

Gestion avancée de l'Active Directory



Microsoft
Active Directory

Sommaire

Sommaire.....	1
Informations additionnelles.....	2
Partie 1 - Présentation d'Active Directory.....	2
Partie 2 - Prérequis.....	2
Partie 3 - Identifiants et mots de passe.....	2
Partie 4 - Création de l'arborescence Active Directory.....	3
Sous partie 1 : Création des Unité d'Organisation.....	3
Sous partie 2 : Création des groupes.....	4
Sous partie 3 : Ajout des utilisateurs dans les groupes :.....	6
Partie 5 - Création des comptes utilisateurs.....	6
Sous partie 1 : Le Profil "Service R&D".....	7
Sous partie 2 : Le Profil "Service Commerce".....	7
Sous partie 3 : Le Profil "Service RH".....	7
Sous partie 4 : Le Profil "Service Informatique".....	8
Partie 6 - Mise en place des partages.....	8
Sous partie 1 : Création d'une nouvelle partition sur C:.....	8
Sous partie 2 : Partage du service Informatique.....	10
Sous partie 3 : Partage des autres services.....	12
Partie 7 - Déploiement automatique des partages sur les postes de travail.....	12

Sous partie 1 : Configuration de la GPO.....	13
Sous partie 2 : Tests de la GPO.....	15
Sous partie 3 : Epingler à l'accès rapide le partage via un script PowerShell contenu dans la GPO.....	16
Partie 8 - Familiarisation avec les GPO.....	18
Sous partie 1 : Déploiement de logiciel (.msi) par GPO.....	18
Sous partie 2 : Ajout d'un fond d'écran par GPO.....	20

Informations additionnelles

Matériel utilisé	
Os utilisé	
Procédure réalisée sur machine virtuelle :	

Partie 1 - Présentation d'Active Directory

Active Directory (AD) est un service d'annuaire développé par Microsoft qui agit comme le cerveau central d'un réseau informatique Windows. Son principe repose sur la centralisation de toutes les informations du réseau (utilisateurs, ordinateurs, imprimantes) dans une base de données hiérarchique unique, permettant aux administrateurs de gérer les identités et la sécurité depuis un seul point de contrôle. Concrètement, lorsqu'un utilisateur se connecte, l'AD vérifie ses identifiants (authentification) et détermine instantanément ses permissions (autorisation) tout en appliquant automatiquement des configurations via des stratégies de groupe (GPO), assurant ainsi que la bonne personne accède aux bonnes ressources avec les bons droits.

Partie 2 - Prérequis

- 1) Avoir réalisé au préalable la partie de l'Active directory sur la procédure de mise en place du réseau.

Partie 3 - Identifiants et mots de passe

Identifiant	Mot de passe
-------------	--------------



TECHNOVA

TECHNOVA\Administrateur	Password1234
TECHNOVA\amartin	Première connexion : rMTk7QLGj5ui Mot de passe : Hop!La88
TECHNOVA\tdurand	Première connexion : Njd2!t!y4a0k Mot de passe : Top!But10
TECHNOVA\sbernard	Première connexion : McPHzr84mnw7 Mot de passe : Chut!Dodo5
TECHNOVA\aplantier	Première connexion : Wja22B6yjdrw Mot de passe : Stop!Pub0

Partie 4 - Création de l'arborescence Active Directory

Sous partie 1 : Création des Unité d'Organisation

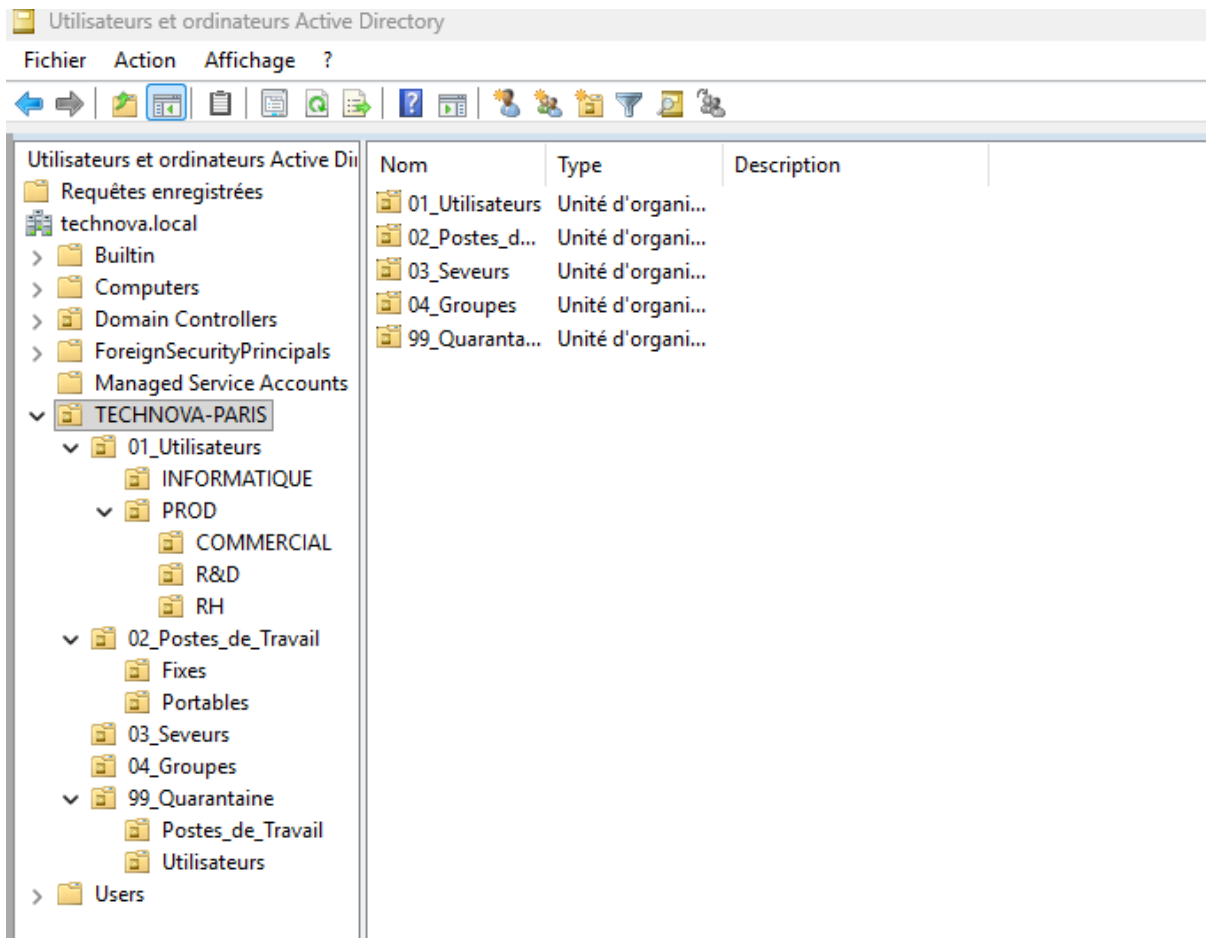
Une Unité d'Organisation (UO) est un conteneur logique, semblable à un dossier, qui permet de regrouper des objets (utilisateurs, ordinateurs) afin de mieux les organiser et de leur appliquer des règles de sécurité spécifiques.

Il faudra ouvrir "Utilisateurs et ordinateurs Active Directory", puis nous allons créer notre "UO" principale du site.

⚠ : Seul l'OU destiné au service informatique sera en dehors de cet OU racine du site de Paris. Cela permet d'isoler les comptes sensibles pour éviter qu'ils n'héritent des restrictions GPO des utilisateurs standards (comme le blocage USB). De plus, les administrateurs gèrent l'ensemble du domaine, ils ne doivent donc pas dépendre hiérarchiquement d'un seul site géographique. Cela est utile si un nouveau site est créé.

- 1) Cliquez droit sur technova.local
- 2) Nouveau
- 3) Unité d'organisation
- 4) Nom : TECHNOVA-PARIS

Maintenant que vous savez créer un OU, vous devez respecter l'arborescence suivante en respectant les OU et les sous OU.



Si vous avez besoin de supprimer un OU, vous devez faire ceci :

Affichage → Fonctionnalités avancées → [Clique droit sur l'OU souhaité] → Propriété → Objet → Décochez "Protéger l'objet contre les suppressions accidentelles"

⚠ Pensez à ranger Ordinateurs et Serveurs dans leurs OU.

Vous remarquerez que l'OU Informatique est volontairement séparé des utilisateurs classiques afin qu'ils ne bénéficient pas des mêmes GPO qui pourraient les bloquer. Naturellement, ils auront besoin de droits supplémentaires.

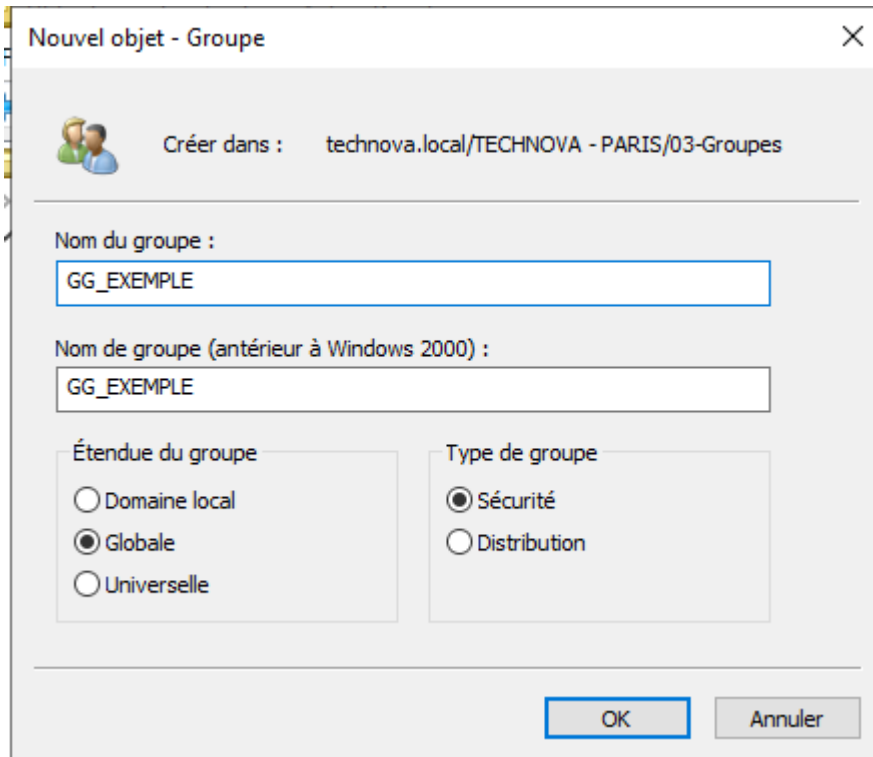
Sous partie 2 : Création des groupes

Si les UO (Unités d'Organisation) servent à ranger tes objets et à leur appliquer des configurations automatiques (GPO), les Groupes sont les badges d'accès qui donnent les permissions.

Nous allons créer 1 groupe par services dans l'OU "04_Groupes". Cela nous permet de savoir créer un groupe. Nous en rajouterons plus tard.

Clique droit → Nouveau → Groupe

Il faudra créer comme ceci. Voici un exemple de création :



Nouvel objet - Groupe

Créer dans : technova.local/TECHNOVA - PARIS/03-Groupes

Nom du groupe :
GG_EXEMPLE

Nom de groupe (antérieur à Windows 2000) :
GG_EXEMPLE

Étendue du groupe

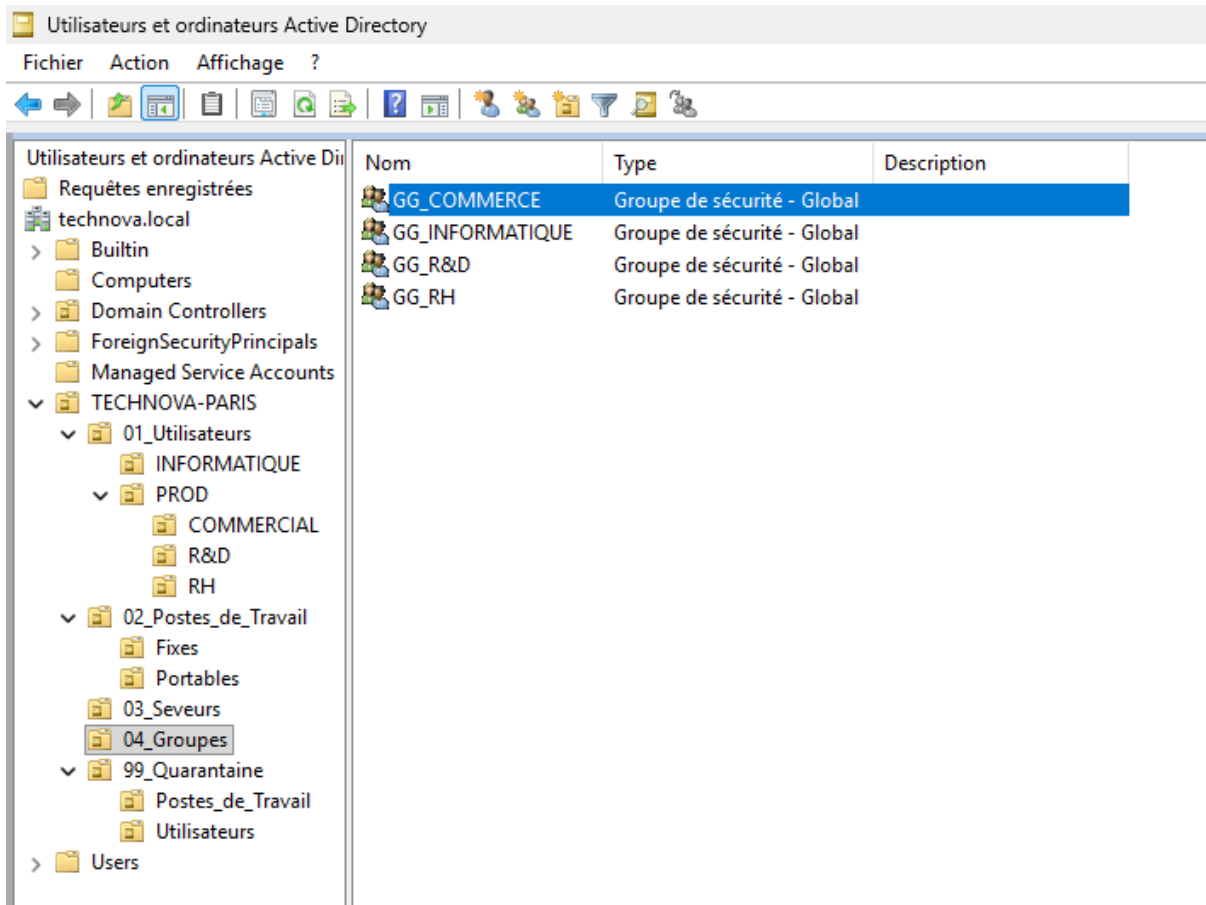
- ☐ Domaine local
- ☒ Globale
- ☐ Universelle

Type de groupe

- ☒ Sécurité
- ☐ Distribution

OK Annuler

Voici à quoi doivent ressembler le résultat :



Sous partie 3 : Ajout des utilisateurs dans les groupes :

Voici la méthode pour ajouter un utilisateur dans un groupe. Nous allons prendre pour exemple aplantier dans le groupe INFORMATIQUE :

Clique droit sur le groupe INFORMATIQUE → Propriétés → Membres → Ajouter → aplantier → Ajouter → Appliquer → Ok

⚠ : Vous ne pouvez pas les ajouter car ils ne sont pas créés. Il faudra revenir sur cette partie après les avoir créées (voir partie 5).

Partie 5 - Création des comptes utilisateurs

Nous devons ensuite créer les comptes utilisateurs afin que les employés puissent accéder à une session sur le domaine technova.local.

Sous partie 1 : Le Profil "Service R&D"

- Comment le créer (UO) : 01_Utilisateurs → R&D → Clique droit → Nouveau → Utilisateur
- Prénom/Nom : Alice Martin
- Login : amartin
- Mot de passe : Nous allons définir un mot de passe par défaut que nous donnerons à Alice. Il n'est pas important qu'il soit fort car il devra être changé dès la première connexion. Pour le générer il faudra se rendre sur <http://srv-web.technova.local>. Un espace est dédié exprès. → rMTk7QLGj5ui
- Groupes à ajouter :
→ Une fois l'utilisateur créé → Clique droit → Propriétés → Membre de → Ajouter → GG_R&D

Sous partie 2 : Le Profil "Service Commerce"

- Comment le créer (UO) : 01_Utilisateurs → Commercial → Clique droit → Nouveau → Utilisateur
- Prénom/Nom : Thomas Durand
- Login : tdurand
- Mot de passe : Nous allons définir un mot de passe par défaut que nous donnerons à Alice. Il n'est pas important qu'il soit fort car il devra être changé dès la première connexion. Pour le générer il faudra se rendre sur <http://srv-web.technova.local>. Un espace est dédié exprès. → Njd2!t!y4a0k
- Groupes à ajouter :
→ Une fois l'utilisateur créé → Clique droit → Propriétés → Membre de → Ajouter → GG_COMMERCE

Sous partie 3 : Le Profil "Service RH"

- Comment le créer (UO) : 01_Utilisateurs → RH → Clique droit → Nouveau → Utilisateur
- Prénom/Nom : Sophie Bernard
- Login : sbernard
- Mot de passe : Nous allons définir un mot de passe par défaut que nous donnerons à Alice. Il n'est pas important qu'il soit fort car il devra être changé dès la première

connexion. Pour le générer il faudra se rendre sur <http://srv-web.technova.local>. Un espace est dédié exprès. → McPHzr84mnw7

- Groupes à ajouter :
→ Une fois l'utilisateur créé → Cliquez droit → Propriétés → Membre de → Ajouter → GG_RH

Sous partie 4 : Le Profil "Service Informatique"

- Comment le créer (UO) : INFORMATIQUE → Utilisateurs_Admin → Cliquez droit → Nouveau → Utilisateur
- Prénom/Nom : Armel Plantier
- Login : aplantier
- Mot de passe : Nous allons définir un mot de passe par défaut que nous donnerons à Alice. Il n'est pas important qu'il soit fort car il devra être changé dès la première connexion. Pour le générer il faudra se rendre sur <http://srv-web.technova.local>. Un espace est dédié exprès. → Wja22B6yjdwr

⚠ : Petite spécification, ce compte sera administrateur :

→ Armel Plantier → Membre de → Ajouter → Administrateur du domaine → Définir le groupe principale → Supprimer utilisateur du domaine

⚠ : Il faudra se déconnecter et se reconnecter.

→ Nous utiliserons toujours ce compte

Partie 6 - Mise en place des partages

Un partage est un dossier situé sur un serveur central que l'on rend accessible à travers le réseau informatique. Il permet à plusieurs utilisateurs de stocker, lire ou modifier des fichiers communs directement depuis leur propre ordinateur, sans avoir à se les envoyer par clé USB ou par email.

Nous allons créer un partage par services. Vous verrez alors à quoi servent réellement les groupes créés précédemment.

Sous partie 1 : Création d'une nouvelle partition sur C:

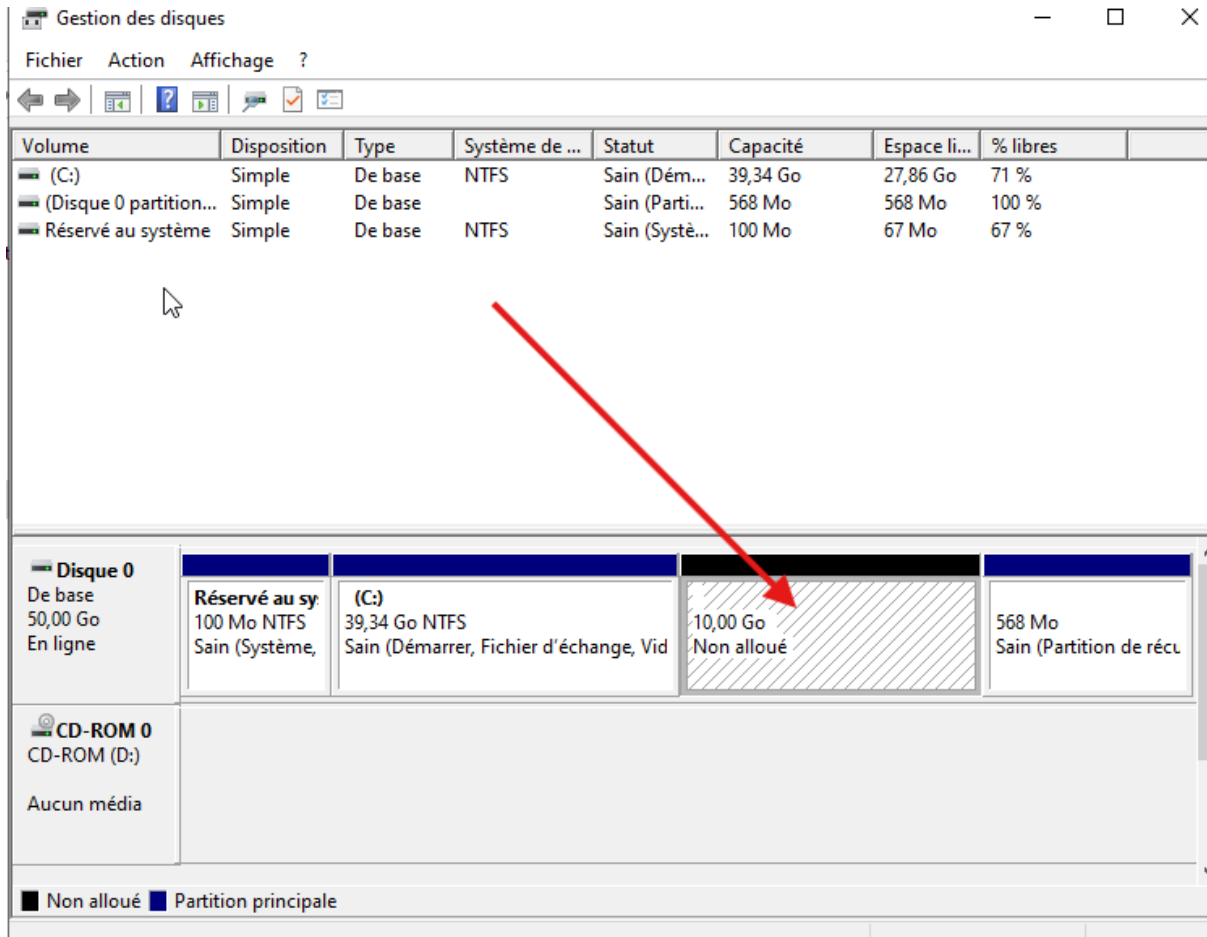


TECHNOVA

Nos partages doivent être séparés de votre disque "C:." ou est installé notre windows. Nous devons alors créer une nouvelle partition afin de les séparer.

Clique droit sur Windows → Gestion des disques → Cliquez droit sur "(C:)" → Réduire le volume → Quantité d'espace à réduire : 10240 mo (10 go) → Réduire

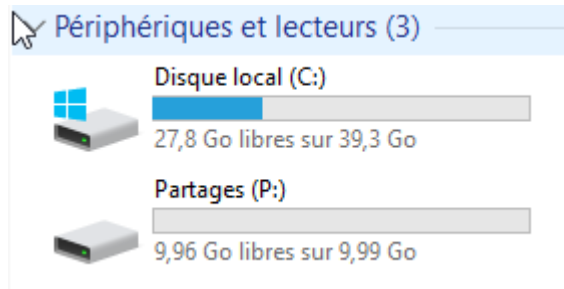
Cela correspond à la taille de notre nouvelle partition.



Il faudra ensuite faire un clic droit sur cette nouvelle partie non alloué puis :

Nouveau volume simple → Suivant → Suivant → Attribuer la lettre "P" puis suivant →
Système de fichier : NTFS puis Nom du volume : Partages → Suivant → Terminer

Une fois que cela est terminé, nous allons créer les partages sur cette nouvelle partition.*



Sous partie 2 : Partage du service Informatique

Nous allons créer le partage dédié au service informatique.

Il faudra respecter l'arborescence suivante :

```
P:\ (Partages)
├── Informatique\
│   ├── Deploy
│   └── Echange
```

Deploy : Ce dossier sera utilisé pour déployer les logiciels notamment via GPO.

Echange : Il s'agit de l'espace d'échange du services informatique.

Pour l'instant nous avons le stricte minimum mais c'est assez pour comprendre le principe. Les dossiers seront évolutifs au fil des procédures.

Passons à présent à la gestion des droits. Nous voulons que uniquement le service informatique ait accès à ce partage.

Voici la méthode pour partager un dossier, et y modifier les droits. Seul le contenu de "Echange" doit pouvoir être modifié. Ni "Informatique" ni "Echange" ne peuvent être modifiés :

Clique droit sur Informatique → Propriété → Partage → Partage avancé → Partager ce dossier → Autorisation → [On supprime tout] et on ajoute GG_INFORMATIQUE en contrôle total.

Ensuite dans l'onglet sécurité → Avancé → [SI BESOIN] Désactiver l'héritage puis Convertir les autorisations héritées en autorisations explicites → [Garder uniquement Administrateur et Système] → Ajouter GG_INFORMATIQUE → S'applique à ce dossier seulement → **Cochez "Lecture et exécution"** → Ok.

Ensuite traitons le dossier échange → Propriété → Sécurité → Avancé :

1. Ajoutez GG_INFORMATIQUE → Type : **Autoriser** → S'applique à : **Ce dossier, les sous-dossiers et les fichiers** → Cochez "Contrôle total".

2. Ajoutez encore GG_INFORMATIQUE → Type : **Refuser** → S'applique à ce dossier seulement → Afficher les autorisations avancées → Cochez uniquement "suppression".

Passons à la configuration de "Deploy" qui sera le dossier pour les déploiement de logiciel via GPO. Il aura la particularité d'être un partage caché pour les utilisateurs.

Propriétés → Sécurité → Avancé → Ajouter → Ajoutez "Ordinateurs du domaine" → Modifier → Lecture et exécution, Affichage du contenu, Lecture.

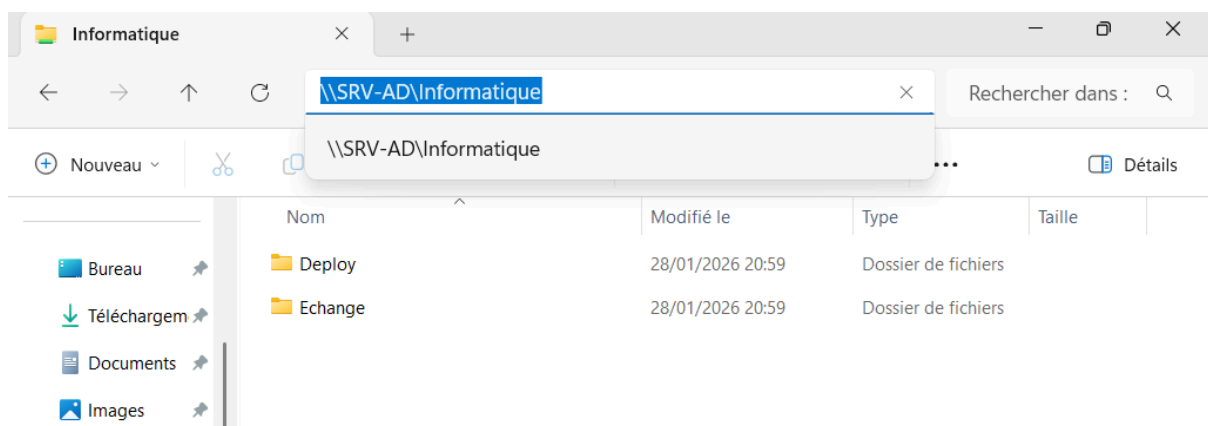
Nous allons mettre en place le partage caché. Toujours sur "Deploy" il faudra aller dans l'onglet partage puis :

Partage avancé → Partager ce dossier → Nom du partage : Deploy\$ → Autorisations → Supprimez "Tout le monde" et ajouter "Ordinateurs du domaine" et appliquer "Lecture" uniquement → Ajoutez également "Admins du domaine" en contrôle total.

Le partage est configuré sur : \\SRV-AD\Informatique

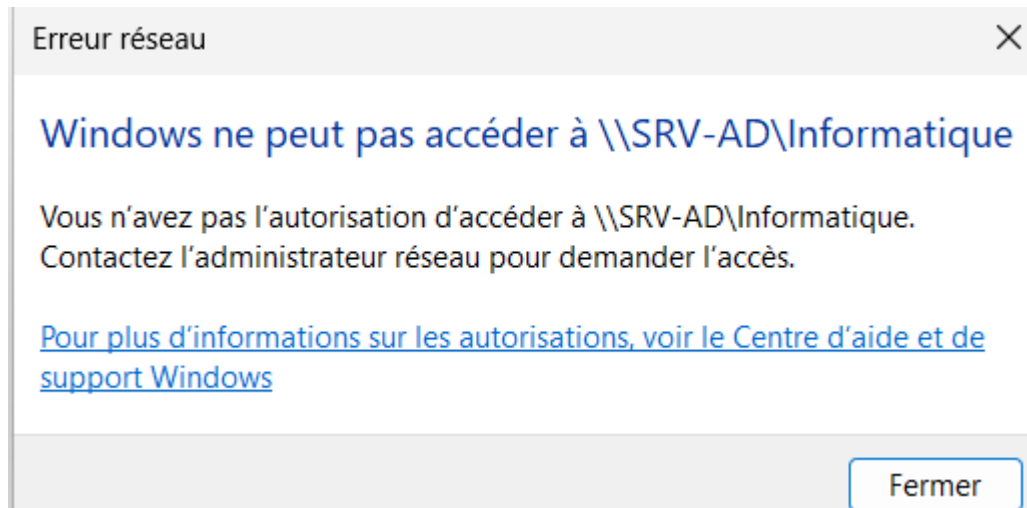
On peut tenter de s'y connecter avec un client (avec un compte du groupe informatique) :

Explorateur de fichiers → \\SRV-AD\Informatique



On ne doit normalement pas pouvoir supprimer Informatique et Échange mais à l'intérieur de échange on doit pouvoir ajouter modifier et supprimer des fichiers. Attention, les comptes admin peuvent supprimer.

Il faudra également vérifier que les utilisateurs hors du groupe INFORMATIQUE n'aient pas accès à ce partage.



Sous partie 3 : Partage des autres services

Il faudra reprendre exactement la même méthode en utilisant le groupe correspondant. Voici l'exemple d'arborescence.

```
P:\ (Partages)
├── R&D(Par exemple)\
│   └── Echange
```

Clique droit sur R&D → Propriété → Partage → Partage avancé → Partager ce dossier → Autorisation → [On supprime tout] et on ajoute GG_R&D en contrôle total.

Ensuite dans l'onglet sécurité → Avancé → [SI BESOIN] Désactiver l'héritage puis Convertir les autorisations héritées en autorisations explicites → [Garder uniquement Administrateur et Système] → Ajouter GG_R&D → S'applique à ce dossier seulement → **Cochez "Lecture et exécution"** → Ok.

Ensuite traitons le dossier échange → Propriété → Sécurité → Avancé :

3. Ajoutez GG_R&D → Type : **Autoriser** → S'applique à : **Ce dossier, les sous-dossiers et les fichiers** → Cochez "Contrôle total".
4. Ajoutez encore GG_R&D → Type : **Refuser** → S'applique à ce dossier seulement → Afficher les autorisations avancées → Cochez uniquement "suppression".

Partie 7 - Déploiement automatique des partages sur les postes de travail

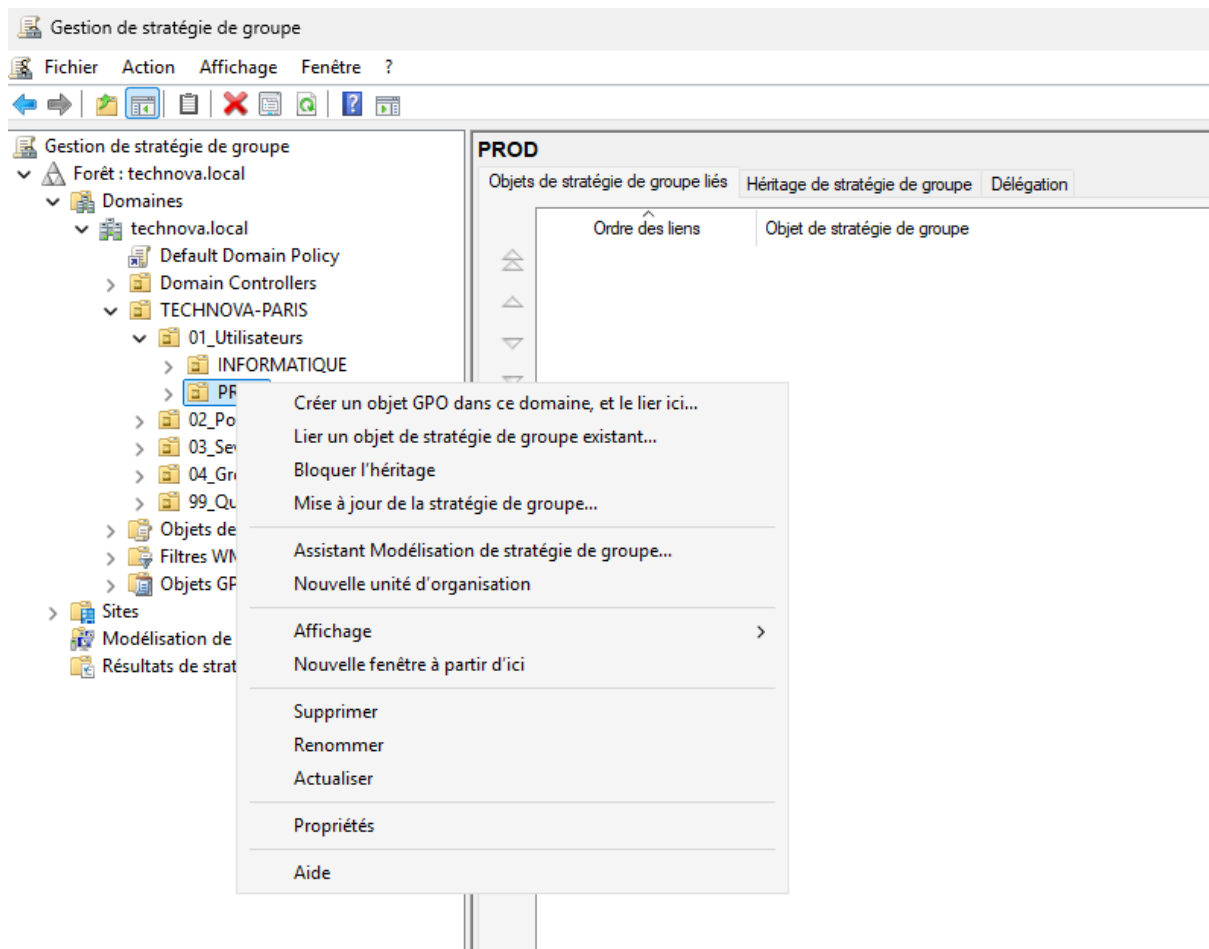


TECHNOVA

Précédemment, nous avons entré le chemin dans l'explorateur de fichier afin d'accéder au partage. Pour éviter cela (surtout pour les utilisateurs), nous allons mettre en place un lecteur réseau déployé par GPO (Gestion de stratégie de groupe).

Sous partie 1 : Configuration de la GPO

Il faudra ouvrir "Gestion de stratégie de groupe" puis ensuite créer la GPO à sur notre OU "PROD" dans "01_Utilisateurs".

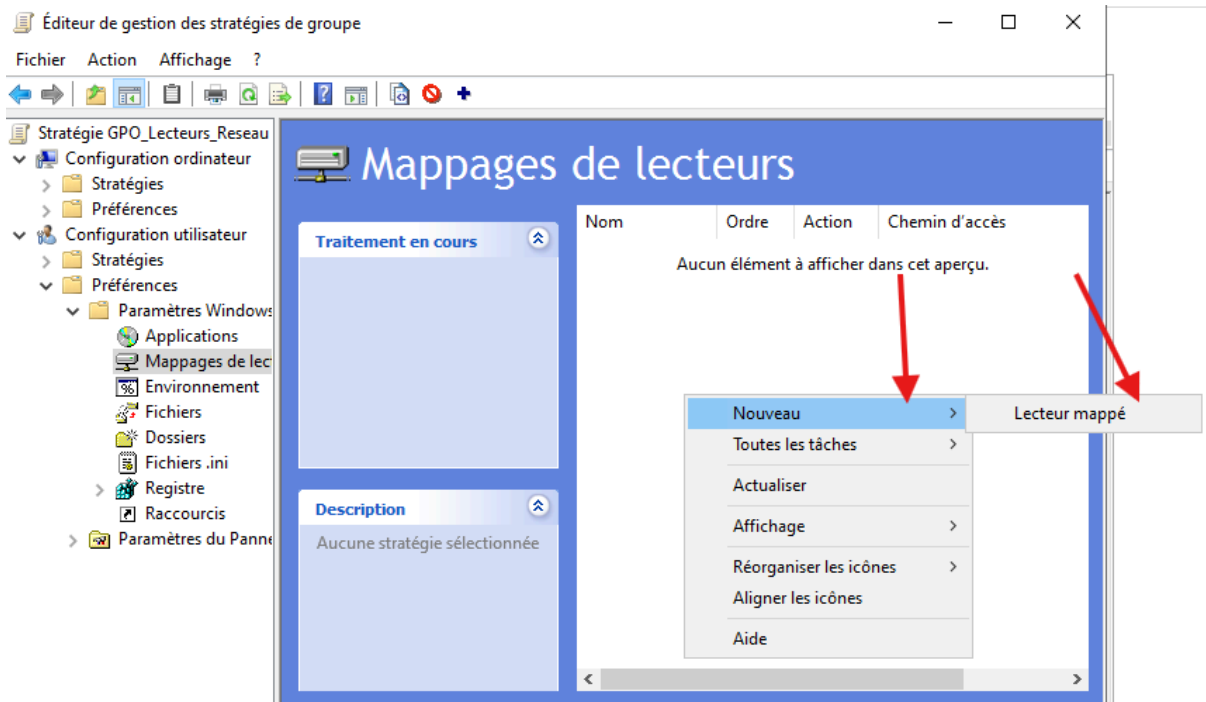


Nom : GPO_Lecteurs_Reseau

Il faudra ensuite la modifier en respectant la configuration suivante :


Configuration utilisateur → Préférences → Paramètres Windows → Mappages de lecteurs.

Il faudra en ajouter un :



Commençons avec le partage Informatique :

- 1) Emplacement : \\SRV-AD\Informatique
- 2) Reconnecter : Cochez la case
- 3) Libellé en tant que : Informatique
- 4) Lettre de lecteur : I

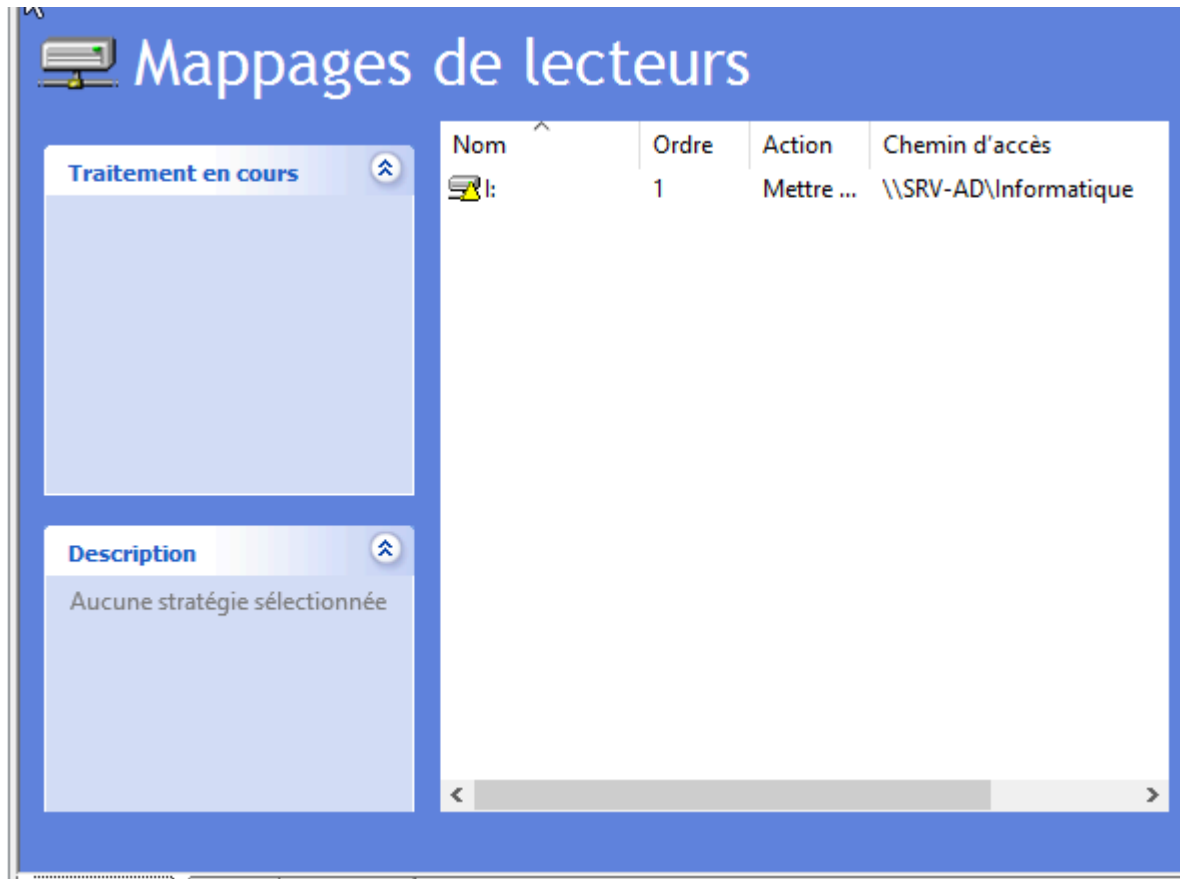
 : Attention à sélectionner des lettres qui ne sont pas déjà utilisés (Notamment C par exemple)

Nous allons ensuite devoir spécifier que ce lecteur est uniquement pour le groupe GG_INFORMATIQUE :

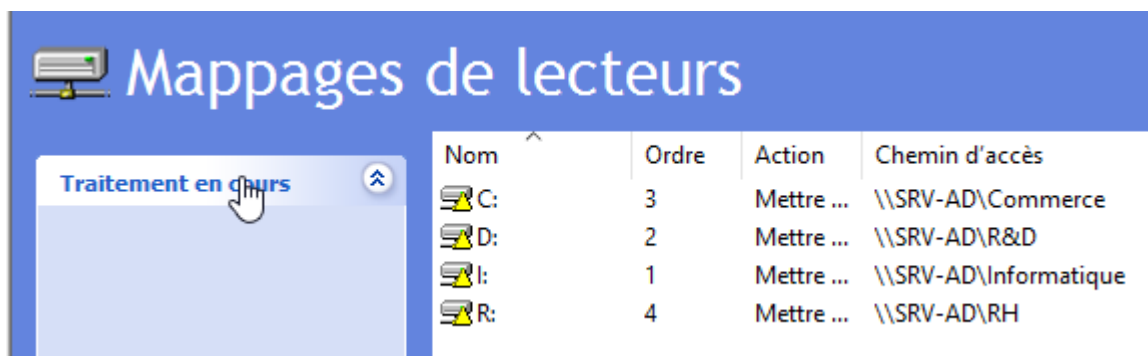
Dans l'onglet "Commun" :

- 1) Cochez la case Ciblage au niveau de l'élément puis cliquez sur le bouton Ciblage → Nouvel élément → Groupe de sécurité. Cliquez sur ... (les trois petits points) à côté de "Groupe". Cherchez et sélectionnez GG_INFORMATIQUE. Vérifiez que la case "Utilisateur dans le groupe" est bien sélectionnée.

Vous pouvez voir l'ajout :



⚠ : Il faudra suivre la même méthode pour ajouter les autres partages créés précédemment. Le résultat doit être le suivant :



La configuration est terminée. Notre GPO est déjà lié à l'OU Utilisateurs comme nous l'avons créé dessus. Il nous reste plus qu'à tester.

⚠ : On peut dupliquer la GPO sur l'ou "Informatique" sinon cela ne va pas fonctionner.

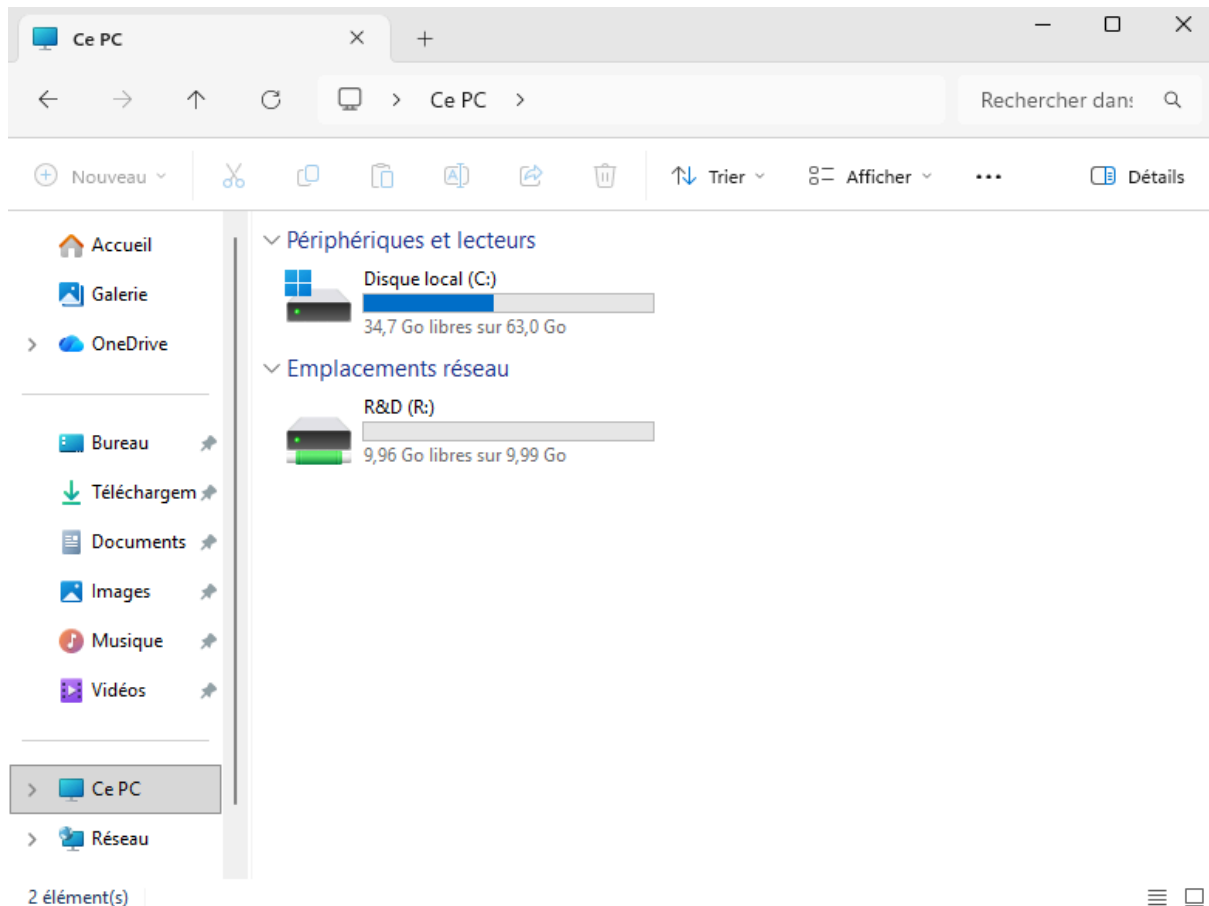
Sous partie 2 : Tests de la GPO

Nous allons nous connecter sur un PC avec aplantier qui est membre du groupe GG_R&D

Normalement le changement doit apparaître, si ce n'est pas le cas il faudra faire la commande suivante :

```
gpupdate /force
```

Cela doit également fonctionner avec une déconnexion et reconnexion de session.



On doit tester sur l'ensemble de nos utilisateurs et ils doivent bien retrouver leurs partages.

Sous partie 3 : Épingler à l'accès rapide le partage via un script PowerShell contenu dans la GPO

Maintenant que nos utilisateurs accèdent à leurs partages nous allons leur rendre la tâche plus simple en épinglant ce partage à l'accès rapide. Il faudra créer un script PowerShell.

il faudra créer le script au nom de Epingler_Partages.ps1 et y ajouter le code suivant :

```
# 1. Petite pause pour laisser à la GPO le temps de mapper les lecteurs dans le registre  
Start-Sleep -Seconds 5
```




```
# 2. On prépare l'outil d'épinglage
$Shell = New-Object -ComObject Shell.Application

# 3. On va lire directement dans le registre au lieu d'utiliser
Get-PSDrive
# C'est LA clé pour contourner le problème des comptes administrateurs
$RegDrives = Get-ChildItem -Path "HKCU:\Network" -ErrorAction
SilentlyContinue

if ($RegDrives) {
    foreach ($Drive in $RegDrives) {
        # On récupère le chemin UNC réel (Ex: \\Serveur\Partage)
        # derrière la lettre
        $UNCPath = (Get-ItemProperty -Path $Drive.PSPath -Name
"RemotePath" -ErrorAction SilentlyContinue).RemotePath

        if ($UNCPath) {
            # On demande à Windows d'épingler le chemin UNC plutôt que
            # la lettre virtuelle
            $Folder = $Shell.Namespace($UNCPath)

            if ($null -ne $Folder) {
                try {
                    $Folder.Self.InvokeVerb("pinto home")
                } catch {
                    # Capture silencieuse des erreurs d'interface
                }
            }
        }
    }
}
```

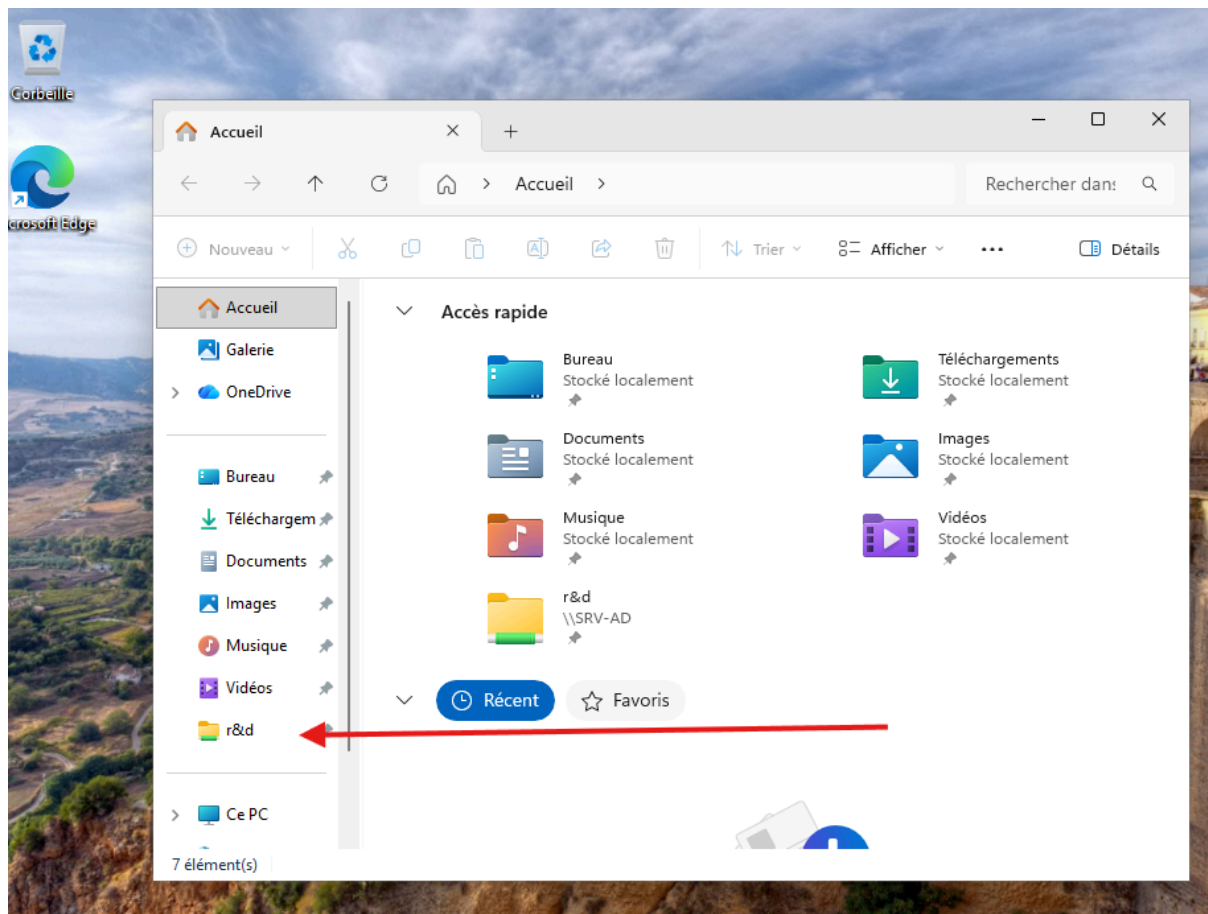
Placez le script dans : \\Srv-ad\sysvol\technova.local\scripts

Au besoin ajouter "Admins du domaine" en contrôle total.

Nous allons modifier notre GPO "GPO_Lecteurs_Reseau".

Configuration utilisateur → Stratégie → Paramètres Windows → Scripts ouverture/fermeture
→ Ouverture de session → Scripts Powershell → Ajouter → Parcourir → Ajoutez le script et
validez.

Au besoin faites un "gpupdate /force" sur le client. Le résultat doit être le suivant :



⚠ : Vous devez avoir essayé avec les autres utilisateurs pour voir s'ils ont bien leurs partages. Attention le dossier peut mettre du temps avant d'être mis dans l'accès rapide et cela est volontaire.

Partie 8 - Familiarisation avec les GPO

Nous n'avons pas beaucoup utilisé de GPO, alors nous allons en créer certaines qui sont basiques.

Sous partie 1 : Déploiement de logiciel (.msi) par GPO

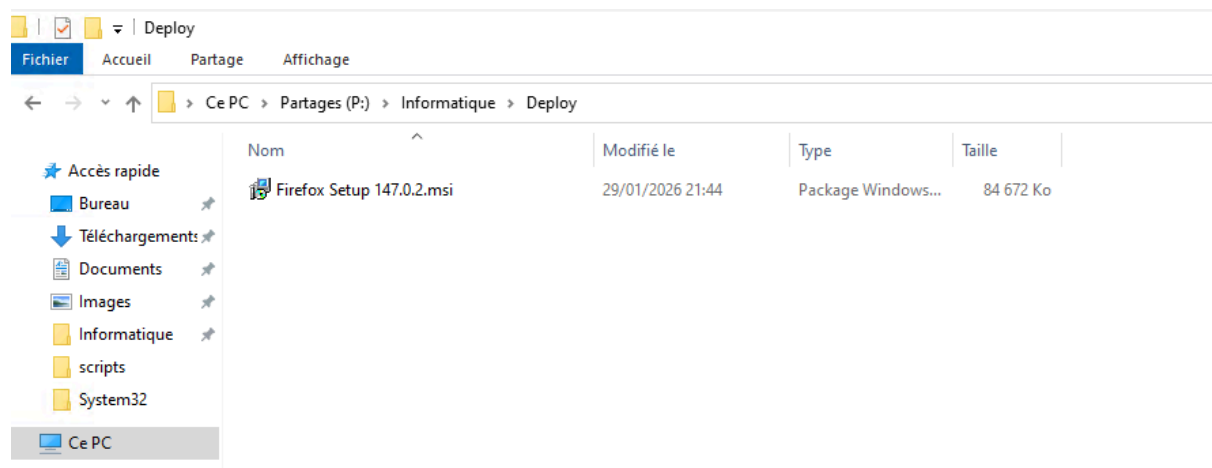
Nous allons utiliser le navigateur FireFox. Il nous faudra le fichier d'installation en .msi.

Vous pouvez le récupérer via ce lien /

<https://www.firefox.com/fr/browsers/enterprise/#download>



Il faudra placer le fichier dans Informatique → Deploy



Configurons ensuite la GPO :

Ouvrir Gestion de stratégie de groupe → Créer la GPO sur l'OU 02_Postes_de_Travail →
Nom : GPO_Deploy_Logiciel

Configuration ordinateur → Stratégies → Paramètres du logiciel → Installation de logiciel →
Nouveau → Package → On sélectionne notre fichier FireFox sur le partage
\\SRV-AD\Deploy\$

Notre fichier est correctement importé, nous allons tester sur TNV-01 avec amartin. Il faudra utiliser gpupdate/force puis redémarrer le poste. Le redémarrage sera un peu plus long que d'habitude.

Vous devez voir ce message :

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

La mise à jour de la stratégie d'ordinateur s'est terminée sans erreur.

Les avertissements suivants ont été rencontrés lors du traitement de la stratégie
de l'ordinateur :

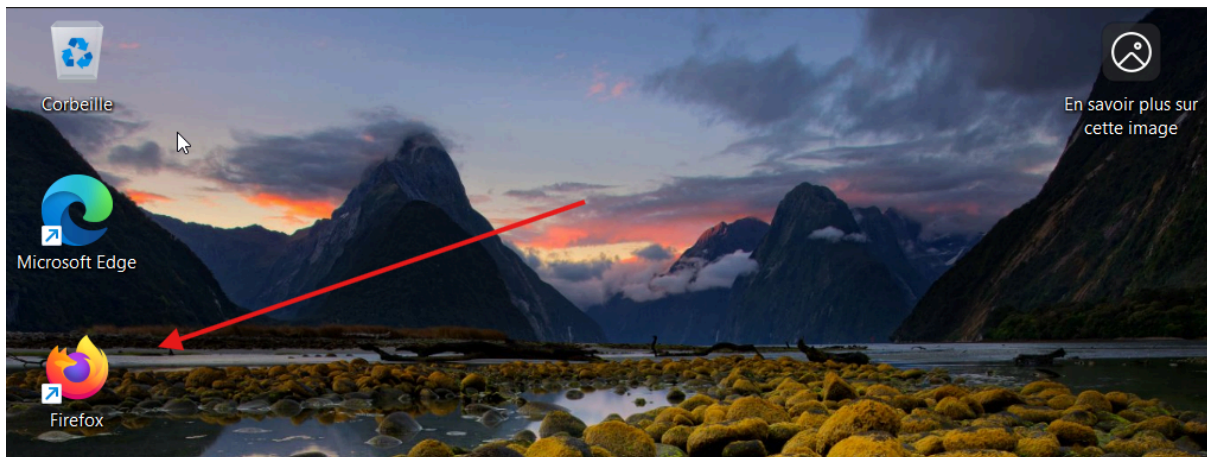
L'extension côté client de la stratégie de groupe Software Installation n'a pas pu
appliquer un ou plusieurs paramètres car les modifications doivent être traitées
avant le démarrage système ou la connexion utilisateur. Le système attendra la fin
complète du traitement de la stratégie de groupe avant de procéder au prochain dé
marrage ou à la prochaine connexion pour cet utilisateur. Ceci peut entraîner un r
alentissement du démarrage et des performances de démarrage du système.
La mise à jour de la stratégie utilisateur s'est terminée sans erreur.

Pour plus de détails, ouvrez le journal des événements ou exécutez GPRESULT /H GPR
eport.html depuis la ligne de commande pour accéder aux résultats de la stratégie
de groupe.

Certaines stratégies d'ordinateurs activées peuvent uniquement être
exécutées pendant le démarrage.

OK pour redémarrer ? (O/N)
```

⚠ : Si cela ne marche pas vérifiez que votre ordinateur est bien dans l'OU
"Poste_de_Travail"



Sous partie 2 : Ajout d'un fond d'écran par GPO

Il faudra placer le fichier dans C:\Windows\SYSVOL\sysvol\technova.local\scripts

Nous allons créer la GPO sur l'OU "01_Utilisateurs"

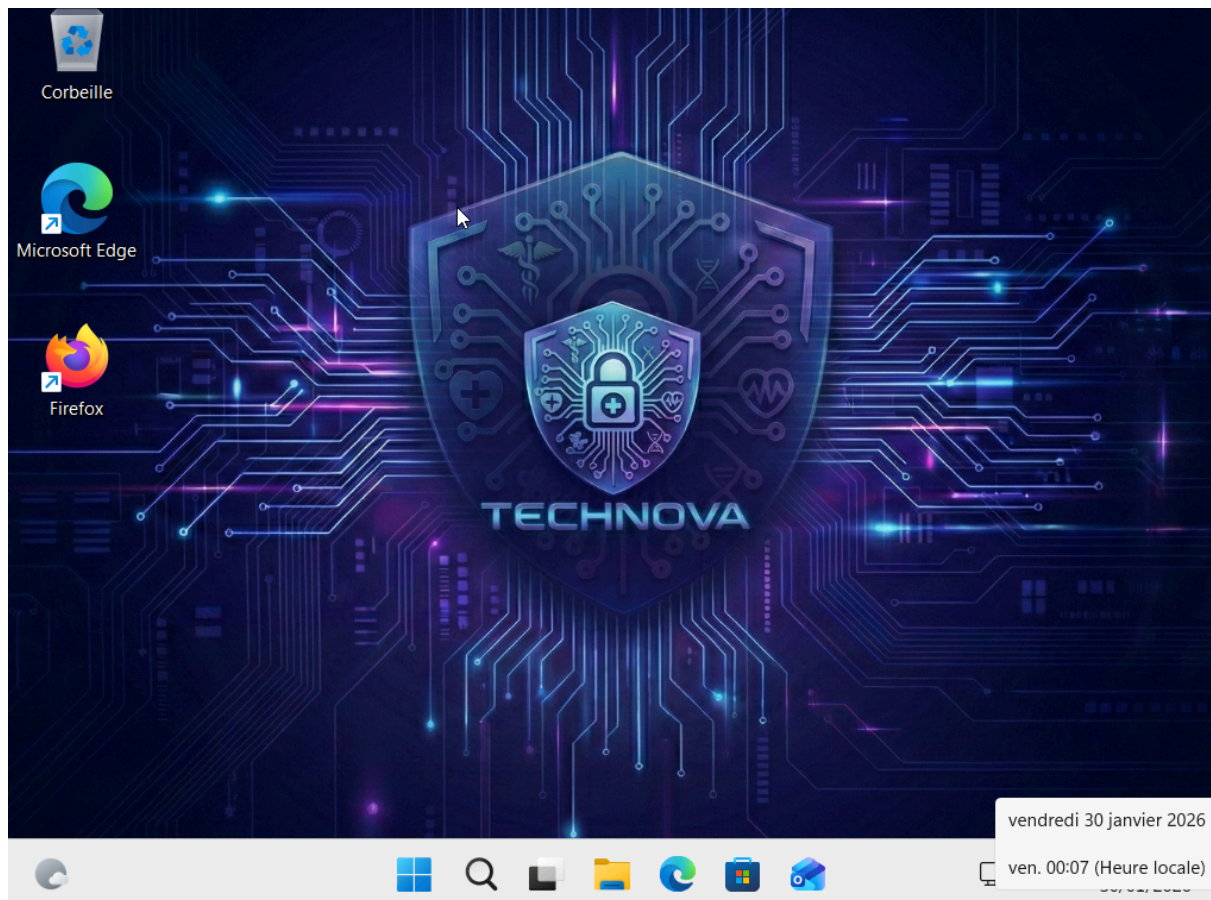
Nom : GPO_Wallpaper_Technova

Configuration Utilisateurs → Stratégies → Modèles d'administration → Bureau → Bureau →
Papier peint du Bureau → Activer → Nom du papier peint :
\\SRV-AD\NETLOGON\technova_wallpaper.png → Style du papier peint : Remplir



TECHNOVA

Sur un client on fait un gpupdate, on déconnecte la session et on la reconnecte puis :



⚠ : A savoir que les GPO utilisateurs GPO s'appliquera toute seule à la prochaine ouverture de session (ou après 90 minutes).