Leçon 6 : Installation d'Active Directory

6.1 Introduction

Active Directory est un élément central des systèmes *Windows Server*. En effet, il s'agit d'installer une base de données d'utilisateur « globale » sur le réseau. Cette base de données globale permet aux utilisateurs de se connecter sur n'importe quelle machine membre du *domaine* configuré.

En plus d'authentifier les utilisateurs depuis le serveur, Active Directory permet de définir et distribuer des politiques de configuration à l'ensemble des machines. Cet aspect particulier rend Active Directory particulièrement puissant et intéressant. Pour les administrateurs cependant, ces configurations peuvent devenir complexes.

Dans la suite de cette leçon, nous allons aborder :

- Une description succincte d'Active Directory
- Les éléments d'installation d'Active Directory
- Les objets à l'intérieur d'Active Directory (Ordinateurs, Utilisateurs, Unité Organisationnelle, Groupe de sécurité, …)
- Active Directory et les profils des utilisateurs

Référence bibliographique

[1] *A. Warren,* Exam Ref 70-742 : Identity with Windows® Server® 2016, 1st edition, Microsoft Press, March 2017

6.2 Description d'Active Directory

6.2.1 Infrastructure d'Active Directory

L'infrastructure d'Active Directory comprend un certain nombre d'éléments (extrait de [1]) :

- ***Active Directory Data Store.*** C'est l'endroit où sont sauvegardées les informations d'identité dans l'annuaire. Le *data store* est hébergé sur un contrôleur de domaine. L'annuaire se concrétise par un fichier particulier (NTDS.DIT) stocké sur le contrôleur de domaine. On y trouve le schéma LDAP[23], la configuration, les objets du domaine (utilisateurs, groupes, ordinateurs, …) et dans certains cas, le catalogue global
- ***Domain controllers.*** Il s'agit de serveurs qui exécutent le rôle AD Domain Service. Ce rôle est responsable du maintien de toutes les informations nécessaires utiles pour le domaine (i.e. une copie du *data store*).
- ***Domain.*** Un ou plusieurs contrôleurs de domaine sont nécessaires pour créer un *domaine Active Directory*. Le domaine comprend toutes les informations d'identité et les objets créés. On trouve cette information répliquée dans tous les contrôleurs de ce domaine. Ainsi, les utilisateurs, groupes et ordinateurs sont créés dans le domaine et cette information est

[23] Le *schéma LDAP* est une définition des objets et données qui peuvent être intégrées dans les objets LDAP. Ainsi, en ajoutant des éléments au schéma LDAP (définissant de nouvelles données), les objets créés peuvent mémoriser de nouvelles valeurs.

répliquée sur tous les contrôleurs de domaine installés. Ainsi, si un contrôleur tombe en panne, un autre prend le relai (puisqu'il dispose de l'information).

- ***Forest.*** Une forêt est une collection d'un ou plusieurs domaines Active Directory. Le premier domaine installé dans une forêt est le *forest root domain*. La forêt contient une seule définition de la configuration réseau, et une seule occurrence du schéma. Il faut bien noter qu'il n'y a jamais de réplication au-delà la forêt.
- ***Tree.*** Les espaces de nom DNS des domaines d'une forêt forment des arbres. Ainsi, si un domaine est enfant d'un autre (`swila.local` et `louis.swila.local`), ceux-ci forment une seule branche alors que 2 domaines différents (`swila.local` et `swinnen.local`) forment deux arbres dans la forêt. Il est possible d'établir des relations particulières (d'approbation par exemple) entre deux domaines d'une forêt.
- ***Functional level.*** Le niveau fonctionnel d'une forêt ou d'un domaine limite ses fonctionnalités. Les niveaux fonctionnels vont de *Windows Server 2000* (première version d'Active Directory) à *Windows Server 2016*. Ce niveau est limité par **le plus vieux contrôleur de domaine** présent dans la forêt. Il est recommandé, pour disposer de toutes les fonctionnalités, d'avoir le niveau fonctionnel le plus élevé. Bien sûr, il est impossible de travailler en niveau fonctionnel *Windows Server 2016* si tous les contrôleurs de domaine ne supportent pas celui-ci (si d'anciens serveurs sont présents).
- ***Organizational units.*** Ces éléments permettent de structurer Active Directory. Pour rappel, la structure LDAP est hiérarchique et l'unité organisationnelle, comme sous Linux, est un moyen de structurer et grouper des objets (utilisateurs, groupes, ordinateurs) créés. Active Directory ajoute, en plus, la possibilité de lier une politique (appelée *Group Policy Object* ou GPO) aux objets d'une unité.

Il faut bien remarquer qu'Active Directory nécessite le service DNS installé. En effet, l'infrastructure AD va inscrire des éléments à l'intérieur de la zone DNS. De plus, le domaine *Active Directory* se confond avec un domaine DNS (il en prend la forme car il nécessite un nom de domaine pour pouvoir fonctionner). Par conséquent, il est impossible d'utiliser *Active Directory* sans disposer d'un service DNS.

Le service DNS interne et externe

Etant donné que Active Directory nécessite un service DNS, il serait tentant d'utilisant un seul service DNS (pour répondre aux requêtes internes et externes) sur le système. Or, il me semble une bonne idée de ne pas publier à l'extérieur les enregistrements d'*Active Directory*. Ainsi, un bon conseil serait de définir deux zones distinctes : la zone *locale* reprenant les entrées *Active Directory* et les informations locales (machines locales, …) et une zone *publique* reprenant les informations à publier à l'extérieur (adresse IP publique et nom du serveur web, information pour le service mail, …).

Ainsi, il n'est pas possible d'obtenir des informations *internes* à l'entreprise en interrogeant le service DNS depuis l'extérieur. Il est également possible d'installer un service DNS sur un autre serveur qui contiendrait uniquement les informations publiées vers l'internet.

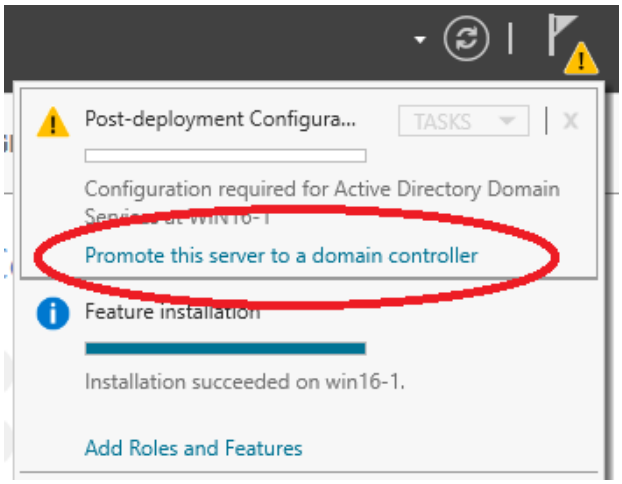
6.2.2 Les différents rôles Active Directory

Windows Server 2016 propose plusieurs rôles différents pour Active Directory en fonction des besoins de l'administrateur et des utilisateurs. Ainsi, on distingue :

- ***Active Directory Domain Services*** *(Services de domaine Active Directory)*. Il s'agit de l'annuaire qui fournira l'authentification, l'autorisation et le monitoring. Il s'agit du service complet d'Active Directory.
- ***Active Directory Lightweight Directory Services*** *(LDS)*. Il s'agit d'une version réduite du service AD DS. Cette version, autonome, sert à héberger les éléments des applications compatibles. Il s'agit réellement d'un sous-ensemble de AD DS (on installe donc pas les deux versions en même temps).
- ***Active Directory Certificate Services*** *(Services de certificats Active Directory)*. Ce rôle, qui peut être ajouté à un rôle AD DS permet de créer une autorité de certification et d'obtenir des certificats pour l'entreprise. Les certificats générés ne sont pas reconnus par des applications externes (et sont donc limités aux ordinateurs du domaine).
- ***Active Directory Rights Management Services*** *(AD RMS)*. Ce rôle particulier permet d'ajouter, à un rôle AD existant, une sécurité renforcée quant aux documents (pour autant que les applications soient compatibles avec le service). Ainsi, il est possible de définir des ACL propres aux documents créés (DACL). L'intérêt étant clairement de contrôler ce que l'on peut faire avec un document produit par l'entreprise (copie, impression, …) dans le but de protéger l'information vitale de l'entreprise.
- ***Active Directory Federation Services*** *(ADFS)*. Ce rôle, qui peut être ajouté à un AD DS existant, permet d'intégrer Active Directory dans une *fédération*. Ainsi, tous les membres d'une fédération peuvent être identifiés et accéder aux ressources misent à leur disposition. Par exemple, si une fédération était créée entre toutes les hautes écoles, n'importe quel étudiant pourrait se connecter, avec ses propres identifiants, dans n'importe quelle école membre de la fédération. La requête de connexion serait acheminée vers l'annuaire qui contient l'utilisateur (ex. : un étudiant de HELMo qui s'identifierait à l'extérieur serait accepté par l'AD de HELMo qui garderait le rôle d'authentification).

6.3 Installation d'Active Directory

Pour l'installer, il faut choisir *Active Directory Domain Services*, il faut passer par le **Server Manager > Manage > Add Roles and Features** et choisir **Active Directory Domain Services** dans la liste. Lors de la sélection, l'assistant propose l'ajout de fonctionnalités particulières qu'il faut accepter. Une fois l'installation terminée, il faut choisir **Promote this server to a domain controller** en cliquant sur le menu pour terminer l'installation d'Active Directory.



Lors de la première installation, il faut *Ajouter une nouvelle forêt* (**add a new forest**) et *Spécifier un nom de domaine racine (***Root domain name**) sous la forme d'un nom DNS pour la forêt. Même si une zone DNS de recherche directe est déjà configurée pour les machines *locales*, il est préférable d'en créer une nouvelle pour le domaine à gérer (pour éviter des problèmes lors de l'installation de ce dernier). Ainsi, nous pourrions choisir *swila.local* comme nom DNS pour la forêt.

Ensuite, il convient de choisir *le niveau fonctionnel de la forêt* (**Functional Level**). En fait, le niveau fonctionnel est limité par le plus vieux contrôleur de domaine actif[24] dans la forêt. Si nous créons une nouvelle structure, nous pouvons choisir le niveau fonctionnel le plus élevé : Windows Server 2016. Il faut également entrer le mod de passe pour le mode de restauration. Je propose de garder le mot de passe `P@ssw0rd` déjà adopté pour le compte Administrateur (il est bien clair que dans un environnement de production, un mot de passe fort est requis).

Le système nous avertit alors : *A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found* (puisque nous utilisons un domaine local). Ce n'est pas un problème et nous pouvons continuer l'installation. Le nom NetBios est ensuite déterminé (partie gauche du domaine). Ensuite, les dossiers hébergeant *le datastore* et les journaux et *SYSVOL* doivent être configurés (les options par défaut sont acceptables). Enfin, après un résumé, l'installation peut se terminer.

Une fois l'installation terminée et le redémarrage réalisé, on remarque que la fenêtre de connexion a changé : en effet, le système nous informe désormais qu'on ouvre une session **sur un domaine** (`swila` dans l'exemple ci-dessous) :

Attention ! Lors de la reconnexion avec le compte `Administrator`, il est possible que le système mentionne que le mot de passe a expiré et doit être changé. Au besoin, vous pouvez changer celui-ci en `Pa$$w0rd`.

6.3.1 Changements suites à l'installation d'Active Directory

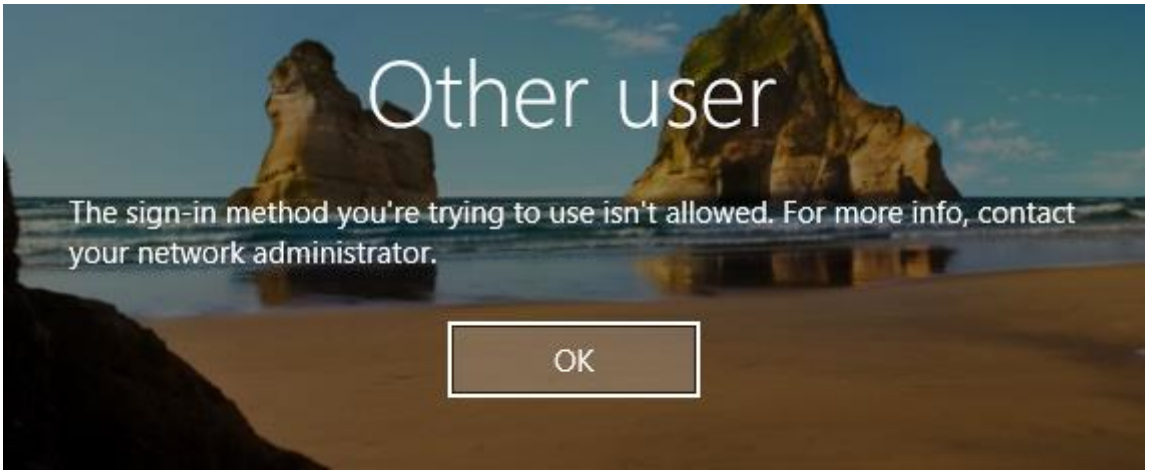
Depuis l'installation d'Active Directory, on remarque qu'il n'y a *plus d'utilisateurs et groupes locaux* (Local Users and Groups a disparu). En effet, puisque le serveur est désormais *contrôleur de domaine*,

[24] Ainsi si un contrôleur de domaine Windows Server 2003 est toujours actif dans la forêt, le niveau fonctionnel doit être limité à cette version.

tous les utilisateurs définis sont *des utilisateurs du domaine*. A l'inverse d'un utilisateur local, un utilisateur du domaine peut s'identifier sur toutes les machines membres du domaine (base de données globale). Si nous avions un second serveur membre du domaine mais pas contrôleur de domaine, il pourrait continuer à définir des utilisateurs (propres au serveur en question alors).

Pour trouver les utilisateurs et groupes du domaine, il est possible d'utiliser une console MMC avec *un composant snap-in* ou, dans le gestionnaire de serveurs, de suivre le chemin suivant : **Server Manager > Tools > Active Directory Users and Computers >** puis choisir votre domaine **> Users**.

Un autre changement important est **que les utilisateurs ne peuvent plus se connecter sur le serveur**. En effet, pour des raisons de sécurité, seul les administrateurs peuvent ouvrir une session sur le contrôleur de domaine.



Nous verrons qu'une politique particulière doit être activée pour autoriser les utilisateurs du domaine à ouvrir une session interactive. Ceci dit, cette précaution est assez logique afin de protéger le serveur des tentatives d'accès.

Un autre changement est **que le service DHCP ne fonctionne plus** depuis le passage en domaine. En effet, afin d'éviter d'avoir plusieurs services DHCP sur le même réseau et dans le même domaine, il est nécessaire d'**autoriser le serveur DHCP**. Pour ce faire, il faut aller dans **Server Manager > Tools > DHCP** choisir votre serveur puis faire un **clic-droit** et choisir **Authorize**.

Depuis l'installation d'Active Directory, la stratégie des mots de passe est active dans le domaine. Pour supprimer cette stratégie, il faut aller dans **Server Manager > Tools > Group Management Policy**. Il faut ensuite déployer les éléments *Forest*, *Domains* puis le *domaine courant* et faire un **clic-droit** sur l'élément *Default Domain Policy* puis choisir **Edit.**

L'éditeur de gestion des stratégies de groupe s'ouvre alors. Il faut aller dans **Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy**. Il faut ensuite modifier les paramètres comme suit :

- Enforce password history : **0 passwords remembered**
- Maximum password age : **0 days**
- Minimum password age : **0 days**
- Minimum password length : **0 characters**

- Password must meet complexity requirements : **Disabled**
- Store passwords using reversible encryption : **Disabled**

Une fois cette modification effectuée, il faut redémarrer le serveur pour qu'elle soit prise en compte.

6.3.2 Structure d'Active Directory

La structure d'Active Directory est visible lorsqu'on déploie **Utilisateur et ordinateur** à partir des **Services de domaine Active Directory**. On y voit l'annuaire LDAP contenant des éléments comme des *utilisateurs, des ordinateurs, des unités organisationnelles* ou encore *des groupes de sécurités*.

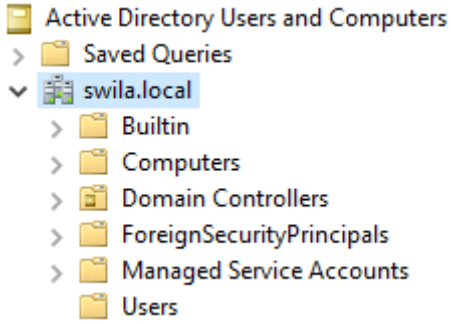


Figure 6.1 : structure LDAP du contrôleur de domaine `swila.local`

Comme nous pouvons le voir sur la figure 6.1, l'annuaire LDAP contient déjà un certain nombre d'éléments : *builtin* qui reprend tous les éléments par défaut présents sur les contrôleurs de domaine. Il n'est pas conseillé de modifier les éléments présents à moins de savoir exactement ce qu'on fait.

Ensuite, il y a l'élément *Computers* qui peut accueillir les ordinateurs qui seront membres du domaine. L'élément *Domain Controllers* reprend tous les contrôleurs de domaine configurés pour le domaine en question. L'élément *Users* reprend les utilisateurs et groupes configurés. Ainsi, on y trouve tous les utilisateurs locaux qui ont été promus dans le domaine, mais également des groupes particuliers. Les deux principaux à ce stade sont :

- *Domain Users* : Reprend tous les utilisateurs membres du domaine qui pourront se connecter sur les machines configurées dans ce domaine.
- *Domain Admins* : Reprend tous les administrateurs du domaine (permet de modifier toute la configuration). Sur un serveur qui n'est pas contrôleur de domaine, il est possible d'avoir un utilisateur membre du groupe *Administrators* de **ce** serveur (pouvant modifier toute la configuration de ce serveur, ajout d'imprimantes, …) mais non membre de *Domain Admins* (ne pouvant donc pas modifier des paramètres de politique du domaine ou des comptes utilisateurs du domaine).

Il est particulièrement courant d'adapter la structure d'Active Directory pour refléter l'organisation interne de l'entreprise. Ainsi, il est courant d'utiliser les conteneurs *Organizational Units* afin de reprendre les différents services de l'entreprise. A l'intérieur de ces unités, il est possible de placer tous les objets mémorisables d'Active Directory comme *les utilisateurs* (**Users**), *les groupes* (**Groups**) ou encore *les ordinateurs* (**Computers**). La hiérarchie créée est ainsi plus facile à gérer, on peut regrouper logiquement les éléments qui sont en relation.

Dans une école, on pourrait ainsi créer les *unités organisationnelles* : Enseignants, Etudiants, Administratifs et Ordinateurs. Dans Etudiants, nous pourrions différencier les étudiants des différentes

sections (*info*, *compta, commex, marketing, …*) et puis placer les étudiants concernés par année (1B, PE et AD). Ainsi, la gestion est beaucoup plus aisée.

6.3.3 Création d'une unité d'organisation

Pour créer une nouvelle unité d'organisation, il faut démarrer **Active Directory Users and Computers** et faire **un clic-droit** sur le nom de domaine (ex : swila.local). Il faut alors choisir l'option *New > Organizational Unit*. Il faut ensuite lui donner un nom. L'unité est alors prête à accueillir des éléments à l'intérieur : d'autres unités d'organisation, des ordinateurs, des utilisateurs ou des groupes de sécurité.

En **ligne de commande**, il faut utiliser la commande `dsadd.exe`. Pour l'aide, il suffit d'exécuter la commande **`dsadd.exe ou /?`**.

```
C:\> dsadd.exe ou "OU=Service Informatique,DC=swila,DC=local"
```

Cette commande permet de créer la nouvelle unité d'organisation `Service Informatique` à l'intérieur du domaine `swila.local`[25].

En **Powershell**, la création d'une nouvelle unité d'organisation peut se faire de trois façons : soit en utilisant les modules spécifiques de PowerShell pour Active Directory, soit en utilisant les objets ADSI ou encore en utilisant une exécution directe de commande. Les objets ADSI **ne sont pas recommandés pour cette opération**, nous n'en parlerons pas.

L'environnement Powershell contient de nouvelles commandes pour gérer et créer des objets dans Active Directory. Ainsi, il est possible de créer une nouvelle unité d'organisation simplement en entrant la cmdlet suivante :

```
PS C:\> New-ADOrganizationalUnit –Name "Service Informatique" –Path
            "DC=swila,DC=local"
```

6.3.4 Création d'un utilisateur de domaine

La création d'un nouvel utilisateur de domaine se fait aisément depuis l'interface **Active Directory Users and Computers**. Il suffit de faire un **clic-droit** et de choisir l'option *New > User*. L'interface de création d'un utilisateur du domaine est un peu différente de celle d'un utilisateur local. Outre le *prénom*, le *nom* et le *nom complet*, il faut mentionner le *nom d'ouverture de session de l'utilisateur* (**User logon name**) et le nom utilisé pour les systèmes antérieur à Windows 2000 (**User logon name pre-Windows 2000**). Ces deux dernières informations reprennent le *login* de l'utilisateur. Un nom conforme à des postes antérieurs à Windows 2000 implique de ne pas utiliser de caractères spéciaux et d'en limiter la taille.

D'une façon générale, il est intéressant de limiter la taille du nom d'utilisateur de façon à permettre à l'utilisateur de ne pas devoir entrer une information trop longue.

[25] L'élément `OU` fait référence à une *unité d'organisation* tandis que l'élément `DC` fait référence au *contrôleur de domaine*. Ainsi `DC=swila, DC=local` fait bien référence au domaine `swila.local`

Une fois le premier écran remplit, le système demande d'entrer un mot de passe et propose les options habituelles. **Attention !** Si la stratégie des mots de passe est toujours active, la complexité du mot de passe sera vérifiée.

L'utilisateur est, par défaut, membre du groupe *Domain Users* et pourra ainsi ouvrir une session sur tous les ordinateurs membres de ce domaine (excepté les contrôleurs de domaine).

En **ligne de commande**, la commande `dsadd.exe` permet de créer des utilisateurs. Pour obtenir l'aide sur cette partie, il faut entrer **`dsadd.exe user /?`**.

```
C:\> dsadd user "cn=Louis SWINNEN,ou=Service Informatique,dc=swila,
       dc=local" -samid lsw -upn lsw@swila.local -fn Louis -ln SWINNEN
       -display "Louis SWINNEN" -pwd "P@ssw0rd" -canchpwd no
       -pwdneverexpires yes
```

Cette commande permet d'ajouter un utilisateur (`Louis SWINNEN`) dans l'unité d'organisation `Service Informatique`, le nom d'ouverture est `lsw@swila.local` et celui pour les systèmes antérieurs à Windows 2000 est `lsw`. Le prénom est fixé à `Louis` et le nom de famille à `SWINNEN`. Le nom affiché sera et le mot de passe `Louis SWINNEN`. Enfin, le mot de passe est fixé `P@ssw0rd` avec les options suivantes : l'utilisateur ne peut changer son mot de passe (`-canchpwd no`) et celui-ci n'expire jamais (`-pwdneverexpires yes`).

Il y a bien d'autres options possibles à la commande `dsadd.exe` notamment celles qui permettent de fixer les chemins vers les dossiers de bases et le profil. Nous en parlerons plus loin dans cette leçon.

En **Powershell**, il est possible d'ajouter un utilisateur en utilisant les commandes spécifiques pour Active Directory comme suit :

```
PS C:\> new-ADUser -Name "Louis SWINNEN" -AccountPassword (ConvertTo-
   SecureString -AsPlainText "P@ssw0rd" -Force) -Enabled $true
   -PasswordNeverExpires $true -CannotChangePassword $true
   -SamAccountName lsw -UserPrincipalName lsw@swila.local
   -Path "OU=Service Informatique,DC=swila,DC=local" -GivenName "Louis"
   -Surname "SWINNEN" -DisplayName "Louis SWINNEN"
```

Cette commande `New-ADUser` permet de créer un nouvel utilisateur dans Active Directory. Dans cet exemple, l'utilisateur est créé dans l'unité d'organisation Service Informatique. Il est nécessaire de consulter la documentation[26] pour connaître toutes les options.

Comme toujours, l'exécution directe permet également d'appeler la commande `dsadd.exe user` directement depuis Powershell.

6.3.5 Création d'un groupe de sécurité

Les groupes de sécurité ont, comme dans le cas des groupes locaux, les mêmes fonctionnalités. La différence principale est que leur portée s'étant à tout le domaine. Ainsi, un groupe de sécurité défini sur le contrôleur de domaine est *visible* sur toutes les machines du domaine. C'est une particularité intéressante qui permet ainsi de définir un groupe depuis le contrôleur de domaine et celui-ci peut alors être utilisé (pour fixer des permissions sur des fichiers et/ou dossiers sur les machines membres du domaine) n'importe où.

[26] http://technet.microsoft.com/en-us/library/ee617253.aspx

Pour créer un groupe de sécurité, il faut faire un **clic-droit** et choisir l'option *New* > *Group*. La fenêtre de création du groupe apparaît alors. Il faut mentionner son nom (et son nom compatible pour les systèmes pré-Windows 2000), mentionner son étendue et son type.

L'étendue peut être *domain local* et dans ce cas, le groupe est connu du contrôleur de domaine seulement, *global* et dans ce cas, le groupe est connu à travers le domaine pour lequel le contrôleur est configuré (c'est l'option par défaut) ou *universal* et, dans ce cas, l'étendue est définie à la forêt complète.

Le type de groupe peut être *Security* et dans ce cas, ils sont utilisés pour définir des droits et autorisations sur des ressources données ou *Distribution* et sont, dans ce cas, utilisable uniquement par le logiciel de courrier électronique pour faire la distribution du courrier à plusieurs utilisateurs directement.

En **ligne de commande**, la commande `dsadd.exe` permet d'ajouter des groupes de sécurité. Pour obtenir l'aide, veuillez-vous référer à la commande `dsadd.exe group /?`.

```
C:\> dsadd group "CN=Informatique,OU=Service Informatique,DC=swila,
        DC=local" -secgrp yes -scope g
```

Cette commande permet de créer un groupe de sécurité nommé Informatique localisé dans l'unité d'organisation Service Informatique. L'étendue de ce groupe est globale.

```
C:\> dsmod group "CN=Informatique,OU=Service Informatique,DC=swila,
        DC=local" -addmbr "CN=Louis SWINNEN,OU=Service Informatique,
        DC=swila,DC=local"
```

Cette commande permet d'ajouter l'utilisateur Louis SWINNEN au groupe de sécurité Informatique présent dans l'unité d'organisation Service Informatique.

En **Powershell**, il est possible d'ajouter un groupe omme suit :

```
PS C:\> New-ADGroup -Name "Informatique" -samAccountName Informatique
         -GroupCategory Security -GroupScope Global
         -Path "OU=Service Informatique,DC=swila,DC=local"
```

Cette commande permet de créer un groupe de sécurité d'étendue globale nommé Informatique et placé dans l'unité d'organisation Service Informatique.

```
PS C:\> Add-ADGroupMember "CN=Informatique,OU=Service Informatique,
         DC=swila,DC=local" -Members "CN=Louis SWINNEN,OU=Service
         Informatique,DC=swila,DC=local"
```

Cette commande permet d'ajouter l'utilisateur Louis SWINNEN au groupe Informatique tous deux situés dans l'unité Service Informatique.

6.3.6 Création d'un compte Ordinateur

Dans Active Directory, les ordinateurs membres du domaine sont stockés sous la forme d'objet particulier, les comptes « Ordinateurs ». Tous les ordinateurs membres du domaine doivent apparaitre dans l'annuaire.

Lorsqu'on ajoute un ordinateur au domaine, le compte ordinateur peut être créé à ce moment. Il est pourtant bien plus commode de créer ce compte au préalable. Ainsi, il est déjà placé dans la bonne unité d'organisation et la structure d'Active Directory reste cohérente.

Pour créer un compte ordinateur, il suffit de connaître le nom de cette machine. Ensuite, il faut faire un **clic-droit** à l'endroit où l'on souhaite ajouter ce compte et choisir l'option *New* > *Computer*. Il faut ensuite mentionner son nom ainsi que le nom compatible pré-Windows 2000.

En **ligne de commande**, l'ordinateur peut être créé par la commande `dsadd.exe`. Pour obtenir l'aide concernant cette commande, référez-vous à la documentation en ligne **`dsadd.exe computer /?`**.

```
C:\> dsadd computer "CN=Win7,OU=Service Informatique,DC=swila,DC=local"
       -samid Win7
```

Cette commande permet de créer un compte ordinateur pour la machine nommée Win7.

En **Powershell**, il est possible d'ajouter un ordinateur comme suit :

```
PS C:\> New-ADComputer –Name "Win7" –SamAccountName "Win7"
         –Path "OU=Service Informatique,DC=swila,DC=local"
```

Cette commande permet de créer un compte d'ordinateur pour la machine Win7. Le compte d'ordinateur est créé dans l'unité d'organisation Service Informatique.

6.4 Les profils itinérants

Nous avons vu dans une leçon précédente que les profils utilisateurs renseignent les paramètres et la configuration de celui-ci. Or, la mise en domaine pose un certain nombre de questions : souhaite-t-on que l'utilisateur dispose d'un profil différent sur chaque machine sur lesquelles il se connecte ? Souhaite-t-on, au contraire, qu'il récupère son profil et retrouve ses documents quelque soit la machine sur laquelle il se connecte ?

Dans la plupart des cas, la seconde proposition est la plus souhaitable : l'utilisateur se connecte sur une machine membre du domaine et il récupère son profil. Pour réaliser cette opération, il est nécessaire que le profil de l'utilisateur soit stocké dans un endroit accessible pour toutes les machines membres du domaine. Il est nécessaire que les autorisations soient fixées correctement pour permettre une modification de ces données.

Ainsi, il convient de sauvegarder le profil de l'utilisateur sur **un partage réseau**. Ce partage doit être renseigné dans les informations de profil de l'utilisateur afin que les machines puissent y accéder dès qu'il se connecte.

Pour ce faire, il va falloir :

- Créer un dossier qui contiendra les données de profil des utilisateurs
- Partager ce dossier de sorte à ce qu'il puisse être accessible sur le réseau (**autorisations de partage & droits**)
- Placer les profils des utilisateurs, ainsi que son répertoire de base dans le dossier créé et renseigner ce dossier dans l'onglet profil de l'utilisateur. **Attention !** Il **faut** mentionner **un chemin réseau valide pour toutes les machines membres du domaine**. Par exemple : `\\SWINNEN\Users\%USERNAME%` pour le dossier de base et `\\SWINNEN\Users\%USERNAME%\ntprof` pour le chemin vers son profil.

Ainsi, le chemin devra commencer par les caractères `\\` mentionnant que le chemin est de type réseau (appelé parfois UNC). On mentionne ensuite le nom du serveur (ou son adresse IP) et puis le nom du

partage contenant les données utilisateurs[27]. Il est intéressant de savoir que la variable `%USERNAME%` désigne le login de cet utilisateur. Ainsi, nous aurons un dossier particulier par utilisateur.

Il convient également de fixer les permissions précisément car l'utilisateur doit disposer d'une permission de type *contrôle totale* sur son dossier de base et sur le chemin vers son profil. Pour rappel, le profil est mémorisé dans le chemin mentionné dans le compte de l'utilisateur. Sans modification particulière du registre, le dossier contenant le profil est suffixé suivant le système d'exploitation utilisé (en supposant que `ntprof` soit renseigné comme chemin du profil) comme suit : « `.V2` » pour les systèmes Vista, 7, Server 2008, Server 2008 R2, 8, Server 2012, 8.1, Server 2012R2 et Windows 10 < 1607 et « `.V6` » pour les systèmes Windows 10 >= 1607 et Server 2016.

Nous remarquons également qu'il est possible de *connecter automatiquement* un lecteur réseau vers le répertoire de base de l'utilisateur. Cela lui permet d'avoir un accès simple à son dossier personnel.

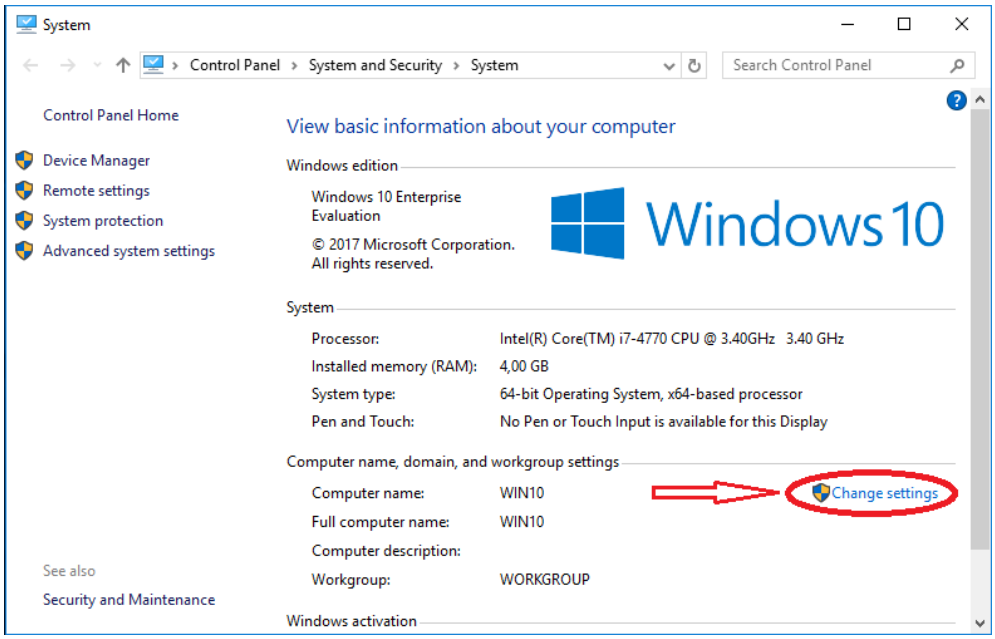
Enfin, il est également possible de créer un profil **itinérant obligatoire**. Il s'agit d'un profil configuré sur le contrôleur de domaine que l'administrateur personnalise selon ses besoins. Une fois terminé, l'administrateur le rend obligatoire et toutes les machines du domaine acceptent une connexion sur base de ce profil mais aucune modification ne peut y être apportée.

6.5 Intégrer une machine à un domaine

Le grand intérêt du passage en domaine est d'intégrer des postes clients dans le domaine afin de permettre une authentification centralisée et distribuer une politique de configuration à l'ensemble des machines.

Cette entrée des machines dans le domaine peut s'opérer de plusieurs manières. La façon la plus courante est la suivante : faire un **clic-droit** sur **This PC** et choisir l'option **Properties**[28]. Il faut alors sélectionner **Change settings** dans la section *Computer name, domain, and workgroup settings.* Dans l'onglet *Computer Name*, choisir le bouton *Change*.

[27] Dans notre exemple, le dossier de base se trouve sur le serveur dont le nom est `SWINNEN` et le nom du partage est `Users`. Un dossier reprend le login de l'utilisateur concerné (`%USERNAME%`) est présent.
[28] Sous Windows XP, Vista et Windows 7, il est également possible d'utiliser l'option **Gérer** en faisant un **clic-droit** sur **Ordinateur** et en choisissant **Gérer** dans le menu.



Ensuite, il convient d'entrer un nom de domaine dans l'option domaine (par exemple `swila.local`).

Afin de pouvoir contacter le contrôleur de domaine, il faut impérativement **que la machine utilise le contrôleur de domaine comme serveur DNS principal.** Pensez-donc à vérifier cela avant de tenter d'introduire une machine dans le domaine.

Une fois le nom de domaine configuré et **pour autant que le serveur puisse contacter le contrôleur** de domaine gérant celui-ci (voir la remarque concernant le DNS dans le paragraphe précédent), il devrait demander d'entrer un compte d'administrateur pour entrer cette machine dans le domaine.

Le compte mentionné doit faire partie du groupe *Domain Admins* afin de permettre l'entrée de la machine dans le domaine. Si tout se passe correctement, la machine est intégrée au domaine et le système vous demande de redémarrer celle-ci (en effet, le nom de la machine a changé).

Si aucun compte machine n'avait été créé au préalable sur le contrôleur de domaine, un compte a été ajouté dans le groupe *Computer* du contrôleur de domaine. Au contraire, si la machine avait déjà un compte à son nom, ce compte est utilisé pour l'affiliation au domaine.

Au redémarrage de la machine, nous observons quelques modifications :

- L'écran de sélection de l'utilisateur a disparu. Il faut entrer l'identité de l'utilisateur avec laquelle on souhaite se connecter
- Par défaut, la machine ouvre une session sur le domaine configuré, sauf pour le compte Administrateur/Administrator où elle choisit une connexion sur la machine locale
- Le firewall est à nouveau actif. En effet, comme un *nouvel emplacement* a été ajouté à la liste (nommé *réseau avec domaine*), le firewall est actif sur cet emplacement. Il convient de désactiver le firewall.

La machine est désormais membre du domaine et accepte l'authentification de n'importe quel compte utilisateur du domaine.

6.6 Exercices

1. Supprimer tous les comptes utilisateurs créés par script (leçon 3, exercice 3)

2. Installer le rôle AD Domain Services et configurez votre contrôleur de domaine AD :
   a. Le nom de domaine est `cgXXdom.local` (où XX est votre numéro de machine)
   b. Utiliser le mot de passe `P@ssw0rd` pour le mode restauration
   c. Fixer le niveau fonctionnel de la forêt à Windows 2016
   d. *(optionel)* Si votre système propose de changer votre mot de passe Administrateur, utilisez `Pa$$w0rd`
   e. Supprimez la stratégie de mot de passe par défaut du domaine

3. Créer un dossier partagé `c:\CGData` muni des autorisations adéquates pour stocker les profils des utilisateurs.

4. Créer une unité d'organisation `CGComputers` et créer un compte d'ordinateur `VM-WIN10` pour la machine virtuelle Windows 10.

5. Réécriver votre script de création des utilisateurs pour :
   a. Créer des utilisateurs membres du domaine AD
   b. Les utilisateurs seront créés dans une OU `CGUsers` et vous créerez une OU par catégorie. Ainsi les utilisaturs de *direction* seront placés dans la branche `CGUsers\direction`.
   c. Créer un groupe de sécurité globale par catégorie. Ainsi, dans le groupe de sécurité `informatique`, on trouvera tous les utilisateurs de la catégorie *informatique*.
   d. Fixer le chemin vers le profil de l'utilisateur vers le chemin `CGData\<login>\netprofile`. Fixer également le chemin vers le dossier de base `CGData\<login>` et connectez un lecteur `P:` (cf. exercice 3).
   e. Fixer les ACL vers les dossiers correctement

6. Ajouter la VM Win10 à votre domaine et tentez une connexion avec un compte utilisateur
   a. Changez son nom en `VM-WIN10` et ajoutez-la dans le domaine
   b. Vérifiez bien que le profil de l'utilisateur est trouvé

7. Créer un compte `helmodom` avec comme mot de passe `cgdom2016` comme étant un compte de domaine obligatoire. Fixer le chemin vers son profil et son répertoire de base (comme pour les utilisateurs créés à l'étape 5).

8. Connectez-vous avec le compte `Administrator` du domaine sur la VM Win10.
   a. Comment procéder ?
   b. Où est stocké le profil ?
   c. Créez un dossier `AdmSys` sur le disque `C:` uniquement accessible aux utilisateurs de la catégorie *informatique*