Mise en place de GPOs dans le cadre de la gestion d'un Active Directory

Table des matières

Introduction

Une stratégie de groupe permet de centraliser les paramètres de configuration et de gestion des postes et des utilisateurs sous Windows. On parle alors d'objets de stratégie de groupes, plus communément appelés GPO, pour définir l'ensemble des paramètres de stratégie de groupe destinés à modeler le système d'exploitation en fonction des groupes d'utilisateurs. Un GPO contient deux parties : la partie utilisateur et la partie ordinateur, depuis lesquelles il est possible de gérer les paramètres logiciels, les paramètres Windows et les modèles d'administration.

Pour être fonctionnel, le GPO doit être créé et lié au domaine. Il peut être créé à la racine du domaine pour s'appliquer à l'ensemble de ce dernier ou encore à l'intérieur des UO pour ne s'appliquer qu'à celles-ci.

Déploiement de logiciels

Dans un premier temps, un dossier partagé comprenant les fichiers d'installation au format MSI et/ou les scripts doit être créé en local sur l'Active Directory (j'ai choisi de le créer directement sur le disque C:). Une fois le dossier créé, il est nécessaire de modifier les permissions en allant dans :

> *Propriétés → Partage → Partager...*

Le but étant d'obtenir une configuration telle que les groupes d'utilisateurs concernés possèdent un doit de lecture et les administrateurs, le droit de lecture et d'écriture.

Mozilla Firefox

Lien de téléchargement :

Mozilla Firefox

Après la création du GPO à la racine du domaine, direction :

> *Computer Configuration → Policies → Software Settings → Software Installation*

A partir de là, il faut créer un nouveau package et y ajouter le fichier d'installation au format MSI en utilisant son chemin réseau. Ensuite, opter pour l'option "Assigner" afin que l'installation s'effectue automatiquement sur tous les postes.

Pour terminer et attester du succès de l'installation, procéder à un `gpupdate /force` sur un poste et le redémarrer : Firefox devrait être installé.

Agent Zabbix

Lien de téléchargement (validité et version contrôlées en 2021) :

Agent Zabbix

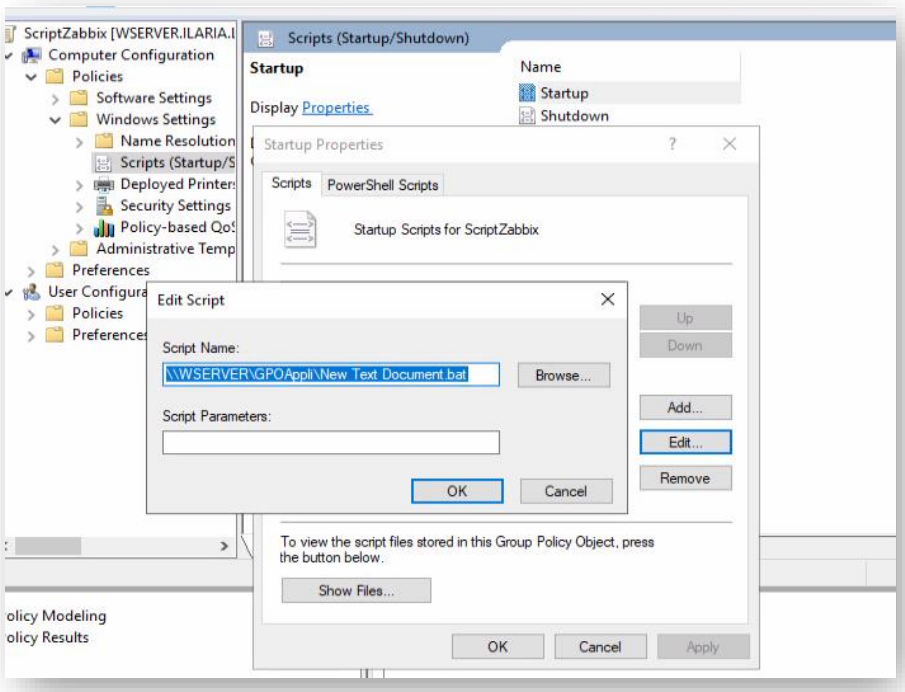
Une fois l'agent téléchargé, il faut le déplacer dans le dossier partagé créé précédemment, accompagné d'un script d'installation au format .bat :

```
msiexec   /i     \\WSERVER\GPOAppli\zabbix_agent-5.4.7-windows-amd64-openssl.msi /qb SERVER=IP_du_serveur_Zabbix
```

Maintenant, on va pouvoir créer le GPO, toujours dans la racine du domaine en ce qui me concerne et ensuite le configurer :

> Computer Configuration → Policies → Windows Settings → Scripts → Startup

Dans cette fenêtre, ajouter un nouveau script en allant chercher le fichier dans le dossier partagé comme ceci :



Pour vérifier le succès de l'installation, ajouter l'hôte dans Zabbix et il devrait remonter.

Facultatif : Il est possible de mettre en place un chiffrement par clé PSK et de configurer l'ajout automatique du Windows Server dans Zabbix.} Pour ce faire, direction l'interface graphique du Zabbix.

Pour générer une clé PSK via un poste Linux, on peut utiliser la commande `openssl rand -hex 32`.

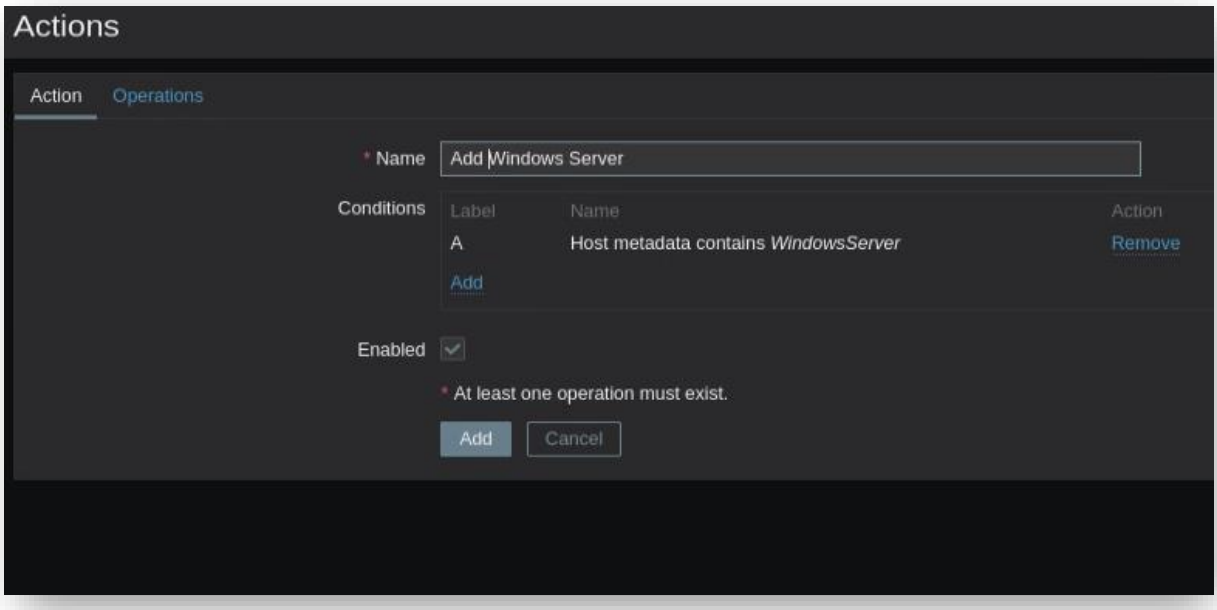
Une fois la clé rentrée, il faudra créer un groupe pour les serveurs Windows et y activer l'auto-registration. Cela se passe dans :

> Configuration → Groupes d'hôtes → Créer un groupe d'hôtes (en haut à droit de la fenêtre)

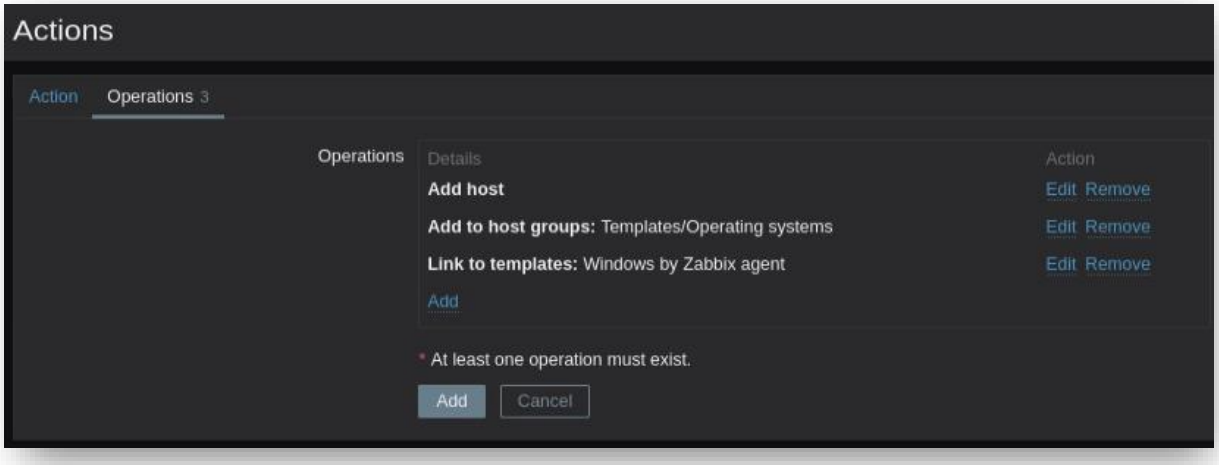
Afin d'activer l'auto-registration :

> Configuration → Actions → Actions d'auto-registration → Créer une action (en haut à droite de la fenêtre)

On donne un nom à l'action et on lui ajoute une condition en définissant la métadonnée présente dans le script.



Finalement, dans la catégorie "Opérations", on ajoute l'hôte et on lui définit un groupe et un modèle.



Le script d'installation sera un peu différent en cas d'utilisation de cette méthode car il faudra rajouter les informations relatives à la clé PSK ainsi que les méta données de l'hôte, ce qui donnera plutôt :

```
msiexec /i  \\WSERVER\GPOAppli\zabbix_agent-5.4.7-windows-
amd64-openssl.msi /qb
SERVER=IP_du_serveur_Zabbix
HOSTNAME=%computerName%
HOSTMETADATA=WindowsServer
TLSCONNECT=psk
TLSACCEPT=psk
TLSPSKIDENTITY=Nom_choisi_pour_la_clé_PSK
TLSPSKVALUE=Clé_générée
```

Fusion Inventory

Lien de téléchargement du script :

Script VBS Fusion Inventory

Modifier ensuite les lignes suivantes pour y indiquer les informations nécessaires :

```
versionverification = "2.6"

fusionarguments                    =                    "/S
/server=""http://glpi.ilaria.lo/glpi/plugins/fusioninventory/"
" /acceptlicense /runnow"

fusionsetupURL                                          =
"https://github.com/fusioninventory/fusioninventory-
agent/releases/download/2.6/fusioninventory-agent_windows-
x64_2.6.exe"
```

Pour la création du GPO :

- L'exécution du script VBS au démarrage :

> Computer Configuration → Policies → Windows Settings → Scripts → Startup

Ajouter le script dans le dossier partagé créé précédemment.
Cliquer sur « Ajouter » et insérer le script VBS.

Thunderbird

Pour Thunderbird, la spécificité était d'y ajouter une extension en plus de l'installer sur les postes du domaine. Cette extension permet d'ajouter un connecteur qui importe l'annuaire de l'AD initialement synchronisé dans BlueMind.

Tout d'abord, pour obtenir ce fameux collecteur, ça se passe dans BlueMind. Il faut connecter le compte admin (ou un compte utilisateur lambda) pour aller le récupérer dans :

> Mon compte → Téléchargements → Connecteur Thunderbird → Télécharger

Le téléchargement d'un fichier au format .xpi se lance, il faudra alors déposer ce fichier dans le dossier partagé de l'AD, ainsi que le fichier d'installation au format .msi, téléchargeable sur :

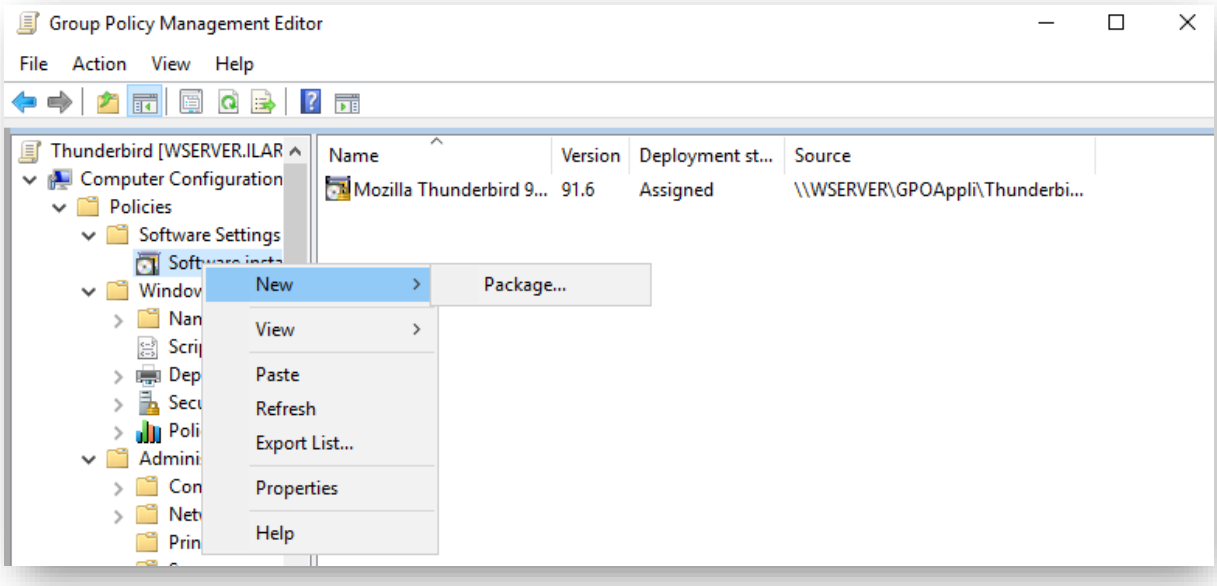
Client Thunderbird

Pour la création du GPO, deux éléments à configurer :

- Pour l'installation du logiciel :

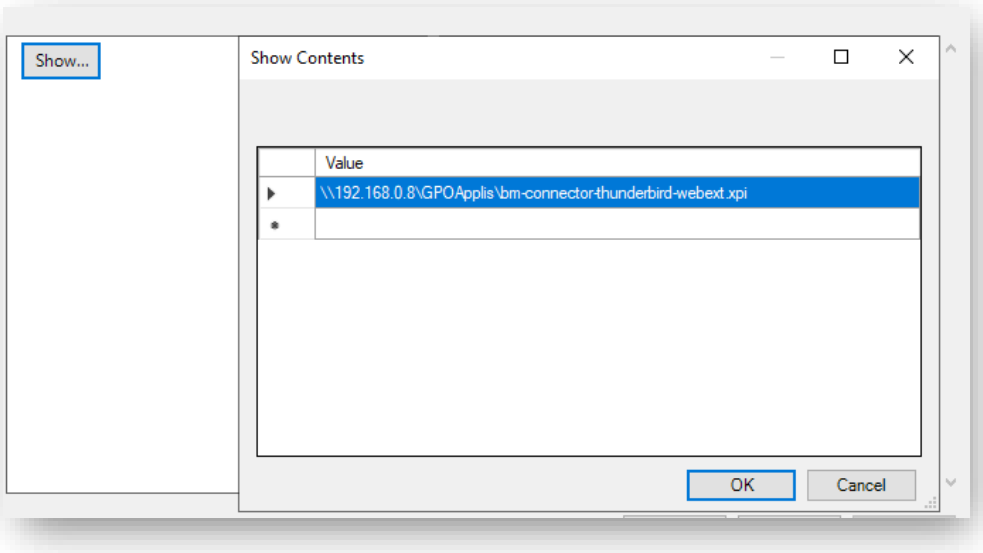
> Computer Configuration → Policies → Software Settings → Software Installer → New → Package

Choisir le fichier au format .msi



- Pour la mise en place de l'extension :

> Computer Configuration → Administrative Temp → Thunderbird → Extensions → Extension Update → Enable → Extensions to Install → Enable → Options : Show → Ajouter le chemin réseau du fichier au format .xpi

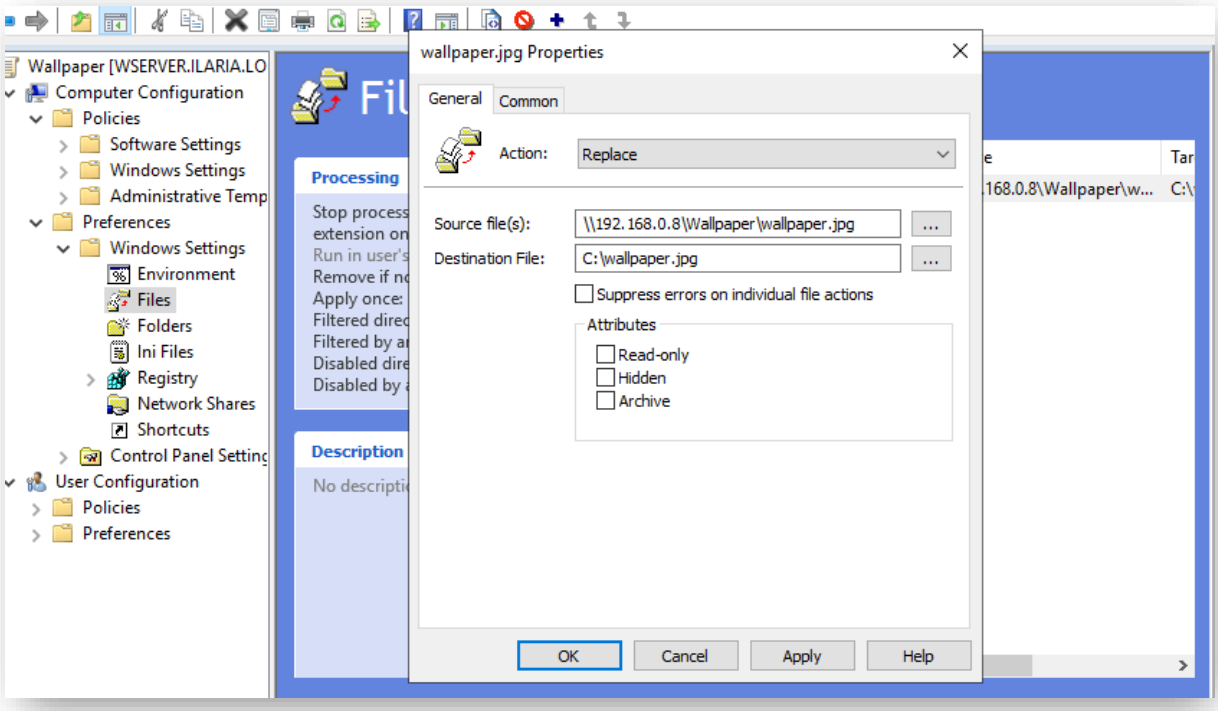


Homogénéisation des fonds d'écran

Pour déployer un fond d'écran identique sur chaque poste, direction :

> Computer Configuration → Preferences → Windows Settings → Files → New → File

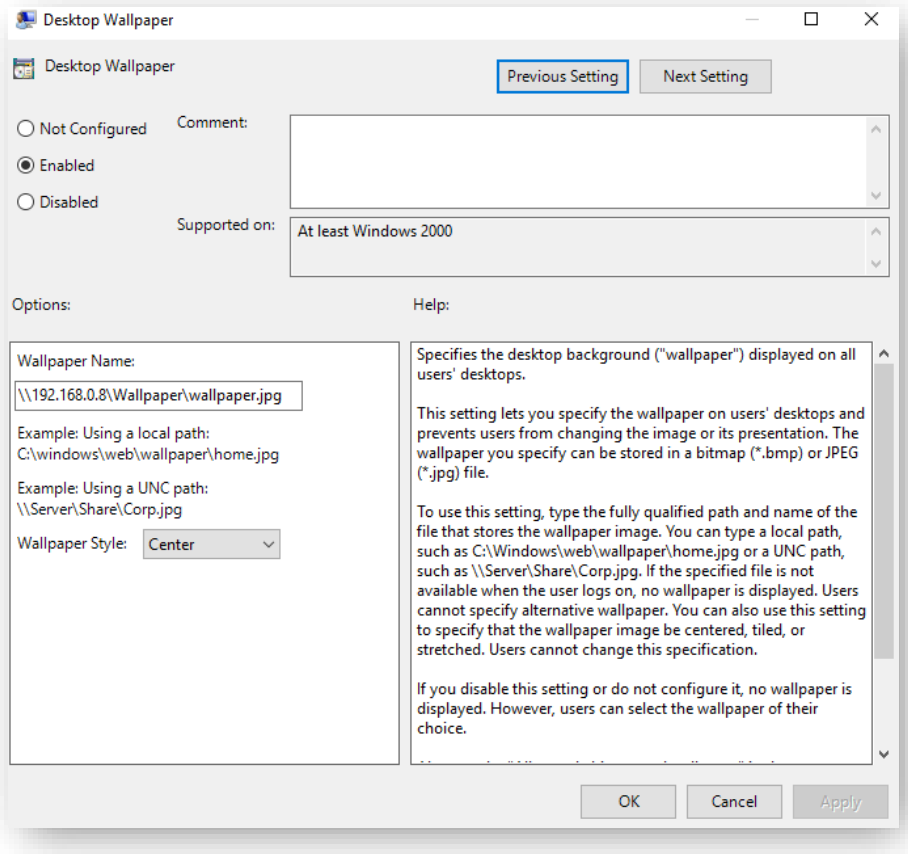
Action : replace
Source file : chemin réseau de l'image à déployer
Destination file : endroit où déposer le fichier sur le poste de destination



Dans l'onglet "Commun", cocher "Apply once and do not reapply" pour que le fichier ne soit pas recopié à chaque fois.

Ensuite, pour appliquer le fond d'écran, aller activer les paramètres dans :

> User Configuration → Policies → Administrative Temp → Desktop → Desktop → Desktop Wallpaper → Enable → Ajouter le chemin réseau de l'image.



Mise en place d'une politique de mot de passe

Rendez-vous ici dans l'ADAC (Active Directory Administrative Center) via l'onglet "Tools". (image)

Ensuite, direction:

> System → Password Setting Container

(image)

Dans le panneau d'affichage des tâches, créer un nouveau paramètre de mot de passe et remplir les champs arborant une étoile rouge (image).

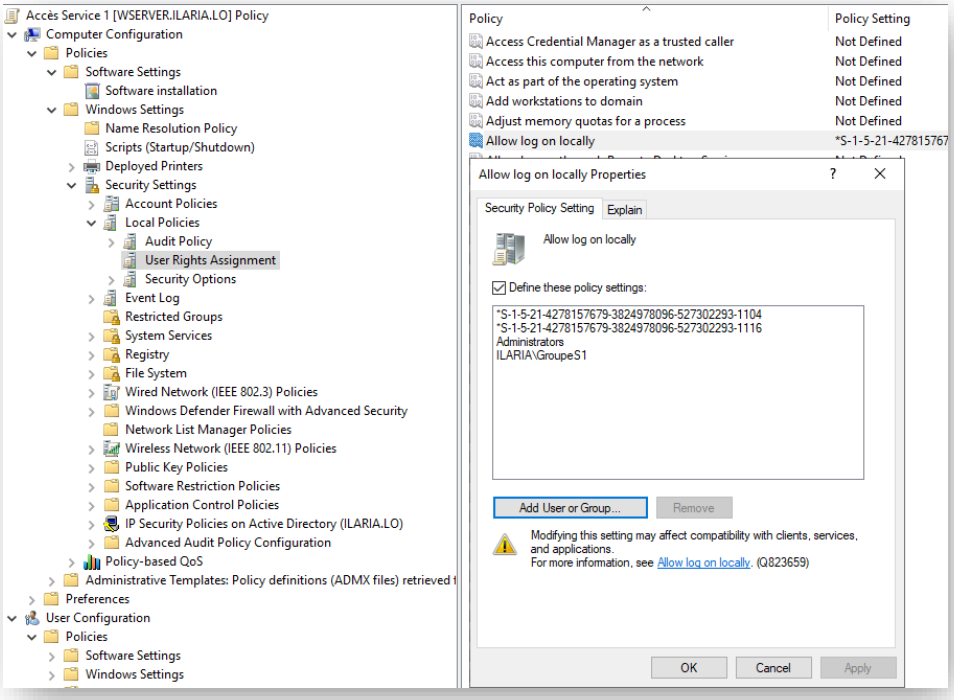
Une fois le nécessaire rempli, il sera possible de choisir les utilisateurs à qui vont s'appliquer ces paramètres en se rendant en bas de la page, dans la section "Directly Applies To" et ajouter les groupes et/ou les utilisateurs concernés. En cliquant sur "OK", on peut constater l'apparition de la politique de mot de passe dans le conteneur. (image)

Pour terminer, il est possible de vérifier le succès de l'application de ces paramètres en identifiant la politique appliquée à un utilisateur en utilisant le panneau latéral gauche de la fenêtre (image).

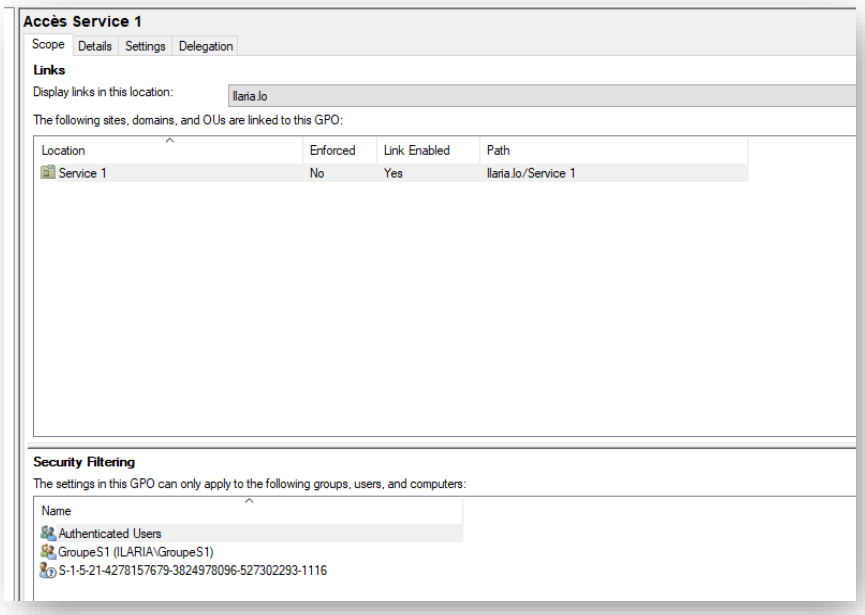
Gestion des accès aux postes en fonction des services

Si on souhaite autoriser les accès à certains postes uniquement à des utilisateurs précis, il suffira d'ajouter lesdits utilisateurs ou les groupes désirés dans :

> Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → User Rights Assignment → Allow log on locally

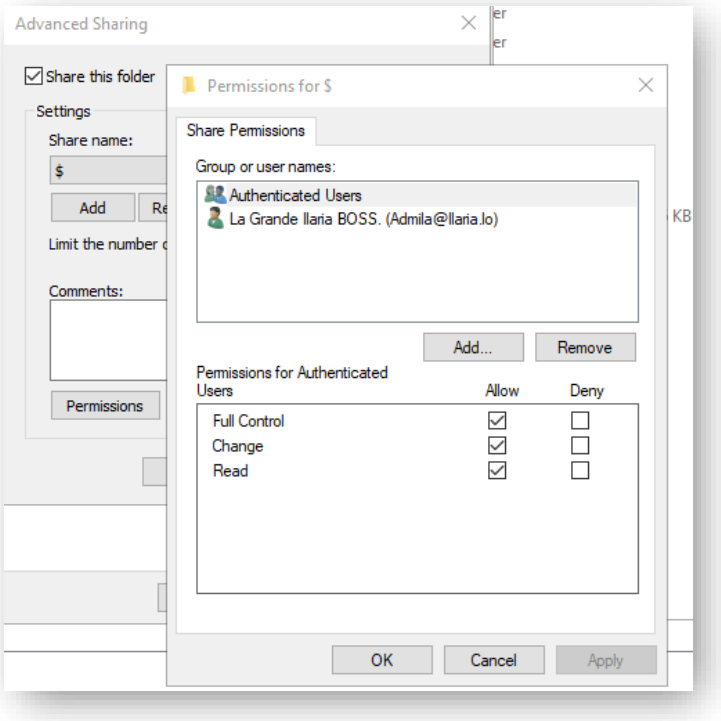


Ce GPO doit être lié directement à l'UO à laquelle il s'applique. Finalement, on peut ajouter les utilisateurs aux filtres de sécurité sur la page d'accueil du GPO :

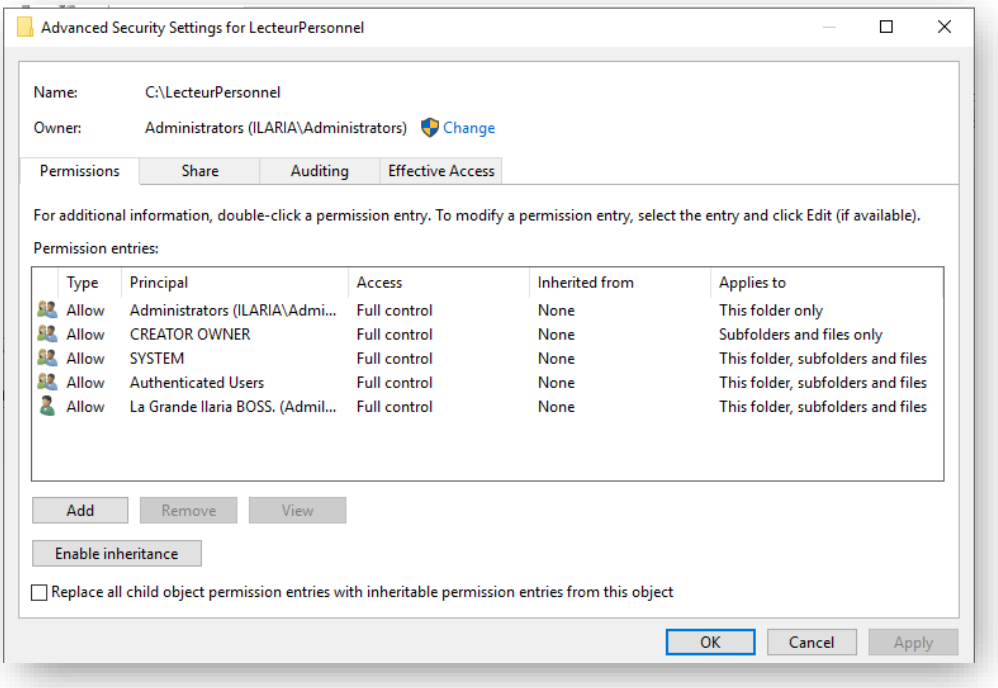


Création d'un lecteur réseau personnel pour les utilisateurs

Pour commencer, créer un dossier partagé sur l'AD et modifier les permissions pour donner les droits suivants :



Ensuite, dans "Sécurité → Avancé", cliquez sur "Désactiver l'héritage" et "Supprimer toutes les autorisations héritées de cet objet" pour remettre à zéro toutes les entrées d'autorisations et enfin paramétrer comme suit :



On passe à la création du GPO à la racine du domaine, puis :

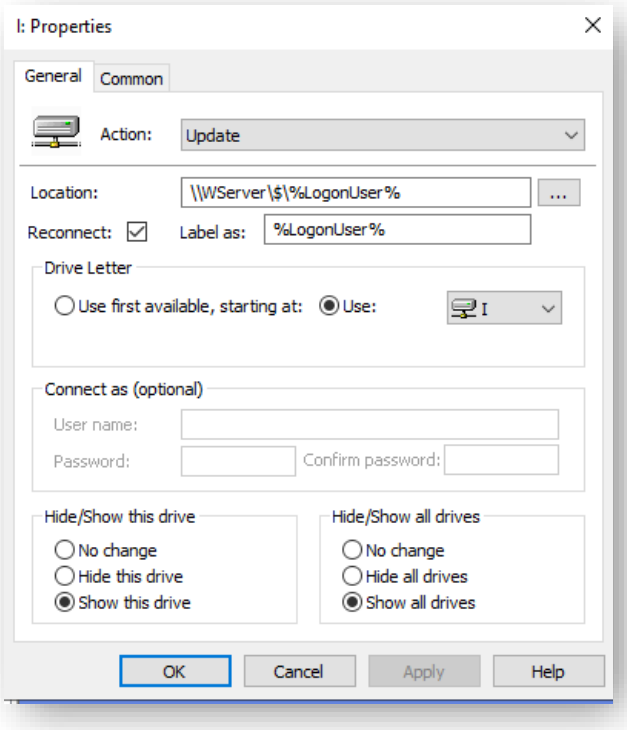
> User Conguration → Preferences → Windows Settings → Drive Maps → New → Mapped

Drive Action : Update

Location : \\AD\dossier_partagé\%LogonUser%

Reconnect (cocher)

Label as : %LogonUser% (de cette façon, la ressource portera le nom de l'utilisateur)



Dans l'onglet "Common", cocher "Run in logged-on user's security context".

Pour tester, ouvrir une session et constater la création automatique d'un dossier au nom de l'utilisateur dans le dossier partagé sur l'AD. Le lecteur réseau au nom de l'utilisateur doit être remonté :