



Active Directory sous 2012

Le site de référence pour vos recherches sur les technologies Microsoft se trouve ici : <http://technet.microsoft.com/fr-fr/library/>

Table des matières

Active Directory sous 2012.....	1
I- Présentation d'Active Directory :.....	2
II- Installation et configuration de base :.....	3
Avant de commencer.....	3
Installation.....	3
III- Gestion des utilisateurs et ordinateurs.....	3
Unités organisationnelles.....	3
Groupes.....	4
Utilisateurs :.....	4
Intégration d'un client dans un domaine :.....	5
Profils utilisateur :.....	5
V- Stratégies de groupes.....	6
Création des GPO :.....	6
Liaison des stratégies de groupe :.....	6
Forcer l'application des stratégies de groupe :.....	6
Activé / Appliqué :.....	7
Un premier cas :.....	7
Vérification et sauvegarde :.....	8
Stratégies complexes :.....	8
GPO Starters :.....	8
Aller plus loin avec AD :.....	9
Scripts de démarrage :.....	9
Déploiement de logiciels publiés ou attribués :.....	9
VI- Architectures Active Directory.....	10
Redondance de contrôleurs.....	10
Domaine et sous-domaines.....	10
Forêts.....	11



I- Présentation d'Active Directory :

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.

Depuis quelle version de Windows Server, existe A.D. ?

Qu'est ce qu'un contrôleur de domaine ?

Quels sont les protocoles utilisés par l'annuaire Active Directory ?

Quels sont les méthodes d'authentification possibles Active Directory ?

Active Directory introduit les notions de **domaine**, **forêt**, **arborescence**. Définissez ces termes :



II- Installation et configuration de base :

Avant de commencer

- Pensez à donner un nom Windows facile à retenir pour votre serveur : serveurX
- Votre serveur doit avoir une adresse IP fixe : 192.168.X.Y (à demander au formateur)

Installation

L'installation de Active Directory se fait ...

- en ajoutant le rôle Service de Domaine Active Directory
- puis en allant dans le rôle, en cliquant sur promouvoir le serveur en contrôleur de domaine
- Cocher l'installation en **mode avancé**.
- Domaine dans une nouvelle forêt
- Le domaine sera **votreville.lan**
- Nom NetBios : **VOTREVILLE**
- Niveau fonctionnel : Windows 2012
- Les autres options seront laissées par défaut.

III- Gestion des utilisateurs et ordinateurs

Unités organisationnelles

Qu'est ce qu'une unité organisationnelle (U.O.) ?

Quelle est la différence entre une U.O. et un groupe (dans quels cas utilise-t-on l'un et l'autre) ?



Créez les trois U.O suivantes :

- Comptabilité
- Secrétariat
- Informatique

Groupes

Pour comprendre le principe des groupes sous Windows 2012, 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.

- 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**

Le mot de passe sera **Azerty77**

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 **Fabien Tant** seront ajoutés à l'U.O **Comptabilité** et dans le groupe **assistants**.



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.

Profils utilisateur :

Faites en sorte que les utilisateurs du groupe accueil ne puissent se connecter que de 8h à 18h.

Imposez à l'utilisateur de se connecter uniquement sur l'ordinateur client que vous venez d'intégrer.

Faites en sorte que l'utilisateur **Sam Secrét** ait un lecteur réseau personnel nommé P: qui pointe vers le partage \\ServeurX\p\ssecrét

Définissez le terme « **profil itinérant** » :

Quels sont les **avantages et inconvénients** des profils itinérants ?

Mettez en place un profil itinérant pour l'utilisateur **Sam Secrét**.

Faites en sorte que l'utilisateur Sam Secrét soit **administrateur de son poste** (et non pas du domaine). Quelle est la différence entre les deux ?



V- Stratégies de groupes

Trouvez une définition des stratégies de groupes Windows ou (GPO : Group Policy Object) :

Les trois phases de la création d'une GPO sont les suivantes :

- Création de la GPO
- Liaison de la GPO
- Application de la GPO

Création des GPO :

La console **gpedit.msc** (à lancer depuis Démarrer > Exécuter) permet d'éditer individuellement les stratégies de groupes locales. Cette console existe pour **tous les Windows** y compris les versions clientes.

La console **gpmc.msc** (à lancer depuis Démarrer > Exécuter) permet une gestion centralisée des GPO dans **Active Directory**. On peut aussi la trouver dans le menu **Outils d'administration > Gestion des stratégies de groupe**.

Liaison des stratégies de groupe :

Après avoir créé une stratégie de groupe, elle doit être liée à un site Active Directory, à un domaine ou à une UO.

Attention, les objets enfants d'Active Directory héritent des objets parents ! Un utilisateur peut donc se voir appliquer plusieurs GPO.

Forcer l'application des stratégies de groupe :

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.htm
```

Activé / Appliqué :

Une stratégie de groupe est par défaut toujours activée dès sa création. Cela signifie qu'elle fonctionne.

Le fait de l'appliquer permet de forcer cette stratégie à s'appliquer même si une stratégie enfant vient s'y opposer.

Un premier cas :

Mettre en place les stratégies de groupe suivantes :

Tout le domaine :

- Interdire aux utilisateurs de partager des fichiers de leur profil.
- Permettre l'utilisation du bureau à distance sur n'importe quelle machine.
- Interdire le menu contextuel (clic droit) dans Internet Explorer

Service Secrétariat :

- Désactiver l'assistant de connexion à Internet d'Internet Explorer.
- Interdire la modification des paramètres de proxy d'Internet Explorer.

Service Comptabilité sauf les chefs comptables :

- Masquer le lecteur D:
- Interdire le 'clic droit > gérer' sur l'icône de l'ordinateur.

Service Informatique :

- Supprimer l'onglet sécurité de l'explorateur Windows.
- Interdire l'accès à l'invite de commandes.



Vérification et sauvegarde :

Forcez la mise à jour des GPO (commande **gpupdate**).
Vérifiez que les stratégies s'appliquent bien aux utilisateurs des différentes unités d'organisation.

Si les GPO ont bien fonctionné, dans la partie Objets de stratégies de groupes, sauvegardez toutes les GPO sur votre Bureau.

Stratégies complexes :

Créer une nouvelle U.O. nommée **production** avec **deux utilisateurs** à l'intérieur.
Cette U.O. concerne des ordinateurs installés dans un contexte de production (commandant des automates ou aidant les techniciens). **Ils doivent être restreints au maximum :**

Les utilisateurs de cette unité d'organisation ne doivent pas pouvoir faire autre chose que d'utiliser le logiciel spécifique (considérons que ce logiciel est Word pour l'exemple).

GPO Starters :

Les GPO starters sont des modèles de GPO. On peut par la suite créer une GPO en partant de ce modèle, ce qui simplifie l'administration des stratégies de groupes.



Aller plus loin avec AD :

Scripts de démarrage :

Créez un script Batch pour les comptes permettant :

- de **mapper un lecteur z:** qui permette d'accéder au partage \\serveur\compta qui soit accessible en lecture et écriture.

La commande permettant d'utiliser un partage réseaux est :

.....

- de **créer ou changer la clé de registre suivante** sur les clients :
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon\EnableFirstLogonAnimation=dword:00000001

La commande permettant de changer une clé de registre sous Windows est :

.....

Intégrez ce script dans une GPO qui s'appliquera à l'unité d'organisation Comptabilité.

Appliquez la GPO et vérifiez son fonctionnement.

Déploiement de logiciels publiés ou attribués :

La publication de logiciel permet à l'utilisateur de retrouver ce logiciel prêt à être installé dans l'ajout/suppression de programmes.
L'attribution ou l'assignation permettent d'installer directement le logiciel au démarrage de l'ordinateur.

Dans la majorité des cas, le déploiement s'applique à l'utilisateur.

Téléchargez le logiciel MBSA depuis le site Web de Microsoft :
<http://www.microsoft.com/en-us/download/details.aspx?id=7558>

Déployez **MBSA** sur tous les postes de votre domaine.

VI- Architectures Active Directory

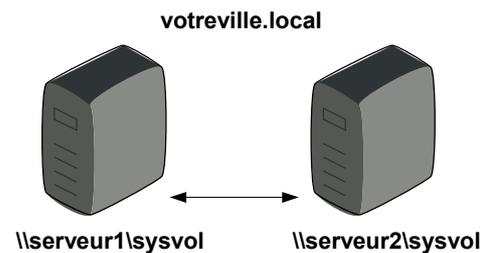
Avant de commencer chaque partie, vous devrez supprimer votre ancien AD avec la commande `dcpromo`.

Redondance de contrôleurs

Ce travail est à effectuer par groupe de 2 serveurs.

Installez deux contrôleurs de domaine pour un seul domaine dans le but de tolérer la panne de l'un d'entre eux.

Le premier serveur sera le contrôleur **principal** du domaine **votreville.local**. Le second sera le contrôleur **secondaire** du même domaine.



Configurez ces deux contrôleurs.

Vérifiez que les informations du serveur principal sont bien recopiées sur le secondaire (comptes utilisateurs, groupes, ordinateurs, U.O, ...).

Tous les combien de temps a lieu la synchronisation des données ?

Quel protocole permet cela ?

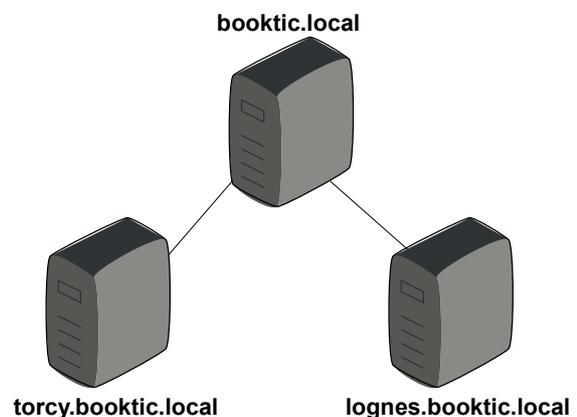
Connectez vos clients au domaine. Débranchez le câble du serveur principal pour simuler une panne, puis redémarrez votre client Windows pour voir si il arrive toujours à se connecter malgré la panne.

Domaine et sous-domaines

Ce travail est à effectuer par groupe de 2 ou 3 serveurs.

Le serveur du formateur représente le siège social de l'entreprise booktic.

Les autres serveurs représentent des agences de l'entreprise situées dans les autres villes.





Chaque site de l'entreprise doit créer:

- Une U.O.
- Dans cette U.O. un groupe
- Dans cette U.O. et appartenant au groupe, trois utilisateurs.

Lors de séminaires, il arrive que les nouveau utilisateurs aient à utiliser des ordinateurs d'une ville autre que leur ville d'attache.

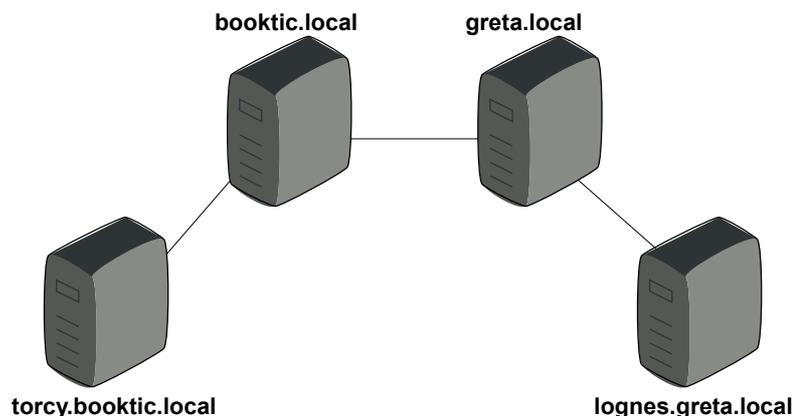
Faites en sorte que les employés puissent se connecter depuis n'importe quel site.

Forêts

Ce travail est à effectuer par groupe de 3 ou 4 machines.

Les sociétés booktic et Greta viennent de fusionner.

Le serveur du formateur doit représenter le siège social de l'entreprise booktic.



L'un des serveurs doit représenter le siège social de l'entreprise Greta.

Les autres serveurs représentent des agences de ces entreprises situées dans différentes villes.

Chaque site de l'entreprise doit créer:

- Une U.O. «Service Communication»
- Dans cette U.O. un groupe «publication»
- Dans cette U.O. et appartenant au groupe publication, trois utilisateurs.

Lors de séminaires, il arrive que les nouveau utilisateurs aient à utiliser des ordinateurs d'une ville et d'une société autre que leur site d'attache.

Faites en sorte que les employés puissent se connecter depuis n'importe quel site.