Création des utilisateurs, des OUs et des groupes

Les comptes utilisateurs

Les utilisateurs sont caractérisés par leurs comptes.

Un compte utilisateur est une représentation d'une personne physique, par exemple un collaborateur d'une entreprise. Il va permettre à cette entité de se connecter à un ordinateur et/ou à un domaine à l'aide d'un identifiant propre et d'un mot de passe secret. Ces comptes s'apparentent aux sessions.

On distingue deux types de compte :

- **Compte local :**

  Un Compte Local est, comme son nom l'indique, un compte propre à une machine. Son profil sera stocké dans la base de données « Security Accounts Manager » (SAM). Il ne sera accessible que depuis l'ordinateur où le compte est référencé. En effet, ce compte n'aura accès qu'à la ressource de la machine et par conséquent dépendra de cette dernière. Ce type de compte est très contraignant car cela nécessite que les comptes soient stockés dans les différentes bases SAM des ordinateurs.

  Ce type de compte comporte par défaut 2 profils :

  - administrateur
  - invité (compte désactivé par défaut)

  Ces comptes ne peuvent être créés que depuis l'ordinateur en question via l'interface de gestion des utilisateurs. Les attributs du compte sont très restreints (nom, prénom) et ne sont pas appropriés pour un listing. Ces comptes sont très difficiles à gérer et par conséquent, ils ne sont pas privilégiés par les entreprises, ces comptes étant réservés aux particuliers.

- **Compte du domaine :**

  Le compte du domaine fonctionne différemment du compte local. Ces comptes ne sont plus stockés dans la base de données SAM de l'ordinateur mais dans la base de données d'Active Directory. Ces comptes sont des objets d'annuaires et sont caractérisés par un ID de sécurité (SID). C'est grâce à ce SID que le compte se verra, ou non, accorder l'accès au domaine. Ainsi, il est possible de se connecter aux comptes utilisateurs depuis n'importe quel ordinateur (à condition que ce dernier soit connecté au domaine et qu'il n'y ait pas de restrictions définies).

  Par défaut, deux types de comptes sont configurés dans la base Active Directory :

  - administrateur
  - invité

  Que ce soit un compte local ou un compte de domaine, ils reposent sur deux principes fondamentaux :

- Authentification de l'utilisateur (nom ou ID de l'individu et mot de passe) : A noter qu'il est possible pour les utilisateurs du domaine de définir des options d'authentification. En effet, une règle peut imposer le fait que l'utilisateur change son mot de passe à la première ouverture de session. On peut également demander à l'utilisateur d'entrer un mot de passe avec un nombre précis de caractère grâce aux GPO. Lors de la création d'un nouvel utilisateur, il est possible de cocher les options d'authentification.
- Autorisation de l'utilisateur (accès aux fonctionnalités propres aux habilitations de la personne) : L'utilisateur se verra accorder l'accès à sa session selon ses habilitations. En effet, selon son niveau d'habilitation, un compte d'utilisateur aura accès à des fonctionnalités différentes. Par exemple, un administrateur aura plus de privilèges qu'un simple stagiaire. Le fait de désactiver ces fonctionnalités permet aux administrateurs d'assurer le contrôle et la sécurité du domaine et empêche un utilisateur lambda d'installer un programme étranger pouvant engendrer une faille dans le réseau.

  Cependant, certains utilisateurs devront avoir accès à ses privilèges. Il est important de pouvoir les identifier rapidement afin de surveiller ces comptes sensibles. De plus, quand une entreprise comporte plusieurs centaines de collaborateurs, il est nécessaire de pouvoir les regrouper par catégories.

La création de ces comptes se fait via la console ordinateur et utilisateurs Active Directory. Il est aussi possible d'utiliser PowerShell.

Au travail maintenant !

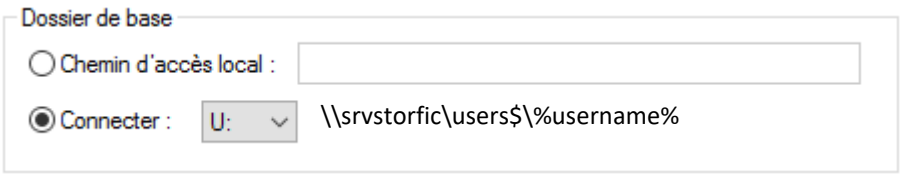
Bien entendu, lors de la création des utilisateurs, vous devrez respecter la nomenclature de votre entreprise concernant le nom d'ouverture de session.

Vous allez commencer par créer un utilisateur modèle (cela se passe sur votre contrôleur de domaine, est-il nécessaire de le rappeler ?). Ce compte servira de base pour créer les comptes restants par copie.

Tout se passe dans les **outils d'administration**, **ordinateurs et utilisateurs Active Directory**.

- Développez votre arborescence Active Directory et cliquez droit sur Users puis Nouvel utilisateur
- Mettez **zmodele** (le Z pour que votre modèle apparaisse en bas de la liste) en prénom, pas de nom et **zmodele** en nom d'ouverture de session.
- Cliquez sur suivant et sélectionnez **L'utilisateur doit changer le mot de passe à la prochaine ouverture de session**. Cliquez aussi sur **Le compte est désactivé**. Mettre en mot de passe Azerty/123
- Sélectionnez ensuite votre utilisateur zmodèle puis faites **Propriétés**. Nous allons nous intéresser aux onglets **Compte** et **Profil**
- Dans l'onglet **Compte**, vous allez modifier les horaires d'accès et interdire à votre utilisateur de travailler entre 20 heures et 6 heures du matin
- Vous constaterez l'existence du bouton **Se connecter à** qui va vous permettre de définir sur quelle machine l'utilisateur peut se connecter et à contrario ne pas se connecter. Il faut évidemment que les machines soient des Objets Active Directory

- Dans l'onglet profil, vous allez vous intéresser à la création du répertoire personnel de l'utilisateur appelé ici Dossier de base. Renseignez comme ceci :



ATTENTION : N'hésitez pas à vérifier l'accessibilité de votre partage

Cela mérite des explications ! **%username%** est une **variable** qui représente le nom d'ouverture de session de l'utilisateur. Le système va donc créer sur votre serveur de fichier dans le répertoire utilisateurs un dossier qui s'appellera **zmodele**. Une lettre de lecteur U : est associé à ce nouveau répertoire (petit rappel : il aurait aussi été possible de créer un script qui connecte directement le lecteur au répertoire de l'utilisateur : **net use u : \\srvstorfic\users$\%username%.**

- Vous pouvez maintenant utiliser votre modèle et créez tous vos comptes utilisateurs (la totalité de l'organigramme). Pour chaque, vous devrez tout de même définir le prénom, le nom, le nom d'ouverture de session et le mot de passe. Lorsque vous avez créé le premier, vérifiez que son dossier de base est bien renseigné ainsi que les horaires d'ouverture de session
- Pour contrôler que les dossiers de base ont bien été créés sur votre serveur de fichier, vous pouvez soit ouvrir une session sur votre serveur de fichiers et regarder dans utilisateurs soit le faire à partir de votre contrôleur de domaine (là où vous vous trouvez normalement en ce moment). Pour faire cela : clic droit sur le menu démarrer puis Exécuter. Tapez alors **\\srvstorfic\users$**. Vous arrivez directement dans votre répertoire utilisateurs. Quelle que soit la méthode utilisée, faites propriétés sécurité sur le répertoire d'un utilisateur. Que constatez-vous ? Qui a les droits ?

Droits de l'utilisateur

L'utilisateur propriétaire du répertoire devrait avoir des droits complets (Contrôle total) sur son propre répertoire. Cela permet à l'utilisateur de lire, écrire, modifier et supprimer les fichiers dans son répertoire.

Droits de l'administrateur :

Le groupe "Administrateurs" ou un compte administrateur devrait également avoir des droits complets (Contrôle total) sur le répertoire.

Droits du système :

Le compte "SYSTEM" devrait également avoir des droits complets (Contrôle total).

Les unités organisationnelles

Définition

Une unité organisationnelle (UO) est un objet de type « conteneur » permettant d'améliorer la structure hiérarchisée d'Active Directory. Ces conteneurs permettent d'accueillir des utilisateurs, des groupes utilisateurs ainsi que des groupes ordinateurs (à condition que ces objets appartiennent au même domaine).

Présentation

Les unités organisationnelles sont la plus petite entité à laquelle on peut affecter une GPO (Group Policy Object). Ainsi, il est très utile et très conseillé d'avoir recours aux unités organisationnelles.

Il est possible d'imbriquer les unités organisationnelles entre elles. Cela permet de mieux hiérarchiser les comptes utilisateurs et ordinateurs. De plus, il est possible de déléguer des droits d'administration aux différentes UO. Ainsi on ne délègue que les droits relatifs à cette UO et on évite ainsi de donner les pleins pouvoirs. Ceci est donc une mesure de sécurité qui fait des UO un système très intéressant.

En effet, dans un parc informatique, tout le monde n'a pas les mêmes droits et les mêmes politiques de sécurités. Ainsi, afin de ne pas gérer les utilisateurs un par un en leurs attribuant des droits spécifiques, on peut les regrouper en UO et ainsi appliquer les GPO propres aux départements où ils se situent.

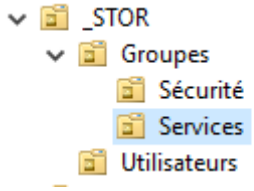
Afin de gérer au mieux le domaine via les UO, il est nécessaire d'appliquer un modèle de hiérarchisation aux UO. Ce modèle doit être choisi en fonction de ces besoins et il doit être évolutif. Le modèle administratif de l'entreprise peut servir de calque à la création d'UO. Cependant, il ne faut pas non plus créer des UO en fonction de son organigramme ou du moins, il faut essayer de ne pas en faire une reproduction.

La création des UO se fait en interface graphique via le panneau utilisateur et ordinateur Active Directory ou via la console PowerShell. Il est nécessaire pour cela de disposer des droits administrateurs.

C'est à vous !

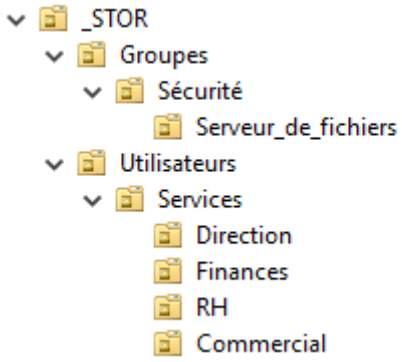
Il est toujours important de réfléchir à l'organisation de notre informatique pour créer des unités d'organisation pratiques. **Les GPO** (les stratégies), que vous verrez plus tard, **s'appliquent sur des OU**, c'est-à-dire que les objets « rangés » dans l'OU seront impactés par la GPO de l'OU.

Utilisez l'outil Utilisateurs et ordinateurs Active Directory. Créez l'arborescence suivante. Pour faire cela, cliquez avec le bouton droit sur le nom de votre domaine (storX.local) et faites Nouveau Unité d'Organisation. Créez toutes les OU



Ah mince, il y a une erreur. Services n'est pas à la bonne place. Déplacez le dans Utilisateurs. Cela ne devrait pas fonctionner. Cherchez pourquoi ? Un indice ? Fonctionnalités avancées !

Créez donc l'arborescence suivante. **Déplacez vos utilisateurs pour les « ranger » dans les bonnes OU**. A noter qu'il est aussi possible de déplacer l'ordinateur de l'utilisateur avec l'utilisateur mais cela n'a pas trop de sens. Il est préférable de laisser les ordinateurs ensemble. Par exemple, si vous voulez déployer des mises à jour sur l'ensemble de vos ordinateurs, il sera préférable qu'ils soient dans la même OU pour pouvoir y **appliquer une GPO**.



Création des groupes

Afin de gérer les utilisateurs plus facilement, il est possible de regrouper les comptes utilisateurs et les comptes ordinateurs en différents groupes.

Mais qu'est-ce qu'un groupe ?

Un groupe est un regroupement d'utilisateurs. Ces groupes sont destinés à faciliter la gestion des utilisateurs en les regroupant en une même entité.

Ainsi, on peut :

- Assigner un ensemble d'autorisation à plusieurs comptes en une fois
- Déléguer des droits d'administration et ainsi décentraliser la gestion du parc
- Créer des listes de distributions

En effet, cela repose sur l'héritage des propriétés et des droits des parents de l'objet. Affecter un utilisateur à un groupe ne veut pas dire pour autant que cet utilisateur est affecté uniquement à ce groupe. En effet, **il est possible à un utilisateur d'être membre de plusieurs groupes**. La création de ces groupes permet aux utilisateurs de ce groupe d'utiliser ou non une ressource (dossier, fichier, imprimante…)

On peut distinguer deux types de groupes :

- Les groupes de sécurité :

  Ces groupes sont utilisés pour gérer la sécurité aux ressources. Imaginons un dossier contenant des dossiers du personnel que seule l'administration peut voir. Au lieu d'ajouter les autorisations de lecture et d'écriture à tous les membres de l'administration un à un, on va placer tous les membres de l'administration dans un groupe spécifique puis on va accorder les privilèges directement à ce groupe. Les propriétés de l'objet parent héritant sur les objets enfant, tous les membres auront les mêmes privilèges que l'objet parent, à savoir le droit de lecture et d'écriture.

- Les groupes de distribution :

  Ces groupes sont souvent utilisés dans le cas de messagerie électronique. Il est parfois utile de regrouper plusieurs personnes dans un même groupe plutôt que de sélectionner ou entrer les nombreux utilisateurs auxquels nous souhaitons envoyer un message électronique. Par exemple, nous souhaitons envoyer un e-mail aux collaborateurs du service de la comptabilité, soit nous inscrivons toutes les adresses e-mail des collaborateurs, soit nous nous servons du groupe comptabilité préalablement créé, afin de pouvoir envoyer le e-mail plus rapidement.

La sélection du type de groupe s'effectue lors de la création du groupe. Vous pourrez voir qu'il y a également un autre champ à remplir lors de la création d'un groupe : l'étendue.

Qu'est-ce l'étendue d'un groupe ?

L'étendue d'un groupe correspond à l'influence et le rayon d'action du groupe. On distingue à ce jour, trois types de portés de groupes :

- Groupe local du domaine :

  Un groupe ayant une étendue locale est un groupe qui pourra avoir une action uniquement dans le domaine où il se trouve.

- Groupe global :

  Un groupe ayant une étendue globale est un groupe qui pourra agir sur toute la forêt set non pas uniquement sur le domaine dans lequel le groupe se trouve. La seule contrainte est que les utilisateurs du groupe doivent provenir du même domaine que celui où le groupe va être créé.

- Groupe universel :

  Un groupe ayant une étendue universelle est un groupe qui est quasi similaire aux groupes globaux à l'exception que les groupes universels peuvent accueillir des utilisateurs situés sur d'autre domaine que celui du groupe.

Bien que le choix de l'étendue se fasse à la création du groupe, il est tout de fois possible de modifier ce critère ultérieurement via la console utilisateur et ordinateur Active Directory.

Bien que les groupes soient un moyen efficace de sécuriser l'accès aux ressources, cela ne suffit pas pour un administrateur pour gérer les nombreux comptes. Pour ce faire, un autre type de « groupe » existe pour administrer plus efficacement un domaine : les unités organisationnelles.

A votre tour !

Vous allez créer des groupes. Ils vont principalement nous servir à affecter les droits sur notre serveur de fichiers.

Je vais vous proposer ma méthode. Ce n'est pas forcément la meilleure mais rassurez-vous ce n'est pas la pire ;) Vous verrez sans doute d'autres méthodes en entreprise… et vous verrez des entreprises sans méthodes !

Voici ce que je propose :

- Il y a deux grandes familles de droits. Soit de la lecture seule, soit des autorisations de modification. On peut définir cela comme ça : groupe_R si droit en lecture seule, soit groupe_RW si contrôle total. Pas de panique je vais donner un exemple plus loin.
- Un répertoire qui doit posséder des droits spécifiques se verra affecter deux groupes : groupe_R et groupe_RW.
- Suivant les autorisations d'accès définies, il vous reste à placer les bons utilisateurs dans les bons groupes.

Prenons un exemple : le répertoire gestion qui se trouve dans Services et Finance

- Pour pouvoir accéder à gestion, il faut d'abord accéder à Services puis à Finance
- Il faut donc créer les groupes suivants :
    - Services_R et Services_RW
    - Finance_R et Finance_RW
    - Gestion_R et Gestion_RW
- Tous vos utilisateurs seront membres de Services_R
- Toutes les personnes du pôle Finance seront dans le groupe Finance_R
- Toutes les personnes du pôle Gestion seront dans le groupe Gestion_RW

Grace à cet exemple, vous êtes maintenant en capacité de créer **tous les groupes correspondant à votre arborescence Services**. N'oubliez-pas de mettre les utilisateurs dans les bons groupes.

Comment créer le groupe :

- Clic droit sur l'OU Serveur_de_fichiers
- Nouveau groupe
- Renseignez le nom du groupe
- Ne touchez à rien d'autre

Pour ajouter un utilisateur dans un groupe :

- Soit sur les propriétés de l'utilisateur, onglet membre de et vous ajoutez les groupes dont il est membre
- Soit sur les propriétés du groupe, onglet Membres et vous ajoutez les utilisateurs qui sont membres.