Administration des systèmes et des réseaux

# B2 – 2eme année

# BTS SIO

lycée MATHIAS

Sommaire



## Référentiel

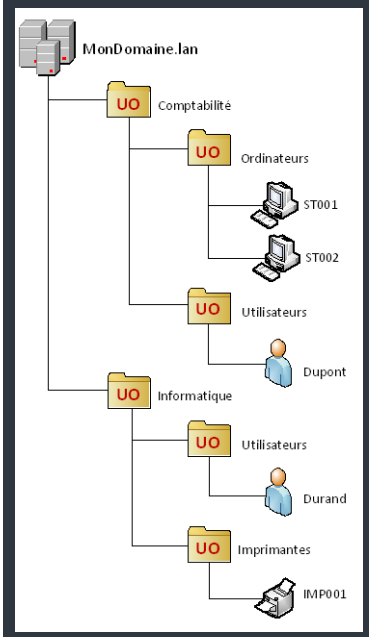
B2.2 –Installer, tester et déployer une solution d'infrastructure réseau.

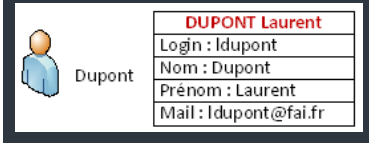
Déployer une solution d'infrastructure.

B2.3 – Exploiter, dépanner et superviser une solution d'infrastructure réseau.

Automatiser des tâches d'administration

## Exemple d'arborescence :



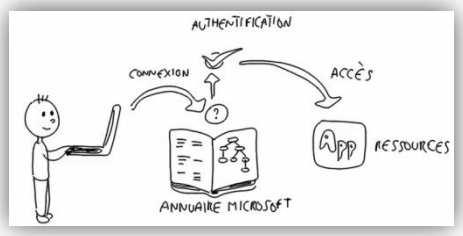




## La gestion des utilisateurs

*(Source : http://www.ofppt.info)*

Active Directory (AD) est la mise en œuvre par Microsoft des services d'annuaire LDAP pour les systèmes d'exploitation Windows.
L'objectif principal d'*Active Directory* est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows. Il permet également l'attribution et l'application de stratégies, la distribution de logiciels, et l'installation de mises à jour critiques par les administrateurs. *Active Directory* répertorie les éléments d'un réseau administré tels que les comptes des utilisateurs, les serveurs, les postes de travail, les dossiers partagés, les imprimantes, etc. Un utilisateur peut ainsi facilement trouver des ressources partagées, et les administrateurs peuvent contrôler leur utilisation grâce à des fonctionnalités de distribution, de duplication, de partitionnement et de sécurisation de l'accès aux ressources répertoriées.

**Comment apprendre l'Active Directory en vidéo** : **https://lc.cx/JwYw**




## I. Fonctionnement d'Active Directory

Un service d'annuaire est un service réseau qui identifie toutes les ressources d'un réseau et met ces informations à la disposition des utilisateurs ainsi que des applications.
Lorsqu'un utilisateur recherche un dossier partagé sur le réseau, le service d'annuaire identifie la ressource et fournit l'information à l'utilisateur.

### 1. Définition du service d'annuaire

Dans de grands réseaux, les ressources sont partagées par de nombreux utilisateurs et applications. Pour permettre aux utilisateurs et aux applications d'accéder à ces ressources et aux informations les concernant, une méthode cohérente est nécessaire pour nommer, décrire, localiser, accéder, gérer et sécuriser les informations concernant ces ressources. Un service d'annuaire remplit cette fonction.
Un service d'annuaire est un référentiel d'informations structuré concernant les personnes et les ressources d'une organisation. Dans un réseau Windows Server, le service d'annuaire s'appelle Active Directory.

## 2. Définition d'un schéma

Le *schéma* Active Directory contient les définitions de tous les objets, comme les utilisateurs, les ordinateurs et les imprimantes stockés dans Active Directory. Les contrôleurs de domaine ne comportent qu'un seul schéma pour toute une forêt. Ainsi, tous les objets créés dans Active Directory se conforment aux mêmes règles.
Le schéma possède deux types de définitions : les classes d'objets et les attributs.
Les *classes d'objets* comme utilisateur, ordinateur et imprimante décrivent les objets d'annuaire possibles que vous pouvez créer. Chaque classe d'objet est un ensemble d'attributs.
Les attributs sont définis séparément des classes d'objets. Chaque attribut n'est défini qu'une seule fois et peut être utilisé dans plusieurs classes d'objets. Par exemple, l'attribut **Description** est utilisé dans de nombreuses classes d'objets, mais il n'est défini qu'une seule fois dans le schéma afin de préserver la cohérence.

## 3. Structure logique d'Active Directory

Active Directory offre un stockage sécurisé pour les informations concernant les objets dans sa structure logique hiérarchique. Les *objets* Active Directory représentent des utilisateurs et des ressources, tels que des ordinateurs et des imprimantes. Certains objets en contiennent d'autres. Lorsque vous aurez compris le rôle et la fonction de ces objets, vous pourrez effectuer des tâches diverses, comme l'installation, la configuration, la gestion et le dépannage d'Active Directory.
La structure logique d'Active Directory inclut les composants suivants :

- ***Les objets.***
  Il s'agit des composants les plus élémentaires de la structure logique. Les *classes d'objets* sont des modèles pour les types d'objets que vous pouvez créer dans Active Directory. Chaque classe d'objet est définie par une liste d'*attributs*, qui définit les valeurs possibles que vous pouvez associer à un objet. Chaque objet possède une combinaison unique de valeurs d'attributs.
- ***Les unités d'organisation (OU, Organizational Unit).***
  Vous utilisez ces objets conteneurs pour organiser d'autres objets de telle manière qu'ils prennent en compte vos objectifs administratifs. La disposition de ces objets par unité d'organisation simplifie la recherche et la gestion des objets. Vous pouvez également déléguer l'autorité de gestion d'une unité d'organisation.
  Les unités d'organisation peuvent être *imbriquées* les unes dans les autres.
- ***Les domaines***.
  Unités fonctionnelles centrales dans la structure logique d'Active Directory, les domaines sont un ensemble d'objets définis administrativement qui partagent une base de données d'annuaire commune, des stratégies de sécurité et des relations d'approbation avec d'autres domaines. Les domaines disposent des trois fonctions suivantes :
  - Une limite d'administration pour objets
  - Une méthode de gestion de la sécurité pour les ressources partagées
  - Une unité de réplication pour les objets
- ***Les arborescences de domaines.***
  Les domaines regroupés en structures hiérarchiques sont appelés arborescences de domaines. Lorsque vous ajoutez un second domaine à une arborescence, il devient *enfant* du domaine racine de l'arborescence. Le domaine auquel un domaine enfant est attaché est appelé *domaine parent*. Un domaine enfant peut à son tour avoir son propre domaine enfant.
  Le nom d'un domaine enfant est associé à celui de son domaine parent pour former son nom DNS (Domain Name System) unique, par exemple **mathias.ac-dijon.fr**. De cette manière, une arborescence a un *espace de noms contigu*.
- ***Les forêts.***
  Une forêt est une instance complète d'Active Directory. Elle consiste en une ou plusieurs arborescences. Dans une arborescence unique à deux niveaux, qui est recommandée pour la plupart des organisations, tous les domaines enfants sont des enfants du domaine racine de la forêt afin de former une arborescence contiguë.
  Le premier domaine de la forêt est appelé le *domaine racine de la forêt*. Le nom de ce domaine fait référence à la forêt, par exemple **ac-dijon.fr**.

### Exercice 1 – Installation d'Active Directory.

Créez une nouvelle machine Windows Server 2019. Nommez-la **SrvAD**.
Installez Active Directory (**Services AD DS**) et le **Serveur DNS**.
Votre domaine sera **btssioX.lan** où **X** représente votre n° de machine.

Mot de passe de l'administrateur : **P@ssw0rd**
Adresse IP : **10.X.0.1**

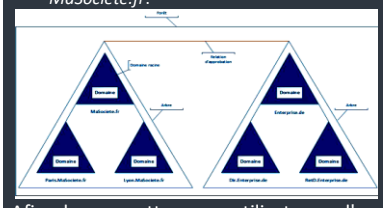
## Forêts, arbres et domaines

*(Source : fr.wikipedia.org/wiki/Active_Directory)*

*Active Directory* introduit la notion de hiérarchie sous la forme d'une arborescence dans laquelle les utilisateurs et les ordinateurs sont organisés en groupes et sous-groupes afin de faciliter l'administration des droits et restrictions utilisateur. C'est aussi *Active Directory* qui gère l'authentification des utilisateurs sur le réseau Windows. *Active Directory* exploite cette notion de hiérarchie intensivement, puisque l'entité de sécurité appelée « domaine » est également hiérarchisée dans un ensemble partageant un espace de nom commun, appelé « arborescence ». L'entité de plus haut niveau regroupant les arborescences de domaines constitue la forêt *Active Directory*.
L'AD permet une réplication multi-maître, c'est-à-dire que chaque contrôleur de domaine peut être le siège de modifications (ajout, modification, suppression) de l'annuaire, sous réserve de permission accordée par ACL, qui seront répliquées sur les autres contrôleurs de domaine. SAM ne disposait que d'une seule base en écriture, les autres répliquas étant en lecture seule.
À noter que les ensembles d'espaces de nom correspondant aux arborescences de l'AD formant la forêt *Active Directory* sont superposables à l'espace de nom formé par les zones DNS. DNS est un service indispensable pour le bon fonctionnement de toute l'architecture AD, localisation des contrôleurs de domaine, réplication, etc.

Une arborescence AD est composée de :

- **La forêt** : structure hiérarchique d'un ou plusieurs domaines indépendants (ensemble de tous les sous domaines *Active Directory*).
- **L'arbre** : domaine et toutes ramifications. Par exemple, dans l'arbre *MaSociete.fr*, *Paris.MaSociete.fr* et *Lyon.MaSociete.fr* sont des sous-domaines de *MaSociete.fr*.
- **Le domaine** : constitue les feuilles de l'arborescence. *Paris.MaSociete.fr* peut-être un domaine au même titre que *MaSociete.fr*.



Afin de permettre aux utilisateurs d'un domaine d'accéder aux ressources d'un autre domaine, AD utilise un mécanisme de relations d'approbation.
Les relations d'approbation au sein d'une même forêt sont automatiquement créées au moment de la création des domaines. Les limites par défaut des relations d'approbation sont fixées au niveau de la forêt, et non du domaine, elles sont implicites, et automatiquement transitives pour tous les domaines d'une même forêt. Toutes les relations d'approbation au sein d'une forêt sont bidirectionnelles et transitives. Cependant, afin de se connecter à d'autres forêts ou à des domaines non-AD, AD met également en œuvre d'autres types de relations d'approbation.

## Les groupes

Il existe 2 types de groupes :

**Les groupes de distribution**
Ces groupes ne sont utilisés que par des applications de messagerie. Ils permettent d'envoyer un message électronique à un ensemble d'utilisateurs.

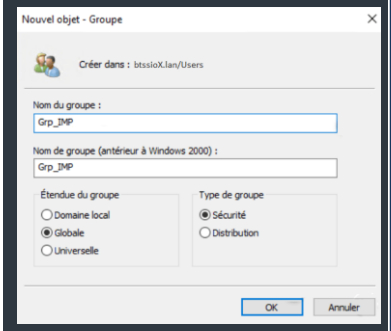
**Les groupes de sécurité**
Ces groupes permettent d'affecter des droits à un ensemble d'utilisateurs et/ou d'ordinateurs.

**Les groupes locaux**
Un groupe local de domaine est un groupe de sécurité ou de distribution qui peut contenir des groupes universels, des groupes globaux, des groupes locaux et des utilisateurs.
Les droits affectés à un groupe local ne peuvent concerner que des ressources appartenant au même domaine que le groupe local.

**Les groupes globaux**
Les membres des groupes globaux peuvent inclure des comptes et des groupes globaux du même domaine que celui du groupe global parent. Les membres de ces groupes peuvent recevoir des autorisations dans n'importe quel domaine de la forêt.

**Les groupes universels**
Les membres des groupes universels peuvent contenir des comptes de tout domaine au sein de la forêt dans laquelle ce groupe universel réside, des groupes globaux de tout domaine au sein de la forêt dans laquelle ce groupe universel réside et des groupes universels de tout domaine au sein de la forêt dans laquelle ce groupe universel réside.

Exemple :



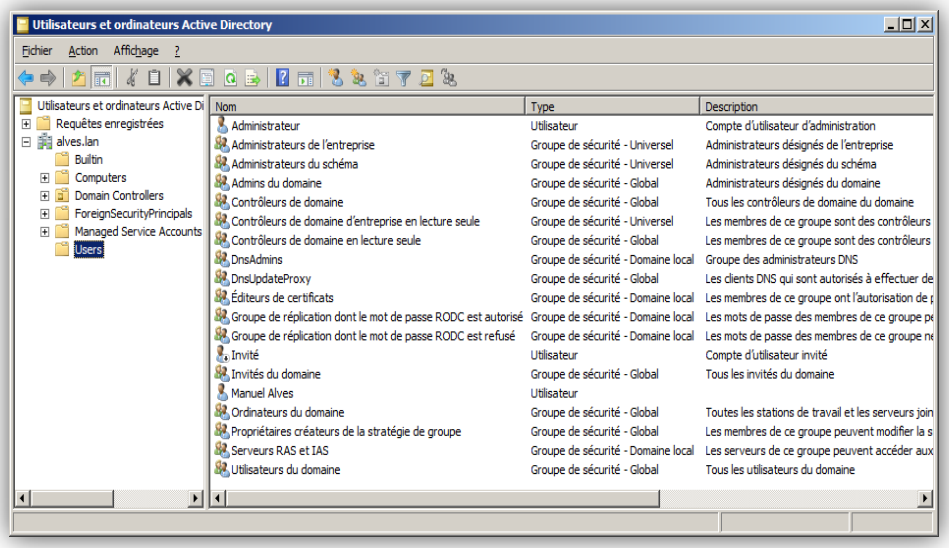

## II. Les utilisateurs

Un *compte d'utilisateur* est un objet stocké dans Active Directory qui permet une *ouverture de session unique*, autrement dit un utilisateur entre son mot de passe une seule fois lors de l'ouverture de session sur une station de travail pour obtenir un accès authentifié aux ressources réseau.

Il existe trois types de comptes d'utilisateurs, chacun ayant une fonction spécifique :

- Un *compte d'utilisateur local* permet à un utilisateur d'ouvrir une session sur un ordinateur spécifique pour accéder aux ressources sur cet ordinateur.
- Un *compte d'utilisateur de domaine* permet à un utilisateur de se connecter au domaine pour accéder aux ressources réseau, ou à un ordinateur individuel pour accéder aux ressources sur cet ordinateur.
- Un *compte d'utilisateur intégré* permet à un utilisateur d'effectuer des tâches d'administration ou d'accéder temporairement aux ressources réseau.

**Exemple :**




### Exercice 2 – Les utilisateurs.

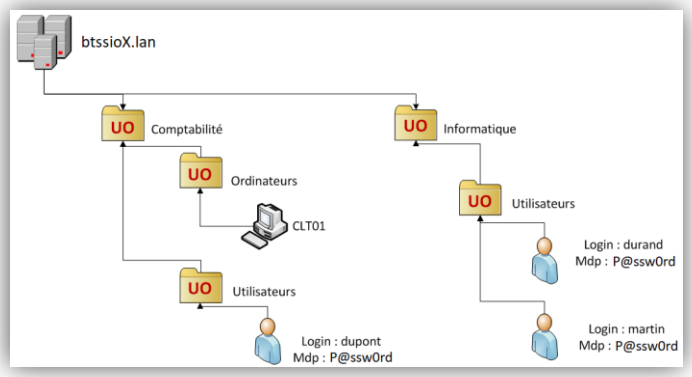
Quel est le compte utilisateur intégré qui réalise les tâches d'administration ? _____

Quel est le compte utilisateur intégré qui peut accéder temporairement aux ressources ? _____

Quel est le compte utilisateur du domaine ? _____

### Exercice 3 – Création des utilisateurs et des groupes.

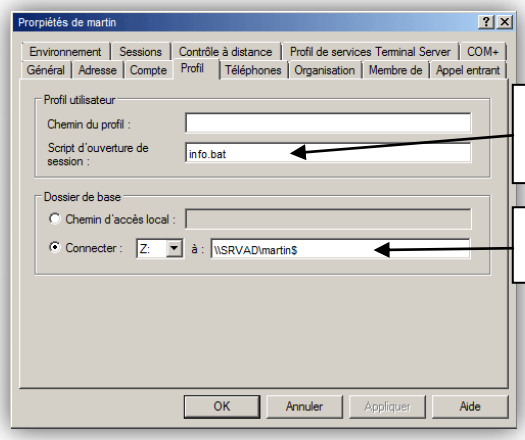
Reproduisez la structure suivante sur votre contrôleur de domaine :




Faites adhérer un poste client à votre domaine que vous nommerez **CLT01** et affectez-le à l'UO **Ordinateurs** de l'UO **Comptabilité**.
Testez la création de vos utilisateurs en vous connectant sur le domaine avec leur login depuis la machine cliente **CLT01**.
Créez dans chaque unité organisationnelle (Comptabilité et Informatique) un groupe global et ajoutez les membres associés.

## III. Les profils et les scripts

Dans les propriétés de chaque utilisateur, il possible de définir un dossier pour entreposer le profil et de définir un script de connexion. Tout ceci se passe dans l'onglet "**Profil**" des "**Propriétés**" de l'utilisateur :




Script **info.bat** présent dans le dossier : **C:\Windows\SYSVOL\sysvol\btssioX.lan**

Dossier personnel affecté au lecteur réseau **Z:**

Un script de connexion est un fichier de commandes batch. Pour connecter un lecteur réseau sur une machine cliente, nous allons utiliser la commande **net use**.

**Syntaxe de net use :** net use lecteur nomDeLaRessource

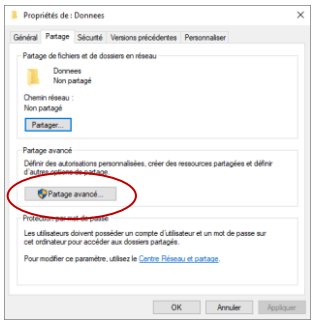
**Exemple :** net use L: \\SrvAd\donnees

### Exercice 4 – Les scripts de connexion.

Créez un dossier "**Donnees**" sur la racine du disque dur C:

Partagez ce dossier en utilisant le "**Partage avancé**", nommez le "**Donnees**". Définissez les droits comme suit :

Groupe Informatique : **Ecriture**
Groupe Comptabilité : **Lecture**




Dans l'onglet "**Sécurité**", ajoutez les 2 groupes avec les mêmes droits. Et supprimez les "**Utilisateurs du domaine**".

Dans le dossier **Netlogon** (pour le trouver, utilisez la commande **net share**), créez un fichier texte que vous nommerez "**info.bat**". Complétez ce fichier avec la commande net use.

Affectez ce script aux deux informaticiens.

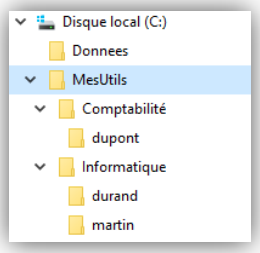
Faites un script "**compta.bat**" et affectez le au comptable.
Testez en vous connectant avec un informaticien et ensuite avec le comptable.

Dans l'onglet profil, on peut également définir le répertoire personnel de chaque utilisateur. Il suffit de cliquez sur l'option "**Connecter**" , de choisir une lettre de lecteur et la de saisir la ressource correspondante.

### Exercice 5 – Connexion au répertoire de base.

Créez un dossier "**MesUtils**" sur la racine du disque dur C:

Créez dans ce dossier, pour chaque groupe, un sous-dossier qui contiendra le répertoire de base de chaque utilisateur. Voici l'arborescence que vous devez obtenir :




Partagez les dossiers des utilisateurs en ajoutant un "**$**" à la fin (ex : martin$). N'oubliez pas les droits associés.

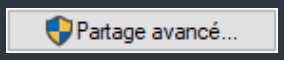
Dans l'onglet profil, affectez à chaque utilisateur, le dossier partagé correspondant. Testez.



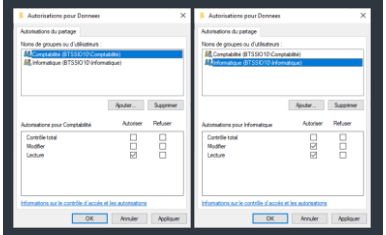
# Définir les droits sous Windows.

## Droits de partage

Cliquez sur l'onglet "**Partage**" :
Cliquez sur :



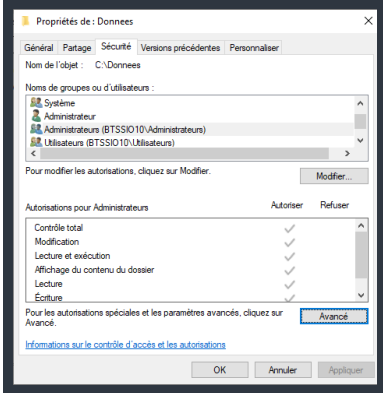

Cochez la case "**Partager ce dossier**".
Le système propose le même nom que nom du dossier. Vous pouvez le changer. Dans l'exemple, nous garderons le même.
Cliquez sur "**Autorisations**".
Supprimez "**Tout le monde**".
Cliquez sur "**Ajouter**" et saisissez le nom du groupe que vous désirez ajouter. Ici, je saisis "**Comptabilité**" et "**Informatique**".
En cliquant sur le nom de chaque groupe, j'affecte les droits et j'obtiens :



Cliquez sur "**OK**" 2 fois.

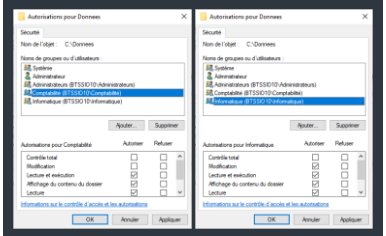
## Droits NTFS (Sécurité)

Cliquez sur l'onglet "**Sécurité**" :
Vous devez obtenir ceci :




Dans le cas où il reste les utilisateurs du domaine. Il faudra supprimer ce groupe de la liste. Il est impossible de le faire directement. Le dossier a hérité des doits du dossier "parent".
Dans ce cas, il faut cliquer sur "**Avancé**".
Et cliquez sur "**Désactiver l'héritage**".
Sélectionnez "**Supprimer toutes les autorisations héritées de cet objet**". Et cliquez sur "**OK**".

Pour ajouter les 2 groupes, cliquez sur "Modifier", puis sur "Ajouter". Et comme pour les droits de partage, saisissez les 2 groupes.
En affectant les bons droits on obtient :



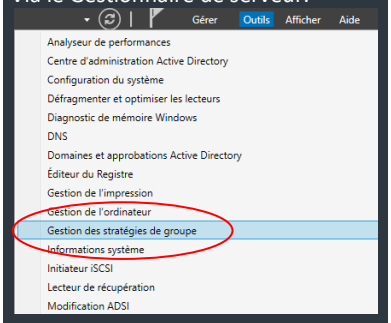
Cliquez sur "**OK**" 2 fois.

# Editeur de stratégie

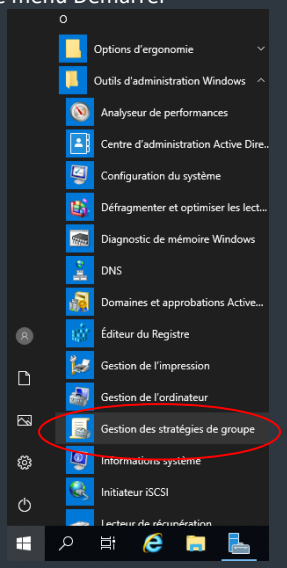
## Comment l'ouvrir ?

**2 possibilités :**

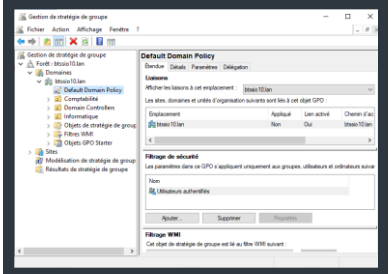
Via le Gestionnaire de serveur.



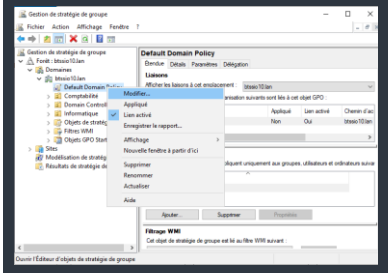

Via le menu Démarrer




## Comment modifier une stratégie ?



Clic droit sur Default Domain Policy



Et cliquez sur "**Modifier...**"

# IV. La gestion de stratégie de groupe (GPO)

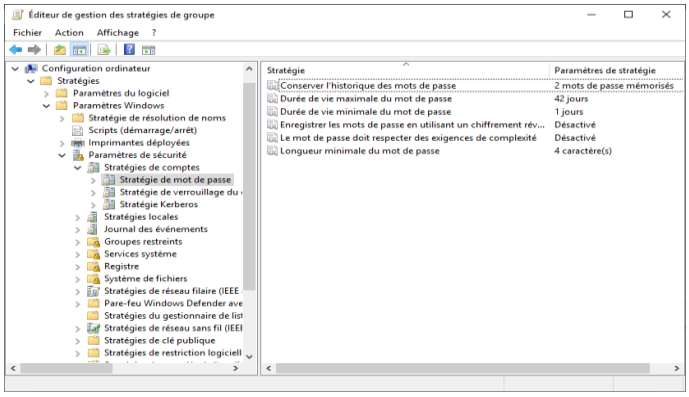
Les stratégies de groupes sont des ensembles de paramètres qui s'appliquent aux utilisateurs et ordinateurs qui se trouvent dans une Unité d'Organisation (UO). Elles permettent à titre d'exemples de rediriger le dossier Mes Documents, de déployer des Logiciels en fonction des services d'une entreprise ou des utilisateurs, de bloquer le Panneau de configuration.

Il existe une stratégie de groupe par défaut : **Default Domain Policy**
L'installation de l'Active Directory crée cette stratégie par défaut. Elle contient des paramètres de stratégie qui s'appliquent à tous les ordinateurs et tous les utilisateurs du domaine.

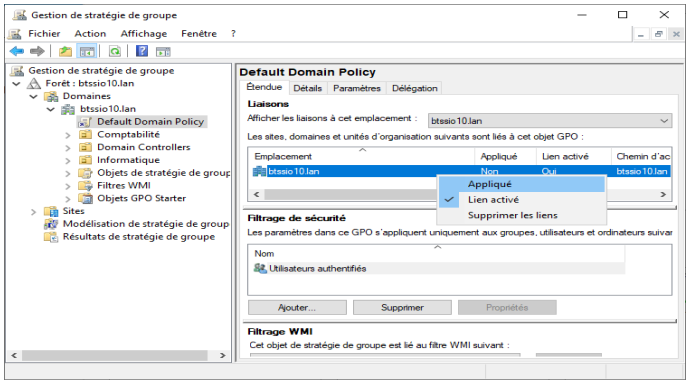
Il est possible de créer ses propres stratégies de groupe et de les affecter à une unité d'organisation (donc aux postes et utilisateurs de cette UO).

**Exemple : Modification de la stratégie de mot de passe**

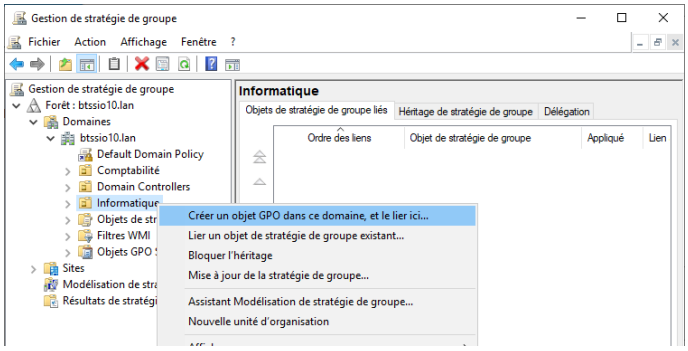
Dans l'exemple ci-dessous, le nombre minimum de caractères est passé à 4, la complexité du mot de passe (maj, min, chiffre + caractères spéciaux) a été supprimée et l'historique est de 2 mots de passes.




Il ne reste plus qu'à l'appliquer :




Pour valider le tout, il suffit de fermer la fenêtre et d'attendre que le système prenne en compte les modifications. Cela peut prendre parfois 30-40 minutes.
Pour gagner du temps, ouvrez une invite de commande et saisissez la commande : **gpupdate /force**
Il est possible de créer sa propre GPO et de l'affecter à une seul UO. Il suffit de réaliser un clic droit sur l'UO concernée :



## Exercice 6 – Exercice récapitulatif.

Avant de commencer, supprimez les Unités d'Organisation que vous avez créées précédemment, ainsi que les 2 dossiers "**MesUtils**" et "**MesDonnees**" du disque dur **C:**

**Sujet :**

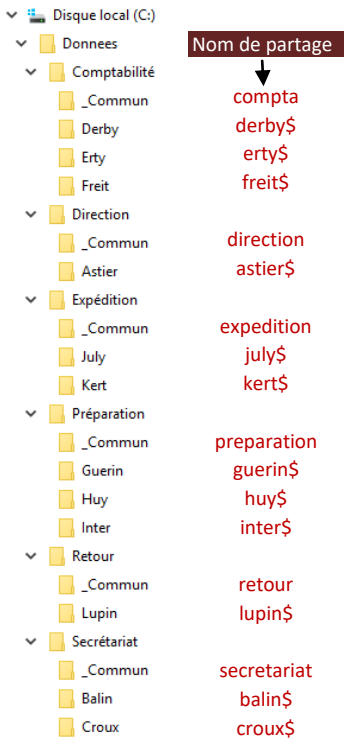
Vous êtes le nouvel administrateur réseau d'une entreprise de transport de marchandises. On vous demande d'administrer le service d'annuaire de cette entreprise.

Modifiez la Gestion de stratégie de groupe afin d'autoriser des mots de passe simples et ayant au minimum **5** caractères.

Voici la liste du personnel (Colonne 1 : Nom d'utilisateur ; Colonne 2 : Mot de passe) ainsi que la liste des services :

| Direction | | Secrétariat | | Comptabilité | | Préparation | | Expédition | | Retour | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Astier | Ast71 | Balin | Bal71 | Derby | Der89 | Guerin | Gue&9 | July | Jul71 | Lupin | Lup#4 |
| | | Croux | Cr&25 | Erty | Ert21 | Huy | Huy-5 | Kert | Ker21 | | |
| | | | | Freit | Fre58 | Inter | Int+9 | | | | |

Arborescence souhaitée :




Créez une UO "**Personnel**" dans laquelle vous placerez tous les comptes et les groupes.

Créez un groupe par service. Affectez les utilisateurs.

Chaque service aura un répertoire partagé (préfixé par le symbole "_"). Affectez le groupe correspondant. Le droit sera en écriture.

Chaque personnel aura accès à son dossier de base ainsi qu'au répertoire partagé de son service (via un script de connexion).

Le directeur doit pouvoir voir le contenu de l'ensemble des dossiers partagés des services. Modifiez son script.

Activez le bureau à distance sur le serveur, et autorisez le directeur à se connecter sur l'AD.

***PS : Le rapport ne devra pas être uniquement composé de copies d'écran. Il faudra justifier vos choix. Faites attention à la rédaction de votre rapport. Les fautes d'orthographe et de grammaire ne seront pas sanctionnées directement, mais elles installent le lecteur dans un à-priori négatif.***

## Les droits

Dans un système Windows, les ressources sont protégées par des droits **NTFS** (New Technology File System) :

**Lecture** : Permet de lire le contenu du fichier

**Affichage du contenu du dossier** : Permet de visualiser le contenu d'un dossier.

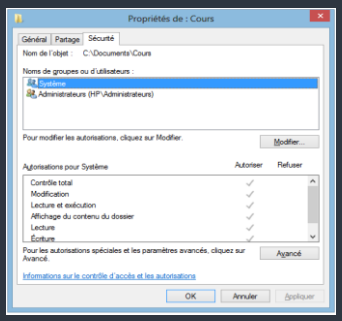
**Lecture et exécution** : Equivaut à "Lecture" + "Affichage du contenu du dossier".

**Ecriture** : Permet de créer des fichiers, de modifier le contenu des fichiers, de créer des dossiers.

**Modification** : C'est la somme de "Lecture" et "Écriture", et en plus le droit d'exécuter et d'effacer le fichier.

**Contrôle total** : Donne toutes les permissions possibles.

**Aucun Accès** : Retire tous les droits à un utilisateur. Ce droit est prioritaire sur les autres.




Le droit réel d'un utilisateur sur un dossier partagé se définit ainsi :

**Droit NTFS** → Droit le plus important défini directement par le compte et les groupes auxquels il appartient.

**Droit de partage** → Droit le plus important défini directement par le compte et les groupes auxquels il appartient.

**Droit d'accès via le réseau** → Droit le plus restrictif des droits NTFS et de partage.