

# PROJET EXPERTY

BTS SIO 2

KUNTZ MATT-THÉO

MONTERASTELLI COLIN

# SOMMAIRE

INTRODUCTION .....3

CONTROLEUR DE DOMAINE .....4

SCRIPTS.....16

CONCLUSION.....38

BTS SIO 2

# INTRODUCTION

L'entreprise EXPERTY souhaite moderniser son infrastructure informatique pour accompagner sa croissance. Elle projette de mettre en place une nouvelle architecture réseau comprenant des serveurs Windows avec un domaine experty.local, deux contrôleurs de domaine redondés et un ensemble de services tels que DNS, DHCP et DFS.

L'objectif est d'assurer une gestion efficace et sécurisée des utilisateurs, en appliquant les bonnes pratiques de sécurité (AGDLP, RAID) et en respectant les préconisations de l'ANSSI pour les mots de passe. L'entreprise souhaite également automatiser le mappage des lecteurs réseau, contrôler l'accès aux ressources et garantir la disponibilité des services critiques (impression, fichiers) tout en mettant en place des profils itinérants pour les utilisateurs.

# CONTROLEUR DE DOMAINE

## 1. Création du domaine "experty.local" et contrôleurs de domaine (DC)

### Étape 1.1 : Installation de Windows Server

Préparer deux serveurs :

Assurez-vous que deux serveurs sont configurés avec une installation de Windows Server 2016 ou supérieure. Ces serveurs serviront de contrôleurs de domaine redondants.

Connectez-les au réseau local et configurez une adresse IP fixe pour chacun.

Configurer le RAID pour la redondance des données :

Lors de l'installation du système d'exploitation, configurez le RAID.

Utilisez RAID 1 pour les disques du système (pour assurer une redondance totale en cas de panne de disque).

Utilisez RAID 5 pour les volumes de données, ce qui permettra une protection des données tout en optimisant l'espace disque.

Vérifiez que les volumes sont bien reconnus par le système.

### Étape 1.2 : Installation des services AD DS (Active Directory Domain Services)

1. Ouvrir le Server Manager sur le premier serveur (DC01) :

Aller dans **Ajouter des rôles et fonctionnalités**.

Sélectionner **Installation basée sur un rôle ou une fonctionnalité**.

Choisir le serveur sur lequel vous voulez installer les services (DC01).

Sélectionner le rôle Active Directory Domain Services (AD DS) et valider l'installation.

2. Configurer le domaine "experty.local" :

Une fois l'installation d'AD DS terminée, une notification apparaît vous demandant de promouvoir ce serveur en tant que contrôleur de domaine.

Cliquer sur Promouvoir ce serveur en contrôleur de domaine.

Sélectionner Ajouter une nouvelle forêt, puis entrez experty.local comme nom de domaine racine.

Sélectionner le niveau fonctionnel de la forêt et du domaine à Windows Server 2016 (ou supérieur).

Configurer un mot de passe pour le Directory Services Restore Mode (DSRM), qui servira en cas de récupération de l'Active Directory.

Redémarrer le serveur une fois la promotion effectuée.

### Étape 1.3 : Promotion du second contrôleur de domaine (DCo2)

1. Répéter les étapes précédentes sur le second serveur (DCo2).

Ouvrir Server Manager, installer AD DS, et choisir de promouvoir ce serveur en tant que contrôleur de domaine supplémentaire pour le domaine expert.local.

Ceci permettra une redondance en cas de défaillance du premier contrôleur de domaine.

2. Vérifier la synchronisation des deux contrôleurs de domaine :

Utiliser la commande Repadmin /replsummary dans l'invite de commande sur l'un des contrôleurs pour vérifier que la réplication est bien en place entre DCo1 et DCo2.

### Étape 1.4 : Politique de mot de passe selon les préconisations de l'ANSSI

Créer une stratégie de groupe (GPO) appliquée au domaine pour imposer des mots de passe complexes (12 caractères minimum, expiration tous les 90 jours, verrouillage après 5 tentatives échouées).

### Étape 1.5 : Application des bonnes pratiques AGDLP (Accounts, Global, Domain Local, Permissions)

Créer des groupes globaux pour les utilisateurs par service (exemple : GG\_IT pour le service informatique) et des groupes de domaine locaux pour les permissions d'accès aux ressources partagées.

## 2. Politique de mot de passe conforme aux préconisations de l'ANSSI

### 1. Créer une stratégie de groupe (GPO) pour les mots de passe :

Ouvrir Group Policy Management sur DCo1.

Créer une nouvelle GPO et nommez-la « Politique de sécurité des mots de passe ».

Lier cette GPO au domaine experty.local pour qu'elle s'applique à tous les utilisateurs.

### 2. Configurer la politique de mot de passe :

Dans la GPO, naviguer vers Computer Configuration > Politiques > Windows Settings > Security Settings > Account Policies > Password Policy.

Longueur minimale du mot de passe : 12 caractères.

Complexité des mots de passe : activée (exige des majuscules, minuscules, chiffres et caractères spéciaux).

Durée de validité du mot de passe : 90 jours (exige que les utilisateurs changent leurs mots de passe tous les trois mois).

Historique des mots de passe : conserver les 5 derniers mots de passe.

Verrouillage des comptes après tentatives échouées : bloquer l'utilisateur après 5 tentatives échouées, pendant 30 minutes.

### 3. Vérifier que la GPO s'applique correctement :

Exécuter la commande gpupdate /force sur les postes clients pour forcer l'application de la stratégie.

### 3. Application des bonnes pratiques AGDLP (Account, Global, Domain Local, Permissions)

#### 1. Créer des groupes globaux pour les utilisateurs :

Ouvrir Active Directory Users and Computers.

Créer des groupes globaux dans l'OU (Unité Organisationnelle) appropriée pour regrouper les utilisateurs par fonction. Par exemple :

GG\_IT pour le service informatique.

GG\_Finance pour le service financier.

GG\_RH pour le service des ressources humaines.

#### 2. Créer des groupes de domaine locaux pour les ressources :

Dans Active Directory User, créer des groupes de domaine locaux pour attribuer des droits d'accès aux ressources partagées. Exemple :

DL\_Fichiers\_IT pour les fichiers partagés du service informatique.

DL\_Imprimantes\_Finance pour l'accès aux imprimantes du service financier.

#### 3. Attribuer les permissions sur les dossiers et ressources partagées :

Sur le serveur de fichiers, assigner les groupes de domaine locaux aux ressources avec les permissions adéquates.

Par exemple, attribuer Lecture et Écriture à DL\_Fichiers\_IT pour le dossier partagé \\experty.local\\informatique.



## 4. Configuration des dossiers personnels avec quotas

### Étape 4.1 : Création des dossiers personnels pour chaque utilisateur

1. **Créer un dossier partagé pour les profils utilisateurs** sur DCo1 :
  - Ouvrir l'**Explorateur de fichiers** et créer un répertoire nommé **Profiless** sur un volume de données dédié.
  - Partager ce dossier sur le réseau avec les permissions suivantes :
    - **Tous les utilisateurs** : accès en **lecture** uniquement.
    - **Administrateurs** et **Service informatique** : **Contrôle total**.
2. **Configurer les permissions NTFS** :
  - Aller dans les **propriétés du dossier Profiless** et dans l'onglet **Sécurité** :
    - Les utilisateurs doivent avoir **Contrôle total** uniquement sur leur propre dossier.
    - Le **service informatique** doit avoir **Contrôle total** sur tous les dossiers.

### Étape 4.2 : Mise en place des quotas (1 Go par utilisateur)

1. **Installer et configurer le File Server Resource Manager (FSRM)** :
  - Ouvrir **Server Manager** sur DCo1 et installer le rôle **File Server Resource Manager (FSRM)**.
  - Une fois installé, ouvrir **FSRM** et aller dans **Quota Management > Create Quota**.
  - Sélectionner le répertoire **Profiless** et créer un quota de **1 Go par utilisateur**.
  - Configurer une alerte pour notifier les utilisateurs et l'administrateur lorsque l'utilisation du quota atteint **90%** (soit **900 Mo**).

## 5. Configuration des stratégies de groupe pour les utilisateurs (GPO)

### Étape 5.1 : Mappage automatique des lecteurs réseau

1. **Créer une nouvelle GPO pour le mappage des lecteurs :**
  - Dans **Group Policy Management**, créer une nouvelle GPO nommée « Mappage des lecteurs réseau ».
  - Lier cette GPO au domaine ou à une OU spécifique (comme **Utilisateurs**).
2. **Configurer les lecteurs réseau dans la GPO :**
  - Aller dans **User Configuration > Preferences > Windows Settings > Drive Maps**.
  - Ajouter trois nouvelles entrées pour mapper les lecteurs réseau suivants :
    - **Lecteur T** : mappé à \\DCo1\\Tous (accessible à tous les utilisateurs).
    - **Lecteur P** : mappé à \\DCo1\\Profiles\$\\%username% pour les dossiers personnels.
    - **Lecteur I** : mappé à \\DCo1\\Informatique (pour le service informatique).

### Étape 5.2 : Configuration du fond d'écran d'entreprise

1. **Déployer un fond d'écran standard pour tous les utilisateurs :**
  - Créer une image du logo de l'entreprise dans un dossier partagé (exemple : \\DCo1\\logos\\wallpaper.jpg).
  - Dans la GPO, aller dans **User Configuration > Politiques > Administrative Templates > Desktop > Desktop Wallpaper**.
  - Indiquer l'emplacement de l'image : \\DCo1\\logos\\wallpaper.jpg.
2. **Empêcher les utilisateurs de modifier leur fond d'écran :**
  - Toujours dans la même GPO, désactiver l'accès aux options de personnalisation via **User Configuration > Politiques > Control Panel > Personalization**.

### Étape 5.3 : Restriction des privilèges administratifs

1. **Empêcher les utilisateurs d'être administrateurs de leurs postes :**

- Dans la GPO, naviguer vers **User Configuration > Politiques > Administrative Templates > Control Panel > User Accounts**.
- Activer l'option « Empêcher les utilisateurs standard de devenir administrateurs sur leurs machines ».

## 2. Bloquer la modification des paramètres de la carte réseau :

- Toujours dans la GPO, aller dans **Computer Configuration > Politiques > Windows Settings > Security Settings > Network Configuration** et bloquer les modifications des paramètres réseau.

### Étape 5.4 : Mise en veille de l'écran

1. **Configurer la mise en veille automatique des écrans après 15 minutes d'inactivité :**
  - Dans la GPO, aller à **User Configuration > Politiques > Administrative Templates > Control Panel > Power Options**.
  - Définir la mise en veille après **15 minutes** d'inactivité.

### Étape 5.5 : Bloquer l'accès à l'invite de commande

1. **Empêcher l'accès à l'invite de commande pour les utilisateurs :**
  - Dans la GPO, naviguer vers **User Configuration > Administrative Templates > System**.
  - Activer l'option **Interdire l'accès à l'invite de commande**.

### Étape 5.6 : Définir la page d'accueil par défaut dans le navigateur Firefox

1. **Définir le site intranet comme page d'accueil par défaut :**
  - Dans la GPO, aller à **User Configuration > Preferences > Control Panel Settings > Internet Settings > Firefox**.
  - Configurer la page d'accueil par défaut sur <http://intranet.experty.local>.

## 4. Configuration des dossiers personnels avec quotas

### Étape 4.1 : Création des dossiers personnels pour chaque utilisateur

#### 3. Créer un dossier partagé pour les profils utilisateurs sur DCo1 :

- Ouvrir l'**Explorateur de fichiers** et créer un répertoire nommé **Profiles\$** sur un volume de données dédié.
- Partager ce dossier sur le réseau avec les permissions suivantes :
  - **Tous les utilisateurs** : accès en **lecture** uniquement.
  - **Administrateurs** et **Service informatique** : **Contrôle total**.

#### 4. Configurer les permissions NTFS :

- Aller dans les **propriétés du dossier Profiles\$** et dans l'onglet **Sécurité** :
  - Les utilisateurs doivent avoir **Contrôle total** uniquement sur leur propre dossier.
  - Le **service informatique** doit avoir **Contrôle total** sur tous les dossiers.

### Étape 4.2 : Mise en place des quotas (1 Go par utilisateur)

#### 2. Installer et configurer le File Server Resource Manager (FSRM) :

- Ouvrir **Server Manager** sur DCo1 et installer le rôle **File Server Resource Manager (FSRM)**.
- Une fois installé, ouvrir **FSRM** et aller dans **Quota Management > Create Quota**.
- Sélectionner le répertoire **Profiles\$** et créer un quota de **1 Go par utilisateur**.
- Configurer une alerte pour notifier les utilisateurs et l'administrateur lorsque l'utilisation du quota atteint **90%** (soit **900 Mo**).

## 5. Configuration des stratégies de groupe pour les utilisateurs (GPO)

### Étape 5.1 : Mappage automatique des lecteurs réseau

#### 3. Créer une nouvelle GPO pour le mappage des lecteurs :

- Dans **Group Policy Management**, créer une nouvelle GPO nommée « Mappage des lecteurs réseau ».

- Lier cette GPO au domaine ou à une OU spécifique (comme **Utilisateurs**).
- 4. **Configurer les lecteurs réseau dans la GPO :**
  - Aller dans **User Configuration > Preferences > Windows Settings > Drive Maps**.
  - Ajouter trois nouvelles entrées pour mapper les lecteurs réseau suivants :
    - **Lecteur T** : mappé à \\DCo1\\Tous (accessible à tous les utilisateurs).
    - **Lecteur P** : mappé à \\DCo1\\Profiles\$\\%username% pour les dossiers personnels.
    - **Lecteur I** : mappé à \\DCo1\\Informatique (pour le service informatique).

#### Étape 5.2 : Configuration du fond d'écran d'entreprise

- 3. **Déployer un fond d'écran standard pour tous les utilisateurs :**
  - Créer une image du logo de l'entreprise dans un dossier partagé (exemple : \\DCo1\\logos\\wallpaper.jpg).
  - Dans la GPO, aller dans **User Configuration > Politiques > Administrative Templates > Desktop > Desktop Wallpaper**.
  - Indiquer l'emplacement de l'image : \\DCo1\\logos\\wallpaper.jpg.
- 4. **Empêcher les utilisateurs de modifier leur fond d'écran :**
  - Toujours dans la même GPO, désactiver l'accès aux options de personnalisation via **User Configuration > Politiques > Control Panel > Personalization**.

#### Étape 5.3 : Restriction des privilèges administratifs

- 3. **Empêcher les utilisateurs d'être administrateurs de leurs postes :**

### 6. Configuration des profils itinérants

- 1. **Activer les profils itinérants pour tous les utilisateurs :**
  - Dans la GPO, aller à **Computer Configuration > Politiques > Administrative Templates > System > User Profiles**.
  - Indiquer le chemin du dossier où seront stockés les profils itinérants : \\DCo1\\Profiles\$\\%username%.
  - Cela permet aux utilisateurs de retrouver leur environnement sur n'importe quel poste du réseau.

---

## 7. Configuration du service DNS

1. Installation du rôle DNS sur les contrôleurs de domaine :
  - Sur DCo1 et DCo2, installer le rôle DNS via Server Manager.
  - Configurer deux zones DNS :
    - intranet.experty.local pour l'intranet interne.
    - [www.experty.local](http://www.experty.local) pour le site web local.
2. Ajouter les enregistrements DNS nécessaires pour les services (A records, CNAME, etc.).

---

## 8. Service DHCP redondé (80/20)

1. Configurer les serveurs DHCP sur DCo1 et DCo2 :
  - Installer le rôle DHCP sur les deux serveurs.
  - Configurer un plan d'adressage IP pour le réseau.
2. Répartir les plages IP en 80/20 pour assurer la redondance :
  - Sur DCo1, attribuer 80 % des adresses.
  - Sur DCo2, attribuer les 20 % restants.

---

## 9. Serveur de fichiers (DFS) et gestion de l'espace partagé

1. Configurer un espace de noms DFS pour centraliser les partages réseau :
  - Créer un espace de noms DFS nommé \experty.local\partage.
  - Ajouter les partages réseau dans cet espace pour simplifier l'accès.
2. Appliquer les bonnes pratiques AGDLP pour les permissions d'accès sur les fichiers.

---

## 10. Service d'impression

1. Installation de l'imprimante via GPO :
  - Configurer une imprimante réseau sur le serveur d'impression.

- Distribuer cette imprimante à tous les utilisateurs via une GPO.
  - Configurer l'impression noir et blanc recto-verso par défaut.
2. Attribuer des priorités d'accès pour les responsables de service.

# SCRIPTS



## Création des groupes selon la méthode AGDLP

```
# Définir la structure de base
```

```
$ouPath = "DC=experty,DC=local"
```

```
# Créer le dossier AGDLP
```

```
New-ADOrganizationalUnit -Name "AGDLP" -Path $ouPath
```

```
# Créer les sous-dossiers de AGDLP
```

```
New-ADOrganizationalUnit -Name "GGlobeaux" -Path  
"OU=AGDLP,$ouPath"
```

```
New-ADOrganizationalUnit -Name "GLocal" -Path "OU=AGDLP,$ouPath"
```

```
New-ADOrganizationalUnit -Name "Site" -Path "OU=AGDLP,$ouPath"
```

```
# Créer les sous-dossiers de Site
```

```
New-ADOrganizationalUnit -Name "Informatique" -Path  
"OU=Site,OU=AGDLP,$ouPath"
```

```
New-ADOrganizationalUnit -Name "Machine" -Path  
"OU=Site,OU=AGDLP,$ouPath"
```

```
New-ADOrganizationalUnit -Name "Utilisateur" -Path  
"OU=Site,OU=AGDLP,$ouPath"
```

```

# Créer les sous-dossiers de Utilisateur

New-ADOrganizationalUnit -Name "Accueil" -Path
"OU=Utilisateur,OU=Site,OU=AGDLP,$ouPath"

New-ADOrganizationalUnit -Name "Administratif" -Path
"OU=Utilisateur,OU=Site,OU=AGDLP,$ouPath"

New-ADOrganizationalUnit -Name "Assistance" -Path
"OU=Utilisateur,OU=Site,OU=AGDLP,$ouPath"

New-ADOrganizationalUnit -Name "Direction" -Path
"OU=Utilisateur,OU=Site,OU=AGDLP,$ouPath"

New-ADOrganizationalUnit -Name "Comptabilité" -Path
"OU=Utilisateur,OU=Site,OU=AGDLP,$ouPath"


# Créer les groupes Read-Only et Read-Write dans GLocal

$glocalGroups = @(
    @{ Name = "GL_RO_Accueil"; Path =
"OU=GLocal,OU=AGDLP,$ouPath" },
    @{ Name = "GL_RO_Administratif"; Path =
"OU=GLocal,OU=AGDLP,$ouPath" },
    @{ Name = "GL_RO_Assistance"; Path =
"OU=GLocal,OU=AGDLP,$ouPath" },
    @{ Name = "GL_RO_Comptabilité"; Path =
"OU=GLocal,OU=AGDLP,$ouPath" },
    @{ Name = "GL_RO_Direction"; Path =
"OU=GLocal,OU=AGDLP,$ouPath" },
    @{ Name = "GL_RO_Informatique"; Path =
"OU=GLocal,OU=AGDLP,$ouPath" },
    @{ Name = "GL_RW_Accueil"; Path =
"OU=GLocal,OU=AGDLP,$ouPath" },

```

A large red graphic on the right side of the page, consisting of two concentric, rounded rectangular shapes that are open on the right side, resembling a stylized 'C' or a bracket.

```
@{ Name = "GL_RW_Administratif"; Path =  
"OU=GLocal,OU=AGDLP,$ouPath" },  
  
    @{ Name = "GL_RW_Assistance"; Path =  
"OU=GLocal,OU=AGDLP,$ouPath" },  
  
    @{ Name = "GL_RW_Comptabilité"; Path =  
"OU=GLocal,OU=AGDLP,$ouPath" },  
  
    @{ Name = "GL_RW_Direction"; Path =  
"OU=GLocal,OU=AGDLP,$ouPath" },  
  
    @{ Name = "GL_RW_Informatique"; Path =  
"OU=GLocal,OU=AGDLP,$ouPath" }  
  
)  
  
foreach ($group in $glocalGroups) {  
    try {  
        New-ADGroup -Name $group.Name -GroupScope Global -  
GroupCategory Security -Path $group.Path  
        Write-Output "Groupe $($group.Name) créé avec succès."  
    } catch {  
        Write-Output "Erreur lors de la création du groupe  
$($group.Name) : $_"  
    }  
}
```

```

# Créer les groupes Globeaux et ajouter les membres GL_RO_* et
GL_RW_*

$ggGroups = @(
    @{ Name = "GG_Accueil"; Members = @("GL_RO_Accueil",
    "GL_RW_Accueil") },
    @{ Name = "GG_Administratif"; Members =
    @("GL_RO_Administratif", "GL_RW_Administratif") },
    @{ Name = "GG_Assistance"; Members = @("GL_RO_Assistance",
    "GL_RW_Assistance") },
    @{ Name = "GG_Comptabilité"; Members =
    @("GL_RO_Comptabilité", "GL_RW_Comptabilité") },
    @{ Name = "GG_Direction"; Members = @("GL_RO_Direction",
    "GL_RW_Direction") },
    @{ Name = "GG_Informatique"; Members =
    @("GL_RO_Informatique", "GL_RW_Informatique") }
)

foreach ($group in $ggGroups) {
    $groupName = $group.Name
    try {
        # Créer le groupe GG_*
        New-ADGroup -Name $groupName -GroupScope Global -
        GroupCategory Security -Path "OU=GGlobeaux,OU=AGDLP,$ouPath"
        Write-Output "Groupe $groupName créé avec succès."
    }
}

```

```

        # Ajouter les membres GL_RO_* et GL_RW_*
        foreach ($member in $group.Members) {
            Add-ADGroupMember -Identity $groupName -Members
$member

            Write-Output "$member ajouté au groupe $groupName."
        }
    } catch {
        Write-Output "Erreur lors de la création du groupe
$groupName ou de l'ajout des membres : $_"
    }
}

# Définir la structure de base
$ouPath = "DC=experty,DC=local"

# Fonction pour créer une OU si elle n'existe pas déjà
function Create-OU {
    param (
        [string]$Name,
        [string]$Path
    )

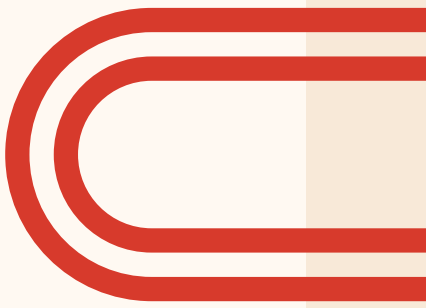
    if (-not (Get-ADOrganizationalUnit -Filter {Name -eq $Name}
-SearchBase $Path -ErrorAction SilentlyContinue)) {
        New-ADOrganizationalUnit -Name $Name -Path $Path
        Write-Output "OU $Name créée avec succès dans $Path."
    } else {
        Write-Output "OU $Name existe déjà dans $Path."
    }
}

```



```
# Fonction pour créer un utilisateur
function Create-ADUser {
    param (
        [string]$UserName,
        [string]$Ou,
        [string]$displayName = $UserName,
        [string]$password = "Adm!secure"
    )
    try {
        New-ADUser -Name $UserName -SamAccountName $UserName -
UserPrincipalName "$UserName@experty.local" -Path $Ou -GivenName
$UserName -DisplayName $displayName -AccountPassword (ConvertTo-
SecureString $password -AsPlainText -Force) -Enabled $true

        Write-Output "Utilisateur $UserName créé avec succès
dans $Ou."
    } catch {
        Write-Output "Erreur lors de la création de
l'utilisateur $UserName dans $Ou : $_"
    }
}
```



```
# Fonction pour ajouter un utilisateur à un groupe
function Add-UserToGroup {
    param (
        [string]$userName,
        [string]$groupName
    )
    try {
        Add-ADGroupMember -Identity $groupName -Members
$userName

        Write-Output "Utilisateur $userName ajouté au groupe
$groupName."
    } catch {
        Write-Output "Erreur lors de l'ajout de l'utilisateur
$userName au groupe $groupName : $_"
    }
}

# Créer le dossier AGDLP
Create-OU -Name "AGDLP" -Path $ouPath

# Créer les sous-dossiers de AGDLP
Create-OU -Name "GGlobeaux" -Path "OU=AGDLP,$ouPath"
Create-OU -Name "GLocal" -Path "OU=AGDLP,$ouPath"
Create-OU -Name "Site" -Path "OU=AGDLP,$ouPath"
```

```
# Créer les sous-dossiers de Site
Create-OU -Name "Informatique" -Path "OU=Site,OU=AGDLP,$ouPath"
Create-OU -Name "Machine" -Path "OU=Site,OU=AGDLP,$ouPath"
Create-OU -Name "Utilisateur" -Path "OU=Site,OU=AGDLP,$ouPath"

# Créer les sous-dossiers de Utilisateur
Create-OU -Name "Accueil" -Path
"OU=Utilisateur,OU=Site,OU=AGDLP,$ouPath"
Create-OU -Name "Administratif" -Path
"OU=Utilisateur,OU=Site,OU=AGDLP,$ouPath"
Create-OU -Name "Assistance" -Path
"OU=Utilisateur,OU=Site,OU=AGDLP,$ouPath"
Create-OU -Name "Direction" -Path
"OU=Utilisateur,OU=Site,OU=AGDLP,$ouPath"
Create-OU -Name "Comptabilité" -Path
"OU=Utilisateur,OU=Site,OU=AGDLP,$ouPath"

# Créer les sous-dossiers de Comptabilité
for ($i = 1; $i -le 13; $i++) {
    Create-OU -Name "compta$i" -Path
    "OU=Comptabilité,OU=Utilisateur,OU=Site,OU=AGDLP,$ouPath"
}
```



# Créer les groupes Read-Only et Read-Write dans GLocal et définir les permissions

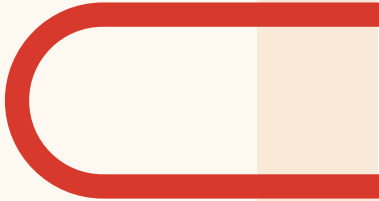
```
$glocalGroups = @(
    @{ Name = "GL_RO_Accueil"; Path =
"OU=GLocal,OU=AGDLP,$ouPath"; Permissions = "Read" },
    @{ Name = "GL_RO_Administratif"; Path =
"OU=GLocal,OU=AGDLP,$ouPath"; Permissions = "Read" },
    @{ Name = "GL_RO_Assistance"; Path =
"OU=GLocal,OU=AGDLP,$ouPath"; Permissions = "Read" },
    @{ Name = "GL_RO_Comptabilité"; Path =
"OU=GLocal,OU=AGDLP,$ouPath"; Permissions = "Read" },
    @{ Name = "GL_RO_Direction"; Path =
"OU=GLocal,OU=AGDLP,$ouPath"; Permissions = "Read" },
    @{ Name = "GL_RO_Informatique"; Path =
"OU=GLocal,OU=AGDLP,$ouPath"; Permissions = "Read" },
    @{ Name = "GL_RW_Accueil"; Path =
"OU=GLocal,OU=AGDLP,$ouPath"; Permissions = "ReadWrite" },
    @{ Name = "GL_RW_Administratif"; Path =
"OU=GLocal,OU=AGDLP,$ouPath"; Permissions = "ReadWrite" },
    @{ Name = "GL_RW_Assistance"; Path =
"OU=GLocal,OU=AGDLP,$ouPath"; Permissions = "ReadWrite" },
    @{ Name = "GL_RW_Comptabilité"; Path =
"OU=GLocal,OU=AGDLP,$ouPath"; Permissions = "ReadWrite" },
    @{ Name = "GL_RW_Direction"; Path =
"OU=GLocal,OU=AGDLP,$ouPath"; Permissions = "ReadWrite" },
    @{ Name = "GL_RW_Informatique"; Path =
"OU=GLocal,OU=AGDLP,$ouPath"; Permissions = "ReadWrite" }
)
```

```

foreach ($group in $glocalGroups) {
    try {
        New-ADGroup -Name $group.Name -GroupScope Global -
GroupCategory Security -Path $group.Path
        Write-Output "Groupe $($group.Name) créé avec succès."
    } catch {
        Write-Output "Erreur lors de la création du groupe
$($group.Name) : $_"
    }
}

# Créer les groupes Globaux et ajouter les membres GL_RO_* et
GL_RW_*
$ggGroups = @(
    @{ Name = "GG_Accueil"; Members = @("GL_RO_Accueil",
"GL_RW_Accueil") },
    @{ Name = "GG_Administratif"; Members =
@("GL_RO_Administratif", "GL_RW_Administratif") },
    @{ Name = "GG_Assistance"; Members = @("GL_RO_Assistance",
"GL_RW_Assistance") },
    @{ Name = "GG_Comptabilité"; Members =
@("GL_RO_Comptabilité", "GL_RW_Comptabilité") },
    @{ Name = "GG_Direction"; Members = @("GL_RO_Direction",
"GL_RW_Direction") },
    @{ Name = "GG_Informatique"; Members =
@("GL_RO_Informatique", "GL_RW_Informatique") }
)

```



```
foreach ($group in $ggGroups) {
    $groupName = $group.Name
    try {
        # Créer le groupe GG_*
        New-ADGroup -Name $groupName -GroupScope Global -
GroupCategory Security -Path "OU=GGlobeaux,OU=AGDLP,$ouPath"
        Write-Output "Groupe $groupName créé avec succès."

        # Ajouter les membres GL_RO_* et GL_RW_*
        foreach ($member in $group.Members) {
            Add-ADGroupMember -Identity $groupName -Members
$member
            Write-Output "$member ajouté au groupe $groupName."
        }
    } catch {
        Write-Output "Erreur lors de la création du groupe
$groupName ou de l'ajout des membres : $_"
    }
}
```



```
# Créer les utilisateurs dans les OUs spécifiques

Create-ADUser -userName "accueil1" -ou
"OU=Accueil,OU=Utilisateur,OU=Site,OU=AGDLP,$ouPath"

Create-ADUser -userName "accueil2" -ou
"OU=Accueil,OU=Utilisateur,OU=Site,OU=AGDLP,$ouPath"


Create-ADUser -userName "ResponsableInfo" -ou
"OU=Informatique,OU=Site,OU=AGDLP,$ouPath"

Create-ADUser -userName "AdminReseaux" -ou
"OU=Informatique,OU=Site,OU=AGDLP,$ouPath"

Create-ADUser -userName "AlternantInfo" -ou
"OU=Informatique,OU=Site,OU=AGDLP,$ouPath"


Create-ADUser -userName "PDG" -ou
"OU=Direction,OU=Utilisateur,OU=Site,OU=AGDLP,$ouPath"


Create-ADUser -userName "AssistanteDirection" -ou
"OU=Assistance,OU=Utilisateur,OU=Site,OU=AGDLP,$ouPath"

Create-ADUser -userName "ApprentieDirection" -ou
"OU=Assistance,OU=Utilisateur,OU=Site,OU=AGDLP,$ouPath"


# Créer les utilisateurs du Service Administratif avec noms
ajustés

for ($i = 1; $i -le 5; $i++) {

    Create-ADUser -userName "ServiceAdmin$i" -ou
    "OU=Administratif,OU=Utilisateur,OU=Site,OU=AGDLP,$ouPath" -
    displayName "Service Administratif $i"

}
```

```

# Créer les utilisateurs de Comptabilité
for ($i = 1; $i -le 13; $i++) {
    Create-ADUser -userName "ResponsableCompta$i" -ou
"OU=compta$i,OU=Comptabilité,OU=Utilisateur,OU=Site,OU=AGDLP,$ou
Path"

    for ($j = 1; $j -le 4; $j++) {
        Create-ADUser -userName "compta${i}_${j}" -ou
"OU=compta$i,OU=Comptabilité,OU=Utilisateur,OU=Site,OU=AGDLP,$ou
Path"
    }
}

# Ajouter les utilisateurs aux groupes
Add-UserToGroup -userName "accueil1" -groupName "GL_RO_Accueil"
Add-UserToGroup -userName "accueil2" -groupName "GL_RO_Accueil"
Add-UserToGroup -userName "AssistanteDirection" -groupName
"GL_RW_Assistance"
Add-UserToGroup -userName "ApprentieDirection" -groupName
"GL_RO_Assistance"

# Ajouter les utilisateurs administratifs au groupe
GL_RW_Administratif
for ($i = 1; $i -le 5; $i++) {
    Add-UserToGroup -userName "ServiceAdmin$i" -groupName
"GL_RW_Administratif"
}

# Ajouter PDG aux groupes GL_RW_*
$pdgGroups = @("GL_RW_Accueil", "GL_RW_Administratif",
"GL_RW_Assistance", "GL_RW_Comptabilité", "GL_RW_Direction",
"GL_RW_Informatique")
foreach ($group in $pdgGroups) {
    Add-UserToGroup -userName "PDG" -groupName $group
}

```

```
# Ajouter tous les utilisateurs de Comptabilité au groupe
GL_RW_Comptabilité

for ($i = 1; $i -le 13; $i++) {

    Add-UserToGroup -userName "ResponsableCompta$i" -groupName
    "GL_RW_Comptabilité"

    for ($j = 1; $j -le 4; $j++) {

        Add-UserToGroup -userName "compta${i}_${j}" -groupName
        "GL_RW_Comptabilité"

    }

}

Write-Output "Tous les utilisateurs ont été créés et assignés
aux groupes avec les permissions spécifiques."
```

## Création de dossier partagé

```
# Variables de base

$basePath = "C:\dossierpartagé"

$informatiqueUsers = @("ResponsableInfo", "alternantinfo",
"adminreseaux")

$quotaTemplateName = "Quota1GB"


# Fonction pour créer le dossier personnel, appliquer les
permissions et le quota

function Create-UserHomeFolder {
    param (
        [string]$UserName
    )

    # Définir le chemin du dossier utilisateur
    $userPath = Join-Path $basePath $UserName
```



```
# Vérifier si le dossier existe déjà, sinon le créer
if (-not (Test-Path $userPath)) {
    try {
        New-Item -Path $userPath -ItemType Directory
        Write-Output "Dossier $userPath créé pour
l'utilisateur $userName."
    } catch {
        Write-Output "Erreur lors de la création du dossier
pour $userName : $_"
        return
    }
} else {
    Write-Output "Dossier $userPath existe déjà pour
l'utilisateur $userName."
}
try {
    $acl = Get-Acl $userPath
    $userIdentity = "$userName@experty.local"

    # Accès complet pour l'utilisateur sur son propre
dossier

    $userAccessRule = New-Object
System.Security.AccessControl.FileSystemAccessRule($userIdentity
, "FullControl", "ContainerInherit, ObjectInherit", "None",
"Allow")

    $acl.SetAccessRule($userAccessRule)
```



```

        # Ajouter les accès pour chaque membre du service
        Informatique

        foreach ($informatiqueUser in $informatiqueUsers) {

            $informatiqueIdentity =
"$informatiqueUser@experty.local"

            $informatiqueAccessRule = New-Object
System.Security.AccessControl.FileSystemAccessRule($informatique
Identity, "Modify", "ContainerInherit, ObjectInherit", "None",
"Allow")

            $acl.AddAccessRule($informatiqueAccessRule)

        }

        Set-Acl -Path $userPath -AclObject $acl

        Write-Output "Permissions définies pour le dossier
$userPath."

    } catch {

        Write-Output "Erreur lors de la définition des
permissions pour $userName : $_"

    }

    # Appliquer le quota de 1 Go

    try {

        if (-not (Get-FsrmQuota -Path $userPath -ErrorAction
SilentlyContinue)) {

            New-FsrmQuota -Path $userPath -Template
$quotaTemplateName

            Write-Output "Quota de 1 Go appliqué au dossier
$userPath."

        } else {

            Write-Output "Quota déjà appliqué pour le dossier
$userPath."

        }
    }

```

```

} catch {

    Write-Output "Erreur lors de l'application du quota pour
$userName : $_"

}

}

# Liste des utilisateurs pour lesquels appliquer les
modifications

$users = @(

    "accueil1", "accueil2", "PDG", "AssistanteDirection",
    "ApprentieDirection",

    "ServiceAdmin1", "ServiceAdmin2", "ServiceAdmin3",
    "ServiceAdmin4", "ServiceAdmin5",

    "ResponsableCompta1", "compta1_1", "compta1_2", "compta1_3",
    "compta1_4",

    "ResponsableCompta2", "compta2_1", "compta2_2", "compta2_3",
    "compta2_4",

    "ResponsableCompta3", "compta3_1", "compta3_2", "compta3_3",
    "compta3_4",

    "ResponsableCompta4", "compta4_1", "compta4_2", "compta4_3",
    "compta4_4",

    "ResponsableCompta5", "compta5_1", "compta5_2", "compta5_3",
    "compta5_4",

    "ResponsableCompta6", "compta6_1", "compta6_2", "compta6_3",
    "compta6_4",

    "ResponsableCompta7", "compta7_1", "compta7_2", "compta7_3",
    "compta7_4",

    "ResponsableCompta8", "compta8_1", "compta8_2", "compta8_3",
    "compta8_4",

```

```

    "ResponsableCompta9", "compta9_1", "compta9_2", "compta9_3",
    "compta9_4",
    "ResponsableCompta10", "compta10_1", "compta10_2",
    "compta10_3", "compta10_4",
    "ResponsableCompta11", "compta11_1", "compta11_2",
    "compta11_3", "compta11_4",
    "ResponsableCompta12", "compta12_1", "compta12_2",
    "compta12_3", "compta12_4",
    "ResponsableCompta13", "compta13_1", "compta13_2",
    "compta13_3", "compta13_4"
)

# Appliquer la fonction pour chaque utilisateur
foreach ($user in $users) {
    Create-UserHomeFolder -userName $user
}

Write-Output "Création des dossiers, application des permissions
et des quotas terminés."

```

## Profils Itinérants

```
# Chemin du dossier partagé pour les profils itinérants
$profilPath = "\\serveur1\ProfilsUtilisateurs"

# Récupère tous les utilisateurs des différentes OU spécifiées
$ous = @(
    "OU=Informatique,OU=Site,OU=AGDLP,DC=experty,DC=local",
    "OU=Accueil,OU=Utilisateur,OU=Site,OU=AGDLP,DC=experty,DC=local"
    ,
    "OU=Administratif,OU=Utilisateur,OU=Site,OU=AGDLP,DC=experty,DC=local",
    "OU=Assistance,OU=Utilisateur,OU=Site,OU=AGDLP,DC=experty,DC=local",
    "OU=Direction,OU=Utilisateur,OU=Site,OU=AGDLP,DC=experty,DC=local"
)

# Ajoute les OU de Comptabilité (compta1 à compta13)
for ($i = 1; $i -le 13; $i++) {
    $ous +=
    "OU=compta$i,OU=Comptabilité,OU=Utilisateur,OU=Site,OU=AGDLP,DC=experty,DC=local"
}
```

```
# Parcourt chaque OU et configure les profils itinérants pour chaque utilisateur
foreach ($ou in $sous) {
    $users = Get-ADUser -Filter * -SearchBase $ou
    foreach ($user in $users) {
        # Définit le chemin du profil itinérant pour chaque utilisateur
        $profilePathUser = "$profilPath\$( $user.SamAccountName)"
        Set-ADUser -Identity $user -ProfilePath $profilePathUser
        Write-Host "Profil itinérant configuré pour l'utilisateur : $( $user.SamAccountName)
dans l'OU $ou"
    }
}
```

# CONCLUSION

Pour conclure, le projet Experty présente une transformation complète de l'infrastructure réseau avec une architecture moderne axée sur la sécurité, la redondance et la gestion efficace des ressources. Grâce à la mise en place de contrôleurs de domaine, de stratégies de groupe et de profils itinérants, l'entreprise assure un environnement sécurisé et flexible, adapté à sa croissance. L'automatisation du mappage des lecteurs réseau et la gestion stricte des droits d'accès optimisent l'expérience utilisateur tout en maintenant la conformité aux normes de sécurité. En somme, cette nouvelle infrastructure permettra à Experty d'atteindre une gestion informatique robuste et résiliente, soutenant ses besoins actuels et futurs.