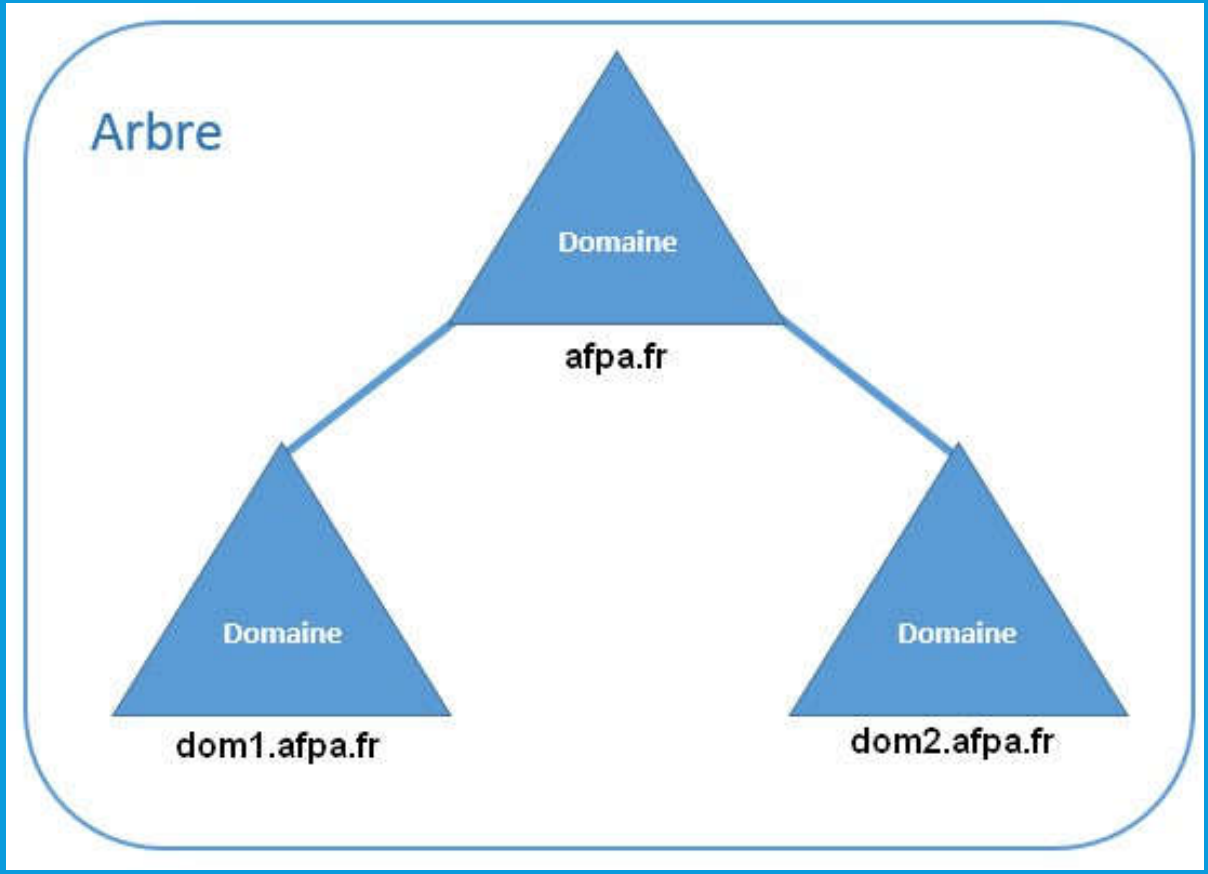
INTRODUCTION

Domaine- Arbre - Forêt

UN ARBRE DE PLUSIEURS DOMAINES

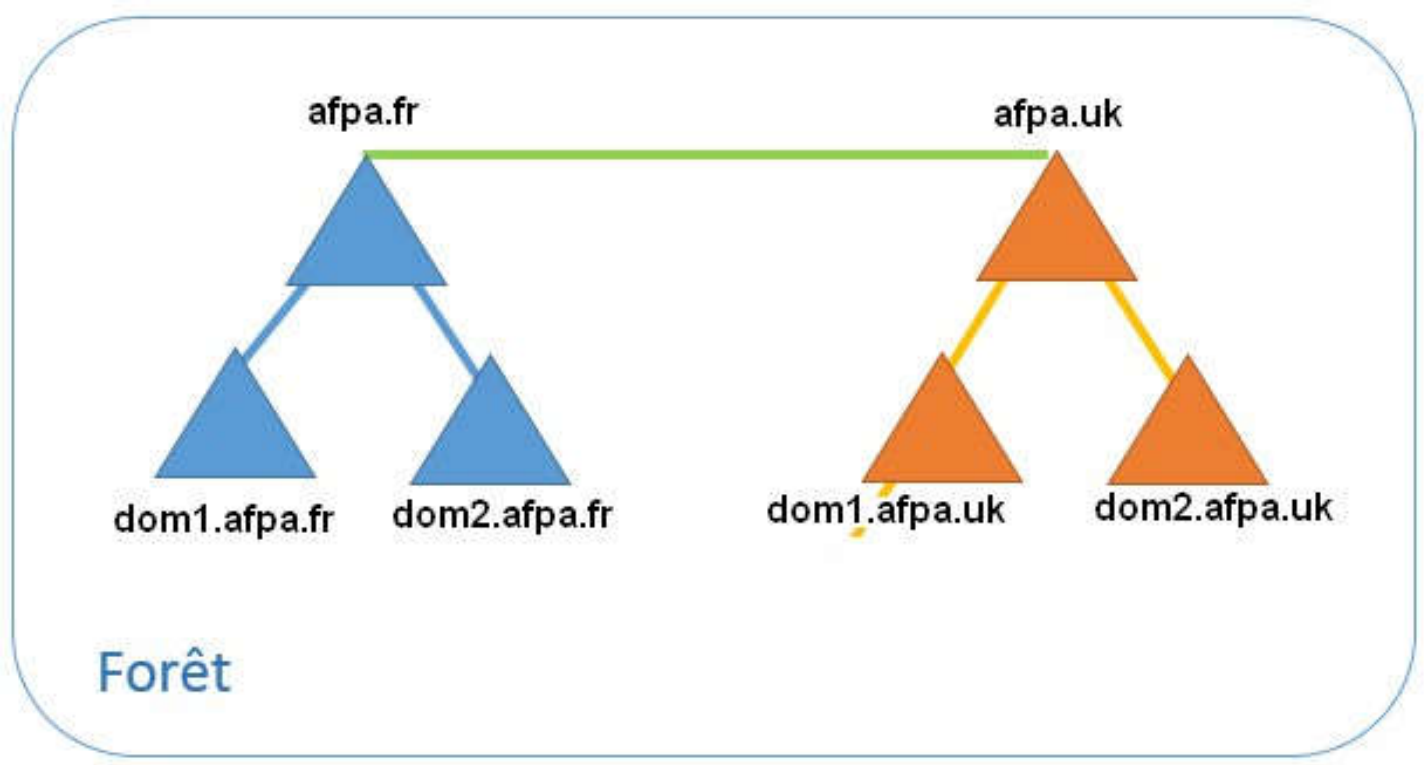


Lorsqu'un domaine principal contient plusieurs sous-domaines on parle alors d'arbre, où chaque sous-domaine au domaine racine représente une branche de l'arbre.

(Le domaine racine étant ici afpa.fr)

Les domaines d'un même arbre partagent un espace de nom contigu et hiérarchique.

DEUX ARBRES FORMANT UNE FORET



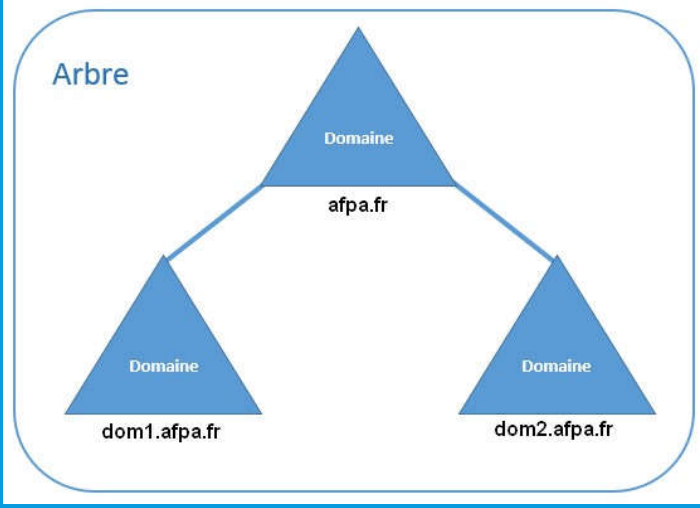
Une forêt est un regroupement d'une ou plusieurs arborescences de domaine, autrement dit d'un ou plusieurs arbres.

Ces arborescences de domaine sont indépendantes et distinctes bien qu'elles soient dans la même forêt.

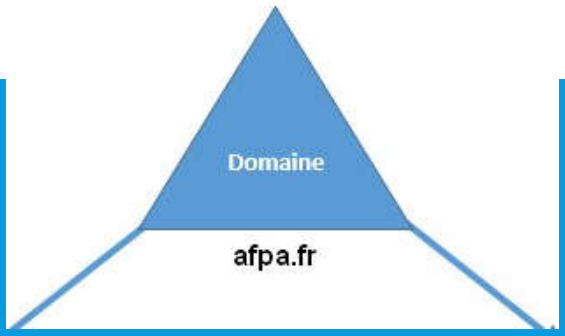
Afpa.uk n'est qu'un exemple …

DOMAINE

Au sein d'un des domaines schématisé, on retrouvera tout un ensemble d'Unités d'Organisation remplies d'objets de différentes classes : utilisateurs, ordinateurs, groupes, contrôleurs de domaine, etc.



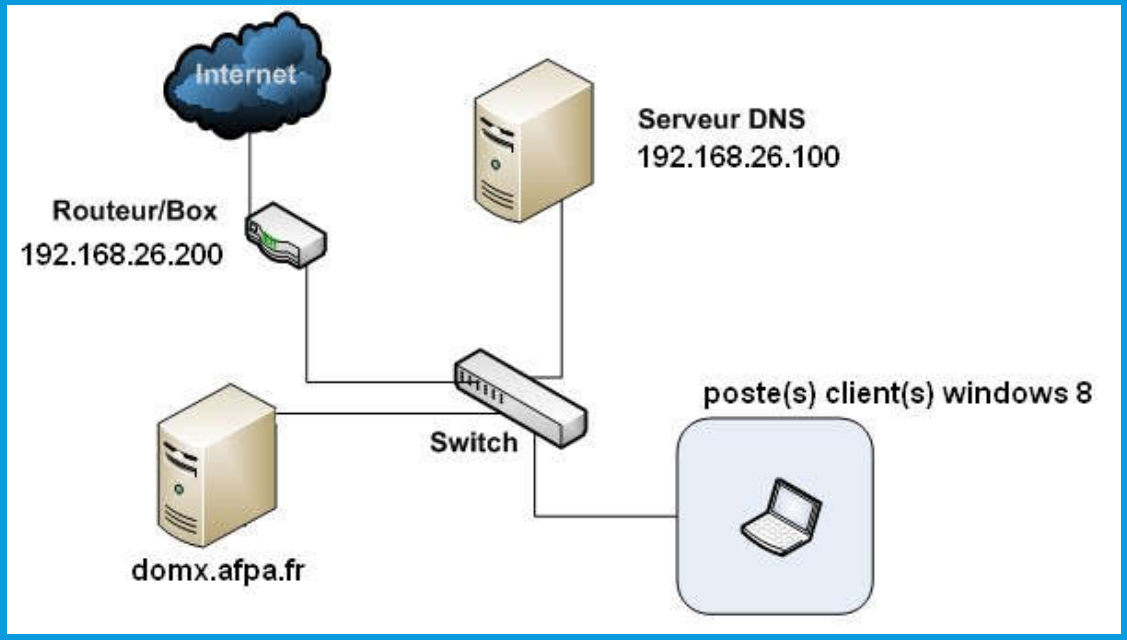
AFPA.FR



Afpa.fr est la racine, il est le serveur de domaine avec ici un rôle DNS.

Son compte administrateur est isogooo$$

Il est maître de schéma
Il est maître de nom de domaine
Il a le catalogue global



« DOMX.AFPA.FR »

Création des domaines

DOMAINE PRIMAIRE ET SECONDAIRE

2ième SERVEUR

Le Contrôleur de Domaine Principal (CPD)

(Synchronisation Horloge)

+ Maître d'infrastructure

(Maj des objets des autres domaines)

192.168.26.112

synchronisation

1ER SERVEUR

Le Contrôleur de Domaine Secondaire (CSD)

+ Maître RID (attribution des SID des objets)

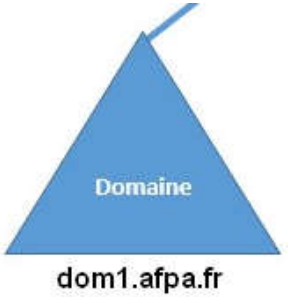
+ Possède le catalogue global (CG)

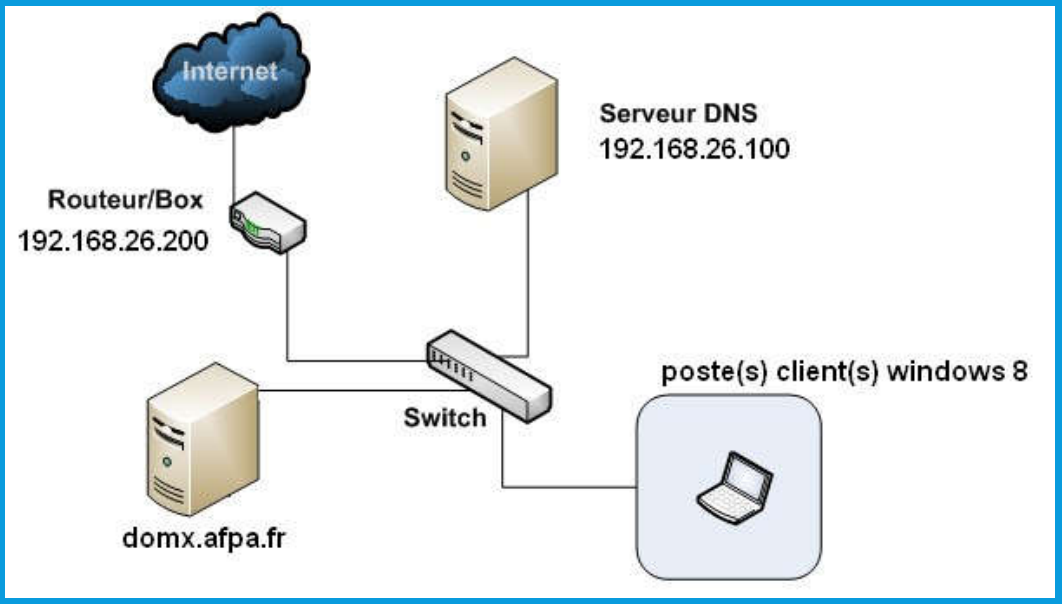
(Permet de rechercher les objets dans la forêt via le port 3268 et possède les infos sur les utilisateurs des groupe Universels).

192.168.26.111

- Fonctionnalités après transfert avec NTDSutil
- Vérifiables avec « net dom query fsmo »

Administrateur local : NomSV1
+ administrateur de restauration des services d'annuaire





« POSTES CLIENTS »

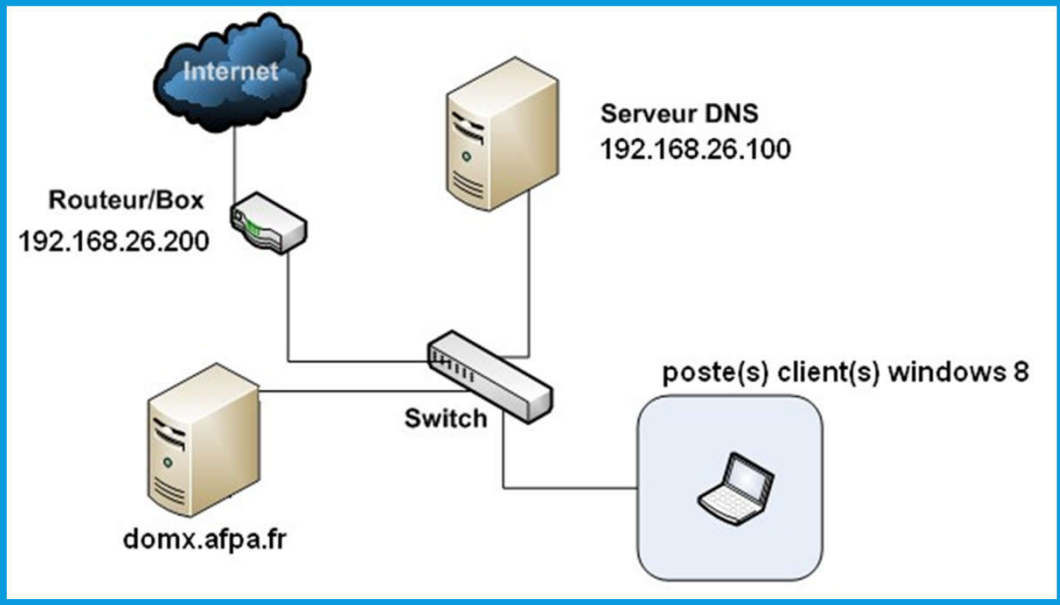
LE(S) POSTE(S) CLIENT(S)

Après avoir rejoins le domaine, l'utilisateur du poste client (Windows 8) sur le domaine est du « type »
utilisateur.domx.afpa.fr

Son IP est 192.168.26.112
La passerelle : 192.168.26.200
Le serveur DNS : 192.168.26.100

Les utilisateurs sont :
- soit des utilisateurs « local » (hors domaine)
- ou des utilisateurs membres du domaine (connexion authentifiée sur le domaine).

Administrateur local : NomSW



« UTILISATEURS, GROUPES, A.G.DL.P/A.G.U.DL.P »

Organisation des objets de l'AD du domaine dans les OU

STRATEGIE DES GROUPES DU CATALOGUE GLOBAL DE NOTRE CONTROLEUR DE DOMAINE

A.G.DL.P pour une forêt qui n'a **qu'un domaine**

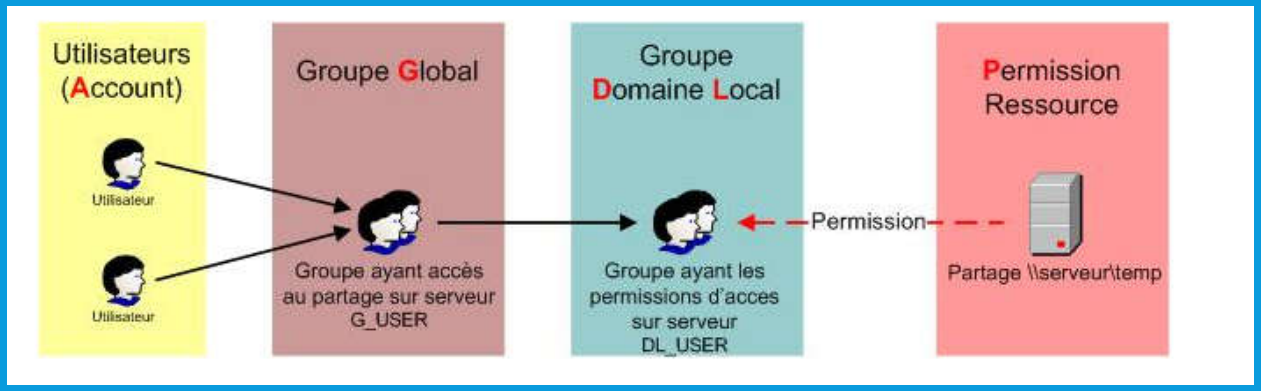
A.G.U.DL.P lorsqu'il y a **plusieurs domaines dans la forêt**

AGLP désigne : Account, Global group, Domain Local group, Permission.

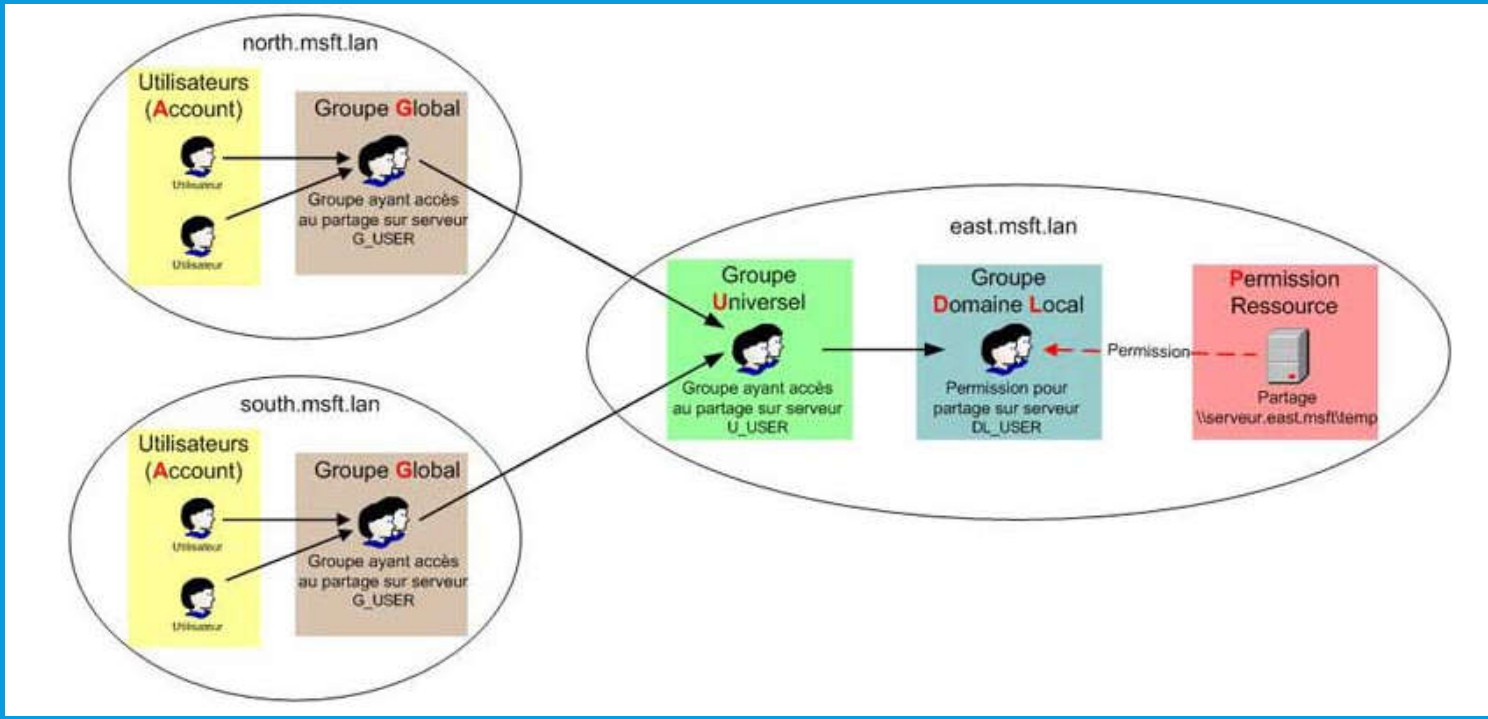
Quand vous créez votre arborescence Active Directory (dans la console « Utilisateurs et ordinateurs Active Directory »), vous devez ajouter vos utilisateurs et vos groupes, **la méthode consiste donc à:**

- Affecter les utilisateurs (accounts) dans des Groupes globaux (Global groups)
- Ajouter les Groupes globaux aux Groupes Locaux (Domain Local group)
- Enfin, ces groupes sont utilisés pour attribuer des permissions NTFS (sur partages, dossiers ou fichiers).

AGDLP



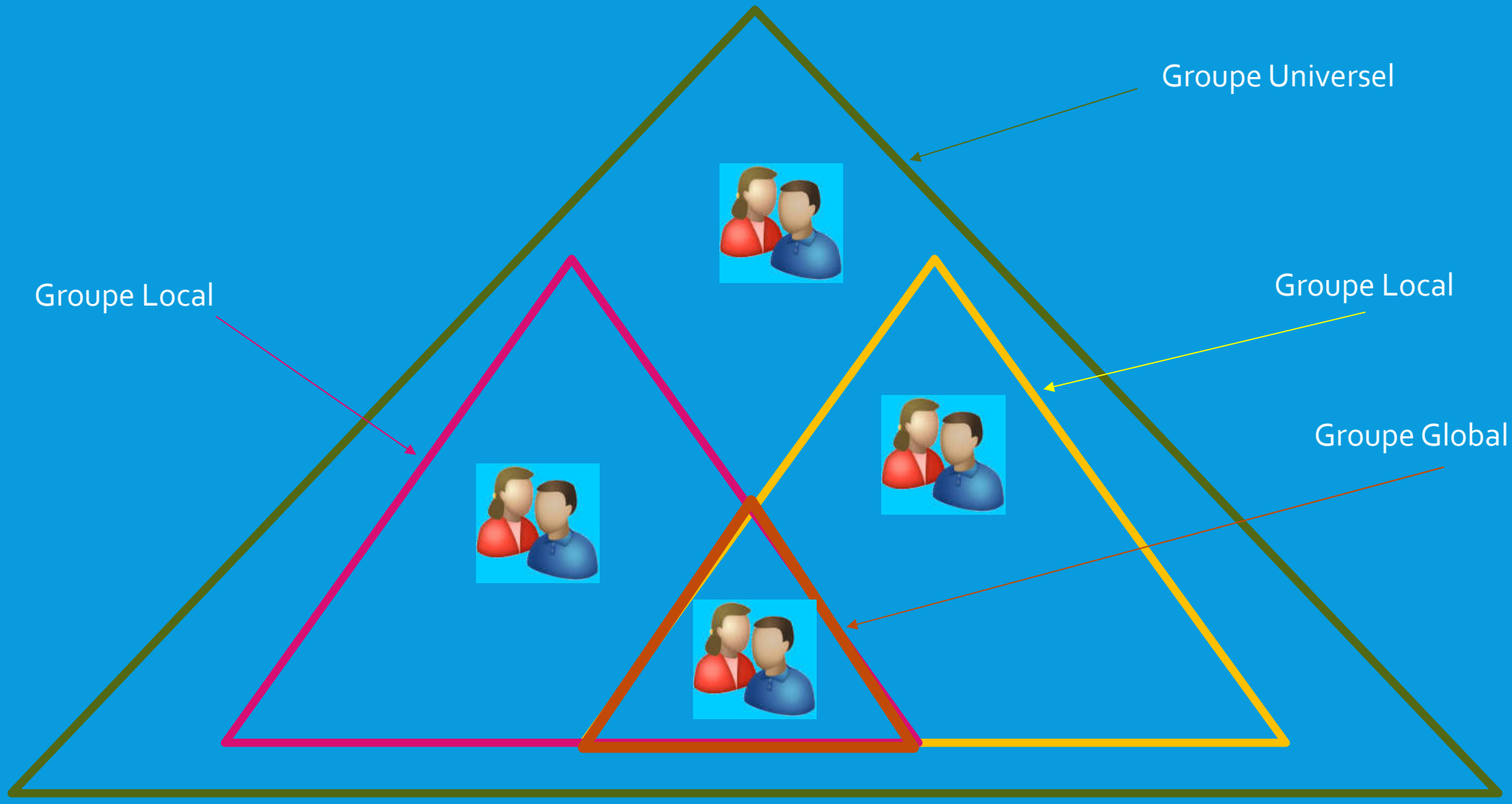
AGUDLP



Un PETIT RECAPITULATIF ...

Scope	Membres	Permissions
Universel	- Compte de n'importe quel domaine appartenant à la même forêt. - Groupe Global de n'importe quel domaine appartenant à la même forêt. - Groupe Universel de n'importe quel domaine appartenant à la même forêt.	N'importe quel domaine ou forêt.
Global	- Compte du même domaine - Groupe Global du même domaine	N'importe quel domaine
Local	- Compte de n'importe quel domaine ou forêt - Groupe Global de n'importe quel domaine ou forêt - Groupe Universel de n'importe quel domaine ou forêt - Groupe Local du même domaine	Uniquement le domaine d'appartenance

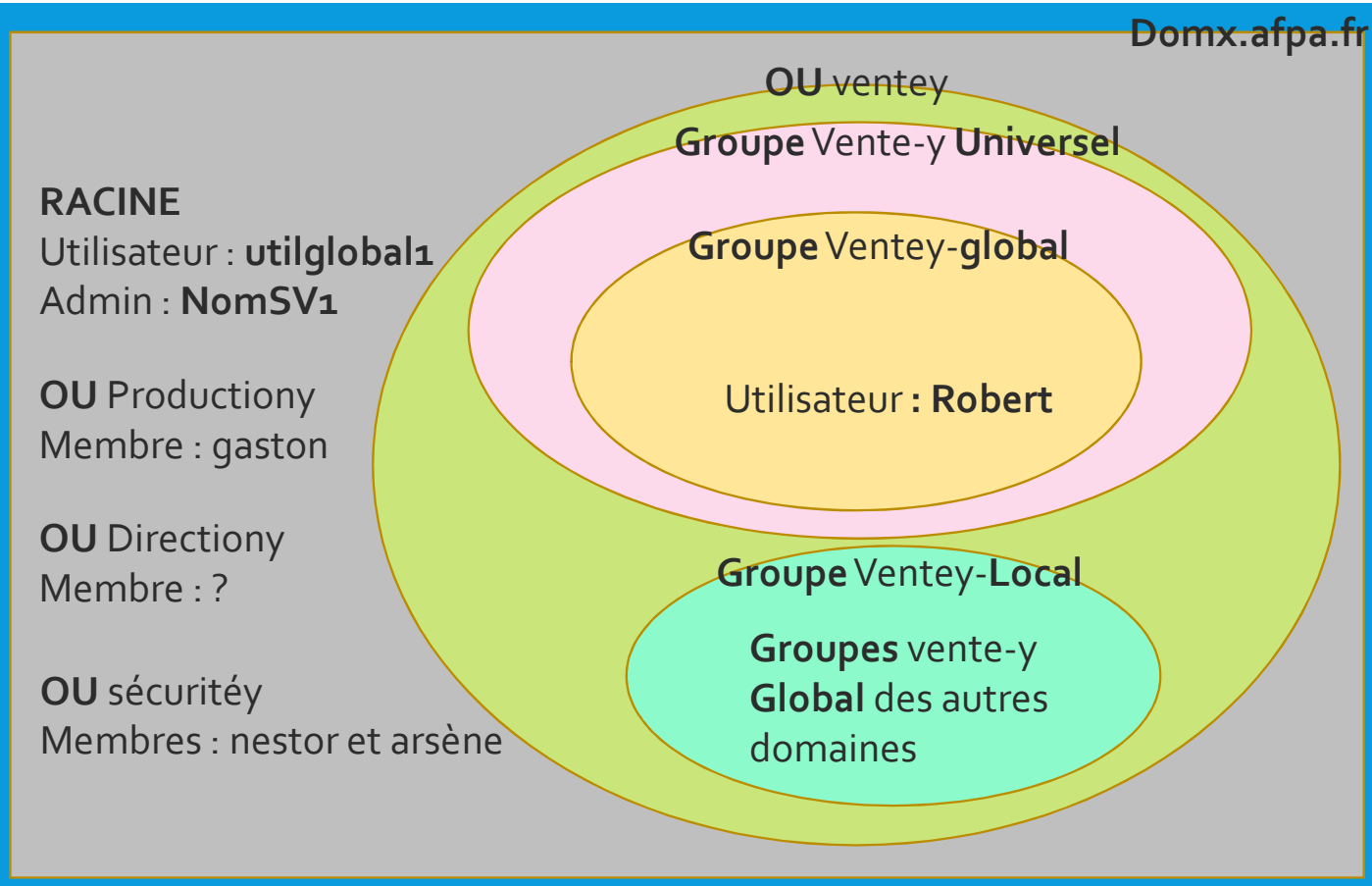
UN DESSIN PLUTÔT QU'UN DISCOURS …



DANS LE TP4
SCHEMA « UTILISATEURS/GROUPES »

OU
Ventey
Productiony
Directiony

Dans l'OU ventey
GROUPE GLOBAL : ventey-global
GROUPE LOCAL : ventey-local
GROUPE UNIVERSEL : ventey-universel



« PROFIL UTILISATEUR DU DOMAINE »

Profil itinérant

DROITS DE PARTAGE ET DROITS NTFS

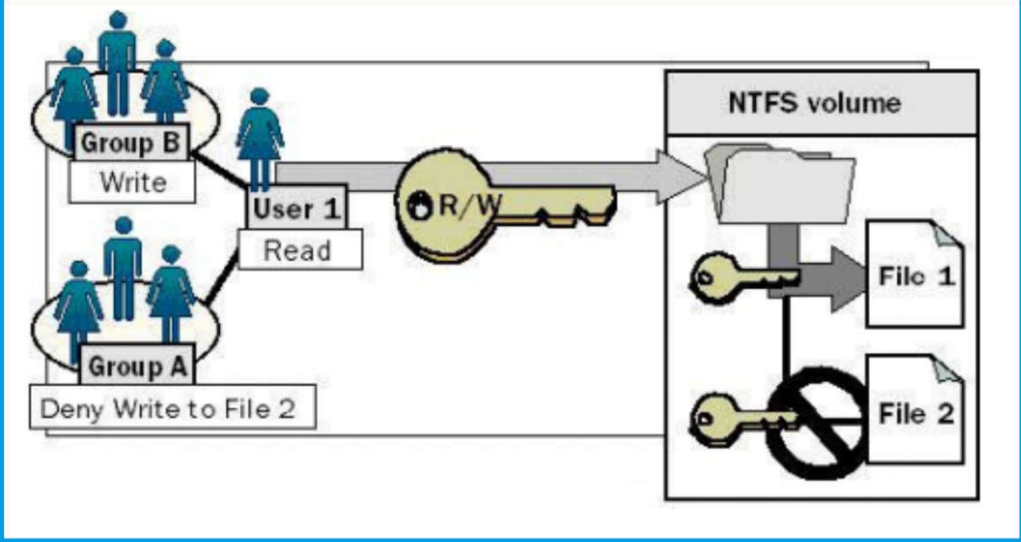
Les autorisations de partage servent à définir les droits d'accès a un dossier via le réseau.

Les autorisations NTFS servent à définir les droits d'accès « tout court » à un dossier ou un fichier, qu'il soit partagé ou pas, par le réseau ou directement sur la machine.

A savoir:

- le fait de mettre des droits NTFS ne rend pour autant le fichiers accessible par le réseau, **il faut quand même le partager.**
- Si tu as des droits différents dans le partage et le NTFS, ce sont **les plus restrictifs qui s'appliquent** (exemple : si un user a contrôle total en partage et lecture seule en NTFS, le droit effectif sera lecture seule.

Pour toutes ces raisons (et pour éviter de se compliquer la vie), les admins pour configurer un dossier à partager mettent contrôle total « tout le monde » en partage, et règlent les droits uniquement avec le NTFS.



UN PETIT RÉCAPITULATIF DES DROITS NTFS APPLICABLES ...

Droits	Contrôle Total	Modifier	Lire et exécuter	Lister le contenu du dossier	Lecture	Ecriture
Traverser le dossier Exécuter le fichier	☑	☑	☑	☑		
Lister les dossiers Lire les données	☑	☑	☑	☑	☑	
Attributes de lecture	☑	☑	☑	☑	☑	
Attributes de lecture étendus	☑	☑	☑	☑	☑	
Créer des fichiers Ecrire des données	☑	☑				☑
Créer des dossiers Ajouter des données	☑	☑				☑
Attributs d'écriture	☑	☑				☑
Arributs d'écriture étendus	☑	☑				☑
Supprimer des sous-dossiers Supprimer des fichiers	☑					
Supprimer	☑	☑				
Lire les autorisations	☑	☑	☑	☑	☑	☑
Modifier les autorisations	☑					
Devenir propriétaire de l'objet	☑					
Syncrhoniser	☑	☑	☑	☑	☑	☑

POUR LE DOSSIER PROFIL « ITINERANT » …

Le dossier « partage » contiendra le dossier « profil » dans lequel seront situés « les profils des utilisateurs itinérants. Dans les autres cas, en l'état actuel, le profil sera stocké en local sur le poste de travail du client.

Le dossier « profil » doit être partagé (pour être accessible par le réseau)
>> ***contrôle total à tout le monde*** (ou à tous les utilisateurs authentifiés de préférence)
NB: *il peut être caché en mettant profil**$** en « nom de partage »*

Les droits NTFS (droits de sécurité) du dossier profil :
Le dossier %username% sera créé à l'ouverture de session « au nom de l'utilisateur » par celui-ci, il n'est pas créé au départ lors de la saisie **du chemin UNC** dans le compte utilisateur.

- Il faut donc permettre la création à l'ouverture de la session d'un utilisateur **%username%**
(on ne connait pas son nom) d'un sous dossier « username » dans le dossier Profil
- Autoriser le système (L'OS) à créer/modifier dans le dossier Profil
- Permettre à l'utilisateur de créer et modifier des fichiers de son profil (il y a mes documents dans le profil ect …)
- Laisser des droits à l'administrateur sur le Dossier Profil

(%username% est une variable de l'environnement de l'OS qui contient le « login » du compte utilisateur)

REMARQUE :

Un utilisateur s'il « parcours » le réseau devrait **avoir accès uniquement à SON PROFIL !!!**

Je m'explique :

Exemple :

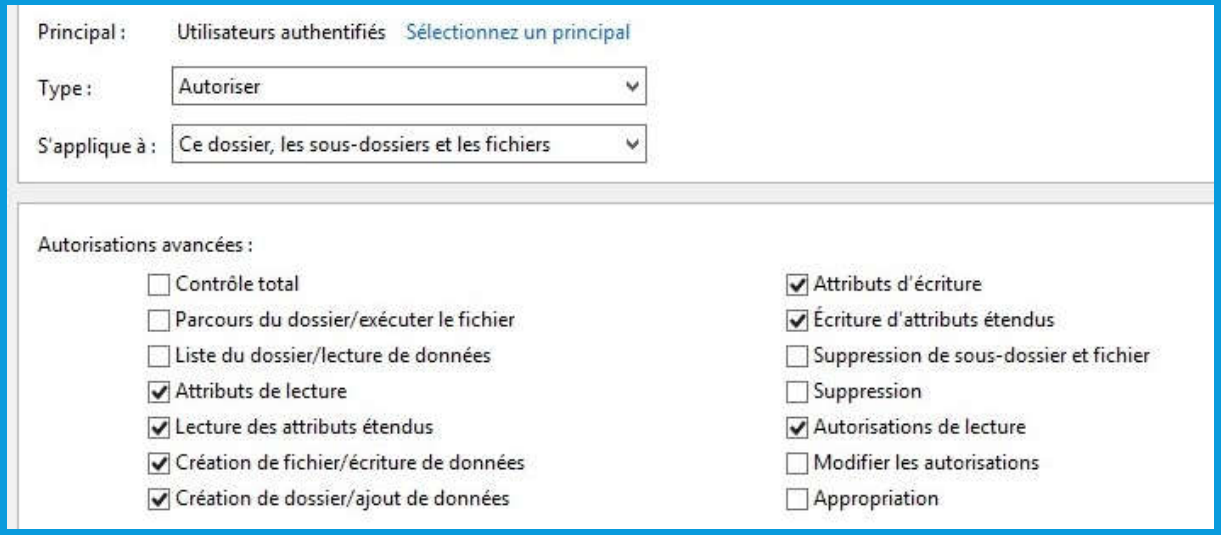
Le Directeur Général à un Profil Itinérant, il se connecte sur un poste et enregistre la liste des futurs licenciements dans son profil utilisateur … puis de déconnecte du poste de travail …

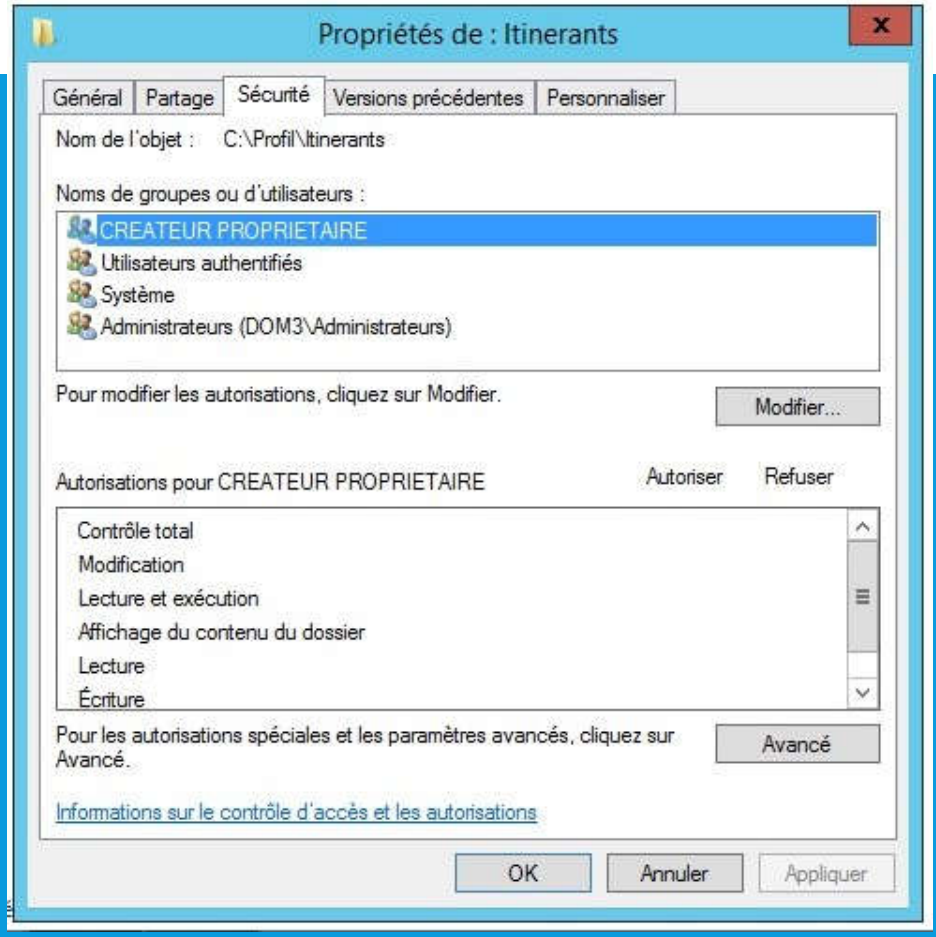
Sur ce poste arrive le délégué syndical qui possède un compte itinérant, il se connecte et « pas de chance » il parcours le réseau et voit le dossier de son DG dans le dossier Profil … il ouvre et regarde le contenu du profil du DG et …. « tombe accidentellement » sur la liste des futurs licenciement ….

DROITS NTFS DU DOSSIER PROFIL

- *Les administrateurs : CT (contrôle Total)*
- *Le système : CT*
- *Le créateur propriétaire : CT*
- *Les utilisateurs authentifiés : (ou les utilisateurs du domaine, plus restrictif …)*

… faire des droits « avancés … comme ci-dessous :





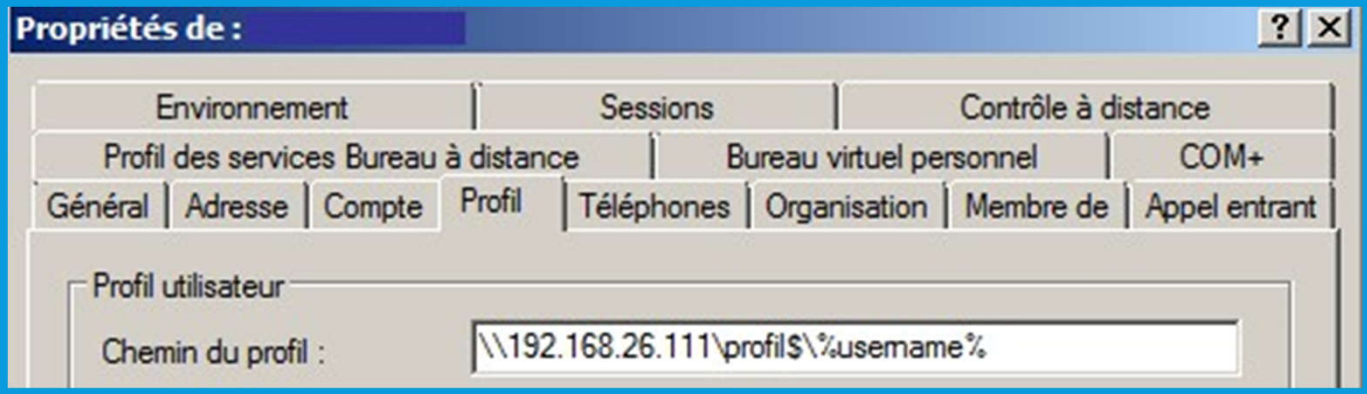
Ne pas oublier de mettre à jour les droits utilisateurs (gpudate /force) sur les postes clients avant la connexion.

PROFIL : CHEMIN UNC

Saisir un « chemin » du type
\\ip du serveur\dossier partagé

Eviter le nom du serveur (\\nom du serveur\dossier partagé\ …si le dns « saute »)
Ne pas utiliser c:\dossier partagé

Exemple :



« BASE DES UTILISATEURS DU DOMAINE »

« aparté .. »

DROITS NTFS DU DOSSIER BASE …

Le dossier base peut servir notamment à « héberger » le dossier mes documents qui a sera redirigé dans le TP sur les GPO afin que ce dernier ne soit plus dans le profil utilisateur …

Il va de soit qu'il ne doit être accessible que par l'utilisateur et pas par ses collègues, c'est son dossier « propre » et ceci n'est pas un espace de stockage collaboratif …

- Les administrateurs : CT (contrôle Total)
- Le système : CT
- Le créateur propriétaire : CT