous :

Tableau des différents lecteurs mappés et des ressources NTFS/partageés

Ressources	**Emplacement**	**Utilisation**	**Lecteur**
Dossiers personnels	Serveur de fichiers	Stockage privé par utilisateur, sauf pour les comptes invités	Q
Dossiers de service	Serveur de fichiers	Stockage partagé par groupe avec accès aux outils par service	Z

Tableau des groupes par service de l'Active Directory

Services	**Groupes de l'Active Directory associés**	**Nombre de postes**
Accueil	accueil	3 postes
Comptabilité	comptabilite	20 postes
Communication	communication	20 postes
Direction	direction	7 postes

Droits d’accès aux dossiers partagés et privés

Groupes	**Dossiers**	**Droits**	**Lecteurs**
Accueil	- Personnel - Outils Accueil	- Contrôle total - Lecture/Ecriture	- Q - Z
Comptabilité	- Personnel - Outils Comptabilité	- Contrôle total - Lecture/Ecriture	- Q - Z
Communication	- Personnel - Outils Communication	- Contrôle total - Lecture/Ecriture	- Q - Z
Direction	- Personnel - Outils Direction	- Contrôle total - Lecture/Ecriture	- Q - Z
Administrateur (2 postes)	- L’ensemble des dossiers du domaine	- Contrôle total	
Invité	- Aucun		

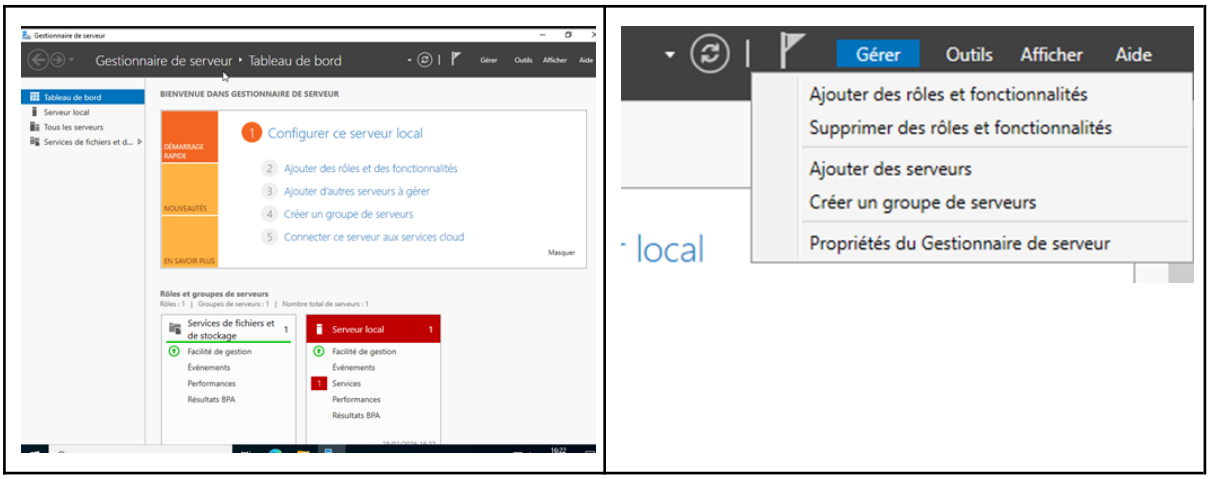
Il est important de retenir que les groupes d’utilisateurs se partageront des ressources groupées dénommées “Outils %nomdugroupe%” et que ces mêmes utilisateurs disposent d’un dossier privé “%nom d’utilisateur%”, le tout, dans des lecteurs mappés afin de faciliter l’accès à ces dossiers. Le dossier outils service aura comme permission seulement la lecture pour les utilisateurs appartenant au groupe qui leur est attribué, les administrateurs du domaines eux, ont accès à l’ensemble des dossiers partagés qu’ils soient personnels ou par groupe, avec un contrôle total en permission et enfin, les dossiers personnels disposent d’un droit de lecture et d’écriture pour les utilisateurs étant attribué individuellement à ceux-ci.

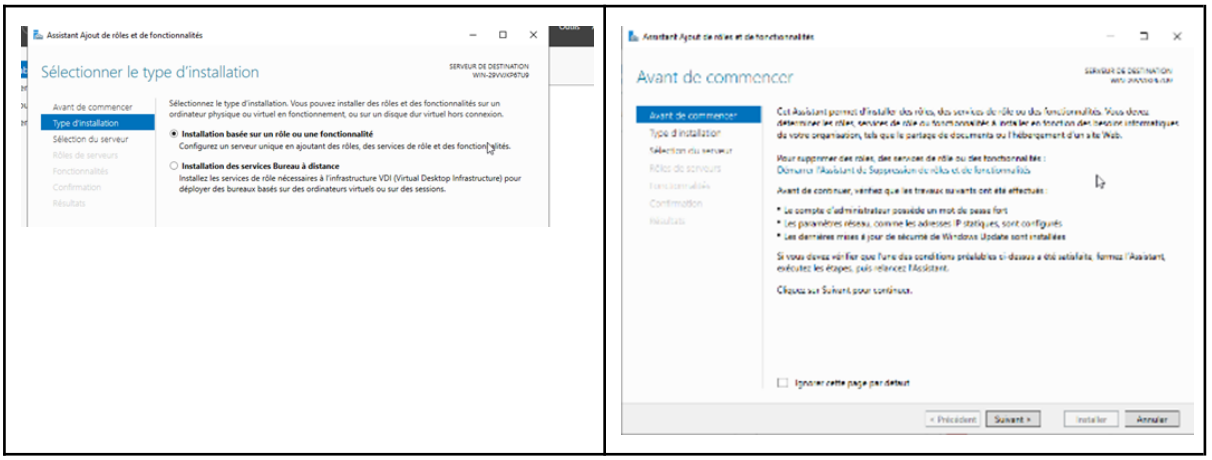
Activité 4. Installation et configuration du contrôleur de domaine (Arthur).

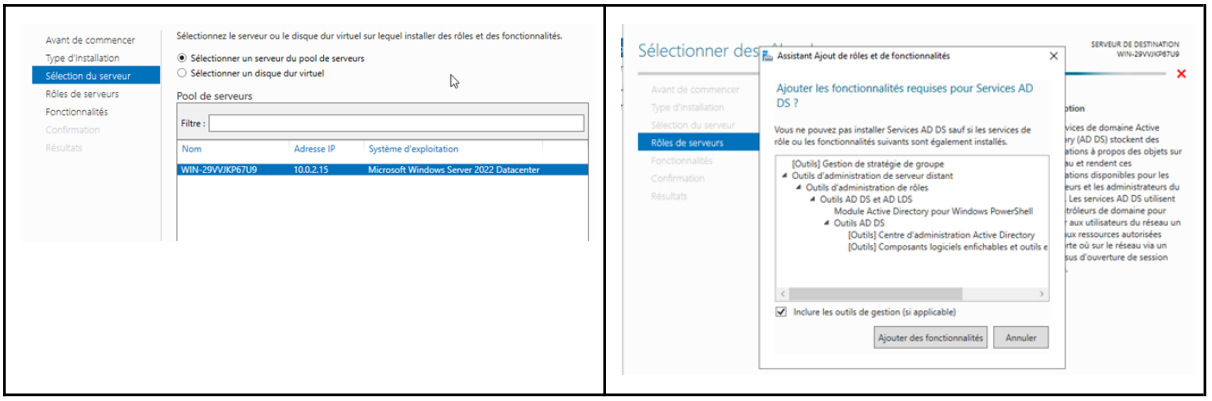
L'installation et la configuration du contrôleur de domaine se réfère à l'installation de notre Windows Server 2022 sur notre hyperviseur de type 1. Il faut donc configurer correctement l'OS à partir de l'installation sur Hypervisor.

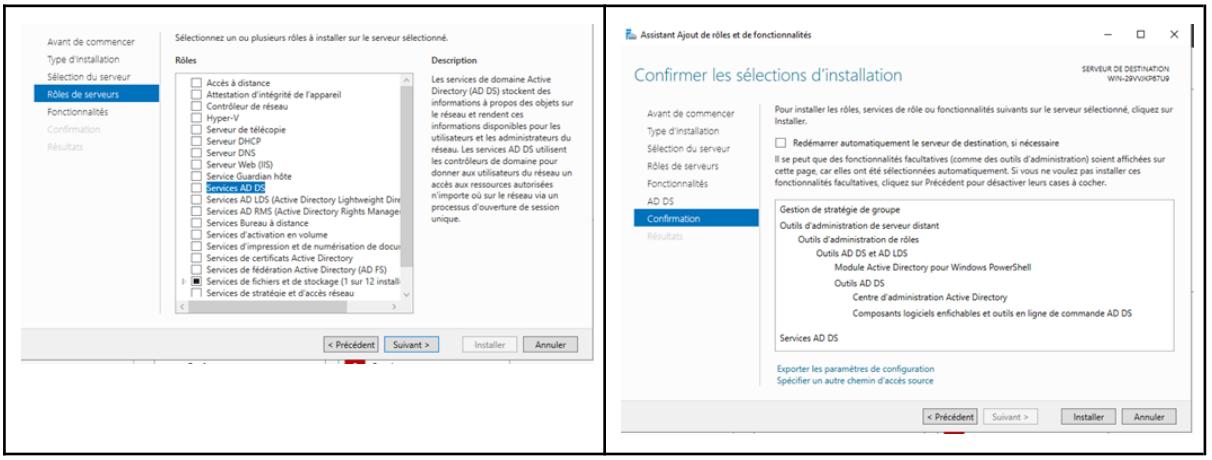
Une fois l'OS installée, on va chercher, dans le gestionnaire de serveur, à terminer la configuration de celui-ci, cela passe par un domaine qu'il convient de créer, nous l'appellerons *MDL.LOCAL* comme indiqué dans notre cahier des charges.
Nous avons également installé l'Active Directory qui va être nécessaire et même central à la réalisation de notre projet, l'installation se fait à partir de l'ajout des rôles et des fonctionnalités.

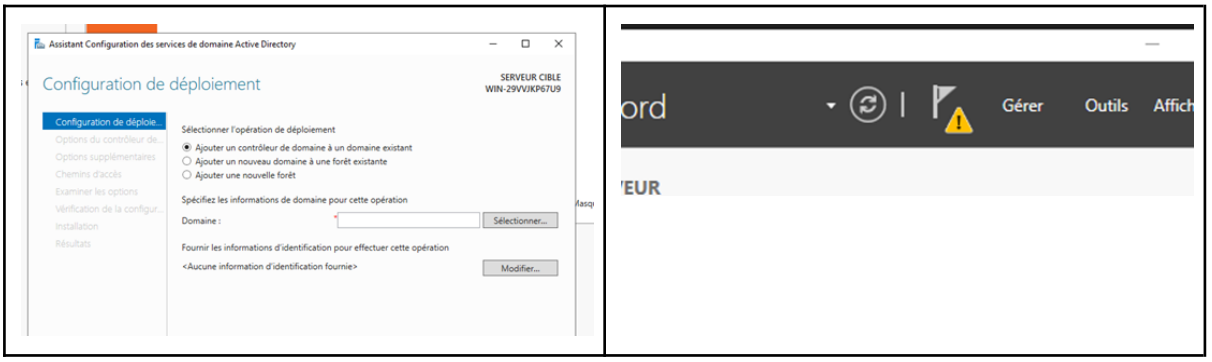
Captures de l'installation du module Active Directory





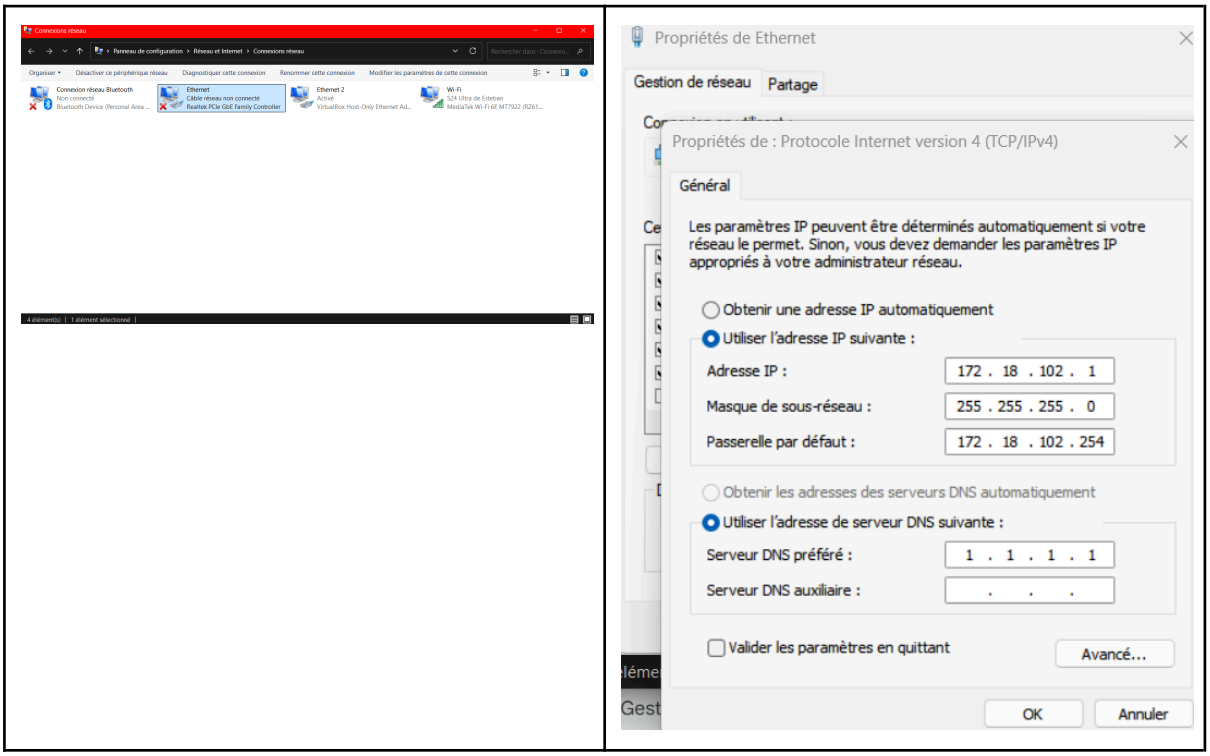






On doit aussi configurer l'ip de notre contrôleur de domaine en y accédant avec ncpa.cpl, on ajoute ensuite l'ip demandée dans le cahier des charges qui est **172.18.40.1**.

Captures de l’accès aux paramètres de la carte réseau du contrôleur de domaine



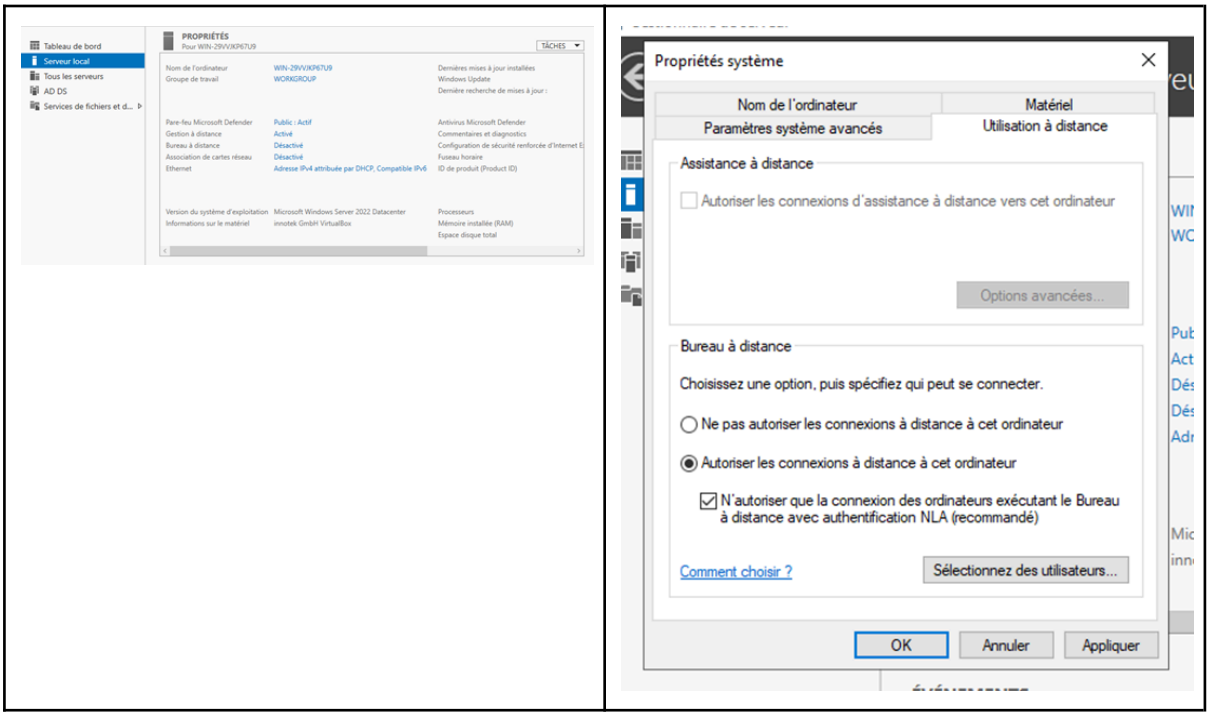
Activité 5. Configuration de l’administration à distance du serveur Windows (Arthur)

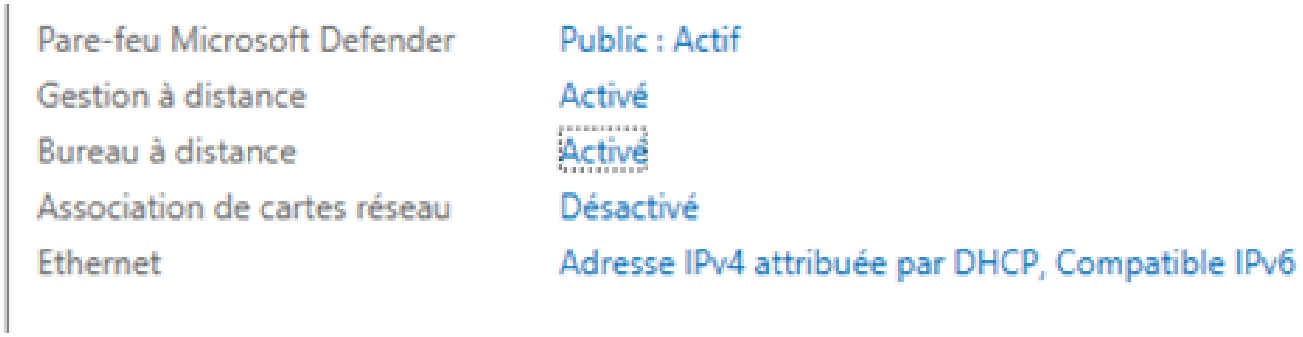
La configuration de l’administration à distance du serveur Windows est primordiale pour le bon déroulé de l’activité, permettant en effet de pouvoir par la suite travailler à deux de manière simultanée sur le contrôleur de domaine.
Le but est donc de créer un accès à distance en utilisant la fonction RDP *(Remote Desktop Protocol)* natif à Windows.

Voici les procédés de la réalisation de cette activité afin de mener à bien cette mission, il faut tout d’abord accéder au serveur local situé dans le Gestionnaire de serveur, sur notre machine contrôleuse du domaine.

Le paramètre Bureau à distance est désactivé par défaut, il nous faut l’activer et autoriser les connexions à distance à cet ordinateur.

Captures de l’activation de notre bureau à distance sur notre contrôleur de domaine





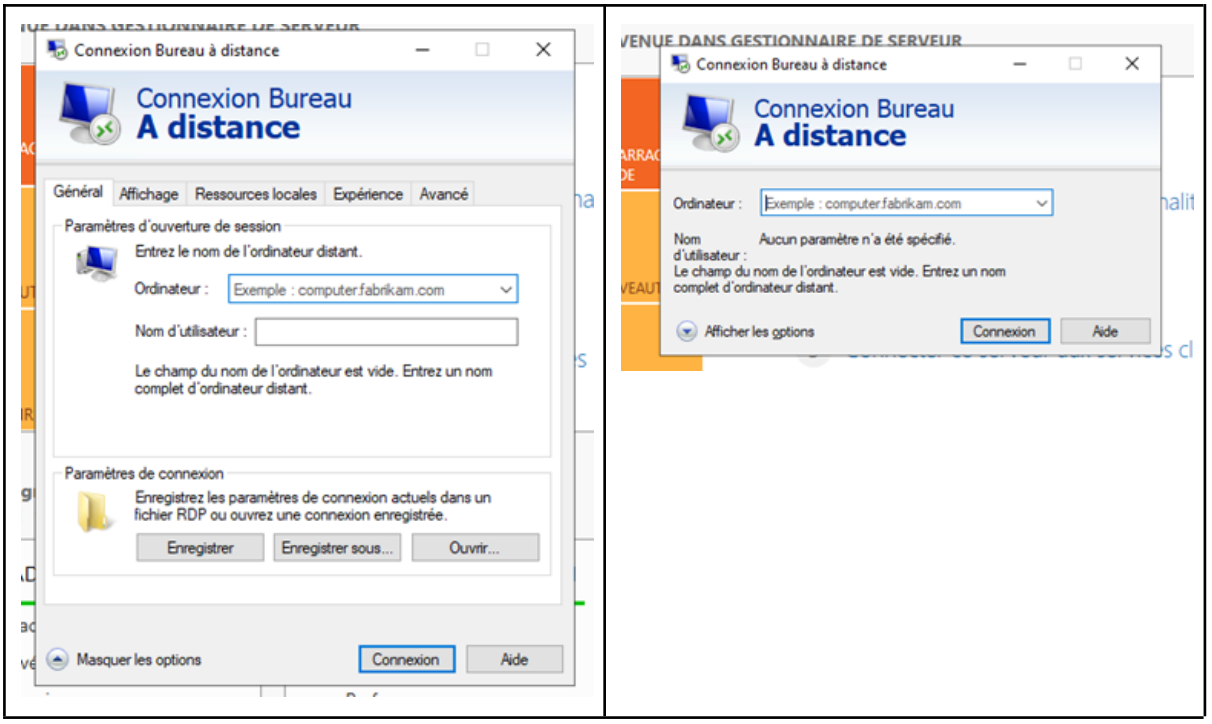
On valide ensuite les modifications apportées.

Pour avoir deux utilisateurs administrateurs sur le réseau qui vont pouvoir paramétrer le contrôleur du domaine en même temps, il nous faut également créer deux comptes administrateurs distincts, pour ce faire, nous allons copier l'user Administrateur déjà nativement présent sur l'unité organisationnelle *Users*, ces utilisateurs copiés disposent donc de deux identifiants distincts représentants les administrateurs du système, ici les deux membres composant le binôme.

Enfin, pour pouvoir se connecter à notre contrôleur de domaine avec nos postes, il faut ouvrir une règle entrant dans le pare-feu Windows en allant dans les fonctions avancées de sécurité. Ainsi, il faut vérifier la règle de bureau à distance - mode utilisateur (TCP-In). On s'assure par la suite que la règle est activée et autorisée pour le profil Domaine.

Enfin, une fois que tout est réalisé, on teste de se connecter en lançant la connexion bureau à distance sur nos postes personnels et en entrant l'identifiant précédemment créé et l'ip du serveur que nous avons réglée également auparavant, lors de l'activité sur la configuration du contrôleur de domaine.
Ainsi, nos deux usagers peuvent se connecter en même temps afin d'administrer le domaine, validant ainsi la configuration de la connexion au bureau à distance.

Captures de l'accès au bureau à distance

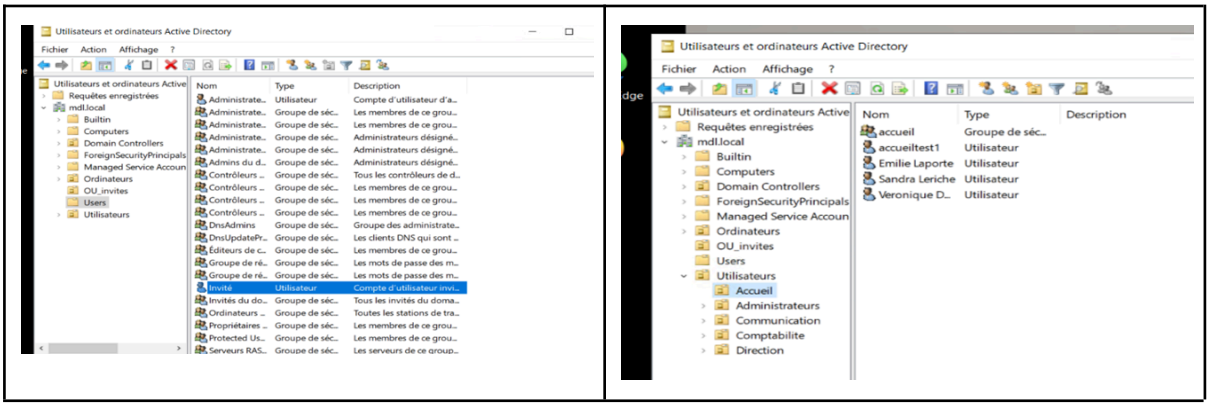

Connexion Bureau à distance
Connexion Bureau
A distance
Général
Affichage
Ressources locales
Expérience
Avancé
Paramètres d'ouverture de session
Entrez le nom de l'ordinateur distant.
Ordinateur :
Exemple : computer.fabrikam.com
Nom d'utilisateur :
Le champ du nom de l'ordinateur est vide. Entrez un nom complet d'ordinateur distant.
Paramètres de connexion
Enregistrez les paramètres de connexion actuels dans un fichier RDP ou ouvrez une connexion enregistrée.
Enregistrer
Enregistrer sous...
Ouvrir...
Masquer les options
Connexion
Aide
Connexion Bureau à distance
Connexion Bureau
A distance
Ordinateur :
Exemple : computer.fabrikam.com
Nom d'utilisateur :
Aucun paramètre n'a été spécifié.
Le champ du nom de l'ordinateur est vide. Entrez un nom complet d'ordinateur distant.
Afficher les options
Connexion
Aide

Activité 6. Configuration des dossiers partagés et des droits NTFS (Arthur).

La configuration des dossiers partagés et des droits NTFS vise à déployer des dossiers partagés sécurisés par groupe ou service, qui seront ici appelées les Outils, ce sont des ressources que l'on cherche à rendre communes. Il est également question de dossier personnel par utilisateur et pour l'utilisateur en question.

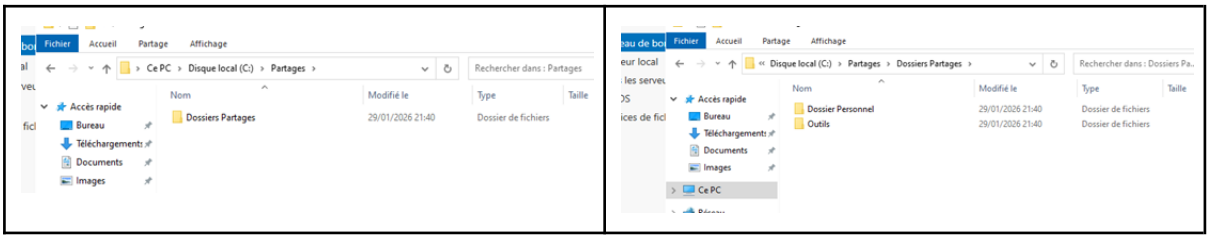
Cependant, notre Active Directory est pour l'instant quasiment vierge, il convient donc de créer nos premières UO afin d'organiser notre domaine. Pour aller dans ce sens, nous allons créer l'UO *Utilisateurs* qui va regrouper l'ensemble des utilisateurs du domaine, les sous-unités organisationnelles ayant le nom de chaque service ainsi que leur groupe de sécurité. Afin de réaliser quelques tests sur nos GPO que nous verrons dans l'activité suivante, nous allons également créer un utilisateur par service que nous placerons dans leur unité organisationnelle respective.

Captures des UO du domaine



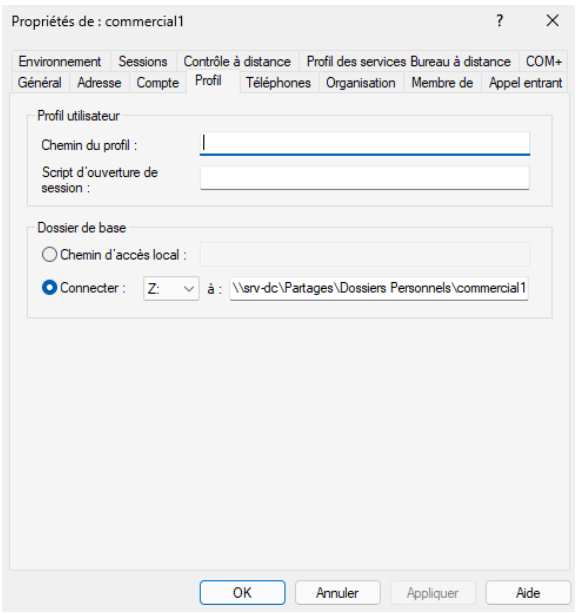
Ensuite, nous allons créer un dossier *Partages* situé sur le C:, dossier que nous allons partager via le menu *partage avancé*, dans ce menu nous allons donner le contrôle total au groupe de sécurité *Administrateurs* et le droit de lecture aux 4 groupes de sécurité représentant nos 4 services différents.

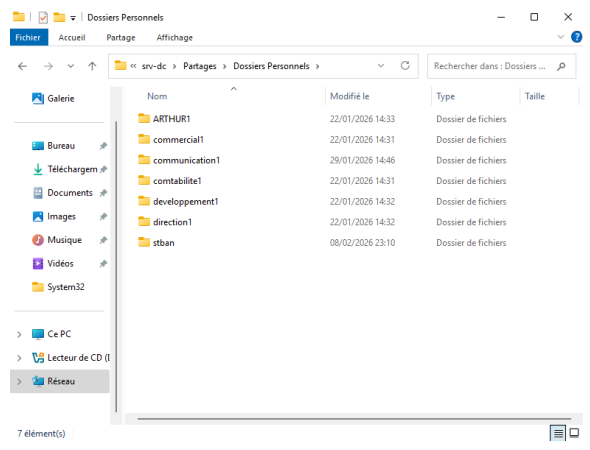
Captures du dossier Partages et de ses sous-dossiers

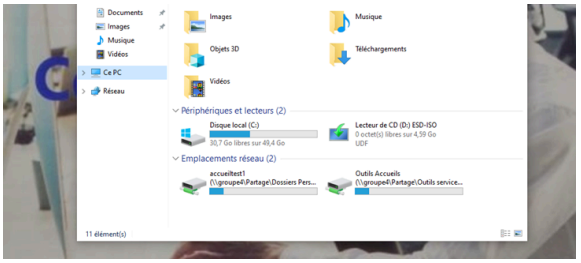


Dans ce dossier *Partages*, nous allons créer deux autres dossiers nommés *Dossiers_Personnels* ainsi que *Outils-Services* et dans ce dernier dossier nous allons créer 4 sous-dossiers *Accueil*, *Comptabilité*, *Communication* et *Direction*. Chacun de ces dossiers devra être mappé avec une GPO lors de la prochaine activité. Pour le dossier personnel, on va manuellement, dans nos utilisateurs de test, se rendre dans les paramètres des comptes et dans le profil afin d'ajouter à chacun des utilisateurs un dossier de base connecté par le lecteur *Z* via le chemin réseau \\nom_du_controlleur\Partages\Dossiers Personnels\%username% donc ici \\srv-dc\Partages\Dossiers Personnels\%username%.

Captures du dossier de base sur lecteur Z et test




Dossiers Personnels
Fichier
Accueil
Partage
Affichage
srv-dc › Partages › Dossiers Personnels ›
Rechercher dans : Dossiers ...
Galerie
Bureau
Téléchargem
Documents
Images
Musique
Vidéos
System32
Ce PC
Lecteur de CD (I
Réseau
Nom
Modifié le
Type
Taille
ARTHUR1 22/01/2026 14:33 Dossier de fichiers
commercial1 22/01/2026 14:31 Dossier de fichiers
communication1 29/01/2026 14:46 Dossier de fichiers
comtabilite1 22/01/2026 14:31 Dossier de fichiers
developpement1 22/01/2026 14:32 Dossier de fichiers
direction1 22/01/2026 14:32 Dossier de fichiers
stban 08/02/2026 23:10 Dossier de fichiers
7 élément(s)

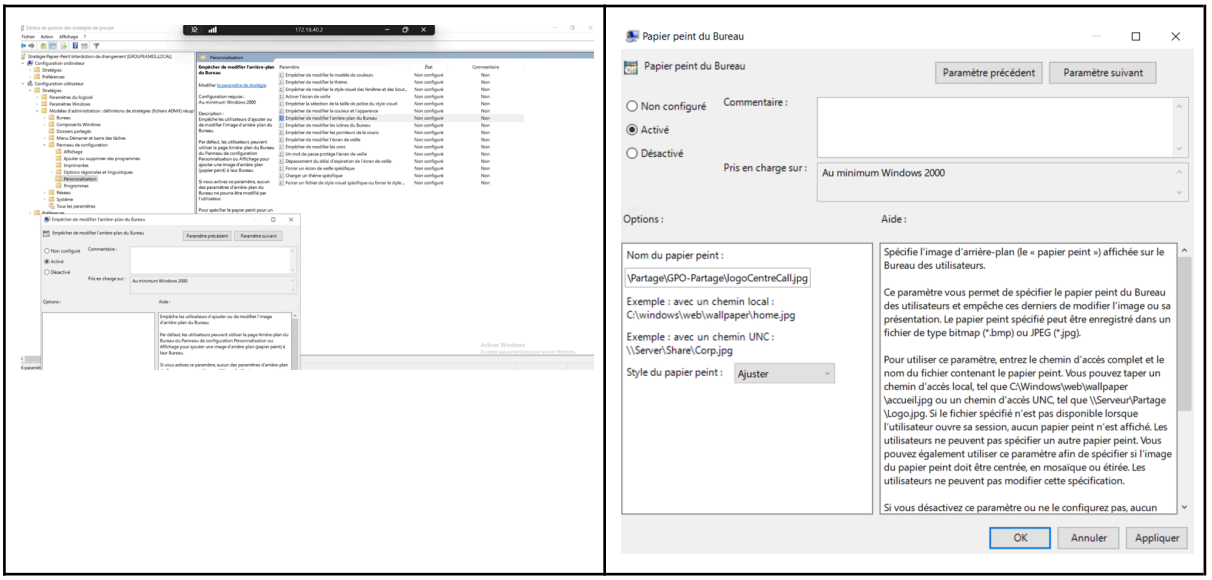

Documents
Images
Musique
Vidéos
Ce PC
Réseau
Images
Musique
Objets 3D
Téléchargements
Vidéos
Périphériques et lecteurs (2)
Disque local (C:)
30,7 Go libres sur 49,4 Go
Lecteur de CD (D:) ESD-ISO
0 octet(s) libres sur 4,59 Go
UDF
Emplacements réseau (2)
accueiltest1
(\\groupe4\Partage\Dossiers Pers...
Outils Accueils
(\\groupe4\Partage\Outils service...
11 élément(s)

Activité 7. Configuration des GPO (Arthur)

Les GPO, aussi appelés stratégies de groupe, ont pour but de mettre en place des configurations et des sécurités sur les ordinateurs ou les utilisateurs d'un domaine Active Directory.
Lors de cet Atelier Professionnel, il est notamment demandé de réaliser des GPO sur les utilisateurs, pour ce faire, nous allons créer 5 GPO distincts, chacun ayant un objectif différent afin de mieux s'organiser et que ce soit également plus simple à analyser lors de notre phase finale de test.
Les GPO seront organisées de la manière suivante :

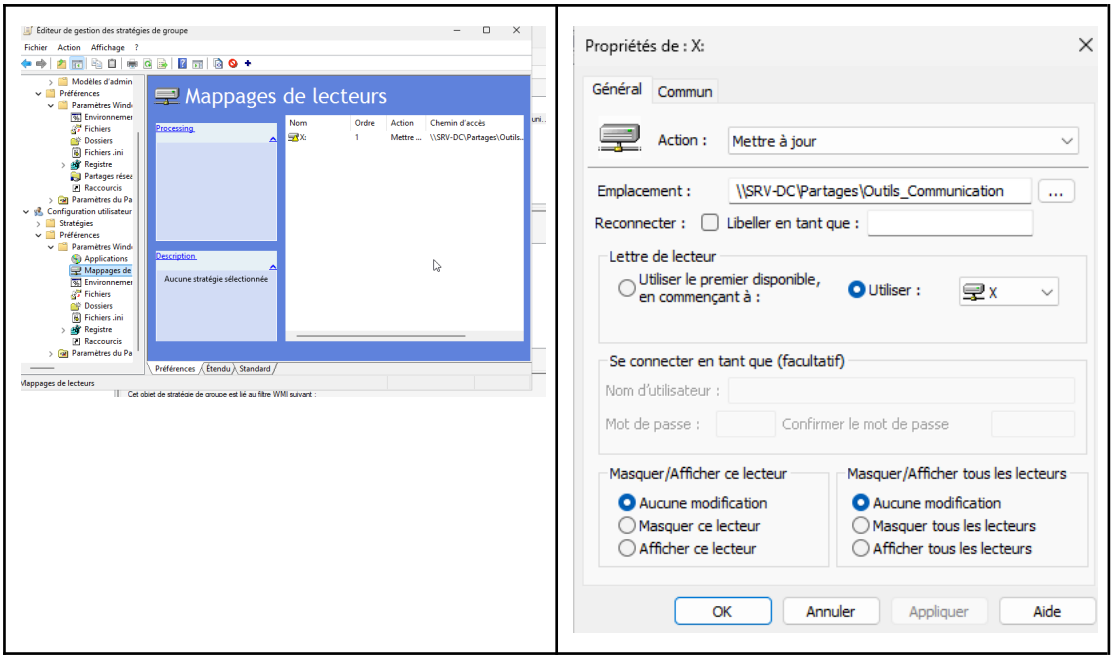
- Une GPO afin d'imposer un fond d'écran et de désactiver le changement de celui-ci, placé directement sur l'ensemble des usagers. Pour créer une GPO, il faut effectuer un ensemble de manipulations; tout d'abord, il faut aller dans la gestion de stratégie de groupes, descendre dans l'arborescence du domaine jusqu'à trouver nos utilisateurs à travers l'unité organisationnelle *Utilisateurs*. Une fois placée dans celle-ci, on va créer une GPO appliquée directement à l'UO que l'on va renommer par praticité, on va pouvoir ensuite la modifier et on retrouve la gestion des fonds d'écrans dans l'arborescence des stratégies suivantes.

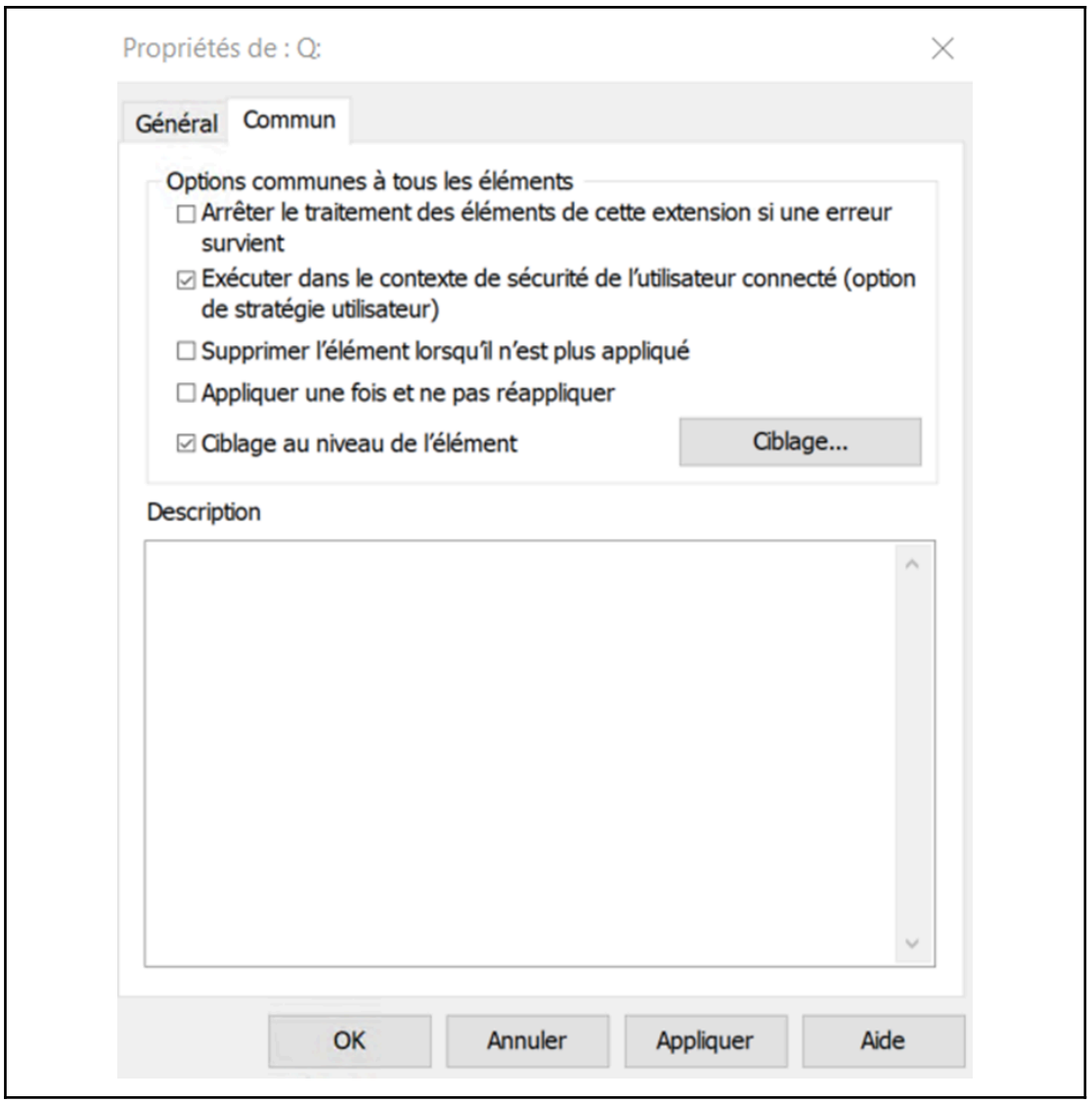
Captures de la mise en place du papier-peint



- Une GPO traitant des différents lecteurs mappés avec le dossier ressources/outils qui va chercher à afficher directement dans le C: de chaque utilisateur le dossier outils du groupe auquel il appartient. Cette UO sera appliquée directement sur les utilisateurs.

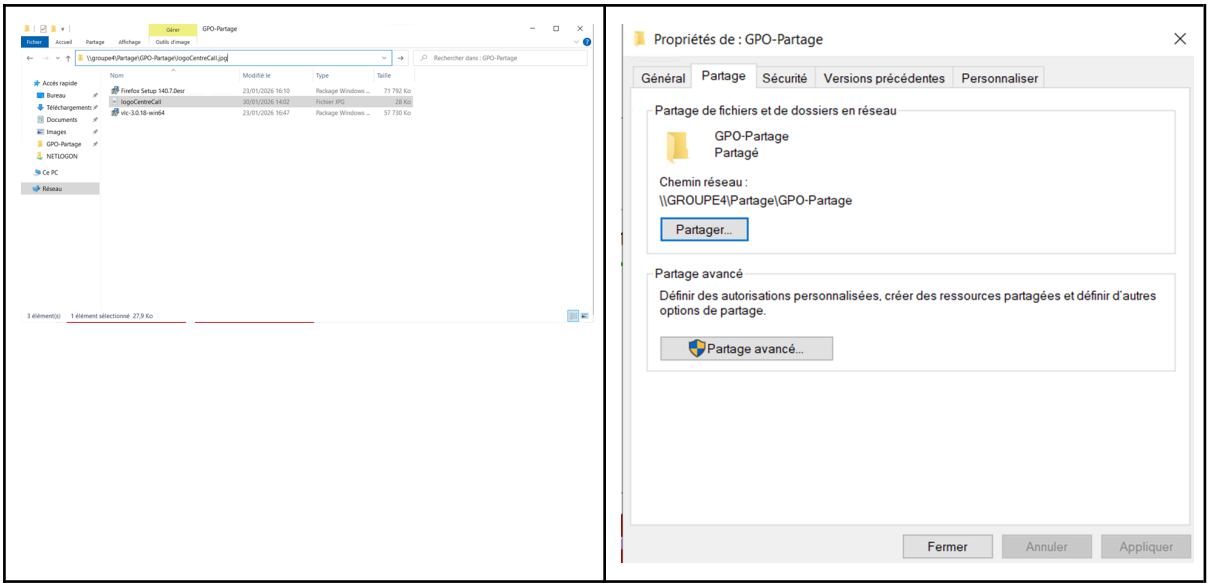
Captures de la mise en place des lecteurs mappés

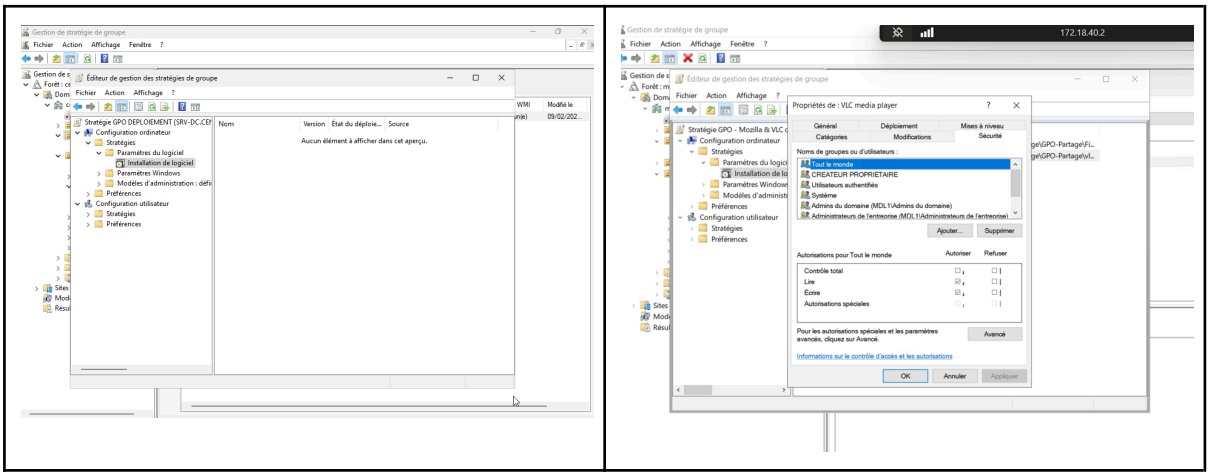




- Une GPO pour le déploiement automatisés des logiciels VLC et Mozilla Firefox, cette GPO est à lier sur les postes, il nous faut également créer un nouveau sous-dossier dans notre dossier partagé à tous les usagers, celui-ci doit contenir les deux logiciels sous l'extension .msi qui permettra donc d'effectuer les installations sur les postes.

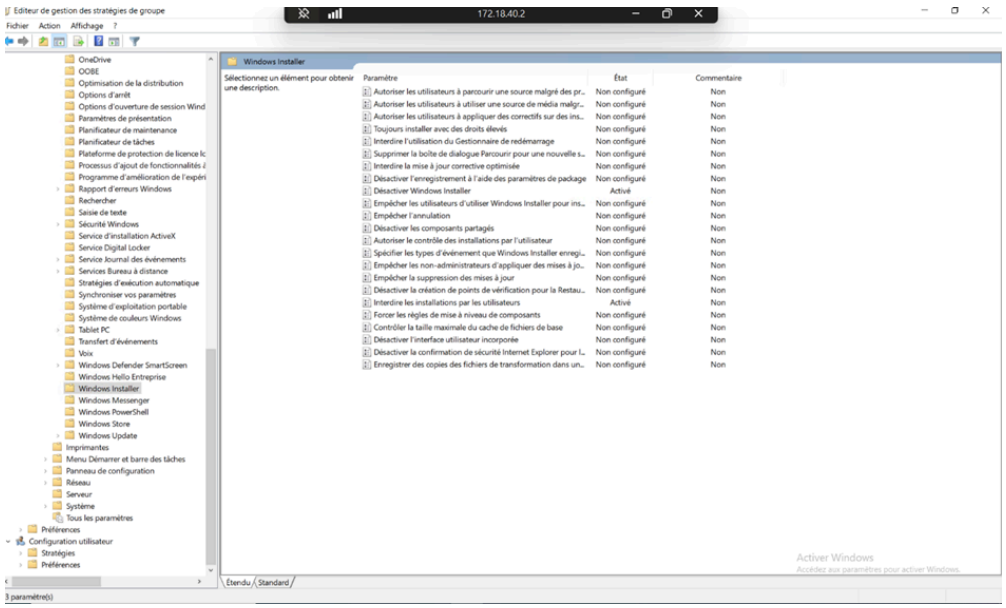
Captures de la mise en place des déploiements logiciels





- Une GPO pour la restriction des utilisateurs qui va chercher à interdire l'accès au panneau de configuration, empêcher l'installation et la suppression de programmes et interdire l'accès aux paramètres systèmes. Cette dernière UO sera placée sur l'unité organisationnelle utilisateurs.

Captures de la mise en place des restrictions pour les utilisateurs

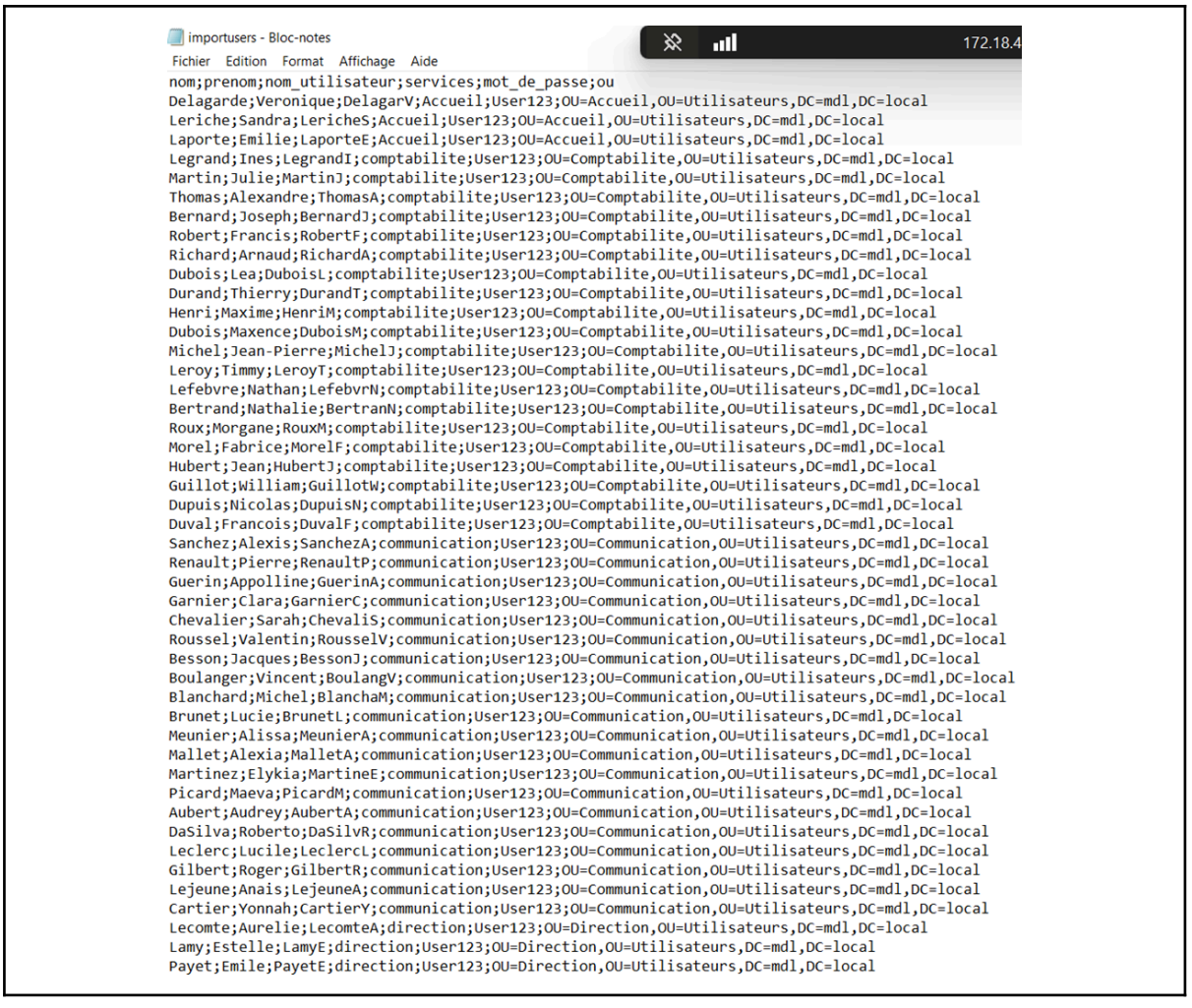


Activité 8. Réalisation du script de création d'utilisateurs (Estéban).

Lors de cette activité, nous avons dû utiliser un fichier d'importations des différents utilisateurs qui devront être intégrés à l'Active Directory du domaine, afin de par la suite avec l'aide de commandes Powershell, les intégrer à notre Active Directory et dans leur groupe de sécurité respectifs.

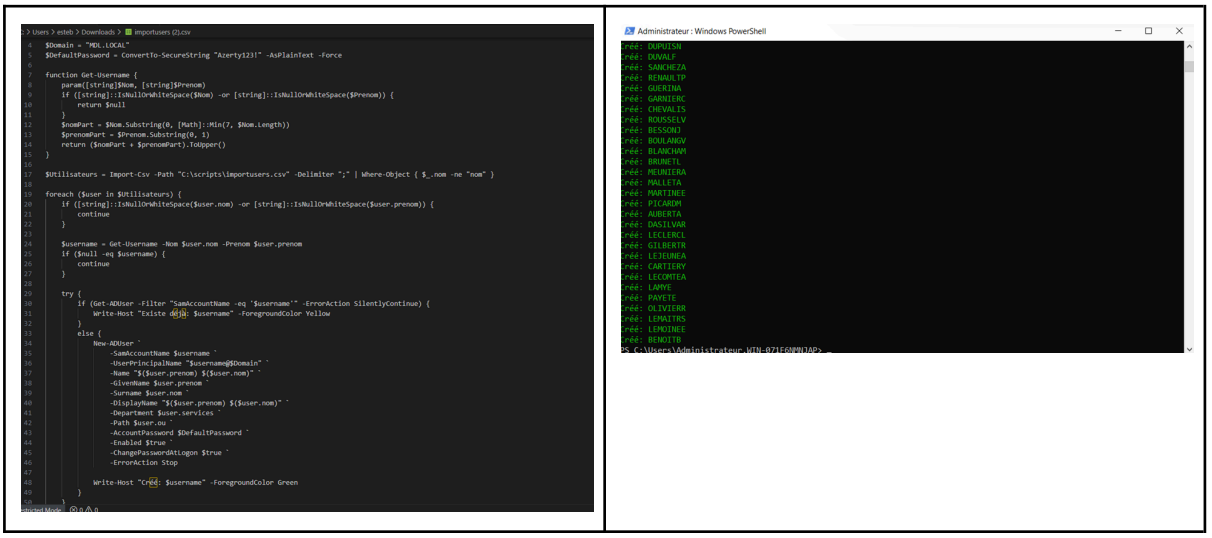
Premièrement, nous avons modifié et utilisé le importuser.csv fourni lors de l'Atelier Professionnel, nous avons rajouté une en-tête avec le nom de nos différentes unités d'organisations de notre Active Directory afin que le fichier soit cohérent avec notre configuration.

Captures du fichier d'importation des utilisateurs



Nous nous sommes ensuite documentés afin de réaliser deux scripts différents, le premier va servir à créer la cinquantaine d'utilisateurs demandés sur le réseau et dans les bonnes unités d'organisations. Nous lançons ensuite le code sur Windows Powershell dans notre contrôleur de domaine et les utilisateurs sont bel et bien créés aux bons endroits avec un mot de passe par défaut et en respectant la règle de nommage des 7 premières lettres du nom et la première lettre du prénom.

Captures du script de création des utilisateurs et test



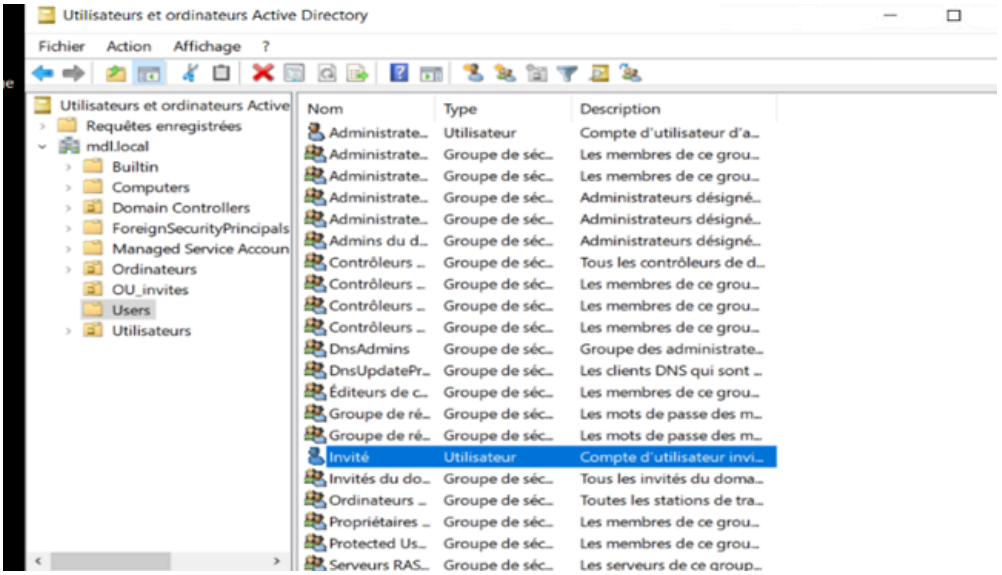
Ensuite, on cherche à attribuer les bons groupes de sécurité à ces utilisateurs, pour ce faire, nous réalisons ce second script qui va nous le permettre. On le lance également sur le contrôleur du domaine avec Powershell et nous vérifions par la suite que les groupes sont attribués, ce qui est le cas.

Captures du script d'attribution des groupes

```powershell
$GroupMapping = @{
    "Accueil" = "accueil"
    "comptabilite" = "comptabilite"
    "communication" = "communication"
    "direction" = "direction"
}

# Importer le CSV
$Utilisateurs = Import-Csv -Path "C:\scripts\importusers.csv" -Delimiter ";" | Where-Object { $_.nom -ne

foreach ($user in $Utilisateurs) {
    if ([string]::IsNullOrWhiteSpace($user.nom) -or [string]::IsNullOrWhiteSpace($user.prenom)) {
        continue
    }

    $nomPart = $user.nom.Substring(0, [Math]::Min(7, $user.nom.Length))
    $prenomPart = $user.prenom.Substring(0, 1)
    $username = ($nomPart + $prenomPart).ToUpper()

    $groupName = $GroupMapping[$user.services]

    if ($null -ne $groupName) {
        try {
            Add-ADGroupMember -Identity $groupName -Members $username -ErrorAction Stop
            Write-Host "Ajouté: $username -> $groupName" -ForegroundColor Green
        }
        catch {
            Write-Host "Erreur $username : $($_.Exception.Message)" -ForegroundColor Red
        }
    }
}
```

```
Ajouté: DELAGARV -> accueil
Ajouté: LERICHES -> accueil
Ajouté: LAPORTEE -> accueil
Ajouté: LEGRANDI -> comptabilite
Ajouté: MARTINJ -> comptabilite
Ajouté: THOMASA -> comptabilite
Ajouté: BERNARDJ -> comptabilite
Ajouté: ROBERTF -> comptabilite
Ajouté: RICHARDA -> comptabilite
Ajouté: DUBOISL -> comptabilite
Ajouté: DURANDT -> comptabilite
Ajouté: HENRIM -> comptabilite
Ajouté: DUBOISM -> comptabilite
Ajouté: MICHELJ -> comptabilite
Ajouté: LEROYT -> comptabilite
Ajouté: LEFEBVRN -> comptabilite
Ajouté: BERTRANN -> comptabilite
Ajouté: ROUXM -> comptabilite
Ajouté: MORELF -> comptabilite
Ajouté: HUBERTJ -> comptabilite
Ajouté: GUILLOTW -> comptabilite
Ajouté: DUPUISN -> comptabilite
Ajouté: DUVALF -> comptabilite
Ajouté: SANCHEZA -> communication
Ajouté: RENAULTP -> communication
Ajouté: GUERINA -> communication
Ajouté: GARNIERC -> communication
Ajouté: CHEVALIS -> communication
Ajouté: ROUSSELV -> communication
Ajouté: BESSONJ -> communication
Ajouté: BOULANGV -> communication
Ajouté: BLANCHAM -> communication
Ajouté: BRUNETL -> communication
Ajouté: MEUNIERA -> communication
Ajouté: MALLETA -> communication
Ajouté: MARTINEE -> communication
Ajouté: PICARDM -> communication
Ajouté: AUBERTA -> communication
Ajouté: DASILVAR -> communication
Ajouté: LECLERCL -> communication
Ajouté: GILBERTR -> communication
Ajouté: LEJEUNEA -> communication
Ajouté: CARTIERY -> communication
Ajouté: LECOMTEA -> direction
Ajouté: LAMYE -> direction
Ajouté: PAYETE -> direction
Ajouté: OLIVIERR -> direction
Ajouté: LEMAITRS -> direction
Ajouté: LEMOINEE -> direction
Ajouté: BENOITB -> direction
PS C:\Users\Administrateur.WIN-071F6NMNJAP>
```

Capture du résultat final

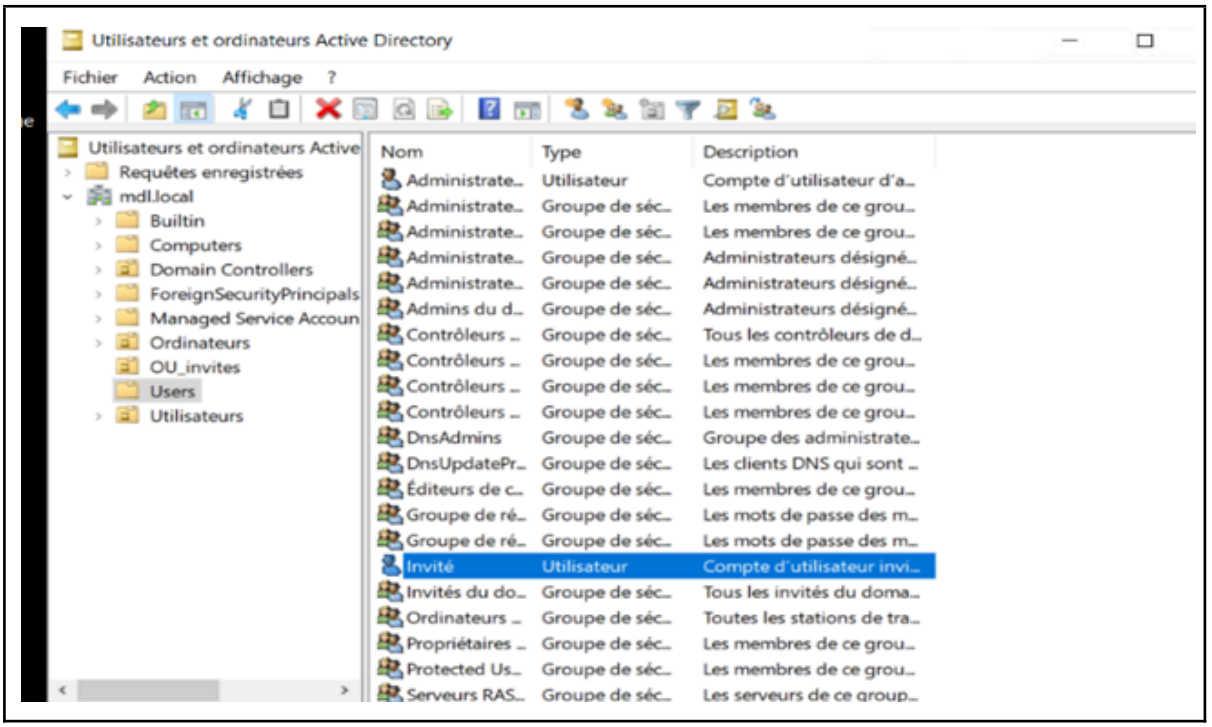


Activité 9. Gestion des comptes invités (Arthur).

Lors de cette activité, nous allons chercher à créer un compte invité accessible sans aucun mot de passe et avec l'identifiant *invite*. Celui-ci est un compte particulier qui ne disposera d'aucun droit, d'aucun accès aux ressources partagées et ne possédant pas un environnement.

Pour ce faire, nous allons nous diriger vers l'unité d'organisation *Users*, natif à notre Active Directory et copier notre utilisateur *invite*.
On va le renommer, ici *invite_default* et on le place dans l'unité d'organisation *Utilisateurs* que nous avons précédemment créer, dans une UO à part entière afin de pouvoir, par la suite, y appliquer des GPO.

Capture du compte invite intégré au domaine



Ce nouvel utilisateur garde donc les propriétés de l'utilisateur *invite* natif et avec des droits préconfigurés par défaut, il ne peut donc pas avoir de session personnelle, n'a pas de droits d'accès sur nos ressources partagées et nous ne lui avons pas non plus donné un dossier de partage personnel. Son environnement se réinitialise donc à la fin de chaque session.

On va ainsi chercher à ce qu'il n'ait pas accès à d'autres applications que les applications déployées (Mozilla et VLC) et qu'il ait des droits très limités.

Pour ce faire, on crée une nouvelle stratégie de groupe, on la modifie pour y appliquer un applocker se situant dans *Configuration ordinateur - Paramètres Windows - Paramètres de sécurité - Stratégies de contrôle des applications*.
C'est ici qu'on va pouvoir autoriser les invité à utiliser seulement Mozilla Firefox se situant dans C:\Program Files\Mozilla Firefox\firefox.exe. De même avec vlc. On peut aussi forcer l'application de ces nouvelles gpo avec un *gpupdate /force* dans le cmd ou tout simplement relancer notre session.

Ainsi, nos comptes invités sont créés et ne disposent pas de droits importants sur notre réseau.

Activité 10. Configuration des postes clients et intégration au domaine (Arthur).

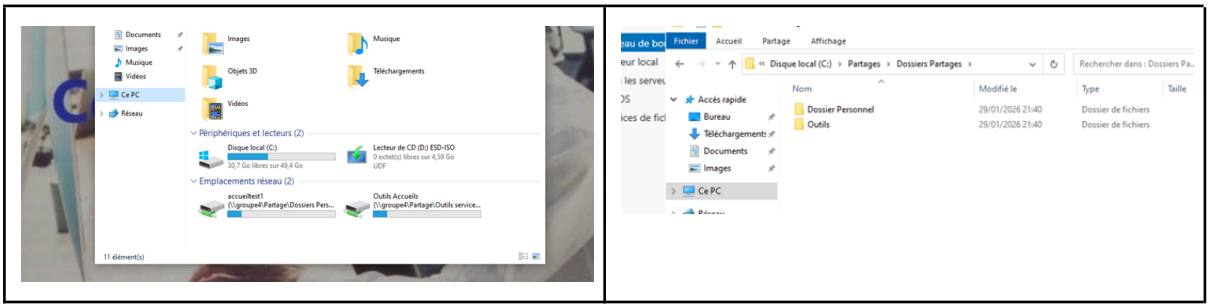
Nous diviserons les postes clients en deux postes, un poste Windows 10 et un poste Windows 11.
On commence par modifier les paramètres des cartes réseaux de nos deux machines virtuelles les simulant, pour y acceder on passe par *ncpa.cpl*. On va configurer les ips afin que le poste Windows 10 possède l'ip **172.18.40.100** et le poste Windows 11 **172.18.40.101**.

On cherche ensuite à ajouter ces deux postes sur le domaine, on va donc dans le panneau de configuration de nos deux machines clientes, on modifie les paramètres de l'onglet *Paramètres de nom d'ordinateur, de domaine et de groupe de travail*, pour ensuite modifier les propriétés systèmes et y ajouter le nom de domaine MDL.LOCAL comme montré ci-dessous.
Les machines apparaissent dès lors dans notre Active Directory dans l'unité organisationnelle *Computers*, on peut les déplacer par la suite de cette zone tampon à notre unité *Ordinateurs*

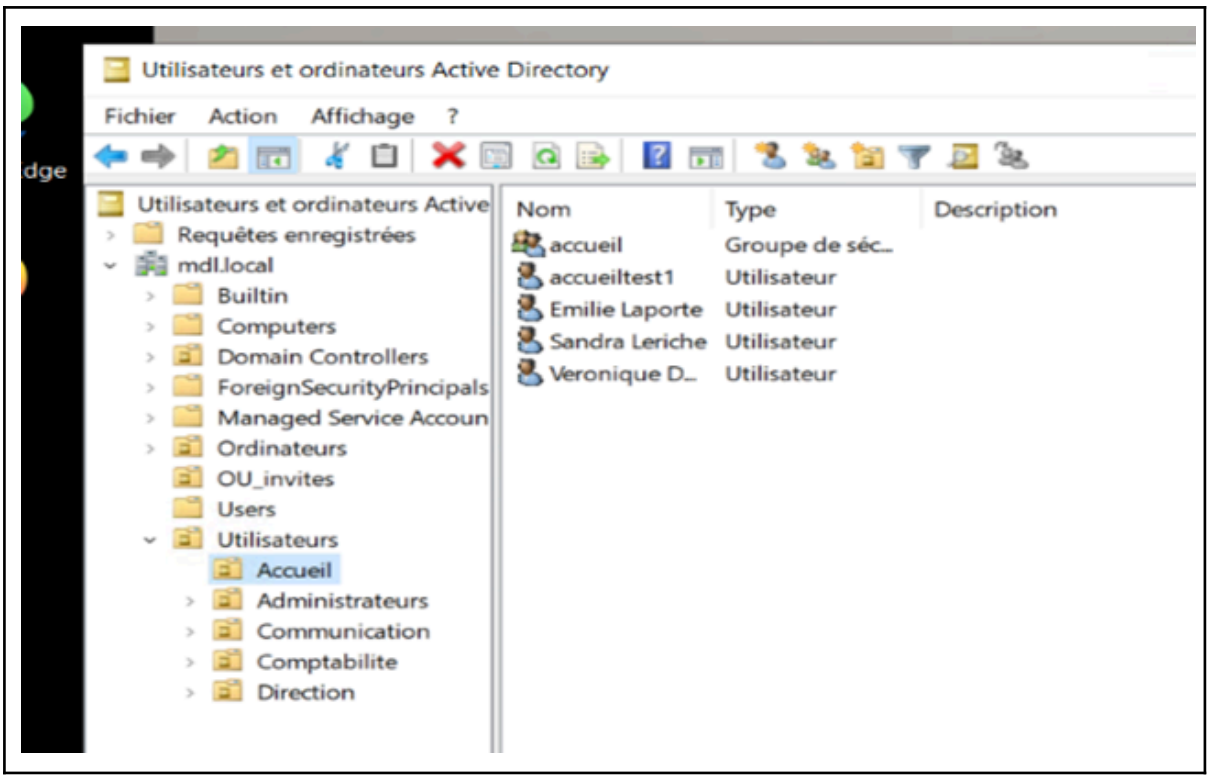
Activité 11. Test d’accès au réseau et aux ressources ainsi que rédaction d’un rapport de tests.

Lors de cette dernière activité, il est question de rédiger un rapport comprenant les tests de l’ensemble des activités précédentes.

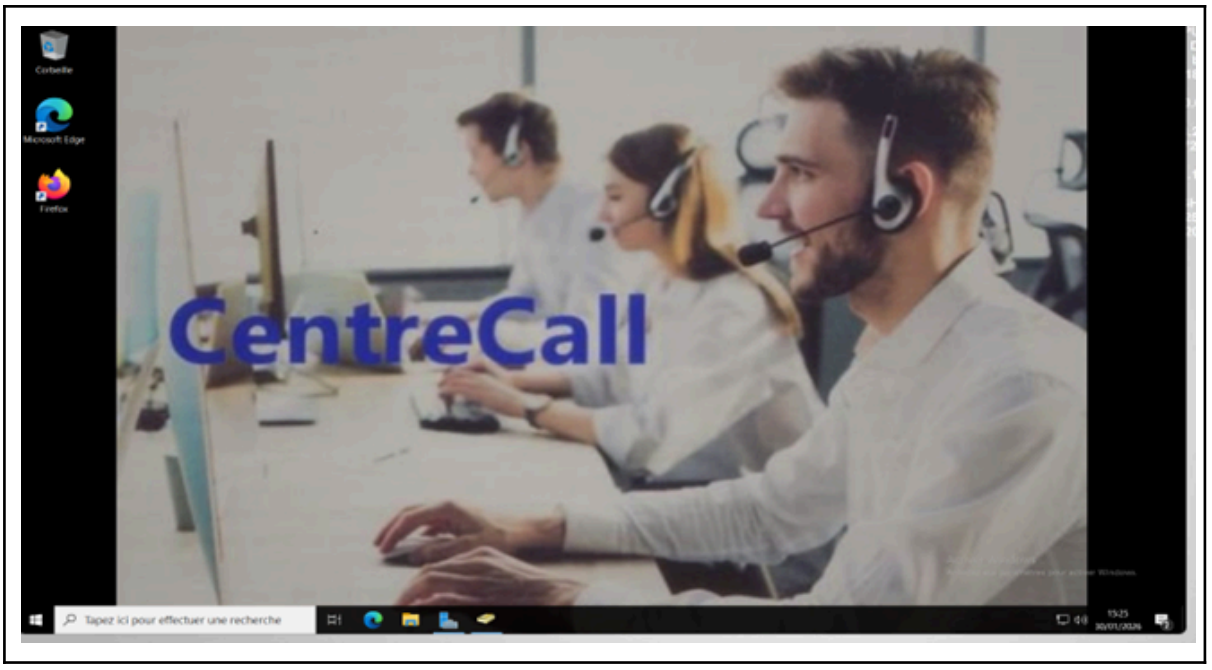
- Nous avons ainsi réalisé différents tests, vérifiant la confidentialité des dossiers partagés qui est validé pour l’ensemble des groupes/services.



- Nous avons également veillé à ce que le compte invite soit accessible et qu’il ne dispose pas d’un environnement sauvegardable.
- Les utilisateurs créés par le script se trouvent tous dans les UO adéquates et dans les groupes de sécurité qui leur sont propres.



- Le contrôleur de domaine ainsi que les deux postes Windows 10 et 11 sont bien paramétrés, intégrés au domaine et peuvent joindre l'Active Directory.
- Le déploiement des logiciels fonctionne pour Mozilla Firefox, mais pas pour VLC media player, peut-être dû à une version du logiciel incompatible avec le déploiement.



- Les GPO de restrictions et de déploiements du fond d'écran fonctionnent comme attendus.
- La connexion des deux administrateurs du domaine (notre binôme) peut se faire simultanément avec nos deux postes.