

Active Directory – Utilisateurs, Ordinateurs et Groupes

Dernière mise à jour : 15/05/24

Table des matières

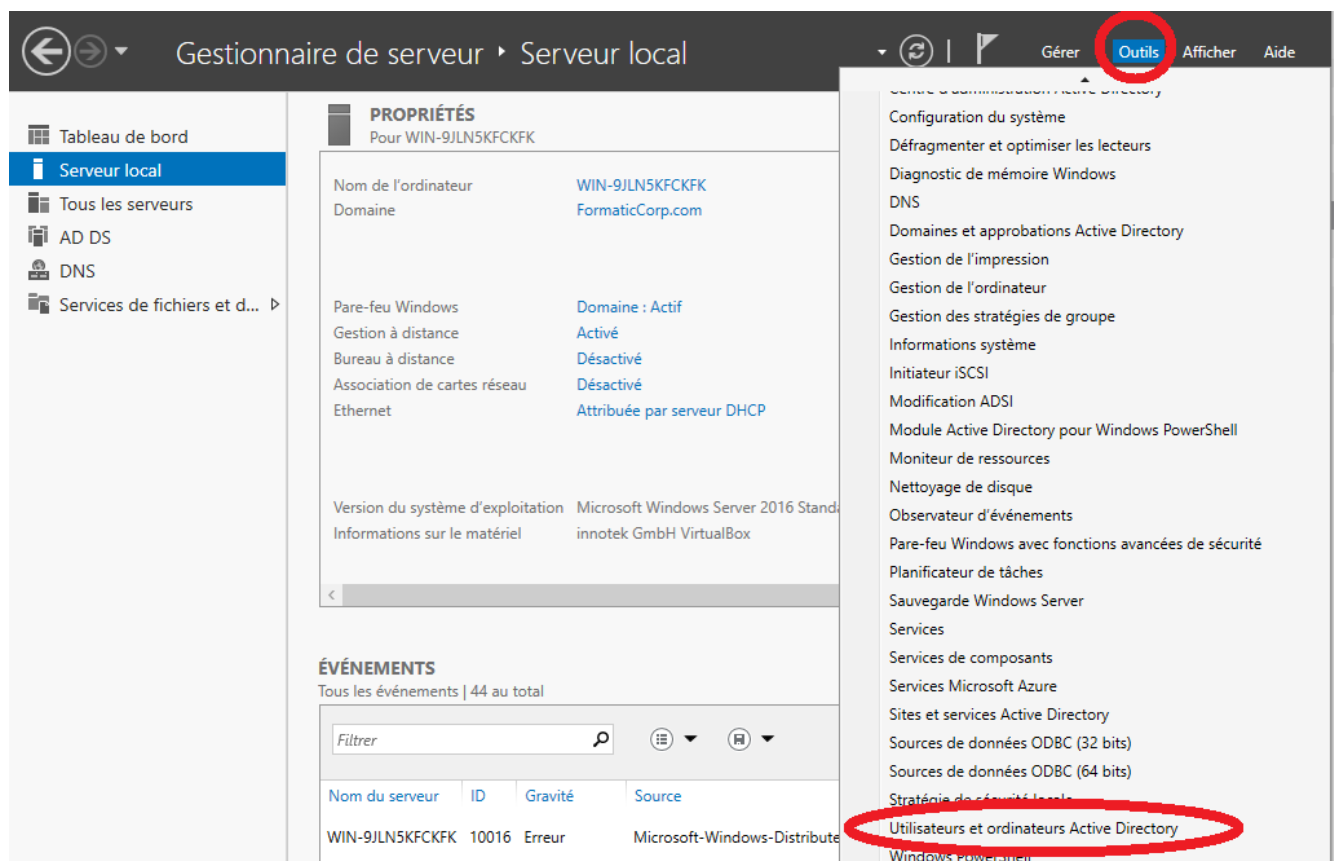
I. Gestion des utilisateurs.....	2
II. Gestion des ordinateurs.....	11
III. Gestion des groupes.....	18

I. Gestion des utilisateurs

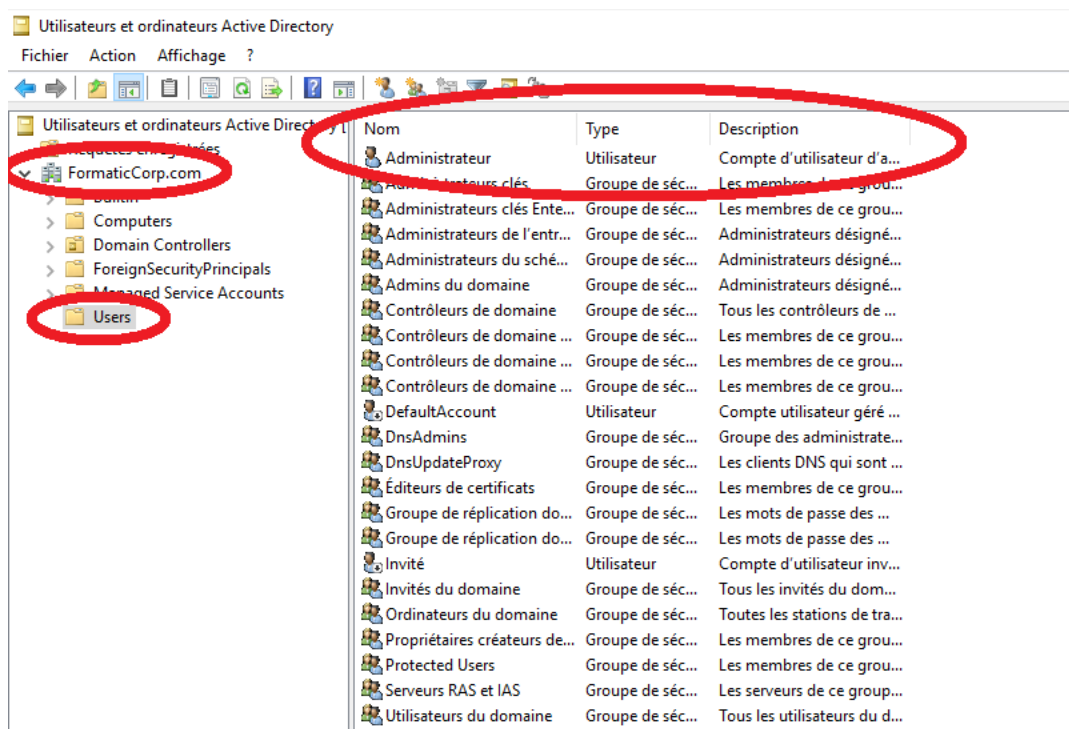
Nous avons vu précédemment que notre annuaire contiendra plusieurs objets qui appartiendront aux classes (puisque'ils ont des attributs propres associés) suivantes :

- **Ordinateur** : Les ordinateurs clients qui ont été intégrés au domaine, mais aussi les serveurs et les contrôleurs de domaine.
- **Contact** : Enregistrer des contacts, sans autorisation d'authentification. Les contacts Active Directory sont des collections de renseignements sur une personne ou une entreprise, tels que leurs numéros de téléphone, l'adresse e-mail, l'adresse postale etc. Ces informations portent sur les personnes à l'intérieur et à l'extérieur de l'entreprise avec lesquelles les utilisateurs souhaitent communiquer. Créer et gérer des contacts Active Directory est intéressant car les contacts ayant une adresse email peuvent être inscrits sur la **liste d'adresses globale** (GAL) ou d'autres listes d'adresses, aidant ainsi les utilisateurs à accéder aux informations de contact et à envoyer des messages.
- **Groupe** : Regrouper des objets au sein d'un groupe pour simplifier l'administration. Nous verrons ces groupes plus en détail mais on pourrait par exemple créer un groupe « Comptabilité » qui attribuerait des droits spécifiques aux utilisateurs comptables de votre entreprise et un groupe « Ordinateurs Comptabilité » qui regrouperait les machines clientes utilisables pour ce groupe de personnes.
- **Unité d'organisation** : Dossier pour créer une arborescence et organiser les objets au sein de votre annuaire AD.
- **Imprimante** : Ressource de type imprimantes.
- **Utilisateur** : Comptes utilisateurs qui permettent de s'authentifier sur le domaine, et accéder aux différentes ressources, aux ordinateurs et aux données de votre réseau.
- **Dossier partagé** : Pour définir des dossiers partagés entre vos utilisateurs.

Nous allons maintenant ouvrir la nouvelle console de gestion « Utilisateurs et ordinateurs Active Directory » dans les outils de notre gestionnaire de serveur :



Nous pouvons voir dans la fenêtre qui s'ouvre que notre domaine est maintenant créé et si vous « déployez » votre domaine vous pouvez voir que votre annuaire comporte déjà certains éléments notamment au niveau de vos utilisateurs « Users » :

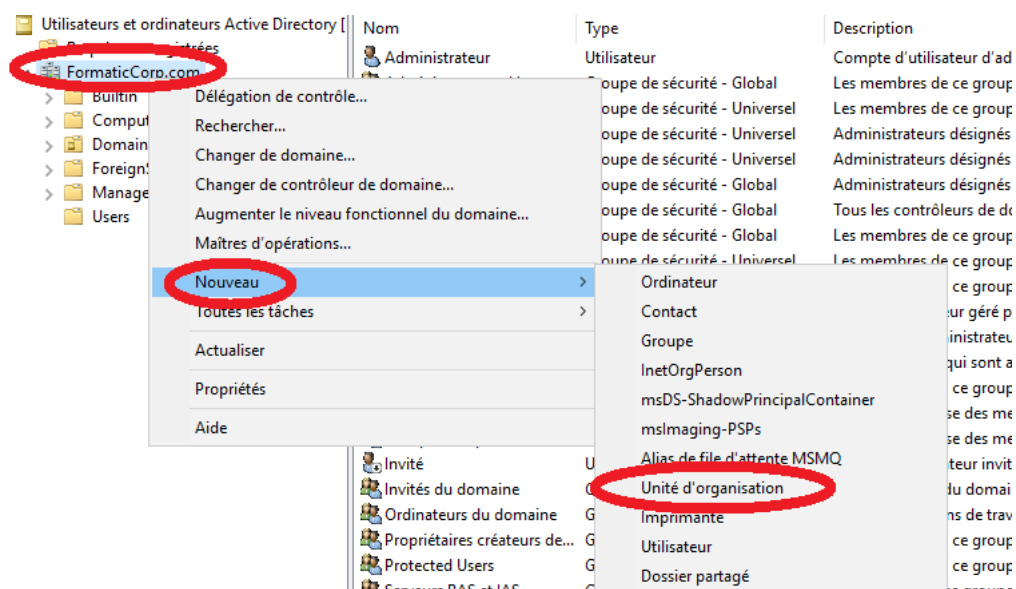


Nous pouvons remarquer qu'un certain nombre d'utilisateurs sont déjà présents : Administrateur, DefaultAccount et Invité. Nous reviendrons plus tard sur la notion de « Groupes de sécurité ».

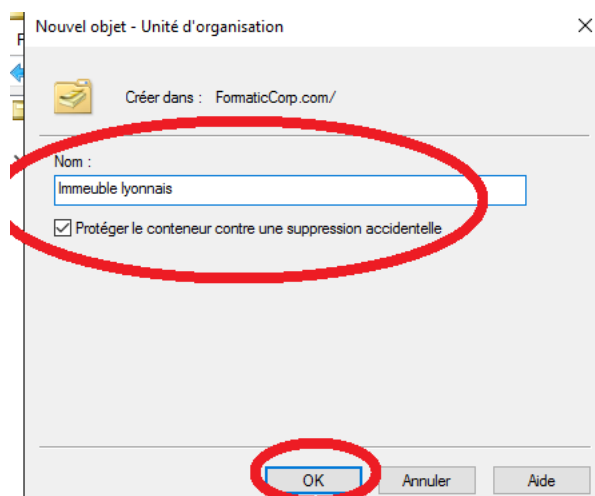
Nous allons maintenant créer les ressources que nous avons commencé à identifier.

(Cf document CasFictifADLight.pdf – I. Architecture de base)

Pour commencer nous allons créer nos unités d'organisation qui correspondront dans notre cas à notre localisation géographique, étages de bâtiments et métiers de notre entreprise fictive. On va ainsi faire un clic droit sur le nom de notre domaine « FormaticCorp.com » et sélectionner « Nouveau » puis « Unité d'organisation » :

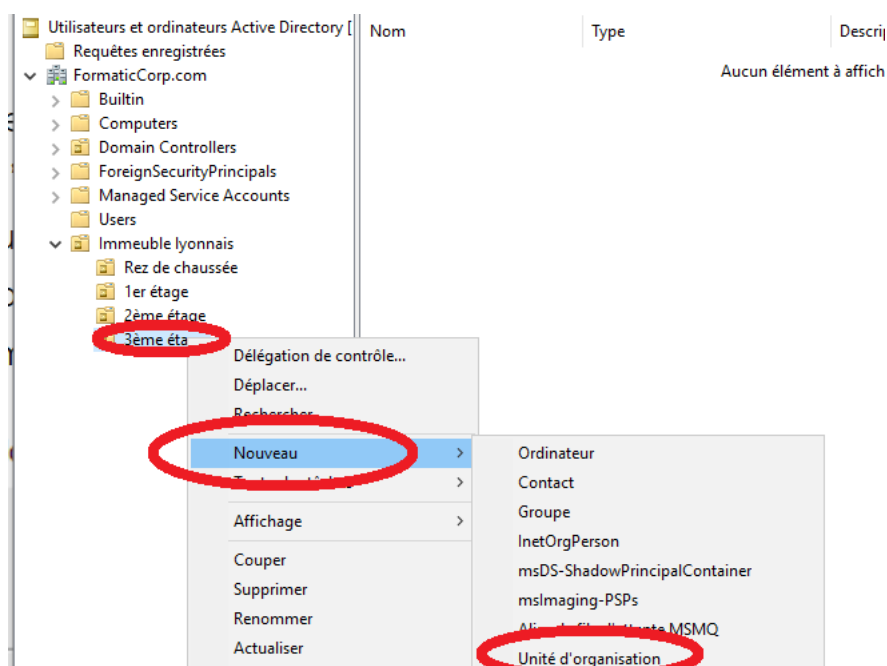


Dans la fenêtre qui s'ouvre nous allons rentrer le nom « Immeuble lyonnais » qui correspondra à notre unité d'organisation racine :

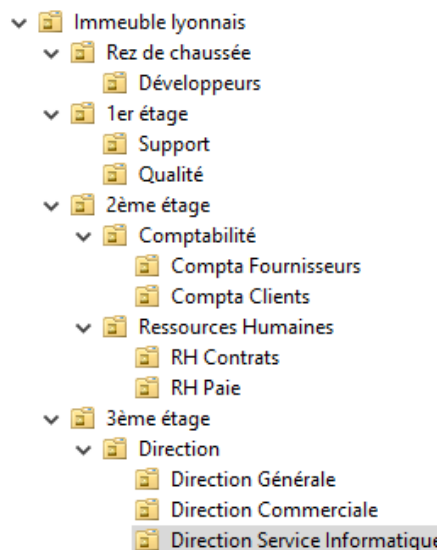


On pourra noter que la case « Protéger le conteneur contre une suppression accidentelle » est cochée par défaut. Elle permettra d'éviter les erreurs de manipulation en effaçant l'ensemble de ses unités organisationnelles (incluant leurs utilisateurs, ressources et groupes) d'une touche... Nous verrons plus tard qu'un système de corbeille peut être mis en place pour votre annuaire AD mais autant éviter un maximum de s'en servir.

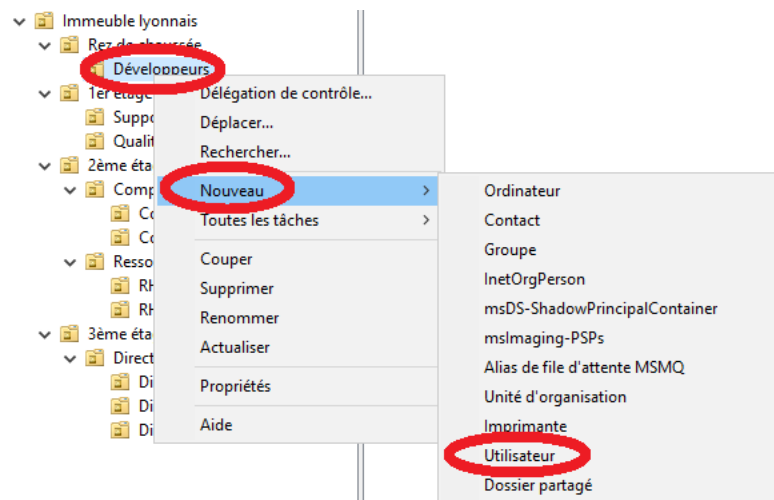
On va ensuite répéter cette opération en faisant cette fois-ci un clic droit sur « Immeuble lyonnais » pour créer nos différents étages. Une fois les 4 étages ajoutés vous devriez avoir l'écran ci-après et nous allons continuer en ajoutant les différents métiers correspondants à nos différents étages :



Une fois l'ensemble des unités organisationnelles (Cf document CasFictifADLight.pdf – I. Architecture de base) créées vous devriez obtenir la hiérarchie suivante :



Nous allons maintenant ajouter des utilisateurs dans nos différentes unités créées, en faisant un clic droit sur les métiers ajoutés et en créant cette fois-ci un nouvel « Utilisateur » :



Pour les utilisateurs on demandera un peu plus d'informations :

A screenshot of the 'Nouvel objet - Utilisateur' (New Object - User) dialog box. The title bar says 'Nouvel objet - Utilisateur' with a close button. Below the title bar, it says 'Créer dans : p.com/Immeuble lyonnais/Rez de chaussée/Développeurs'. The form contains several fields: 'Prénom :' with the value 'Alice', 'Initiales :' with the value 'AM', 'Nom :' with the value 'Martin', and 'Nom complet :' with the value 'Alice AM. Martin'. Below these is a section for 'Nom d'ouverture de session de l'utilisateur :', with a text box containing 'a.martin' and a dropdown menu showing '@FomaticCorp.com'. Below that is another section for 'Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :', with two text boxes containing 'FORMATICCORP\' and 'a.martin'. At the bottom, there are three buttons: '< Précédent', 'Suivant >' (highlighted with a blue border), and 'Annuler'.

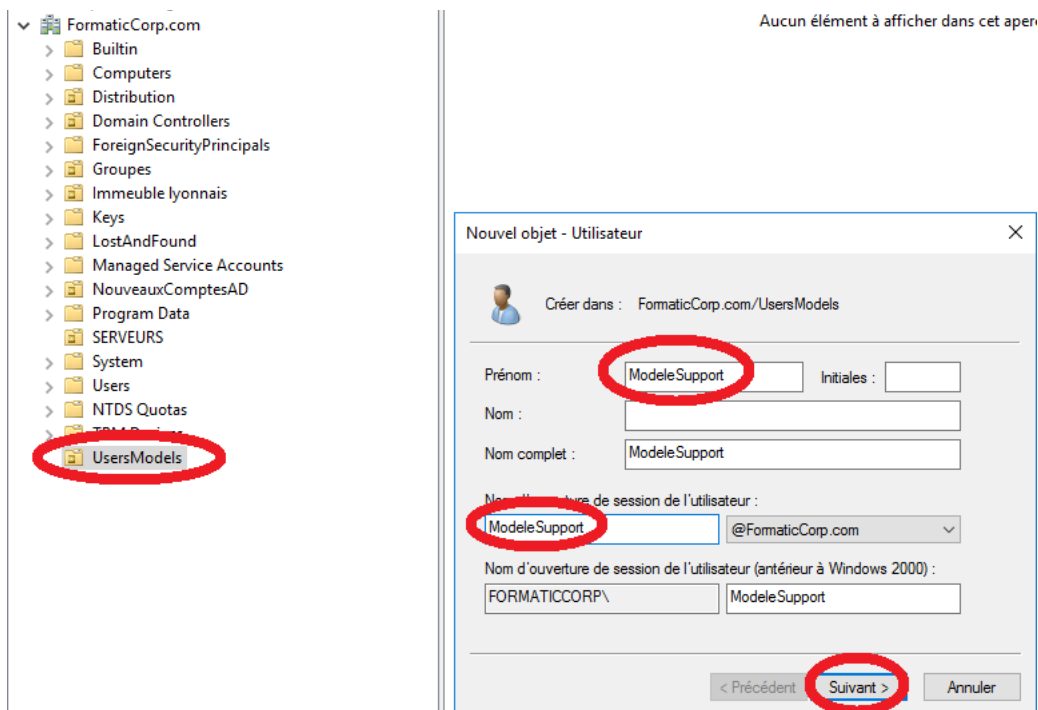
Les seules informations obligatoires sur cette fenêtre sont le « Prénom » de votre utilisateur (« Nom complet » se remplit automatiquement) et le « Nom d'ouverture de session de l'utilisateur » (le « Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) » se remplissant automatiquement quand on renseigne le premier).

Plus on fourni d'information à ce niveau et plus notre annuaire contiendra d'informations et donc pourra vous être utile par la suite. Dans notre cas on pourra se contenter d'indiquer le « Prénom » de la personne indiqué dans le document annexe CasFictifADLight.pdf – II. Utilisateurs Active Directory et de le copier dans le « Nom d'ouverture de session de l'utilisateur ».

Dans les entreprises, le nom d'ouverture de session sera très souvent la première lettre du prénom suivi de son nom, séparé par le caractère « . ». Vous aurez quelques problèmes comme vous pouvez déjà l'imaginer, si vous avez des noms et des premières lettres de prénoms similaires (surtout si vos comptes d'utilisateurs AD sont créés automatiquement par votre système d'information).

Sur l'écran suivant la case « L'utilisateur doit changer le mot de passe à la prochaine ouverture de session » est cochée par défaut mais d'autres options sont possibles.

On pourra aussi créer des modèles utilisateurs pour faciliter l'insertion de nouveaux objets de type « Users » au sein de notre annuaire Active Directory. Pour cela nous allons tout d'abord créer une nouvelle unité d'organisation nommée « UsersModels ». Dans cette UO on va ensuite créer un utilisateur « ModeleSupport » :



On va ensuite rentrer différentes informations, notamment dans l'onglet «Organisation » :

Propriétés de : ModeleSupport

Membre de	Réplication de mot de passe	Appel entrant	Objet	Sécurité
Environnement	Sessions	Contrôle à distance		
Profil des services	Bureau à distance	COM+	Éditeur d'attributs	
Général	Adresse	Compte	Profil	Téléphones
Organisation				
Certificats publiés				

Fonction :

Service :

Société :

Gestionnaire

Nom :

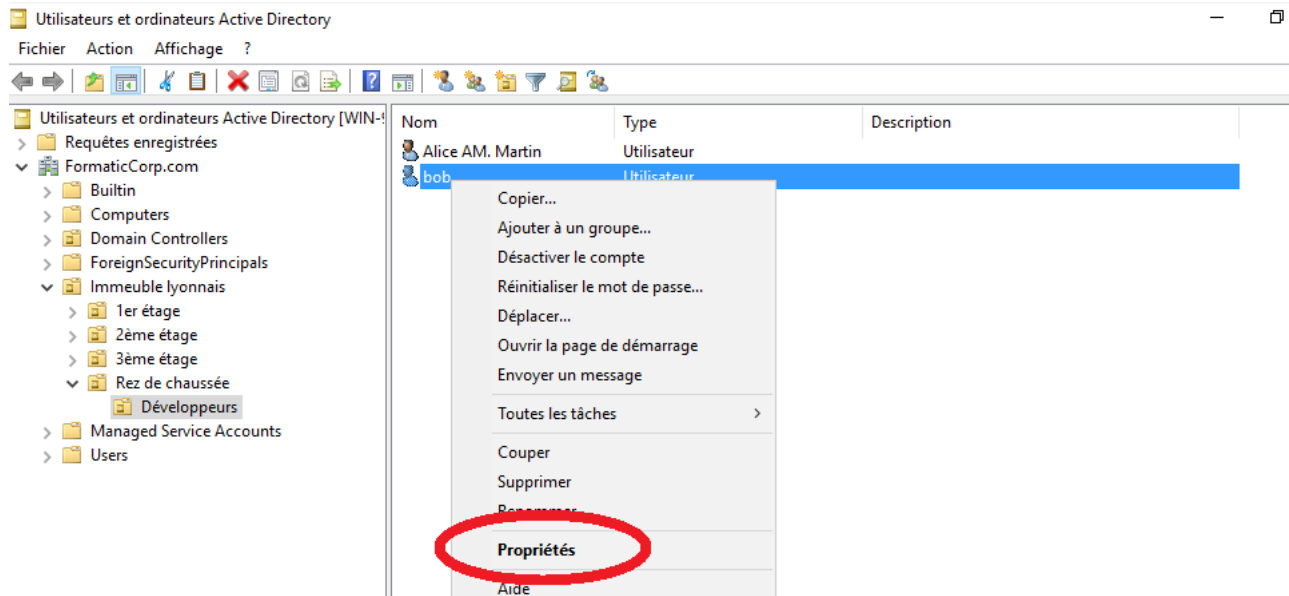
Collaborateurs :

On pourra ensuite faire un clic droit sur ce modèle, puis sélectionner « copier ». On indique alors le nom et le compte d'ouverture de session de notre utilisateur final ainsi que son mot de passe comme d'habitude. Vérifiez que les informations de l'onglet « Organisation » ont bien été récupérées depuis votre modèle. On pourra noter que la « Fonction » n'a pas été récupérée car cet attribut est considéré unique pour un objet AD de type « User ».

L'utilisation des modèles d'utilisateurs pourra donc grandement vous faciliter la gestion et maintenance de vos utilisateurs AD. En deux clics, le nouvel employé du service support aura la plupart de ses informations propres pré-remplies. On verra plus tard qu'on pourra paramétrer aussi son profil itinérant, mais aussi mettre en place les partages de dossiers et droits associés sur ces derniers. Cela permettra donc en plus de vous faire gagner du temps d'uniformiser vos utilisateurs suivants les UO que vous avez définis.

Créez donc maintenant l'ensemble des utilisateurs de notre entreprise fictive (Cf document CasFictifADLight.pdf – II. Utilisateurs Active Directory).

Si on fait un clic droit puis « Propriétés » sur chacun de nos utilisateurs on peut voir qu'on peut entrer une multitude d'informations supplémentaires :



On a aussi d'autres fonctionnalités comme « Ajouter à un groupe.... » (de sécurité existant, que nous verrons plus tard), « Désactiver le compte », « Réinitialiser le mot de passe », etc...

Comme bien souvent, ces opérations peuvent se faire manuellement comme nous venons de le voir, mais dans le cadre d'une grande entreprise avec de très nombreux objets Active Directory à gérer on automatisera leurs créations.

Ainsi, on peut imaginer que notre système d'information génère automatiquement les utilisateurs lorsqu'un contrat est créé au niveau du service RH de votre entreprise. Les informations générales seraient alors remplies (Nom, Prénom et l'adresse d'ouverture de session utilisateur associée de type « première lettre du prénom ». « nom ») mais aussi d'autres éléments, par exemple l'onglet « Adresse » avec les coordonnées du nouveau collaborateur de l'entreprise, son adresse mail, etc...

Une fois les utilisateurs créés dans le dossier de base « Users » nous n'aurions alors plus qu'à les déplacer dans notre cas vers le bon étage et métier au niveau de notre structure AD.

Chaque objet de notre annuaire disposera d'identifiants uniques avec les 2 attributs **Distinguished-Name** et le **GUID**.

Le **DistinguishedName** (DN) représente le chemin LDAP qui permet de trouver l'objet dans l'annuaire Active Directory. Nous aurons par exemple : CN=bob,OU=Développeurs,OU=rez de chaussée,OU=Immeuble lyonnais,DC=FormaticCorp,DC=com

CN (CommonName) étant le nom de votre objet.

OU : la ou les unités d'organisation

DC : pour indiquer le domaine cible

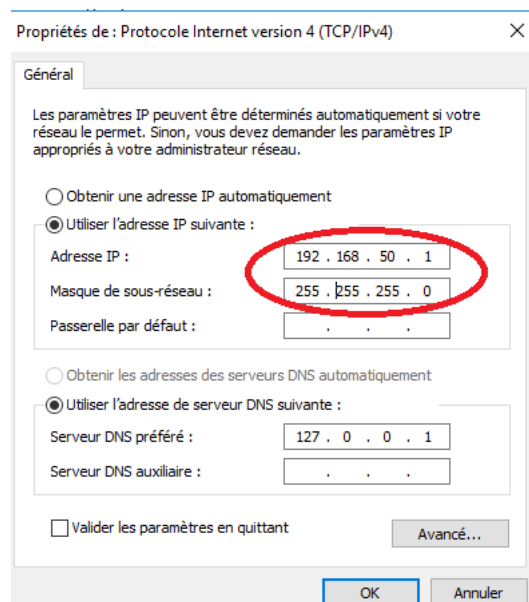
II. Gestion des ordinateurs

Nous avons précédemment identifié les utilisateurs qui allaient « peupler » nos différentes unités d'organisation, nous allons désormais nous intéresser aux matériels informatiques auxquels ces personnes ont accès.

(Cf document CasFictifADLight.pdf – III. Équipements informatiques)

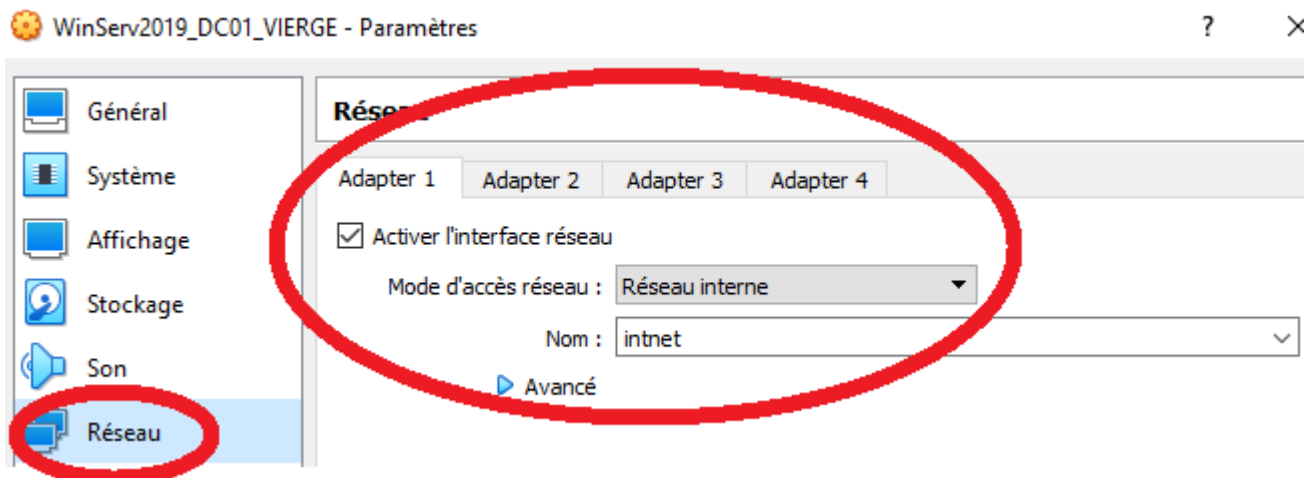
Si ce n'est pas déjà fait, nous allons procéder à l'installation d'une (idéalement 2) versions clientes de Windows. Installez au minimum une machine virtuelle sous Windows 10 64 bits (et idéalement une autre avec Windows 11 voir les différences entre ces 2 systèmes d'exploitation par la suite).

Nous allons désormais attribuer une adresse IP fixe à notre serveur si cela n'a pas déjà été fait (nous avons vu précédemment qu'il faudra toujours définir des adresses Ips fixes pour vos serveurs), par exemple 192.168.50.1 (cf Plan Adressage) :



Veuillez ensuite effectuer les opérations suivantes :

1) Paramétrez vos cartes réseaux dans votre hyperviseur, de manière à avoir la première carte en « réseau interne » (sur VirtualBox, LAN segment sur VMWare) :



Paramétrer éventuellement votre 2ème carte réseau en accès NAT ou accès par pont (bridge sur VM-Ware) pour avoir accès à internet.

Ceci n'est pas obligatoire, nous n'avons pas besoin d'internet pour intégrer un poste client à notre domaine, il suffit que les 2 machines soient sur le même réseau et qu'elles communiquent !

2) Paramétrez les adresses Ips de votre client (+ indiquer l'adresse DNS de votre Windows Serveur où nous avons installé Active Directory : AD01 ou DC01)

3) Vérifier que vos 2 machines communiquent (ping, tester dans les 2 sens, il se peut que cela ne marche pas d'1 côté, du à vos règles de parefeu).

Une fois ceci fait vous allez pouvoir intégrer votre machine cliente à votre domaine « FormaticCorp.-com ». Vous pouvez passer par le panneau de configuration puis « Système », ou faire un clic droit sur votre poste de travail, puis sélectionnez « Propriétés », utiliser le raccourci clavier « Windows + Pause » ou encore utiliser la commande « sysdm.cpl ». Lorsque vous allez valider le domaine dans lequel vous souhaitez intégrer votre machine cliente, celle-ci va chercher à joindre le serveur DNS responsable de ce domaine.

C'est à ce moment qu'intervient le rôle DNS : une requête DNS va être émise pour identifier un enregistrement DNS particulier permettant de trouver un contrôleur de domaine disponible pour le domaine. Comme nous avons installé le rôle DNS en même temps qu'Active Directory, nous aurons bien une zone de recherche directe qui permettra de **résoudre** « FormaticCorp.com » (le DNS renverra l'adresse IP de notre serveur, 192.168.1.12 dans mon cas et l'intégration de la machine dans le domaine sera possible).

Lorsque vous modifiez les paramètres réseaux de votre carte et notamment le DNS, il peut être nécessaire d'utiliser des commandes pour réinitialiser, nettoyer vos anciens paramètres.

Si vous avez du mal à vous connecter à votre réseau local ou à Internet, que votre connexion est lente, ne fonctionne plus du tout, ou encore que vous rencontrez des problèmes pour intégrer votre machine cliente au sein de votre domaine, vous pourrez tester les commandes suivantes.

Le catalogue Winsock gère les envois et réceptions de paquets, avec la commande suivante vous pourrez l'effacer, le cache DNS sera purgé et vous récupérerez une nouvelle adresse IP de votre routeur (vous allez réinitialiser le catalogue Winsock aux paramètres par défaut, dans un état propre) :

netsh winsock reset

Les commandes suivantes pourront résoudre les problèmes d'adresses IP :

netsh int IP reset (all)

ipconfig /release

ipconfig /renew

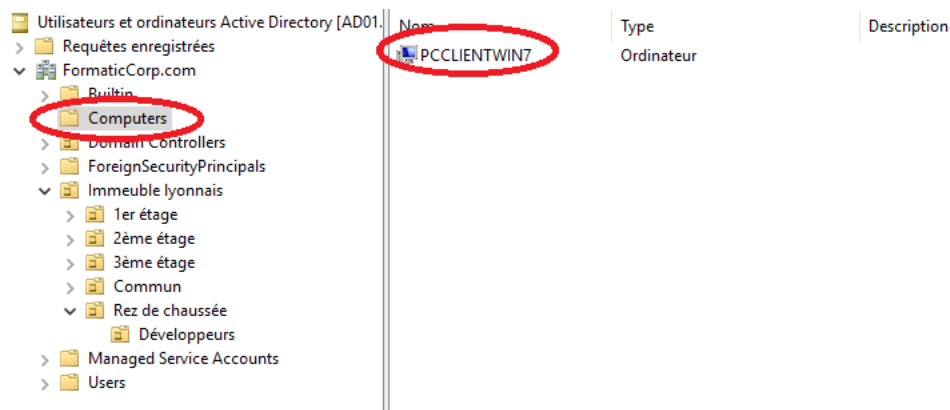
ipconfig /flushdns

Après le redémarrage, vous devrez utiliser la connexion à votre domaine avec le nom NETBIOS : FormaticCorp\Administrateur. En fait vous pourrez toujours vous connecter avec votre premier utilisateur, administrateur du poste local. Cependant, se sera un compte **local**. En mettant « FormaticCorp\Administrateur » vous vous connectez sur la machine avec l'**utilisateur Administrateur du domaine FormaticCorp**.

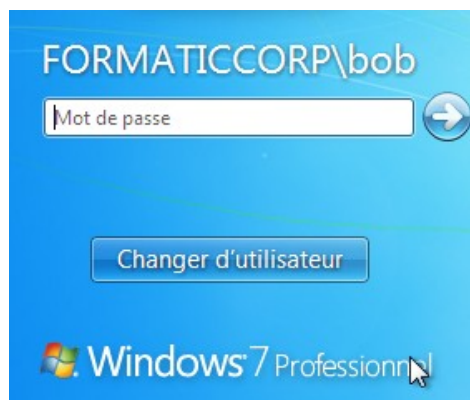
Un nouveau profil utilisateur est créé et l'ancien, bien que toujours disponible n'est plus utilisé. Le **RID Master** (rôle que nous verrons plus tard) génère des identifiants uniques sur le réseau et est utilisé pour générer un identifiant de sécurité (SID). Grâce à ce nouveau profil, l'utilisateur et les droits sur les fichiers seront associés aux SID du poste nouvellement intégré dans votre domaine ainsi que le SID de l'utilisateur avec lequel vous vous êtes authentifié.

À chaque nouvel utilisateur, un nouveau profil sera créé et les droits positionnés avec le SID de l'utilisateur. Ainsi deux profils utilisateurs sur un même poste ne pourront être accédés sans autorisations particulières.

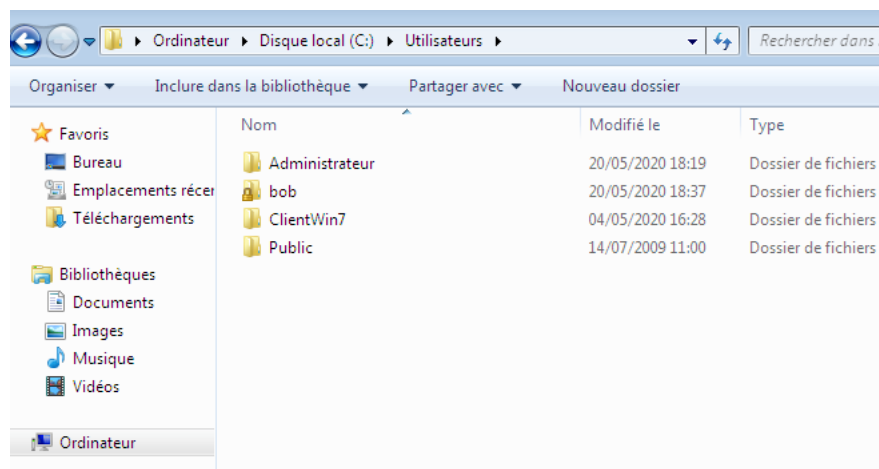
Une fois ceci fait, si vous sélectionner « Computers » (Ordinateurs si votre Windows est en français), au niveau de votre serveur DC01 vous allez bien voir apparaître l'ordinateur que vous venez d'ajouter au domaine :



On pourra ensuite faire un test de connexion avec un des utilisateurs que nous avons créé, par exemple : `FORMATICCORP\bob` (le fait de mettre le nom netbios en minuscule ou majuscule n'a aucune incidence comme vous pouvez le voir) :



Une fois connecté avec l'utilisateur bob, on peut ouvrir le dossier « Utilisateurs » dans C : pour voir les différents comptes qui se sont connectés sur cette machine et qui auront chacun leur dossier personnel :

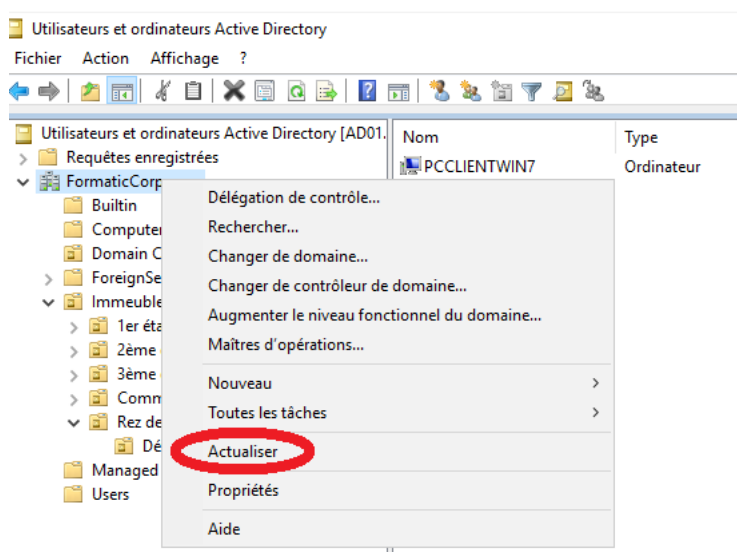


Le dossier « Public » est créé lors de l'installation de Windows. « ClientWin7 » est le compte administrateur **local**. Le dossier « Administrateur » est le compte administrateur du domaine. Pour finir, le dossier « bob » est le compte d'un utilisateur du domaine que nous venons d'utiliser pour nous connecter sur notre machine.

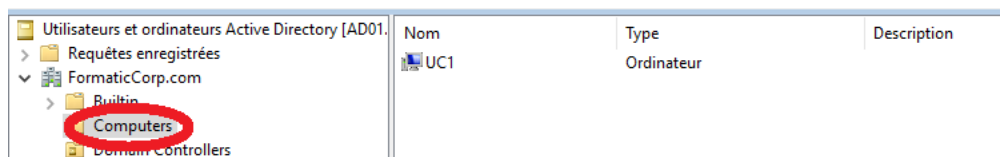
On pourra de nouveau essayer de changer le nom de l'ordinateur. A ce moment on vous demandera un nom d'utilisateur. Seuls les administrateurs du domaine peuvent changer bien entendu le nom de l'ordinateur et l'intégrer dans un domaine. Nous allons changer le nom en « UC1 » pour respecter la structure que nous avons défini.

(Cf document CasFictifAD.pdf – III. Équipements informatiques)

Après redémarrage de l'ordinateur client, on devra actualiser notre annuaire Active Directory pour voir les changements :

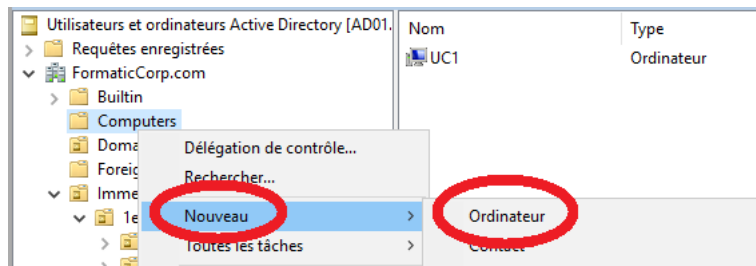


On peut aussi faire un clic droit puis « Actualiser » directement sur « Computers » pour ne pas recharger tout l'annuaire. Vous devriez désormais bien voir votre « UC1 » dans la liste de vos ordinateurs :

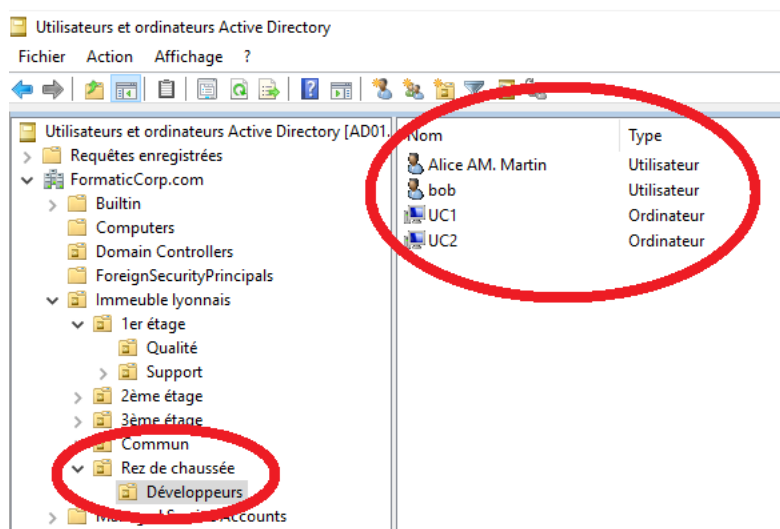


Vous pourrez ainsi ajouter l'ensemble de vos machines clientes à votre domaine.

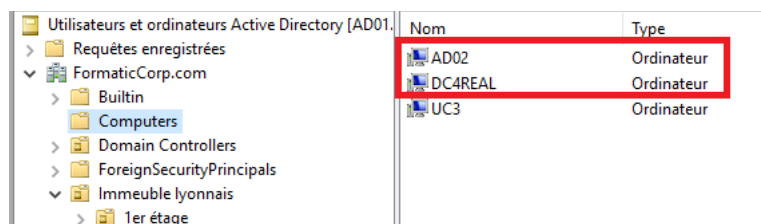
Nous pouvons ensuite ajouter manuellement les autres ordinateurs correspondant à notre entreprise fictive :



On peut ensuite « faire glisser » les ordinateurs créés dans les unités d'organisation correspondantes (ou directement créer les ordinateurs dans les bonnes unités car nous faisons cette opération manuellement) :



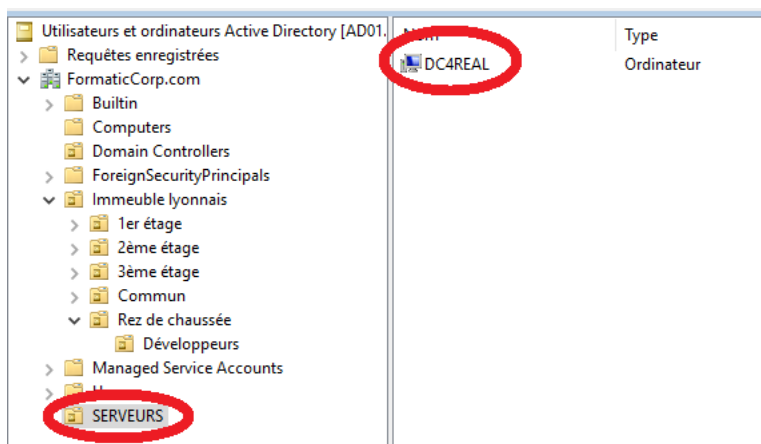
On pourra maintenant intégrer nos serveurs de la même façon dans notre domaine. AD répertoriera indifféremment vos ordinateurs et vos serveurs :



Les 2 premiers noms encadrés sont bien des serveurs.

Il différenciera uniquement les serveurs de type contrôleurs de domaine qu'il placera dans l'UO « Domain Controllers ».

Se sera à vous de créer une nouvelle unité d'organisation pour trier vos serveurs de vos ordinateurs :



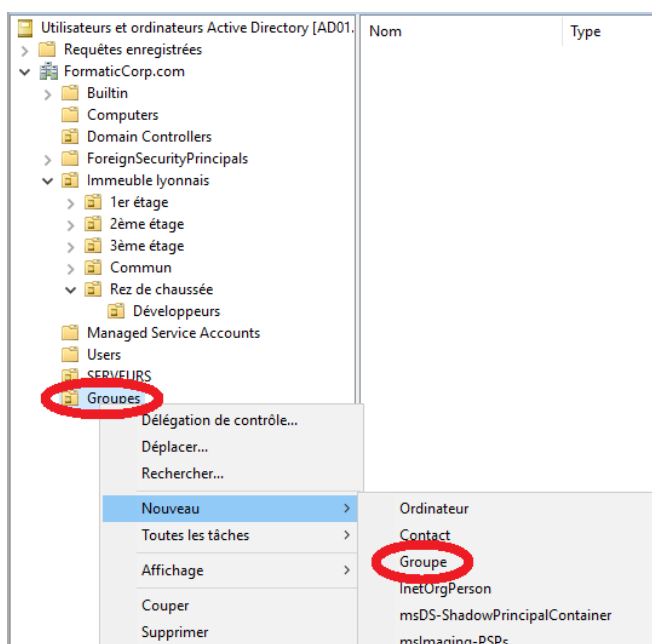
Tout comme vos objets « Users », vos objets « Computers » aurons des informations (dont certaines spécifiques comme la version du système d'exploitation), accessibles avec un clic droit sur votre machine en sélectionnant « Propriétés ».

III. Gestion des groupes

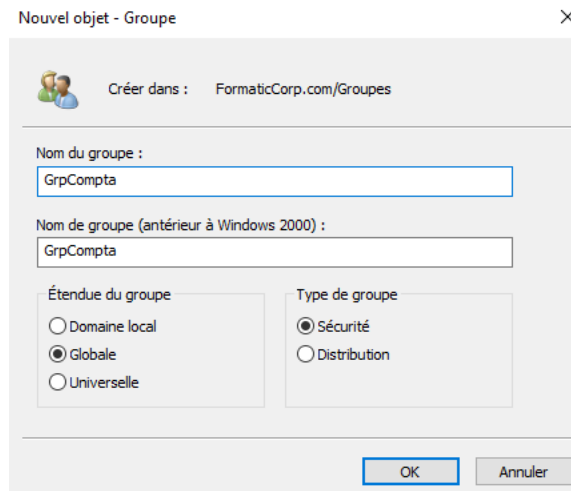
Un **groupe** va nous permettre de regrouper plusieurs objets au sein d'un même objet. Prenons l'exemple d'un dossier partagé, accessible via le réseau aux utilisateurs du domaine. Ce dossier nommé « Partage » ou « Comptabilité » devra être accessible à toutes les personnes du service comptabilité de mon entreprise. Plutôt que de donner les droits à chaque utilisateur du service comptabilité, nous allons créer un groupe. Ce groupe nommé « GrpCompta » contiendra l'ensemble des utilisateurs correspondant aux collaborateurs du service comptabilité.

Ensuite, au niveau de votre dossier partagé, plutôt que d'ajouter vos utilisateurs un par un dans la gestion de vos droits **NTFS**, il vous suffira de paramétrer les droits sur le dossier pour le « GrpCompta ». Cela permettra plus de clarté (moins de listes à rallonge quand vous consultez les droits d'un dossier) et facilitera la maintenance de vos serveurs (tout particulièrement de vos serveurs de fichiers).

Si on retourne sur notre contrôleur de domaine, dans la fenêtre « Utilisateurs et ordinateurs Active Directory », nous allons créer une nouvelle unité d'organisation « Groupes » puis y ajouter un nouveau groupe :



Dans la fenêtre qui s'ouvre, vous devrez indiquer le nom de votre groupe et définir son étendue ainsi que son type :



L'**étendue** d'un groupe correspond à sa portée au niveau de l'arborescence Active Directory, ainsi le groupe que l'on va créer pourra exister sur notre domaine local ou sur la forêt entière.

Il existe donc trois étendues différentes :

- **Domaine local** : peut être utilisé uniquement dans le domaine dans lequel il est créé. Ainsi on ne pourra contrôler l'accès aux ressources uniquement au niveau du domaine local pour les membres de ce groupe.
- **Globale** : peut être utilisé dans le domaine local, mais aussi dans tous les domaines approuvés (notion que nous verrons par la suite) par le domaine de base. C'est cette option qui est sélectionnée par défaut.
- **Universelle** : Ce groupe aura la portée maximale au niveau de notre annuaire AD puisqu'il est accessible dans l'ensemble de la forêt, ce qui implique qu'il soit disponible sur tous les domaines de la forêt. Un groupe universel peut contenir des groupes et objets provenant de n'importe quel domaine de la forêt. De la même manière, il est possible de l'utiliser pour définir l'accès aux ressources sur tous les domaines de la forêt. Ce type d'étendue est défini au sein d'un **catalogue global**.

Les étendues sont dépendantes du niveau fonctionnel de la forêt et du domaine, ainsi que de la complexité de l'architecture en place, notamment au niveau des relations d'approbations entre les différents domaines et arbres. Si vous créez un groupe à étendue universelle, mais qu'il n'y a pas de relation avec un autre domaine ou une autre forêt, cela n'aura pas d'intérêt.

Nous reviendrons plus en détail plus tard sur ces notions complexes de notre annuaire.

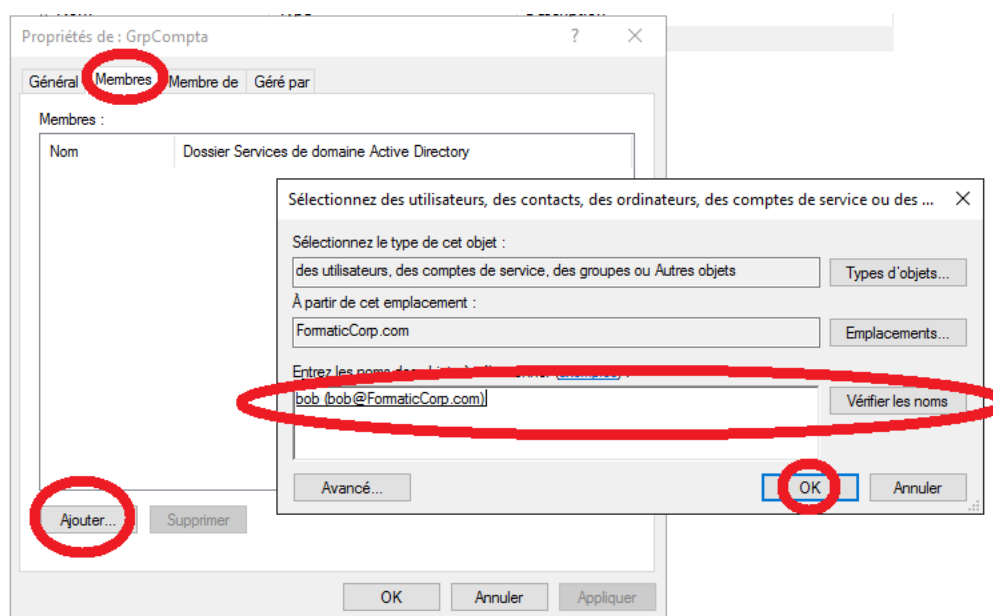
Le **type** est divisé en 2 catégories :

- **Sécurité** : Ce sont les plus utilisés et ceux que vous manipulerez le plus souvent (il est d'ailleurs sélectionné par défaut). Ils permettent d'utiliser les groupes pour gérer les autorisations d'accès aux ressources. Chaque groupe de ce type disposera d'un identifiant de sécurité SID.

- **Distribution** : Ces groupes sont utilisés principalement par des applications de messagerie, comme Microsoft Exchange. Ils permettent de créer des listes de diffusion : on crée une liste de distribution d'adresses mails.

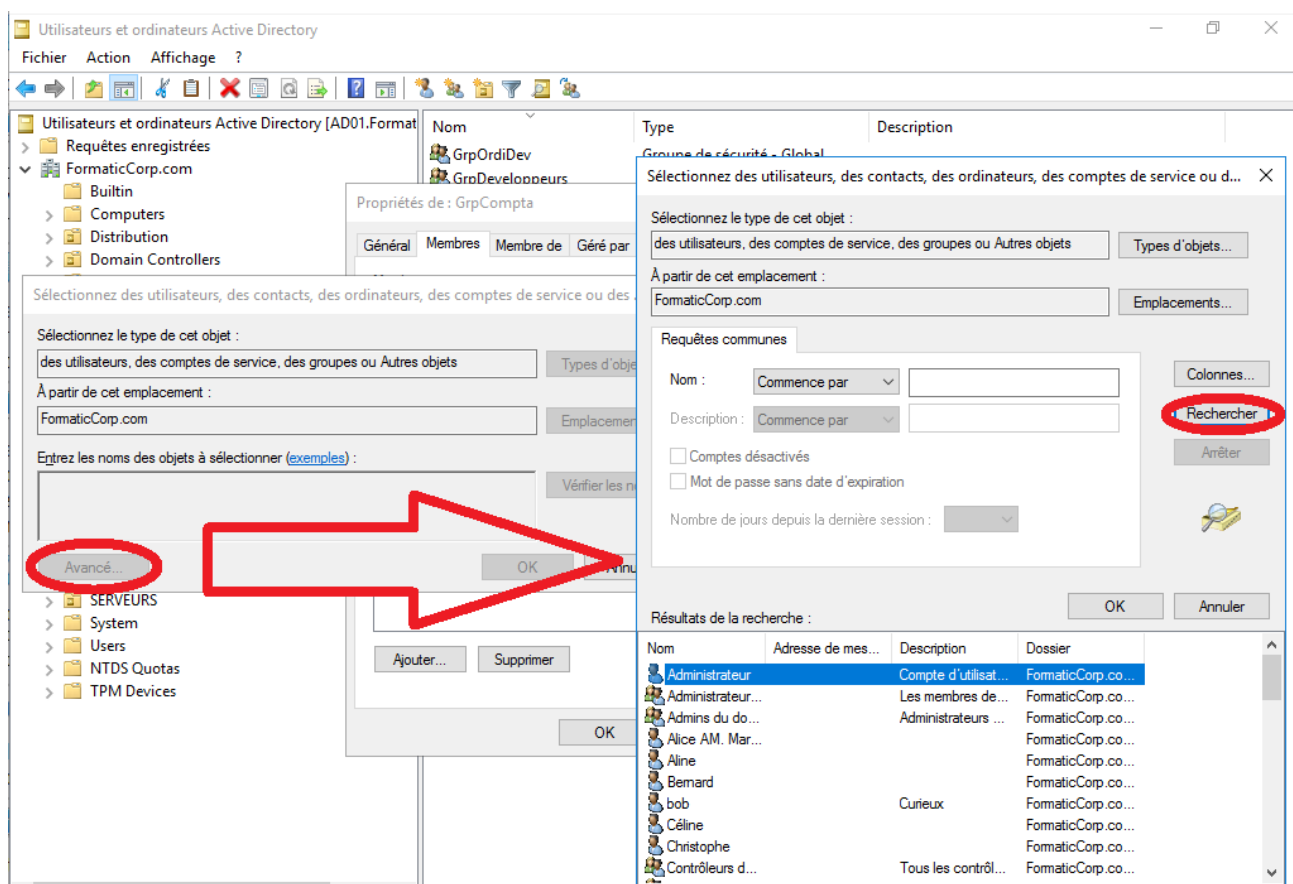
On pourra ainsi créer un groupe de sécurité dans notre UO « Groupes » nommé « GrpSupport » et créer une nouvelle UO « Distribution » pour y insérer un groupe de type distribution nommé « DiffusionSupport ». Avec ces 2 groupes on pourra gérer leurs accès aux dossiers partagés et leur envoyer des mails à tous.

Pour ajouter des membres à ces 2 nouveaux groupes on fait un clic droit dessus puis « Propriétés ». Dans l'onglet « Membre » on va ajouter tous les membres du support, ici on pourra faire le test avec notre utilisateur bob :



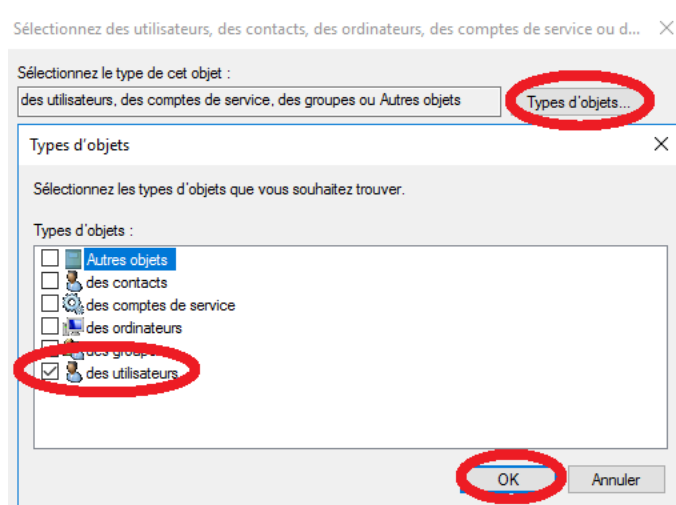
Lors de l'ajout de membres dans un groupe, plusieurs possibilités s'offrent à vous. Soit vous connaissez le nom de votre utilisateur (ou au moins les premières lettres du compte utilisateur) et vous utilisez le bouton « Vérifier les noms » comme l'impression d'écran ci-dessus.

Soit vous utilisez le bouton « Avancé » :

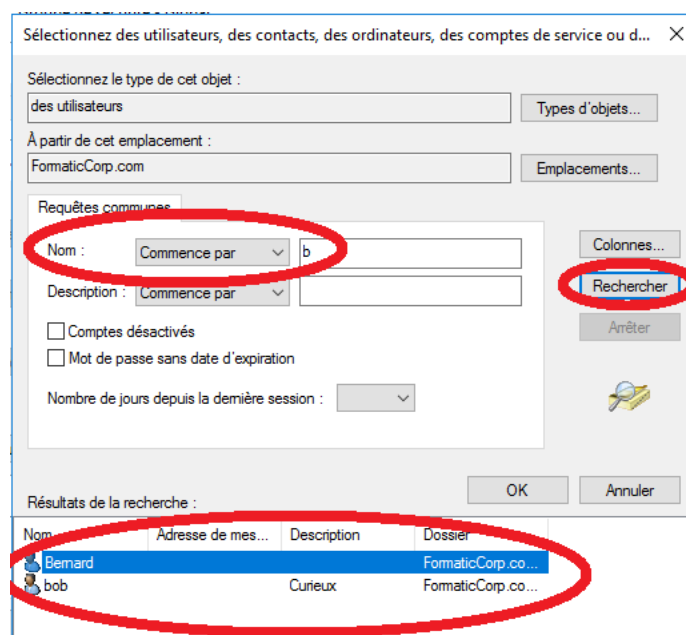


Si on clique directement sur le bouton « Rechercher » dans la nouvelle fenêtre, l'ensemble de vos utilisateurs et groupes vont s'afficher (incluant les groupes « spéciaux » créés automatiquement lors de la mise en place d'AD).

On pourra bien entendu affiner nos recherches, par exemple en sélectionnant le type d'objets AD que l'on recherche :

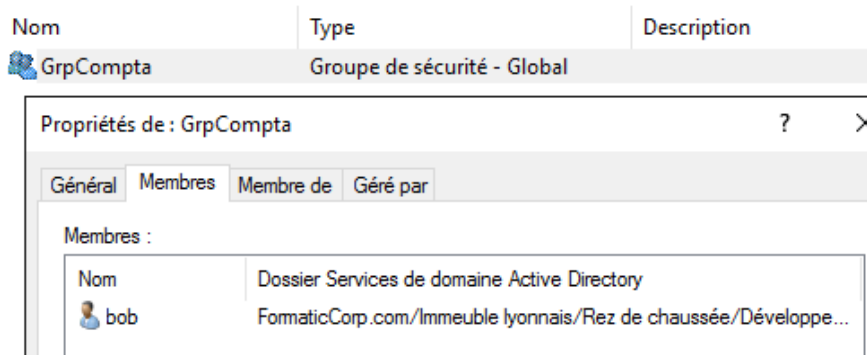


Puis en demandant la liste des objets (ici uniquement des objets de type utilisateurs par rapport au paramétrage effectué ci-dessus) commençant par la lettre « b » :

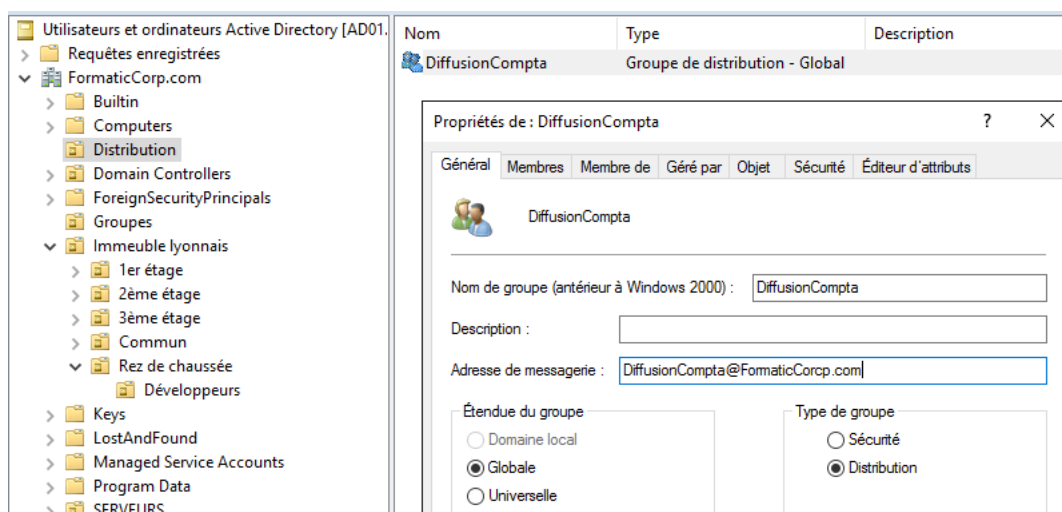


Pour finir avec cet écran de recherche d'objets AD, on pourra cliquer sur le bouton « Emplacements » pour ne rechercher des objets qu'au sein d'une unité d'organisation en particulier (par défaut on recherche dans notre domaine complet « FormaticCorp.com »). On pourra aussi personnaliser les résultats de la recherche en ajoutant des colonnes (par exemple le « Supérieur direct » si cette information a bien été rempli pour votre objet utilisateur, ce qui pourra vous permettre de constituer plus facilement vos groupes).

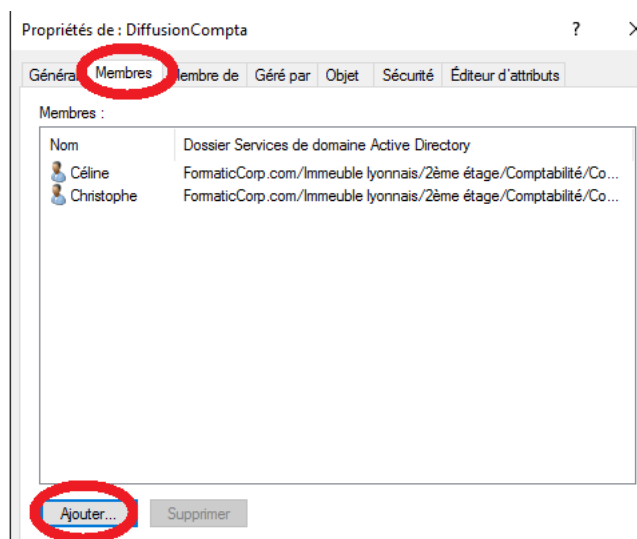
Une fois ajouté vous devriez avoir ceci dans la liste des membres de votre groupe :



Pour notre groupe de distribution « DiffusionSupport », nous allons indiquer l'adresse de messagerie suivante : « DiffusionSupport@FormaticCorp.com » :

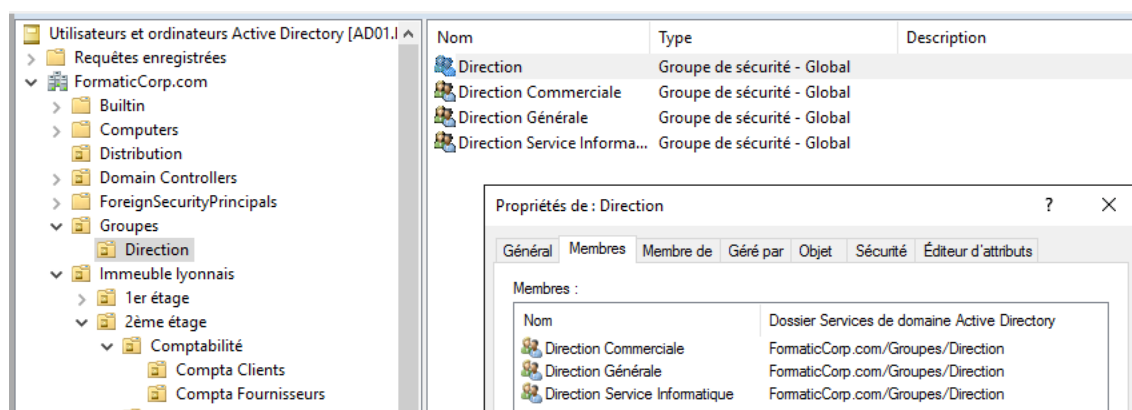


Puis nous allons y ajouter nos 2 utilisateurs du support : Aline et Bernard :



Désormais, si vous écrivez un mail à l'adresse de messagerie suivante : DiffusionSupport@Formatic-Corp.com, les utilisateurs Aline et Bernard recevront tous 2 le mail dans leur boîte de réception.

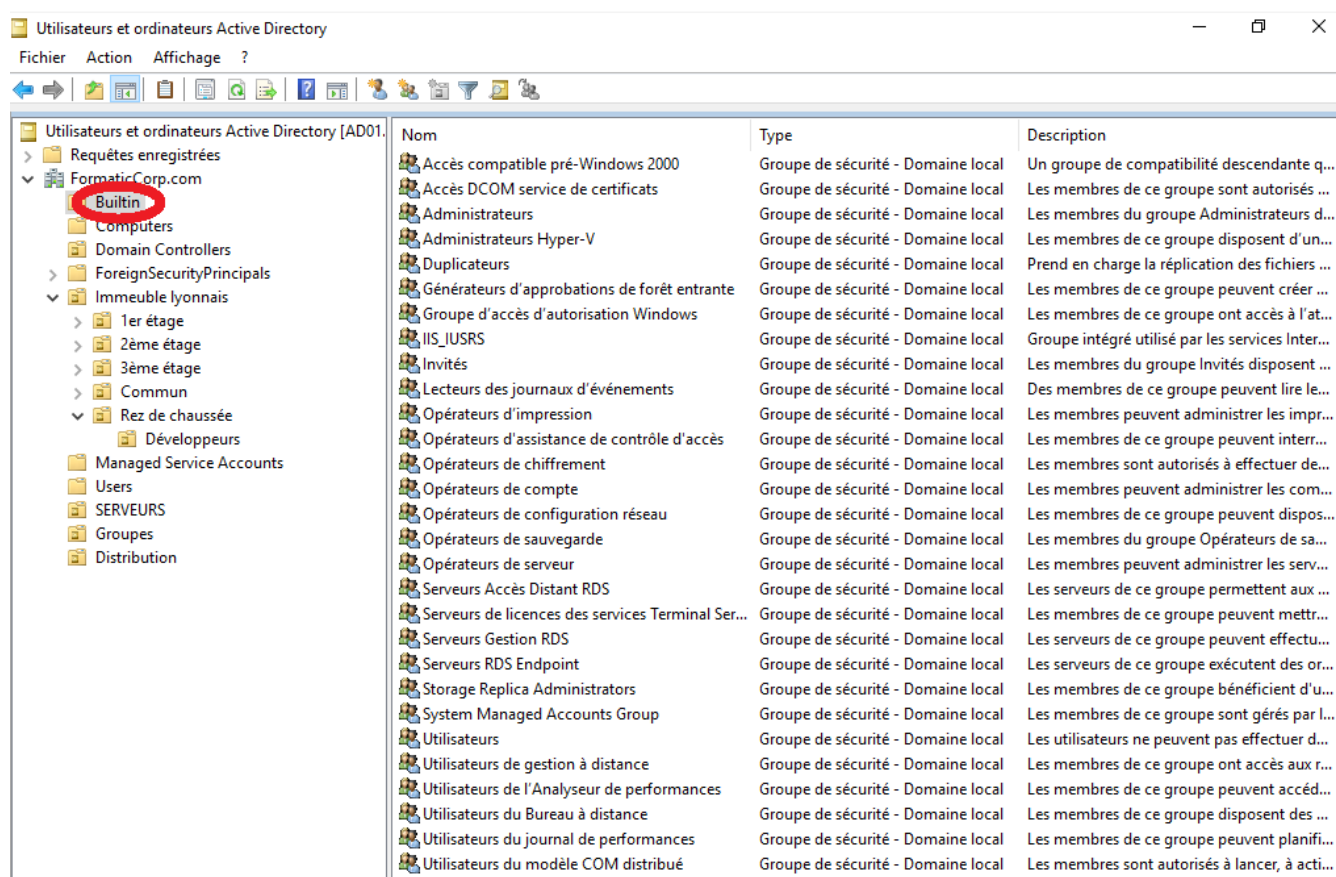
On pourra créer 3 groupes de sécurité « Direction Générale », « Direction Commerciale » et « Direction Service Informatique » et y insérer les utilisateurs correspondants à ces services. On créera un dernier groupe de sécurité (ou de diffusion) « Direction » dont les membres seront les 3 précédents groupes. Ainsi, on pourra appliquer des droits (ou envoyer des mails) à notre groupe « Direction Générale », ou à l'ensemble des groupes de directions si on utilise le groupe « Direction ». On pourra regrouper tous ces groupes dans une nouvelle UO Direction :



Nous reviendrons plus en détail sur ces notions de groupes quand nous verrons les stratégies de groupes, avec des exemples concrets d'utilisation.

Lors de l'installation d'Active Directory, de nombreux groupes par défaut ont été créés.

Si on sélectionne « Built-in » on aura une liste de groupes ayant été déjà défini :



On peut ainsi voir qu'on a un groupe Administrateurs, Invités ou encore Utilisateurs. On peut voir aussi que certains groupes concernent des fonctionnalités (IIS, utilisateurs du bureau à distance, RDS, Hyper-V, Opérateurs de sauvegarde, etc.). Leur étendue est locale et ne s'appliquera donc qu'au domaine géré par ce contrôleur de domaine.

Ces groupes donnent accès à certaines fonctionnalités, il suffit d'ajouter des membres à ces groupes existants.

On pourra aussi aller consulter les groupes prédéfinis dans « Users ».