

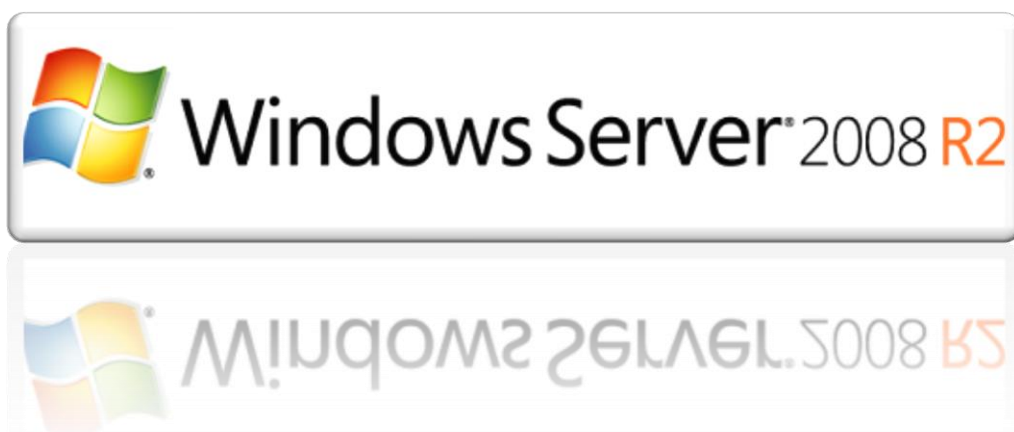
Stratégie de groupe dans Active Directory

16 novembre

2012

Dans ce document vous trouverez des informations fondamentales sur les fonctionnements de Active Directory, et de ses fonctionnalités, peut être utilisé en tant que support d'aide par exemple, ou bien TP de part sa présentation en étape structuré. N'oubliez pas de vous documenter sur le support Microsoft qui récence de nombreuses informations importante lorsque vous rencontré un problème.

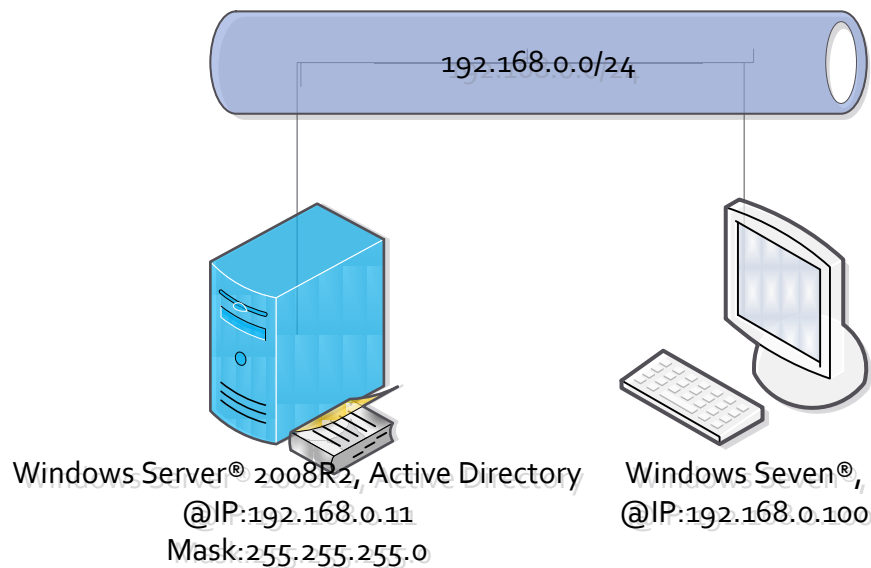
Windows
Server®
2008R2



Sommaire

I.	Introduction.....	3
II.	Installation et configuration de base.....	5
1.	Avant de commencer	5
2.	Installation AD	5
III.	Gestion des utilisateurs et ordinateur.....	5
3.	Unités organisationnelles.....	5
4.	Groupe.....	7
5.	Intégration d'un client dans un domaine	7
6.	Discrimination clients AD	8
7.	Profil itinérant	9
IV.	Stratégies de Groupe.....	10
8.	Domaine GPO	10
9.	Activation de GPO	11

I. Introduction



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.

Active Directory existe depuis la version 2000, Le service d'annuaire Active Directory peut être mis en œuvre sur Windows 2000 Server, Windows Server 2003 et Windows Server 2008, il résulte de l'évolution de la base de compte plane SAM. Un serveur informatique hébergeant l'annuaire Active Directory est appelé « contrôleur de domaine ».

Active Directory stocke ses informations et paramètres dans une base de données centralisée. La taille d'une base Active Directory peut varier de quelques centaines d'objets pour de petites installations à plusieurs millions d'objets pour des configurations volumineuses.

Dans les premiers documents Microsoft mentionnant son existence, Active Directory s'est d'abord appelé NTDS (pour NT Directory Services, soit « Services d'annuaire de NT » en français). On peut d'ailleurs encore trouver ce nom dans la littérature couvrant le sujet ainsi que dans certains utilitaires AD comme NTDSUTIL.EXE par exemple, ou le nom du fichier de base de données NTDS.DIT.

Le protocole principal d'accès aux annuaires est LDAP qui permet d'ajouter, de modifier et de supprimer des données enregistrées dans Active Directory, et qui permet en outre de rechercher et de récupérer ces données. N'importe quelle application cliente conforme à LDAP peut être utilisée pour parcourir et interroger Active Directory ou pour y ajouter, y modifier ou y supprimer des données. Il utilise également DNS, Kerberos V, SMTP, SMB/CIFS, MSRPC.

Active Directory introduit les notions de domaine, forêt, arborescence:

Une arborescence Active Directory est donc composée de :

La forêt : structure hiérarchique d'un ou plusieurs domaines INDEPENDANTS (ensemble de tous les sous domaines Active Directory). L'arbre ou l'arborescence : domaine de toutes les ramifications. Par exemple, dans l'arbre domaine.tld, sous1.domaine.tld, sous2.domaine.tld et photo.sous1.domaine.tld sont des sous-domaines de domaine.tld. Le domaine : constitue les feuilles de l'arborescence. photo.sous1.domaine.tld peut-être un domaine au même titre que domaine.tld.

Le modèle de données Active Directory est dérivé du modèle de données de la norme X.500 : l'annuaire contient des objets représentant des éléments de différents types décrits par des attributs. Les stratégies de groupe (GPO) sont des paramètres de configuration appliqués aux ordinateurs ou aux utilisateurs lors de leur initialisation, ils sont également gérés dans Active Directory.

II. Installation et configuration de base

1. Avant de commencer

- Pensez à donner un nom Windows facile à retenir pour votre serveur : PODx,...
- Votre serveur doit avoir une adresse IP fixe : 192.168.X.Y

2. Installation AD

– Ajoutant le rôle Service de Domaine Active Directory

Avec la commande « **dcpromo** » :

- Cocher l'installation en mode avancé.
- Domaine dans une nouvelle forêt
- Le domaine sera votreville.local
- Nom NetBios : VOTREVILLE
- Niveau fonctionnel : Windows 2008R2
- Les autres options seront laissées par défaut.

III. Gestion des utilisateurs et ordinateur

3. Unités organisationnelles

L'unité d'organisation est un type d'objet annuaire particulièrement utile, contenu dans les domaines. Les unités d'organisation sont des conteneurs Active Directory dans lesquels vous pouvez placer des utilisateurs, des groupes, des ordinateurs et d'autres unités d'organisation. Une unité d'organisation ne peut pas contenir des objets d'autres domaines.

Une unité d'organisation est l'étendue ou l'unité la plus petite à laquelle vous pouvez attribuer des paramètres de Stratégie de groupe ou déléguer une autorité administrative. Avec les unités d'organisation, vous pouvez créer des conteneurs à l'intérieur d'un domaine afin de représenter les structures hiérarchiques et logiques de votre organisation. Vous pouvez ensuite gérer la configuration et l'utilisation des comptes et des ressources en fonction de votre modèle d'organisation. Pour plus d'informations sur les paramètres de Stratégie de groupe, voir Stratégie de groupe (avant GPMC).

Tel qu'il apparaît dans l'illustration, les unités d'organisation peuvent contenir d'autres unités d'organisation. Vous pouvez développer une hiérarchie de conteneurs selon vos besoins afin de traduire la hiérarchie de votre organisation à l'intérieur d'un domaine. Avec les unités d'organisation vous pouvez minimiser le nombre de domaines requis pour votre réseau.

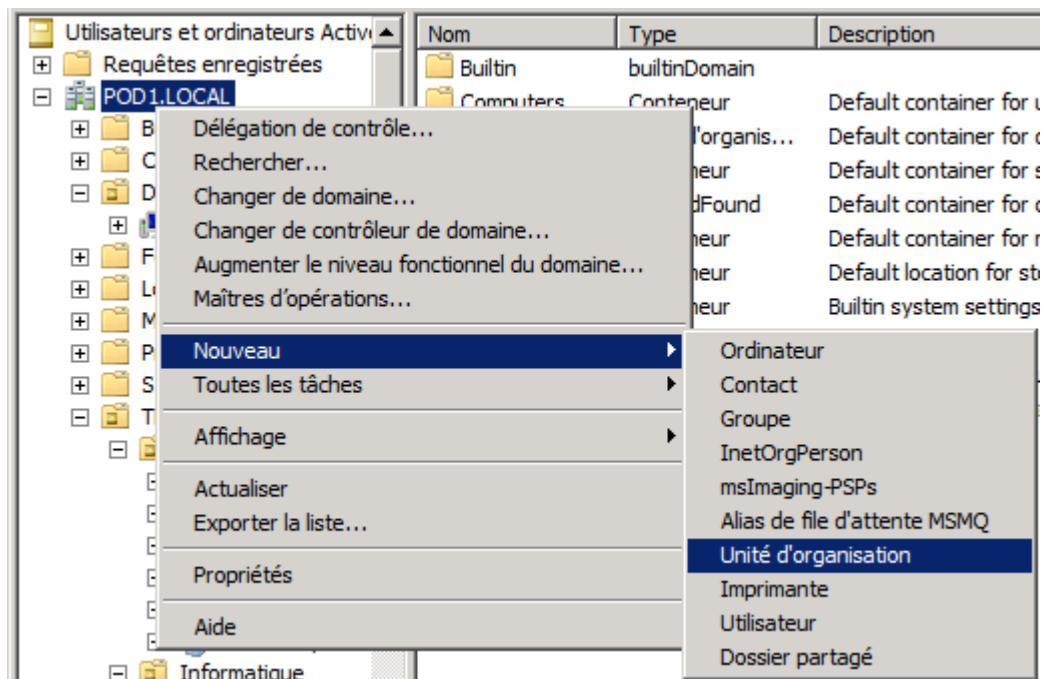
Vous pouvez utiliser des unités d'organisation pour créer un modèle administratif auquel vous pourrez appliquer une échelle quelconque. Un utilisateur peut recevoir des droits

d'administration pour toutes les unités d'organisation d'un domaine ou pour une seule unité d'organisation. Un administrateur d'une unité d'organisation ne requiert pas des droits d'administration pour les autres unités d'organisation du domaine. Pour plus d'informations sur la délégation d'autorité administrative, voir Délégation de l'administration.

Les UO sont des conteneurs logiques dans lesquels des utilisateurs, des groupes, des ordinateurs et d'autres UO sont placés. Elles ne peuvent contenir que des objets de leur domaine parent. Une UO est la plus petite unité à laquelle il soit possible d'appliquer une stratégie de groupe ou une délégation d'autorité.

Créez les trois U.O suivantes :

Dans utilisateurs et Ordinateurs Active Directory :



Entrez un nom pour créer votre UO.



- Comptabilité
- Secrétariat
- Informatique

4. Groupes

Pour comprendre le principe des groupes sous Windows 2008, vous pouvez lire cet article :

<http://www.alexwinner.com/articles/win2008/9-groupead.html>

Active Directory est un annuaire référençant notamment les utilisateurs et les groupes d'une entreprise. Tous les utilisateurs et groupes existant sous Windows avant l'installation d'AD ont été copiés dans AD.

Comme pour l'unité D'UO, cliquez droit maintenant sur l'UO, et faite Ajouter => Groupe

- Dans l'U.O. Comptabilité, créez le groupe assistants et le groupe chefs comptables.
- Dans l'U.O. Secrétariat, créez le groupe accueil et le groupe assistantes de direction.
- Dans l'U.O. Informatique, créez le groupe développeurs et le groupe techniciens réseau.

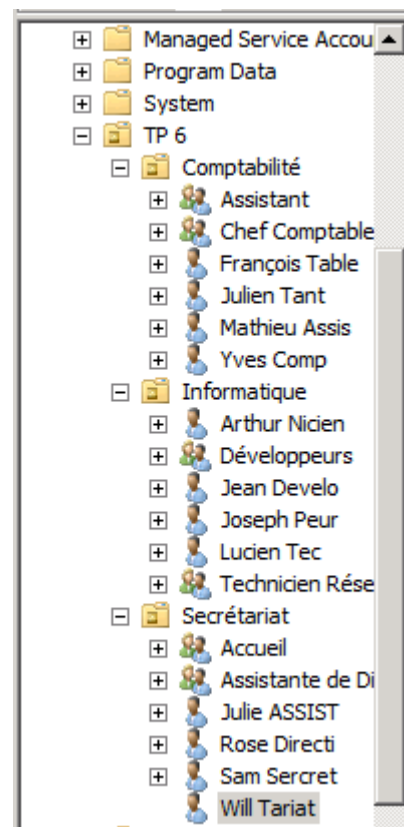
Utilisateurs :

Chaque utilisateur devra pouvoir se connecter par le login suivant :

Première lettre du prénom, nom complet, par exemple Sam Secrét devra taper : ssecrét

Définissez un mot de passe. Les utilisateurs ne pourront pas changer de mot de passe.

- Sam Secrét et Will Tariat seront ajoutés à l'U.O Secrétariat et dans le groupe Accueil.
- Julie Assist et Rose Directi seront ajoutés à l'U.O Secrétariat et dans le groupe Assistantes de direction. Jean Develo et Joseph Peur seront ajoutés à l'U.O Informatique et dans le groupe Développeurs.
- Lucien Tec et Arthur Nicien seront ajoutés à l'U.O Informatique et dans le groupe Techniciens réseau.
- Yves Comp et François Table seront ajoutés à l'U.O Comptabilité et dans le groupe chefs comptables.
- Mathieu Assis et Julien Tant seront ajoutés à l'U.O Comptabilité et dans le groupe Assistants.



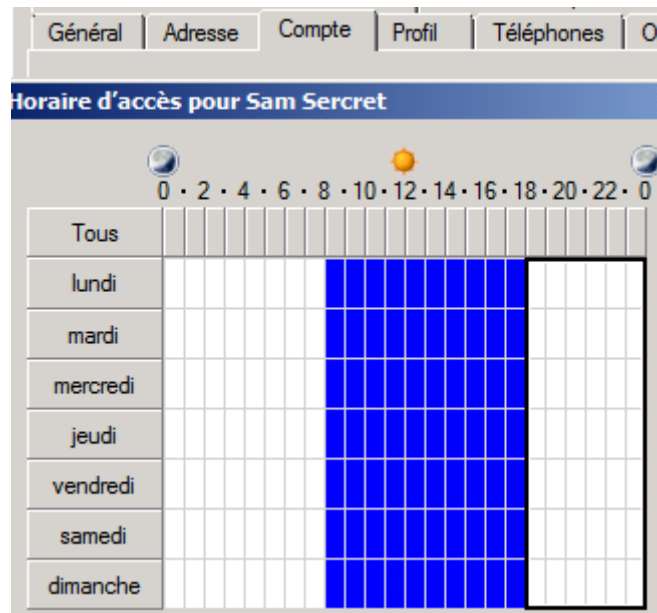
5. Intégration d'un client dans un domaine

Avec votre client XP ou Seven, intégrez votre domaine (clic droit > propriétés sur le poste de travail, onglet nom de l'ordinateur).

Indiquez un nom d'utilisateur du groupe Secrétariat pour vous connecter.

6. Discrimination clients AD

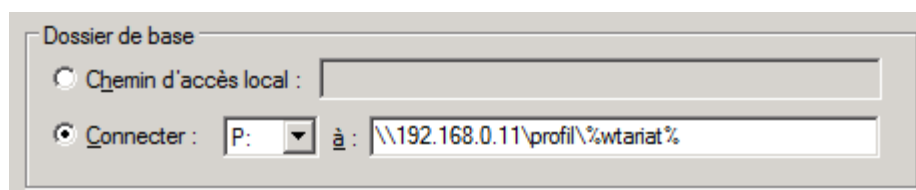
Une option utile en entreprise d'un point de vue sécurité, vous pouvez définir des plages d'horaires où les utilisateurs sont autorisés à se connecter. Cliquez sur un utilisateur => « **Propriétés** », dans l'onglet compte définissez la plage d'horaires.



Dans le même onglet, imposez à l'utilisateur de se connecter uniquement sur l'ordinateur client que vous venez d'intégrer.

A l'ouverture de session du client, nous allons définir dans son poste de travail, un lecteur P : personnel, qui pourra contenir ses documents de travail, l'avantage étant d'y avoir accès de n'importe quelle poste informatique.

Utilisez n'importe quels utilisateurs, dans ses propriétés, onglet « **Profil** »,



Ici on peut voir qu'un dossier a déjà été créé situé à la racine du serveur et dans un dossier profil, le dossier enfant comportant le nom de l'utilisateur. Crée ce dossier où vous le désirez, et affectez lui des sécurités en n'autorisant l'accès qu'à l'utilisateur concerné, ainsi qu'à l'administrateur système par exemple.

7. Profil itinérant

Il peut arriver qu'une personne utilise plusieurs ordinateurs, avec le même compte d'utilisateur. Lorsqu'il va utiliser un ordinateur, il pourra avoir un environnement différent de celui présent sur l'autre ordinateur. Dans ce cas, il pourra être intéressant de configurer pour cet utilisateur un profil itinérant. En effet, le fait d'utiliser ce type de compte va permettre à votre utilisateur de conserver ses documents, ses paramètres, et son environnement de travail, quelque soit l'ordinateur sur lequel il ouvre une session. Les profils itinérants vont stocker leurs informations sur un serveur que vous choisirez

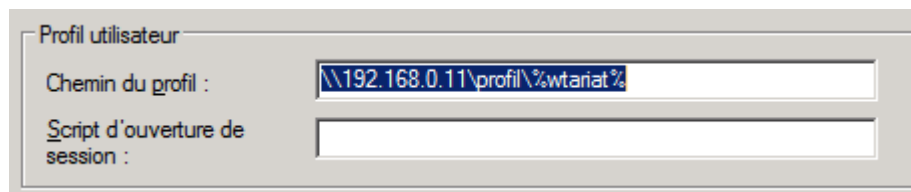
Quels sont les avantages et inconvénients des profils itinérants ?

Pour créer un profil itinérant, il d'abord crée un dossier à la racine de notre serveur par exemple, en le nommant profil. Configurez-le :


- Cliquez droit partage et sécurité, Partagez le dossier
- Donnez le contrôle total à tous le monde (Autorisations)
- Commentez le partage (Profil itinérants)

Dans utilisateurs Active Directory :

- Cliquez droit sur le profil en question, dans onglet profil :
 - o Chemin du profil : \\@IPServeur\[Dossier_Parent]\%[Dossier_du_profil]%



Une fois connecté l'utilisateur créera ses dossiers et pourra y accéder de n'importe qu'elle autre poste, vérifier la fonctionnalité de votre configuration dans poste de travail sur le client :

- Cliquez droit propriété Poste de travail
- Cliquez sur  Paramètres système avancés
- Profil des utilisateurs -> Paramètres

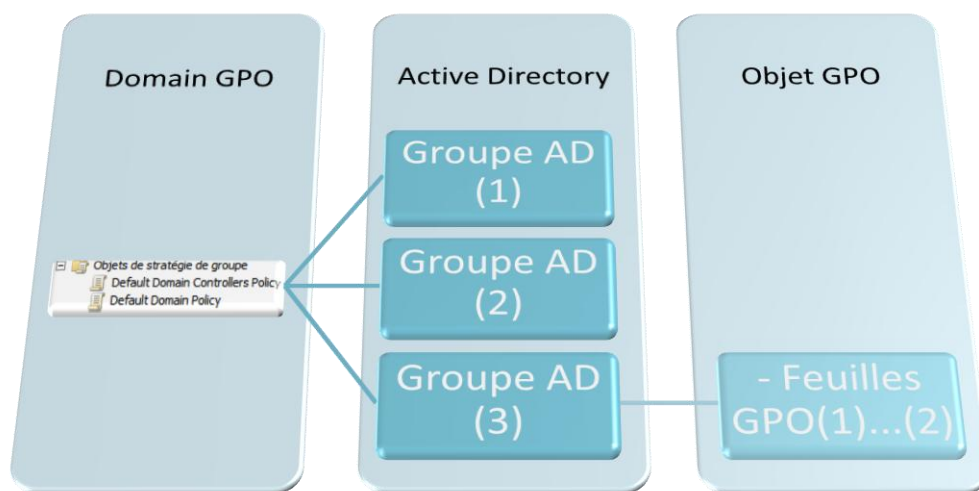
Changer le fond d'écran par exemple, crée des fichiers, déconnectez-vous, et connectez vous d'une autre machine. Vous allez pouvoir constater qu'en se connectant le fond d'écran correspond, et dans l'explorateur Windows® taper le chemin du profil pour accéder aux documents.

IV. Stratégies de Groupe

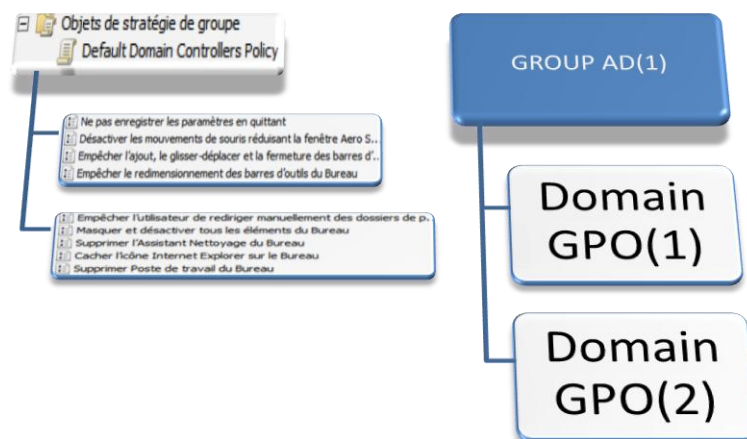
8. Domaine GPO

Lorsque vous configurez les stratégies de groupe et d'ailleurs pour n'importe quelle applications Windows Server®, il faut être particulièrement méthodique. La base de GPO repose sur une problématique de gestion d'entreprise, de sécurité, d'accès aux données, Qui a le droit de faire quoi ?

On peut schématiser le processus d'action des GPO :



En règle générale on distingue chacun des groupes AD par des Domaines GPO contenant les feuilles GPO. (Expliquer ci-dessous). On peut également classer les Domaines GPO par type de restriction. Des groupes AD peuvent correspondre à plusieurs Domaines GPO.

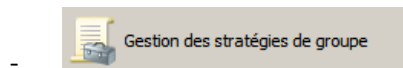


9. Activation de GPO

a. Domain GPO ; Objet de stratégie de groupe

Une liste de GPO de base est disponible, vous pouvez néanmoins créer les vôtres, ceci dit elle ne présente que très peu d'intérêts, mise à part pour des cas très particuliers, la liste fournie de base est complète, comme vous allez pouvoir le constater

Dans le menu démarrer :

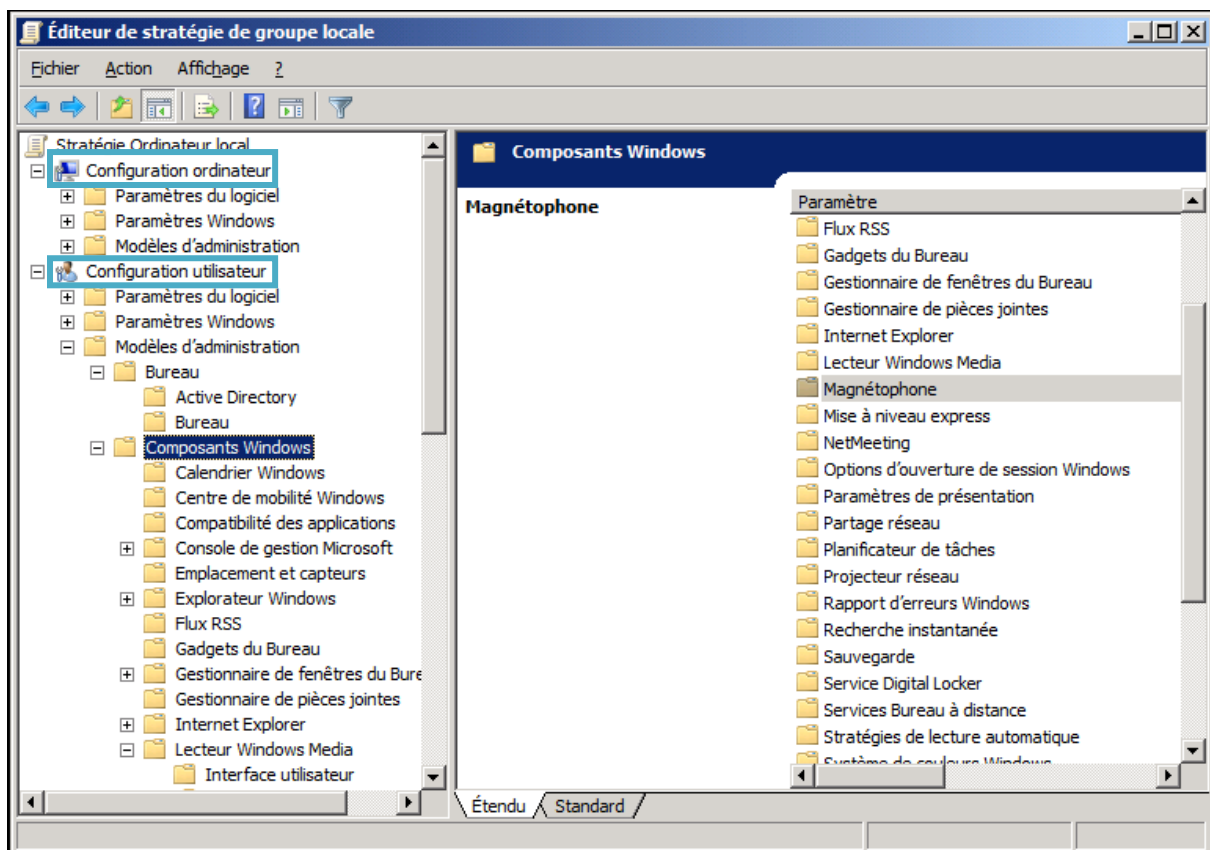


Dans l'arborescence déployer votre forêt, dans Objets de stratégie de groupe vous avez deux Domain GPO de base, prenant pour notre exemple Default Domain Policy

- Cliquez droit, Modifier.
- Activer toutes les feuilles GPO qui vous intéresse pour ce Domain.


b. Feuilles de stratégie de groupe


Arborescence de gauche présenté tout d'abord 2 grandes parties :

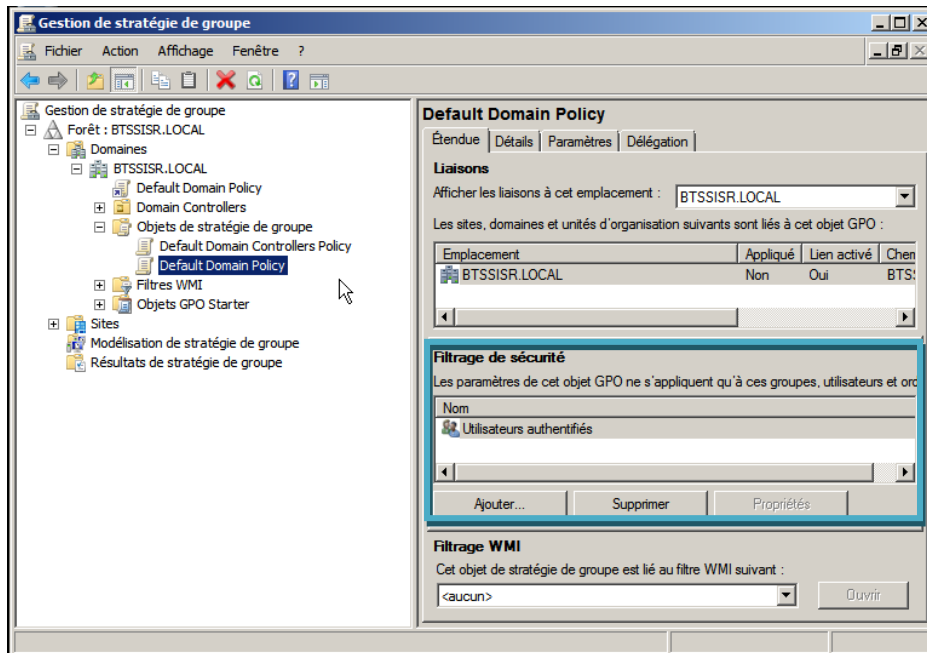


Comme vous pouvez le voir de nombreuses options sont disponibles, les fichiers se trouvant dans Modèles d'administration. Maintenant comment se passe l'activation.

Très simplement, cherchez la GPO que vous voulez appliquer :

- Cliquez droit, Modifier
-  **Activé**, OK

Spécifier dans  les groupes qui hériteront de ce Domain GPO avec ses feuilles correspondantes.



Pour ajouter un Domain GPO, cliquez droit  , « **Nouveau** ».

Le client de stratégie de groupe du poste récupère la configuration (par défaut au bout de 60 à 120 minutes) qui est applicable à l'ordinateur et/ou à l'utilisateur connecté. Pour forcer l'application des GPO, vous pouvez utiliser la commande :

gpupdate /force

Pour vérifier le résultat de l'application des GPO, vous pouvez utiliser la commande :

gpresult /h rapport.