Alesio ARAPI BTS SIO

Amine ATTMANIE 1ere année

RAPPORT DE PROJET

La Méthode AGDLP :

Account Global Domain Local Permissions

Sommaire :

1.Comment ça marche.

La méthode AGDLP est un principe de gestion des droits d'accès aux ressources partagées d'une entreprise, préconisé par Microsoft, basé sur les groupes de sécurité d'Active Directory et leurs étendues**.**

Cette méthode consiste à rendre membre des utilisateurs (**Account**), de groupes globaux (**Global**), ajouter ces groupes globaux dans des groupes de domaine local (**Domain Local**) et pour terminer, attribuer aux groupes de domaine local des permissions NTFS sur les ressources (**Permissions**), les permissions NTFS étant les autorisations attribuées sur un objet dossier ou fichier.

Définition des étendues de groupes :
L'étendue d'un groupe définit les objets qui peuvent en être membre ainsi que l'emplacement où ils peuvent être utilisés, c'est-à-dire seulement dans le domaine où il a été créé ou dans toute la forêt. Il existe 3 étendues de groupe de sécurité :

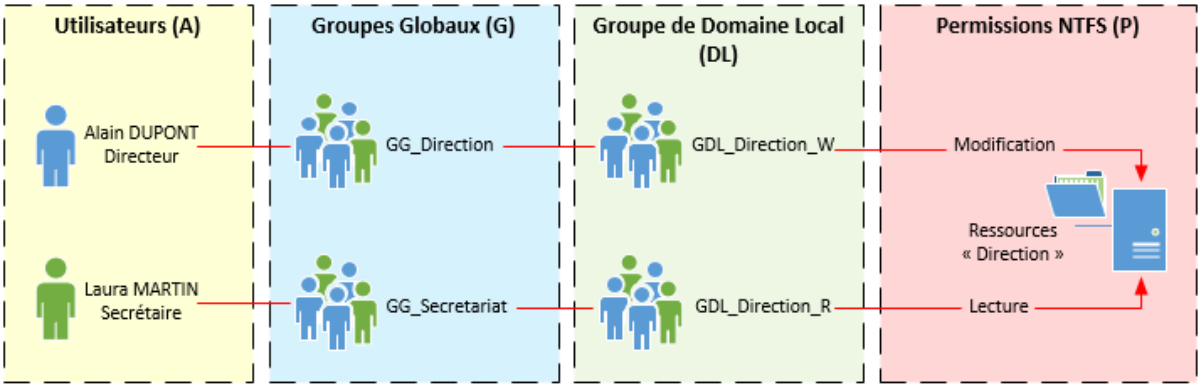
Groupe de domaine local (GDL): il peut contenir des utilisateurs, des groupes globaux et universels de tous les domaines de la forêt et des groupes de domaine local de son propre domaine. Il peut seulement être utilisé pour fixer des permissions à des ressources dans le domaine dans lequel il a été créé.

Groupe global (GG): il peut contenir des comptes utilisateurs et des groupes globaux du même domaine et tous autres objets d'un domaine approuvé. Il peut être utilisé dans toute la forêt pour donner des permissions aux ressources de son propre domaine mais aussi celles sur les domaines de la forêt qui ont une relation d'approbation.

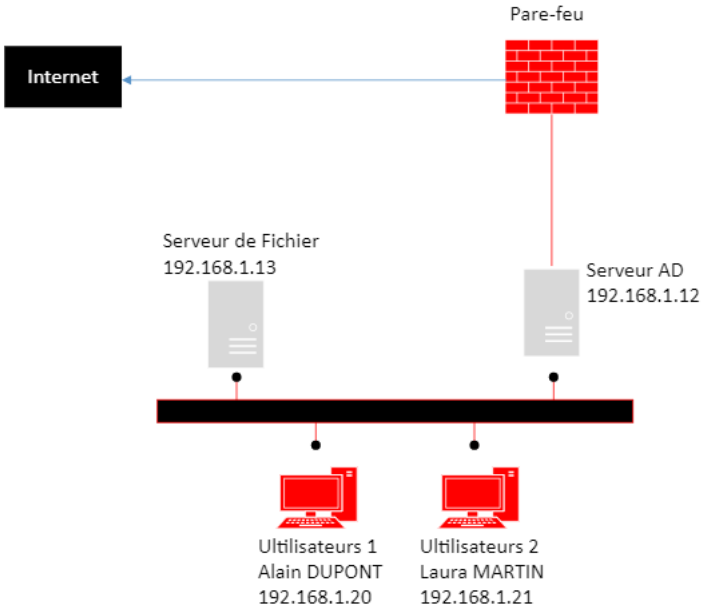
Groupe universel (GU): il peut contenir des comptes utilisateurs, des groupes globaux et universels de n'importe quel domaine de la forêt. Ce groupe a une portée maximale puisqu'il est accessible dans l'ensemble de la forêt.

2.Schema réseaux de l'environnement.

Pour ce cas précis, voici une illustration des groupes que nous pouvons créer et des droits que nous pouvons appliquer tout en respectant le principe de la méthode AGDLP :



Ce qui donne ça en schéma réseaux :



3. Création des machines et création des groupes

Pour commencer il faut déjà créer les machines et les groupes.

Pour les machines on aura comme le montre le schéma ci-dessus :

- 2 utilisateurs

- 1 serveur AD

- 1 serveur de fichier

Et on aura aussi deux groupes :

Groupe 1 :

GG_Direction

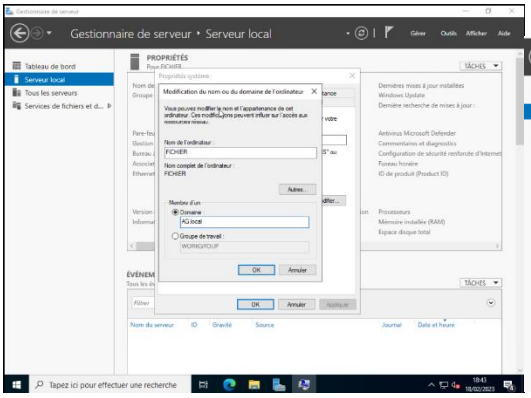
GDL_Direction_W

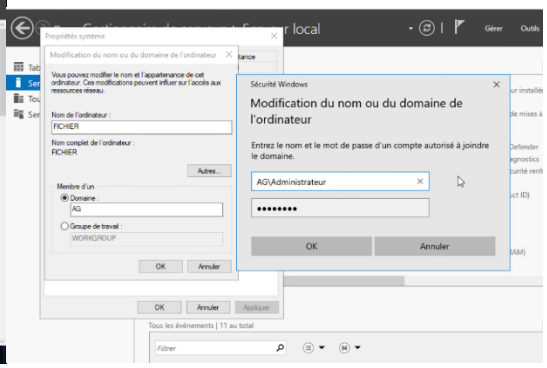
Groupe 2 :

GG_Secretariat

GDL_Direction_R

Donc pour commencer on ajoute le serveur de fichier dans l'AD

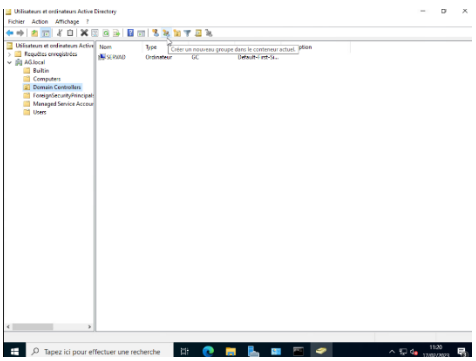


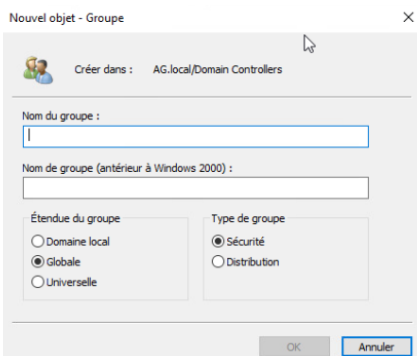


Et ensuite on commence à créer les groupes :

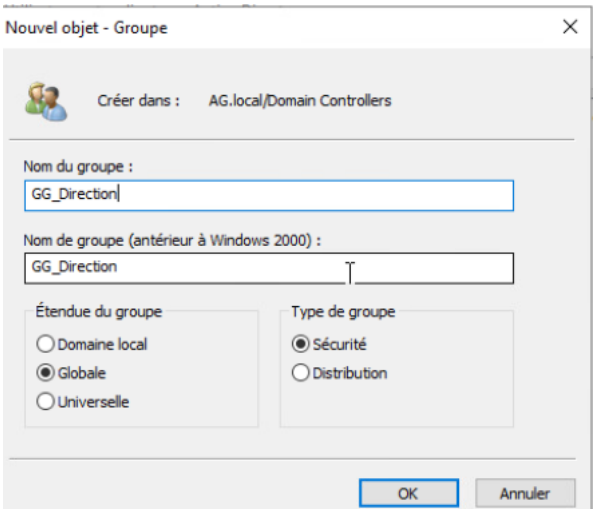
Groupe 1 : Direction

Pour commencer on commence par aller dans le gestionnaire des utilisateurs et on créer un nouveau groupe





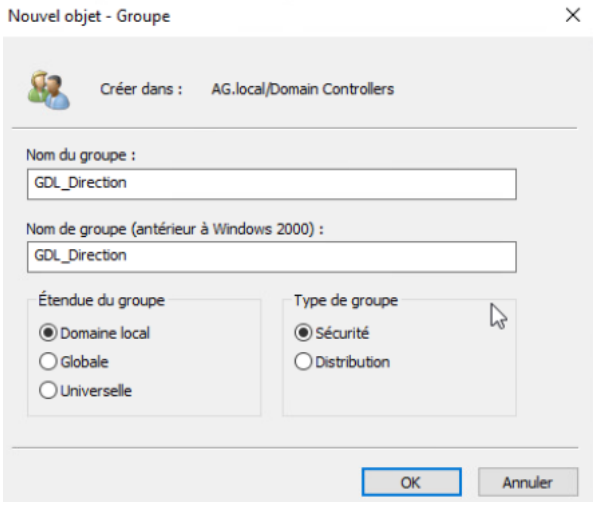
Et on met le nom du groupe ici c'est GG_Direction



Puis on confirme

En étendue globale puisque GG = Groupe Globale

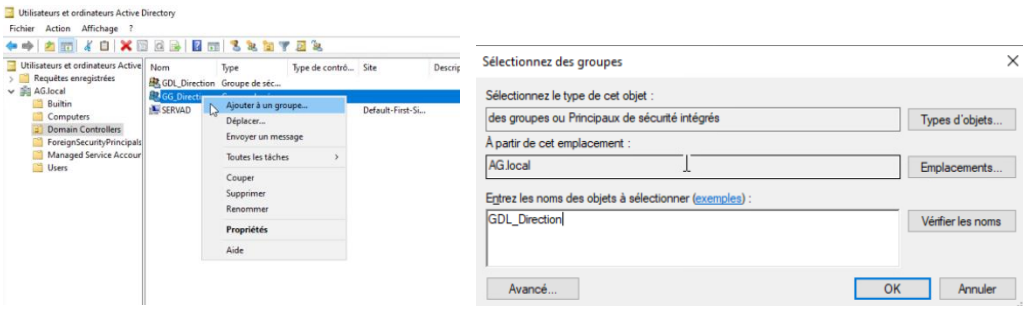
Puis on créer un autre groupe GDL_Direction

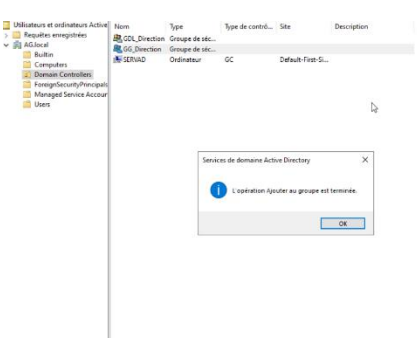


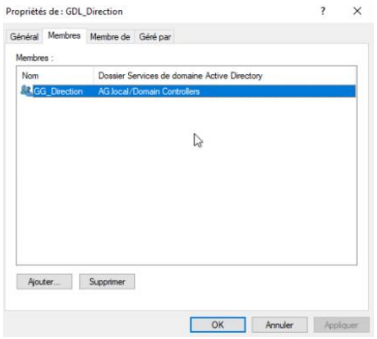
Ici en domaine local

GDL = Groupe Domaine Local

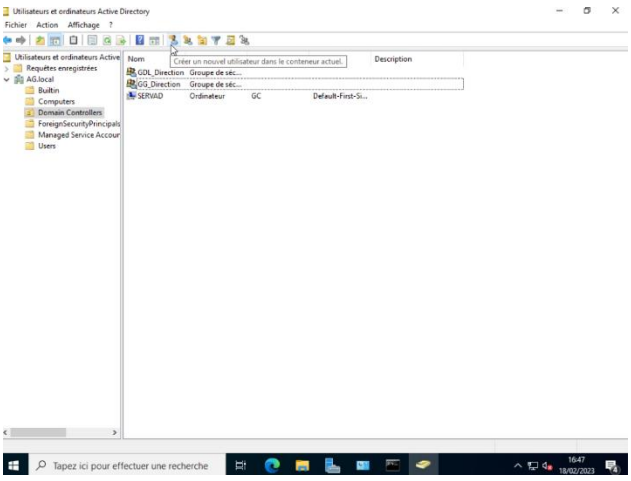
Puis on ajoute le groupe GG dans le Groupe GDL



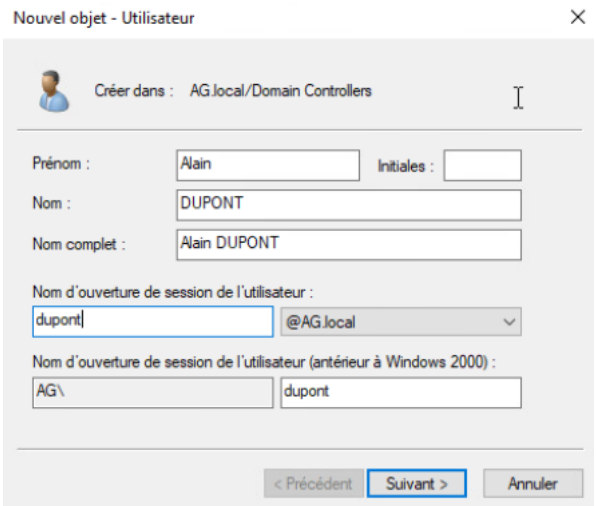


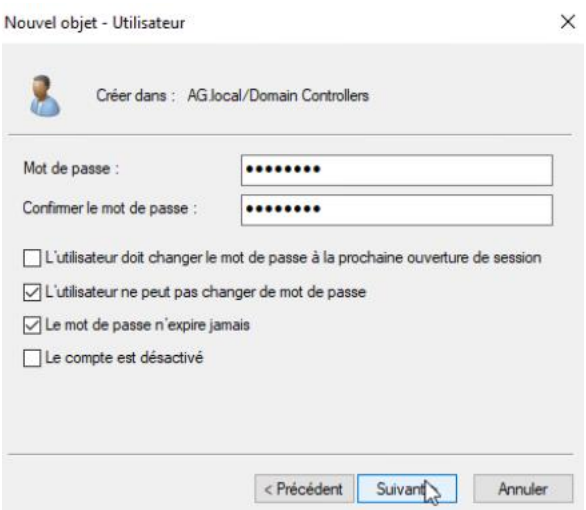


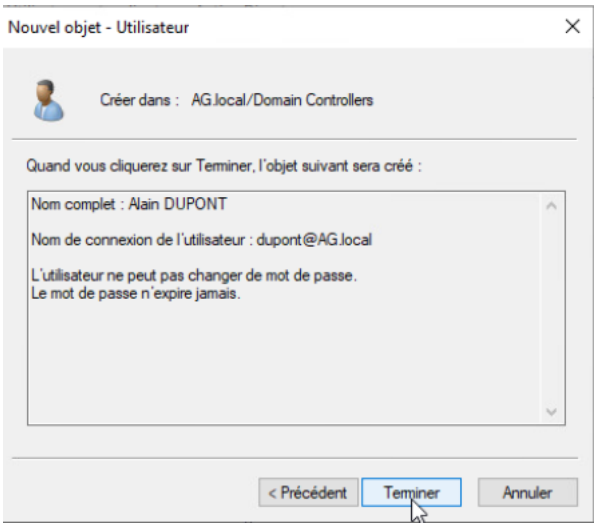
Puis on va créer un utilisateur qui va aller dans le groupe :



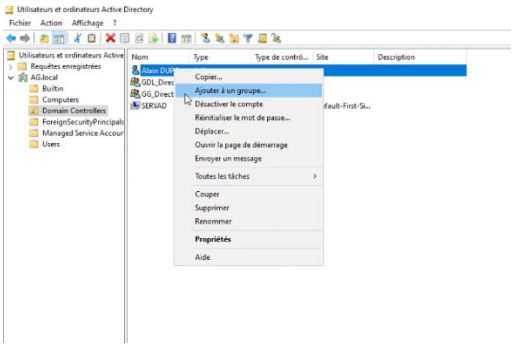
Et on rentre les info de la personne en question

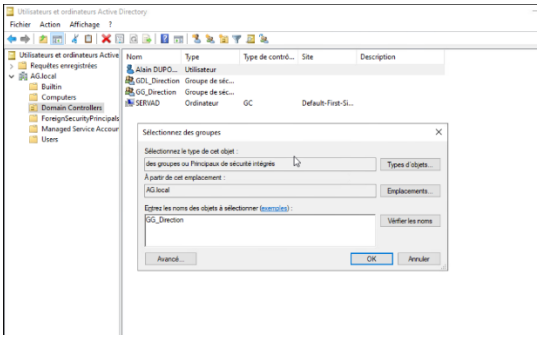




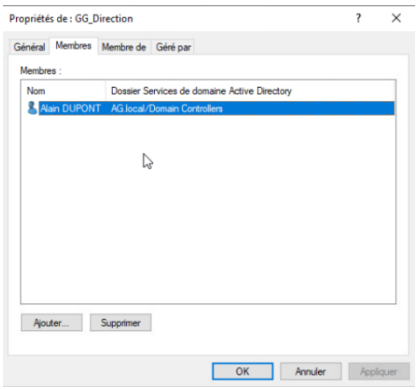


Puis on ajoute l'utilisateur au groupe GG_Direction :

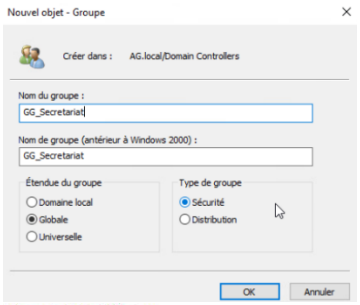


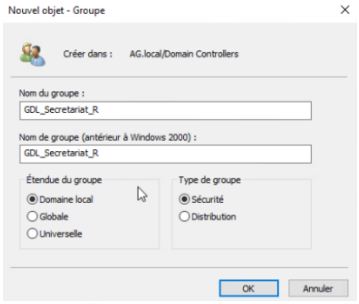


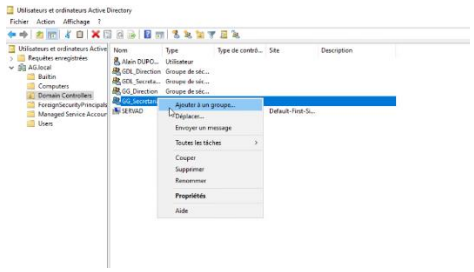
Et on peut voir qu'il est bien à l'intérieure dans les membres

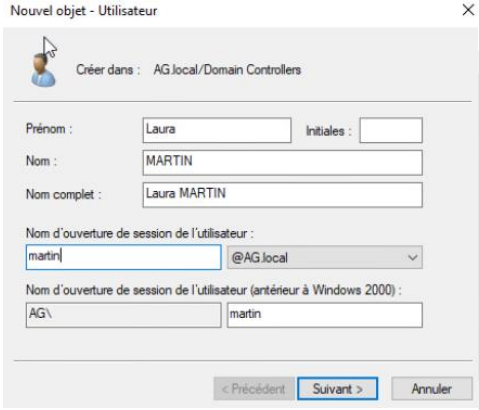


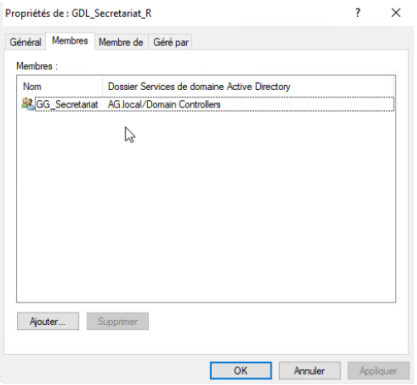
Puis on fait pareil pour le Groupe Secretariat

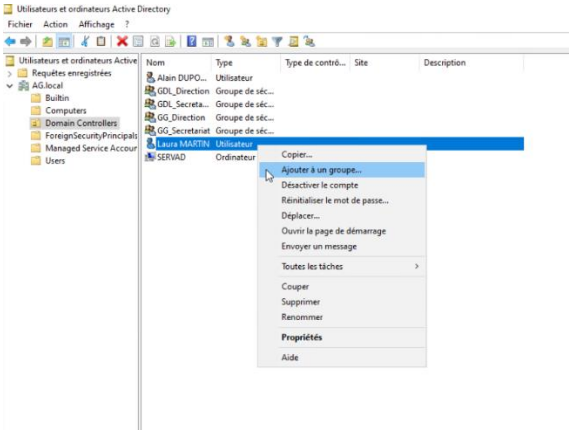

Nouvel objet - Groupe
Créer dans : AG.local/Domain Controllers
Nom du groupe :
GG_Secretariat
Nom de groupe (antérieur à Windows 2000) :
GG_Secretariat
Étendue du groupe
Domaine local
Globale
Universelle
Type de groupe
Sécurité
Distribution
OK
Annuler

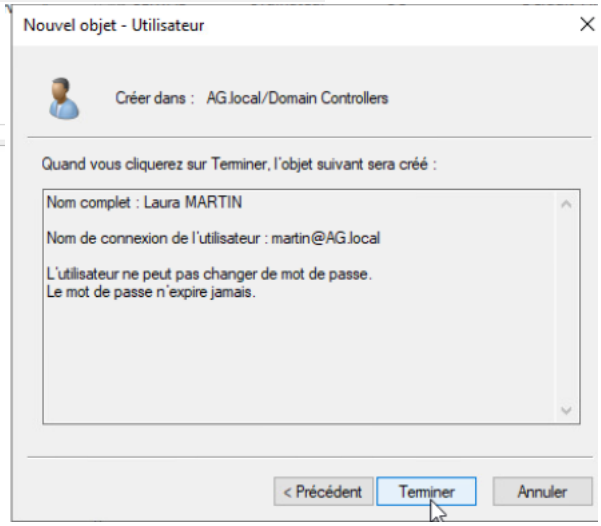

Nouvel objet - Groupe
Créer dans : AG.local/Domain Controllers
Nom du groupe :
GDL_Secretariat_R
Nom de groupe (antérieur à Windows 2000) :
GDL_Secretariat_R
Étendue du groupe
Domaine local
Globale
Universelle
Type de groupe
Sécurité
Distribution
OK
Annuler

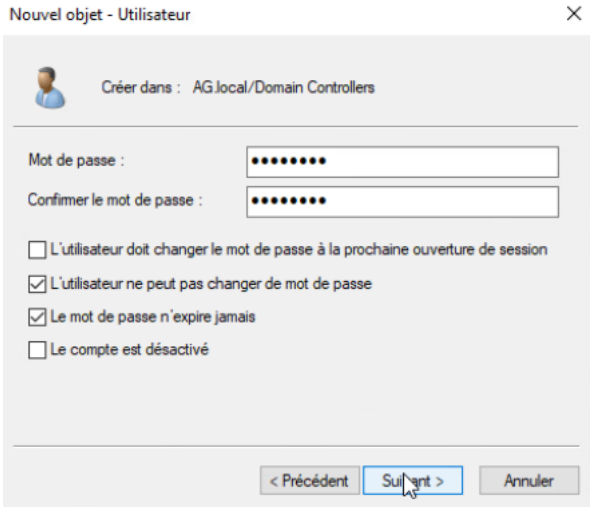

Utilisateurs et ordinateurs Active Directory
Fichier Action Affichage
Ajouter à un groupe...
Déplacer...
Envoyer un message
Toutes les tâches
Couper
Supprimer
Renommer
Propriétés
Aide


Nouvel objet - Utilisateur
Créer dans : AG.local/Domain Controllers
Prénom : Laura
Initiales :
Nom : MARTIN
Nom complet : Laura MARTIN
Nom d'ouverture de session de l'utilisateur :
martin
@AG.local
Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :
AG\
martin
< Précédent
Suivant >
Annuler

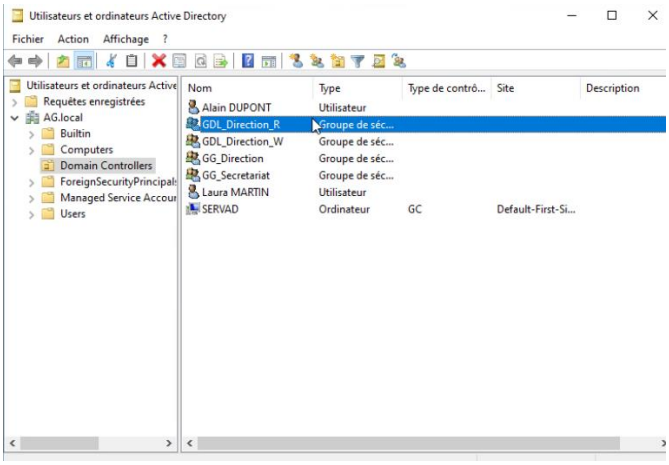

Propriétés de : GDL_Secretariat_R
Général
Membres
Membre de
Géré par
Membres :
Nom
Dossier Services de domaine Active Directory
GG_Secretariat
AG.local/Domain Controllers
Ajouter...
Supprimer
OK
Annuler
Appliquer


Utilisateurs et ordinateurs Active Directory
Fichier Action Affichage
Requêtes enregistrées
AG.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accour
Users
Nom
Type
Type de contrô...
Site
Description
Alain DUPO...
GDL_Direction
GDL_Secreta...
GG_Direction
GG_Secretariat
Laura MARTIN
SERVAD
Utilisateur
Groupe de séc...
Ordinateur
Copier...
Ajouter à un groupe...
Désactiver le compte
Réinitialiser le mot de passe...
Déplacer...
Ouvrir la page de démarrage
Envoyer un message
Toutes les tâches
Couper
Supprimer
Renommer
Propriétés
Aide


Nouvel objet - Utilisateur
Créer dans : AG.local/Domain Controllers
Quand vous cliquerez sur Terminer, l'objet suivant sera créé :
Nom complet : Laura MARTIN
Nom de connexion de l'utilisateur : martin@AG.local
L'utilisateur ne peut pas changer de mot de passe.
Le mot de passe n'expire jamais.
< Précédent
Terminer
Annuler

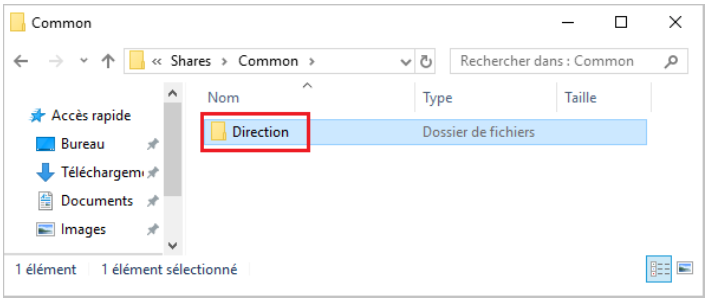

Nouvel objet - Utilisateur
Créer dans : AG.local/Domain Controllers
Mot de passe :
Confirmer le mot de passe :
L'utilisateur doit changer le mot de passe à la prochaine ouverture de session
L'utilisateur ne peut pas changer de mot de passe
Le mot de passe n'expire jamais
Le compte est désactivé
< Précédent
Suivant >
Annuler

Pour mieux renconnaitre on a renommer le groupe GDL_Secretariat en GDL_Direction_R comme sur le schema

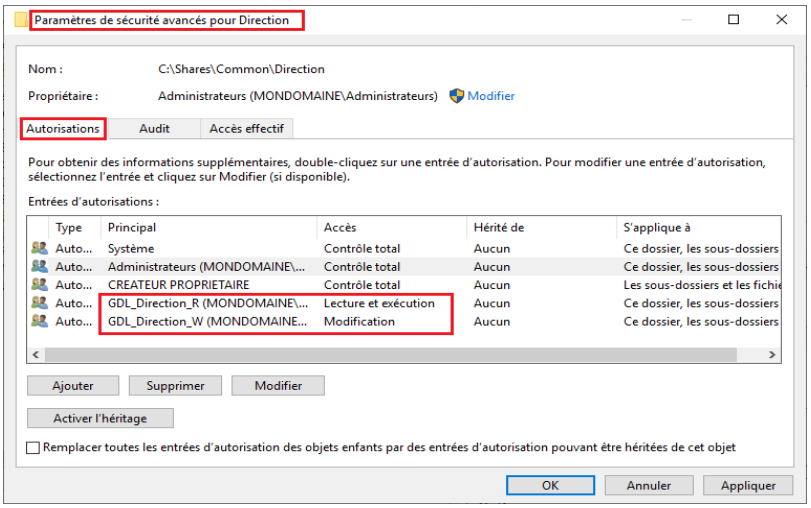


4.Comment donner les permissions

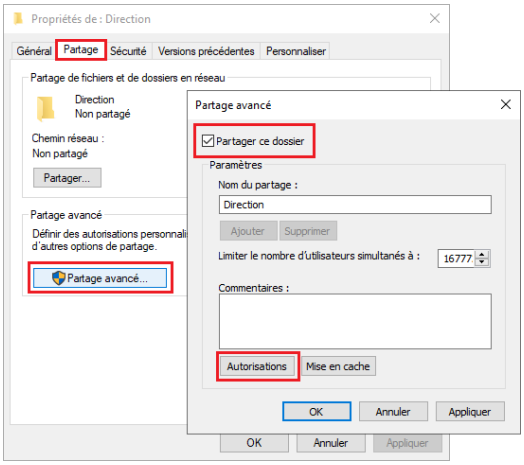
Créer le dossier sur le serveur de fichiers



Désactiver l'héritage et supprimer les permissions données par défaut au groupe utilisateurs, et attribuer les droits aux groupes de Domaine Local



Ensuite il faut aller dans l'onglet partage, partage avancer et cocher la case partager ce dossier



Voila et si jamais un autre utilisateur a besoin d'accéder au fichier il faudra juste l'ajouter dans le groupe qui lui correspond.

En conclusion je dirais que la méthode AGDLP est un réel gain de temps pour les administrateurs mais aussi un moyen de sécuriser son serveur de fichiers. Et il est plus simple de faire un suivi des droits utilisateurs sur un dossier s'ils sont tous répertoriés dans un seul groupe.