

Organiser l'annuaire

Introduction

Les objectifs de ce cours sont :

- Identifier une Unité d'Organisation
- Identifier les rôles que joue un serveur Active Directory
- Créer un modèle d'utilisateurs
- Créer et supprimer une Unité d'Organisation
- Identifier les groupes intégrés, prédéfinis et spéciaux

Dans un cours précédent nous avons vu comment installer le rôle Active Directory sur le serveur.

Nous allons maintenant voir comment structurer notre annuaire de façon à ce qu'il représente l'organisation de l'entreprise.

Pour rappel, l'organisation de l'entreprise est la suivante :



Structure de l'annuaire

C'est l'outil **Utilisateurs et ordinateurs Active directory** qui permet de structurer l'annuaire.

Un domaine Active Directory est simplement un groupe d'ordinateurs qui partagent la même base d'annuaire.

En effet, lorsqu'un ordinateur est intégré au domaine Active Directory, il lui est possible de consulter les ressources que lui propose l'annuaire.

Les noms de domaine Active Directory doivent être uniques.

Par exemple, vous ne pouvez avoir deux domaines nommés contorse.local, mais vous pouvez avoir un domaine parent contorse.local, ayant des domaines enfants comme nantes.contorse.local, stbrieuc.contorse.local .

Comme nous sommes dans un réseau privé et que notre serveur AD n'a pas pour objectif d'être accessible depuis Internet, le nom de domaine n'a pas d'importance, on aurait pu très bien mettre contorse.com ou contorse.org par exemple.

Cependant, si vous souhaitez que vous utilisateurs puissent bénéficier des services proposés par l'annuaire en dehors de l'entreprise alors il sera nécessaire d'acheter un nom de domaine.

Il est possible d'enregistrer un nom de domaine par le biais de n'importe quel bureau d'enregistrement de noms de domaine.

Le site de l'AFNIC liste les bureaux d'enregistrements.

Concernant la structure de l'annuaire, par défaut un certain nombre de répertoires sont présents et d'autres ne sont pas visibles actuellement.

Nous n'allons pas tous les détailler dans ce cours mais nous allons voir les éléments principaux.

Le contrôleur de domaine

Par exemple, ce dossier qui contient un annuaire se nomme une Unité d'organisation ou une OU (Organizational Unit) en Anglais.

Ces Unités d'Organisation sont très utiles à l'organisation des objets afin de refléter une structure fonctionnelle ou professionnelle de l'entreprise.

Pourtant ce n'est pas la seule raison pour utiliser des OU, il y a notamment les raisons suivantes :



Lorsqu'un contrôleur de domaine s'enregistre dans l'annuaire, il est automatiquement placé dans l'OU « Domains controllers ».

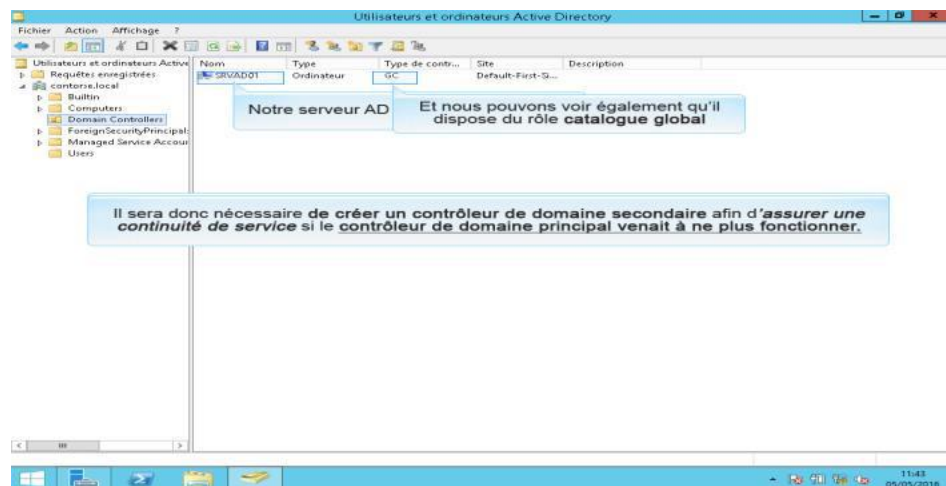
Des stratégies spécifiques vont s'appliquer sur le serveur.

Une stratégie permet d'appliquer un certain nombre de règles comme ajouter un lecteur réseau, imposer un fond d'écran, etc...

Cela signifie donc que la stratégie s'appliquera aux ordinateurs et/ou utilisateurs qui sont présents dans l'OU sur laquelle elle s'applique.

Nous verrons plus tard qu'il existe plusieurs types de stratégies mais certaines nécessitent de redémarrer l'ordinateur afin qu'elles puissent s'appliquer.

C'est pourquoi, il est nécessaire de redémarrer le serveur Active Directory après installation du rôle.



Notre serveur AD est présent dans l'OU.

Nous pouvons voir également qu'il dispose du rôle catalogue global.

Comme nous l'avons précisé lors de l'installation du rôle Service AD DS, les catalogues globaux sont importants puisqu'ils sont utilisés pour ouvrir une session du domaine et pour la recherche d'informations sur tous les domaines d'une forêt.

Un contrôleur de domaine, désigné en tant que catalogue global, stocke une copie complète de tous les objets de l'annuaire pour son domaine hôte et un réplica partiel pour tous les autres domaines de la forêt.

Cela signifie que s'il y a des domaines enfants appartenant au domaine contorse.local, le contrôleur de domaine parent ne stockera que certaines propriétés des objets enfants car seules certaines propriétés sont nécessaires pour les ouvertures de session et les opérations de recherche.

L'intérêt de la réplication partielle est que moins d'informations circulent sur le réseau.

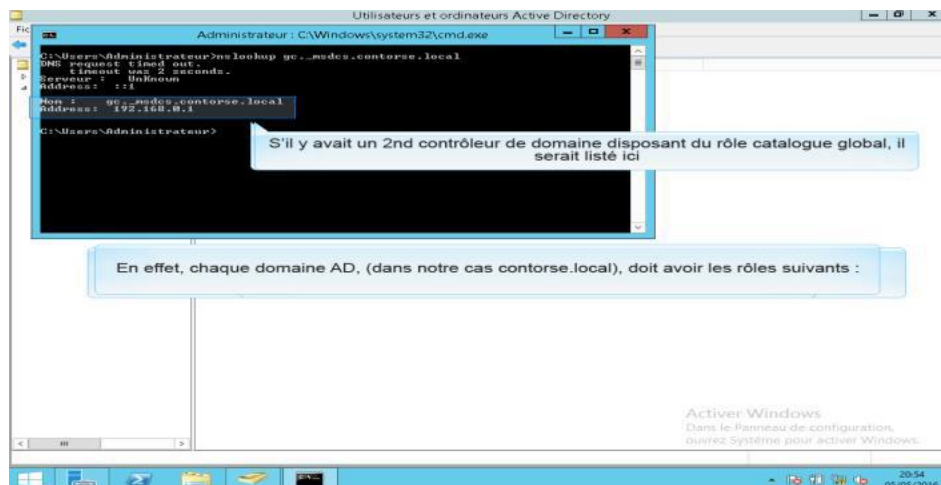
Dans tous les cas, il est important de comprendre que si le catalogue global est indisponible alors les utilisateurs du domaine ne pourront pas ouvrir de session sur le domaine.

Il sera donc nécessaire de créer un contrôleur de domaine secondaire afin d'assurer une continuité de service si le contrôleur de domaine principal venait à ne plus fonctionner.

Lorsque l'on arrive dans une infrastructure existante, bien que cela ne soit pas le cas dans ce cours, il est important de savoir quels sont les serveurs AD qui jouent le rôle de catalogue global.

Pour cela il existe une commande qui permet de la savoir :
nslookup gc._msdcs.contorse.local

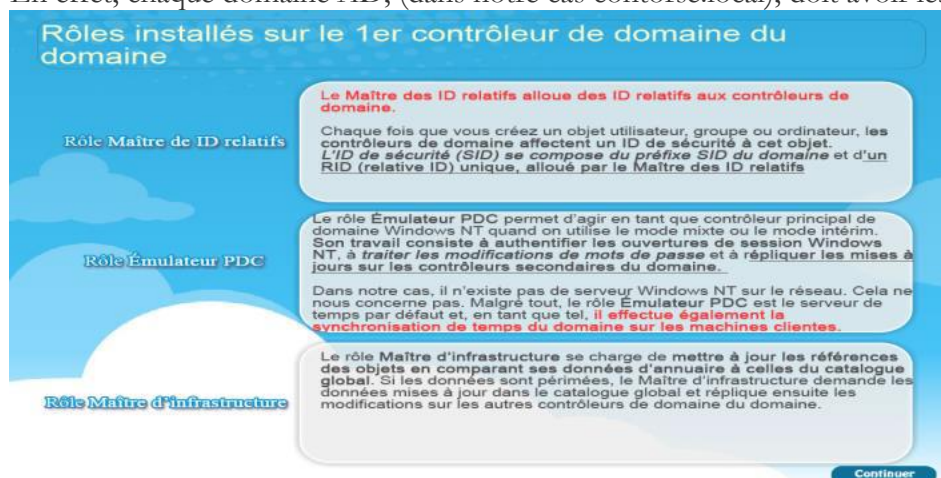
Nslookup est un utilitaire qui permet de rechercher des informations dans le serveur DNS. En saisissant cette commande, nous faisons une recherche depuis le domaine contorse.local et des domaines enfants (s'il y en a) constitués d'un catalogue global.



La commande affiche tous les catalogues globaux existants sur le domaine. S'il y avait un 2nd contrôleur de domaine disposant du rôle catalogue global, il serait listé ici.

Bien que nous l'ayons déjà dit, il est quand même utile de le rappeler, le 1er contrôleur de domaine installé est automatiquement désigné comme catalogue global mais il joue également d'autres rôles.

En effet, chaque domaine AD, (dans notre cas contorse.local), doit avoir les rôles suivants :



Rôle Maître de ID relatifs (RID)

Le Maître des ID relatifs alloue des ID relatifs aux contrôleurs de domaine.

Chaque fois que vous créez un objet utilisateur, groupe ou ordinateur, les contrôleurs de domaine affectent un ID de sécurité à cet objet.

L'ID de sécurité (SID) se compose du préfixe SID du domaine et d'un RID (relative ID) unique, alloué par le Maître des ID relatifs.

Emulateur PDC

Ce rôle permet d'agir en tant que contrôleur principal de domaine Windows NT quand on utilise le mode mixte ou le mode intérim.

Son travail consiste à authentifier les ouvertures de session Windows NT, à traiter les modifications de mots de passe et à répliquer les mises à jours sur les contrôleurs secondaires du domaine.

Dans notre cas, il n'existe pas de serveur Windows NT sur le réseau. Cela ne nous concerne pas. Malgré tout, le rôle Emulateur PDC est le serveur de temps par défaut et, en tant que tel, il effectue également la synchronisation de temps du domaine sur les machines clientes.

Maître d'infrastructure

Le rôle Maître d'infrastructure se charge de mettre à jour les références des objets en comparant ses données d'annuaire à celles du catalogue global. Si les données sont périmées, le Maître d'infrastructure demande les données mises à jour dans le catalogue global et réplique ensuite les modifications sur les autres contrôleurs de domaine du domaine.

Pour chaque rôle, il existe une commande qui permet de savoir sur quel serveur il est installé. Par exemple pour savoir quel serveur héberge le rôle Maître des ID relatifs, il faut saisir la commande :

dsquery server -hasfsmo rid

La commande dsquery permet d'effectuer des requêtes sur l'annuaire.

Pour connaître tous les commutateurs disponibles pour cet utilitaire, saisir dsquery /?

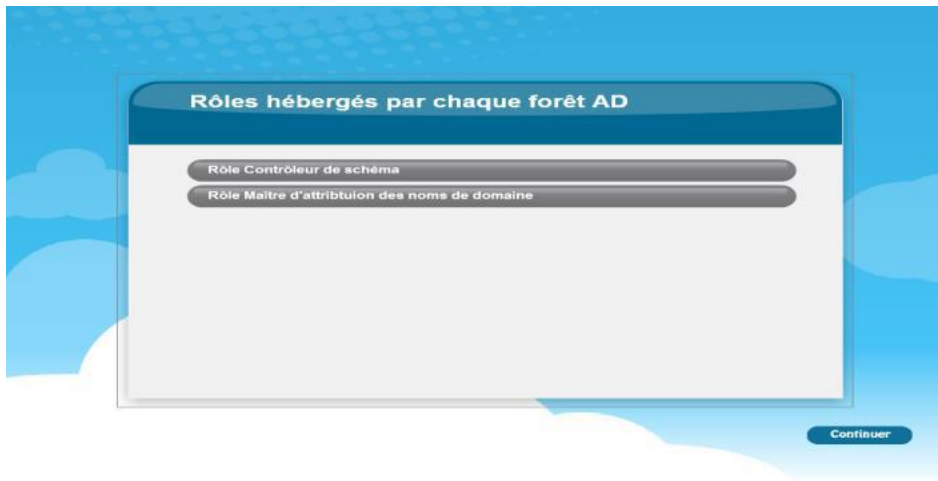
La commande nous dit que le serveur SRVAD01 héberge le rôle Maître RID.

N'oubliez pas que si nous avons un domaine enfant de contorse.local, il y aurait un second Maître RID puisque chaque serveur AD doit héberger ce rôle, ainsi que les rôles Émulateur PDC et Maître d'infrastructure.

Pour savoir qui héberge le rôle de « Emulateur PDC », il faut saisir la commande :

dsquery server -hasfsmo pdc

Et enfin, nous vous rappelons que dans chaque forêt Active Directory un serveur doit jouer les rôles suivants :



Pour déterminer quel serveur joue le rôle de Contrôleur de schéma, saisir la commande :
dsquery server -hasfsmo schema

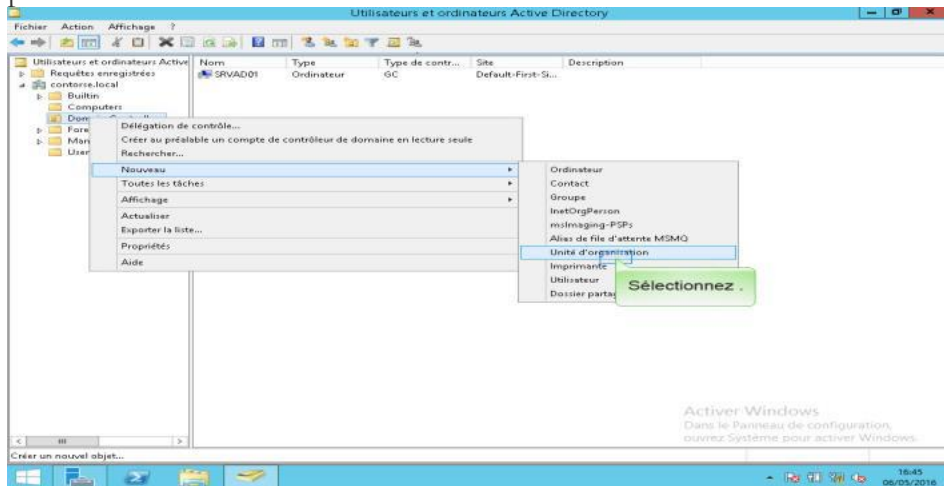
Les rôles contrôleur de schéma et maître de l'attribution de noms de domaine doivent être uniques dans une forêt.

Comme dans notre cas, notre serveur AD est le 1er contrôleur du domaine, dans une nouvelle forêt, il héberge ces 5 rôles.

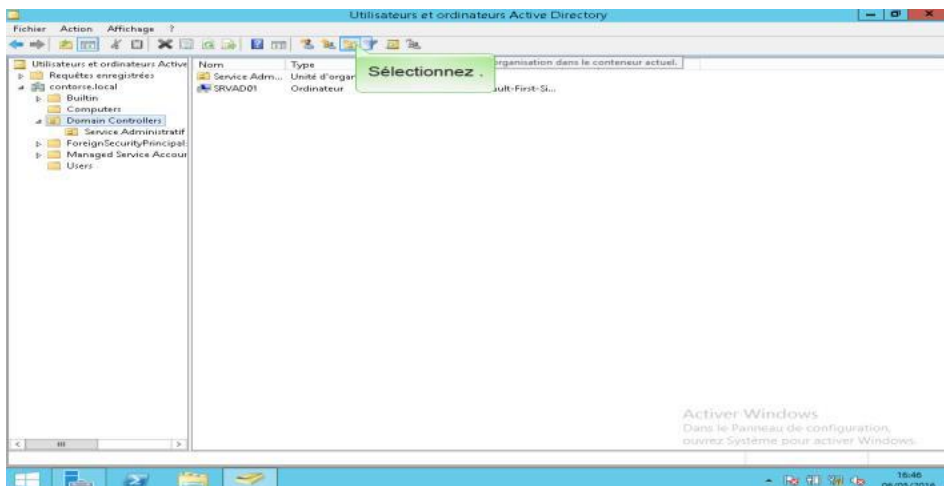
Organisation de l'annuaire

Il existe 2 manières pour créer des Unités d'organisation :

- par le menu contextuel

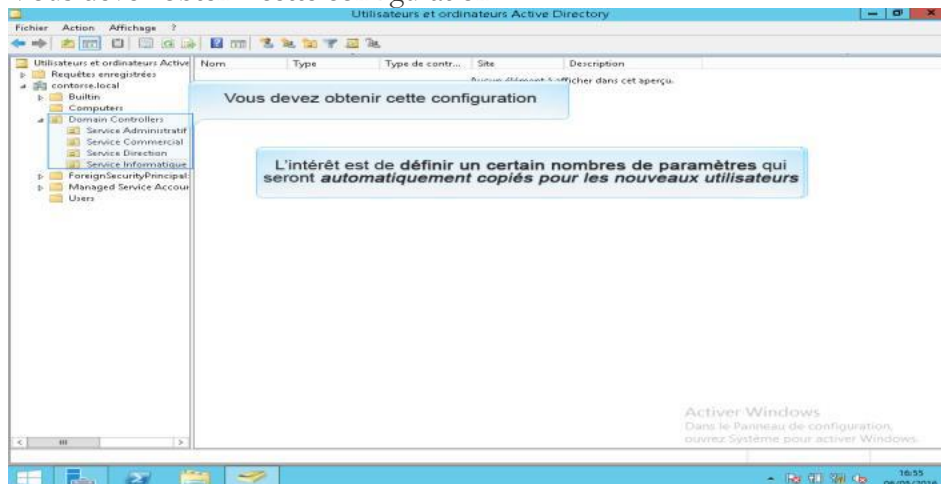


- par les raccourcis



Créer une UO pour chaque service de l'entreprise : Service Commercial, service Administratif, ...

Vous devez obtenir cette configuration :



Nous allons maintenant créer les objets utilisateurs et les affecter dans les bonnes OU.

Il est important de savoir que les objets placés dans une OU ne peuvent provenir que du domaine parent.

Par exemple, les OU associées à contorse.local contiennent uniquement des objets de ce domaine.

Comme il existe plusieurs utilisateurs à créer, il est possible de créer un utilisateur modèle.

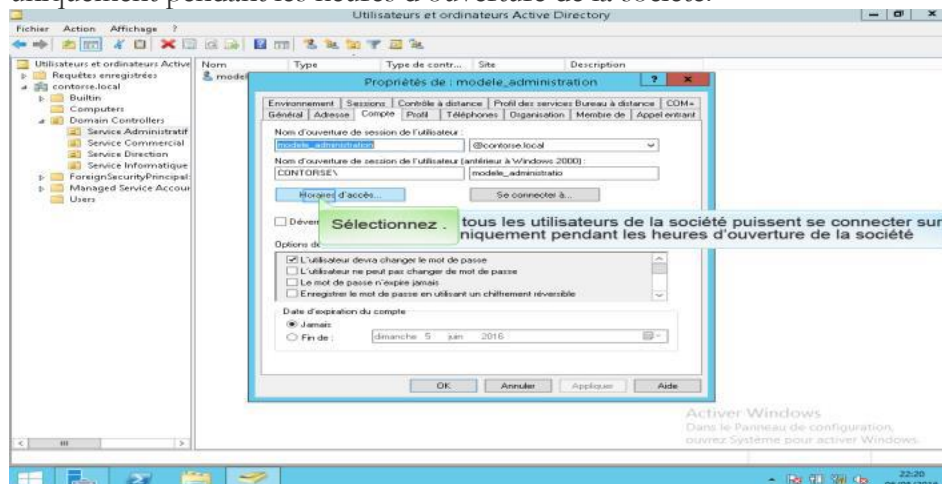
L'intérêt est de définir un certain nombre de paramètres qui seront automatiquement copiés pour les nouveaux utilisateurs.

Créez un utilisateur et nommez-le « modèle_administration ».

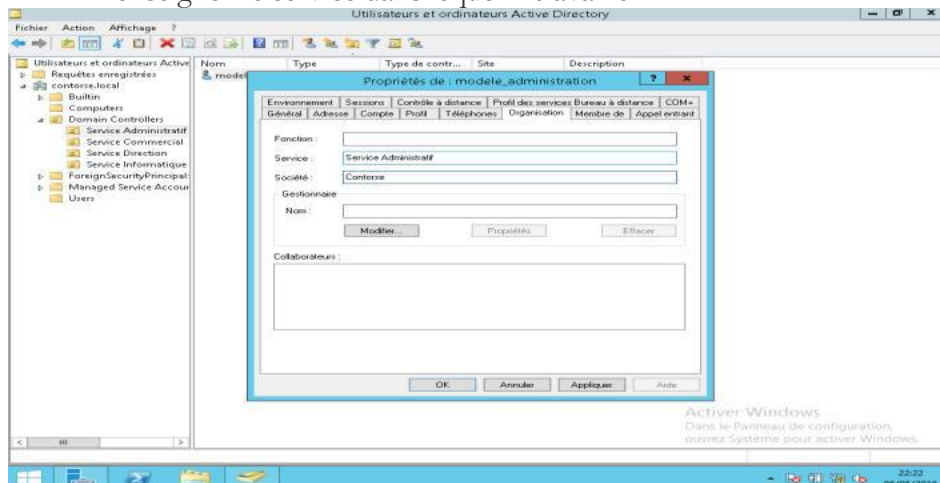
En effet, on pourrait créer un utilisateur modèle différent selon les services.

- on impose à l'utilisateur de changer son mot de passe car il est personnel et vous ne devez pas le connaître
- indiquez les horaires de connexion entre 8h et 18h.

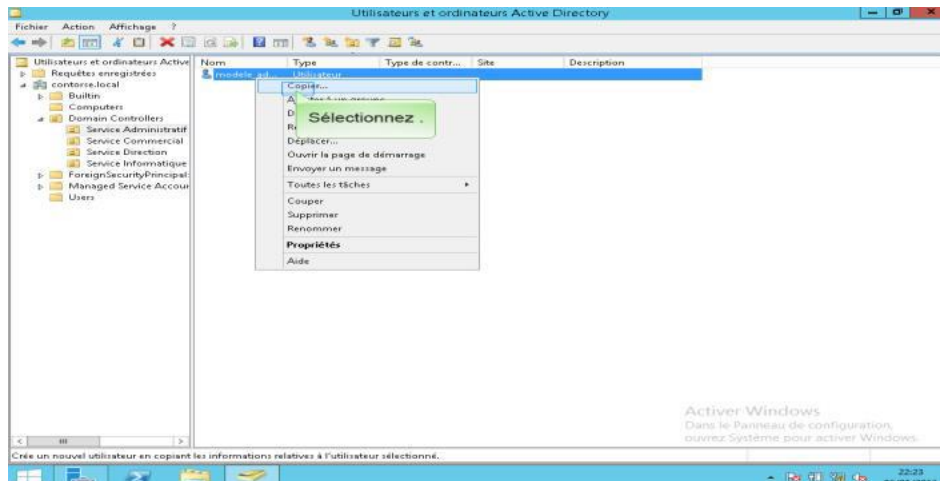
On voudrait que tous les utilisateurs de la société puissent se connecter sur le domaine uniquement pendant les heures d'ouverture de la société.



- renseignez le service dans lequel il travaille



Notre utilisateur modèle est paramétré, il nous reste qu'à créer des utilisateurs à partir de ce modèle en le copiant.



Nous créons Véronique MANSON à partir de ce modèle.

Par défaut, les stratégies de sécurité du domaine, obligent à utiliser un mot de passe comprenant 8 caractères comprenant des caractères spéciaux ainsi que des chiffres et des lettres.

Vérifiez que les informations renseignées dans le modèle utilisateur se trouvent bien dans l'utilisatrice Véronique MANSON.

Cependant, certaines données sont différentes en fonction des utilisateurs (nom, adresse mail..) et de ce fait, ces informations ne peuvent pas être copiées.

Nous avons vu comment créer un utilisateur modèle ou de référence, il vous reste maintenant à créer les autres utilisateurs du service Administratif.

Les groupes

Nous allons maintenant créer un groupe qui va contenir les employés du service administratif. Dans Active Directory, les groupes peuvent avoir des étendues différentes :

- Les groupes de **domaine locaux** sont définis pour accorder des autorisations au sein d'un domaine unique

Les membres de ces groupes peuvent être issus de n'importe quel domaine de la forêt et des domaines d'approbation des autres forêts.

En clair, cela signifie que si votre forêt contient plusieurs domaines comme stbrieuc.contorse.local, nantes.contorse.local, etc..., il sera alors possible d'ajouter des groupes ou utilisateurs provenant de ces différents domaines au groupe « Service Administratif »

Mais en revanche ce groupe est uniquement utilisable sur le domaine local. C'est-à-dire que ce groupe ne sera pas visible à partir d'un autre domaine.

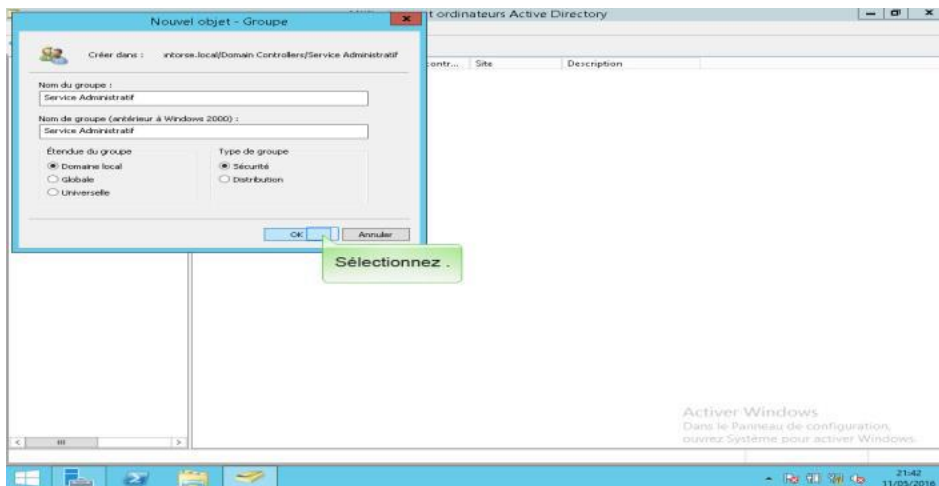
- Les groupes **globaux** sont conçus pour définir des ensembles d'utilisateurs ou d'ordinateurs d'un même domaine et qui partagent un rôle, une fonction ou une tâche similaire.

Les membres de ces groupes ne peuvent comprendre que des comptes et des groupes du domaine où ils sont définis.

Pour faire simple, un groupe global, peut être intégré dans tous les domaines approuvés, mais il ne peut contenir que des objets du domaine.

Il faut donc utiliser ce groupe si on possède plusieurs domaines ou plusieurs forêts.

- L'étendue **Universelle** peut contenir des membres de n'importe quel domaine de la forêt et être utilisé dans tous domaines de la forêt.



Lorsque l'on crée un groupe, il est possible de choisir entre deux types de groupe :

- Sécurité
- Distribution

Chacun des deux types ne remplit pas les mêmes fonctions.

Le type **sécurité** porte bien son nom car il permet de gérer la sécurité.

A la différence d'un groupe de distribution, le groupe de sécurité dispose d'un SID et permet de gérer les accès pour des ressources comme pour les droits sur un répertoire ou une imprimante partagée.

Un utilisateur faisant partie d'un groupe de sécurité utilisera le SID de ce dernier (donc du groupe), pour accéder à la ressource, si bien entendu le groupe de sécurité a été défini dans l'ACL.

Lorsqu'un utilisateur rejoint un groupe de sécurité, il accède automatiquement et dynamiquement aux ressources disponibles pour ce groupe.

La tâche d'un groupe de type **distribution** est d'offrir une ressource ou un service mais avec la particularité de ne pas inclure de mécanisme de sécurité.

Le groupe de distribution servira par exemple à créer une liste de distribution pour une adresse électronique, comme par exemple salaries@contorse.local.

Le groupe de distribution ne dispose pas de SID.

Nous créons un groupe de domaine local de type sécurité.
Il nous reste maintenant à ajouter les membres à ce groupe.

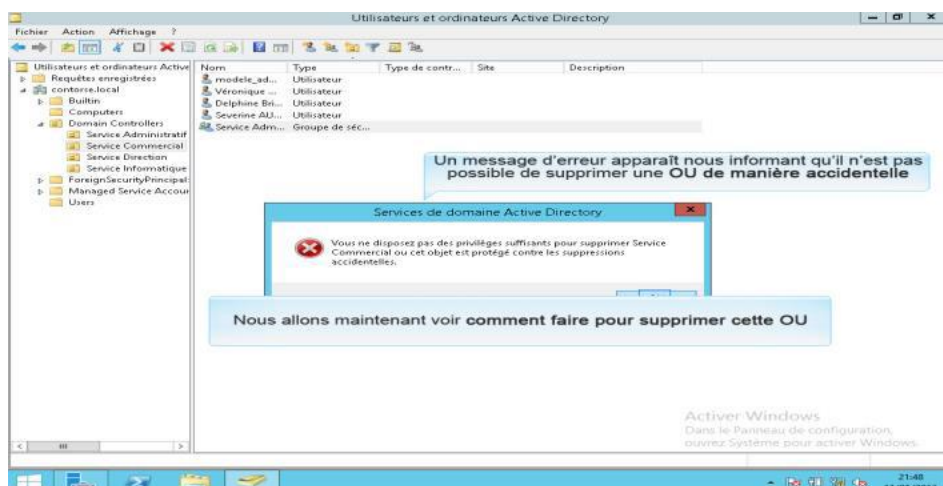
Comme il s'agit d'un groupe de domaine local, seuls les objets du domaine local pourront être ajoutés à ce groupe.

Nous venons d'ajouter les employés du service administratif dans leur groupe

Supprimer une OU

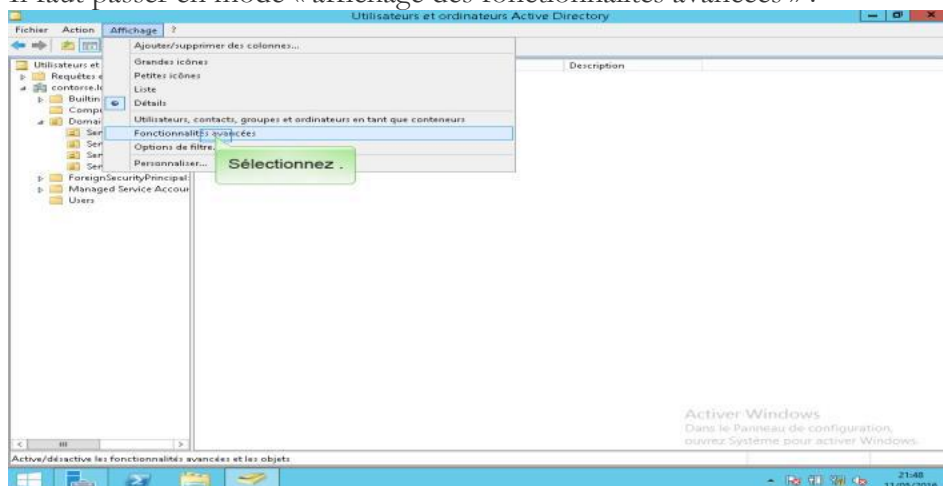
Nous allons maintenant voir comment supprimer une OU.

En effet, depuis Windows 2008, et pour des raisons de sécurité, il n'est plus possible de supprimer une OU par mégarde.

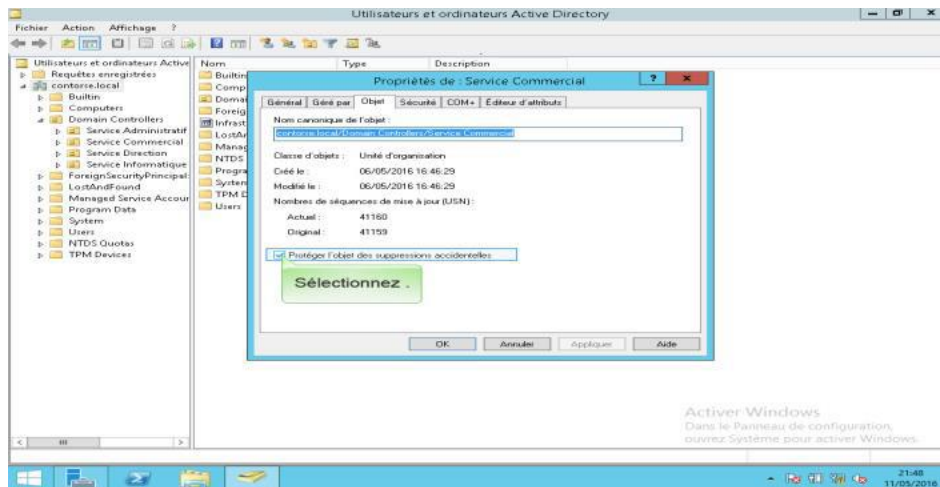


Un message d'erreur apparaît nous informant qu'il n'est pas possible de supprimer une OU de manière accidentelle.

Il faut passer en mode « affichage des fonctionnalités avancées » :



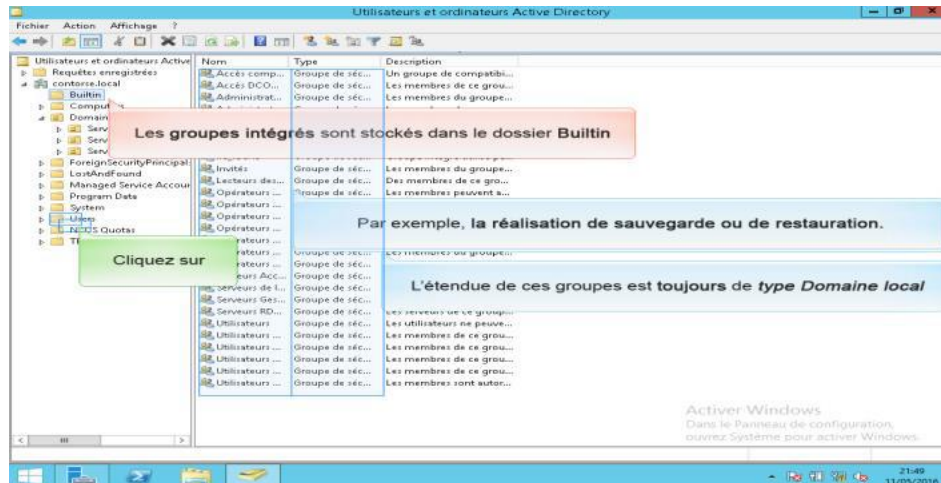
Puis décocher la case de protection dans les propriétés de l'UO à supprimer :



Il est ensuite possible de la supprimer.

Les groupes intégrés, prédéfinis et spéciaux

Et enfin pour terminer ce cours, nous allons voir 3 types de groupes qui sont créés par défaut et qu'il est important d'identifier.

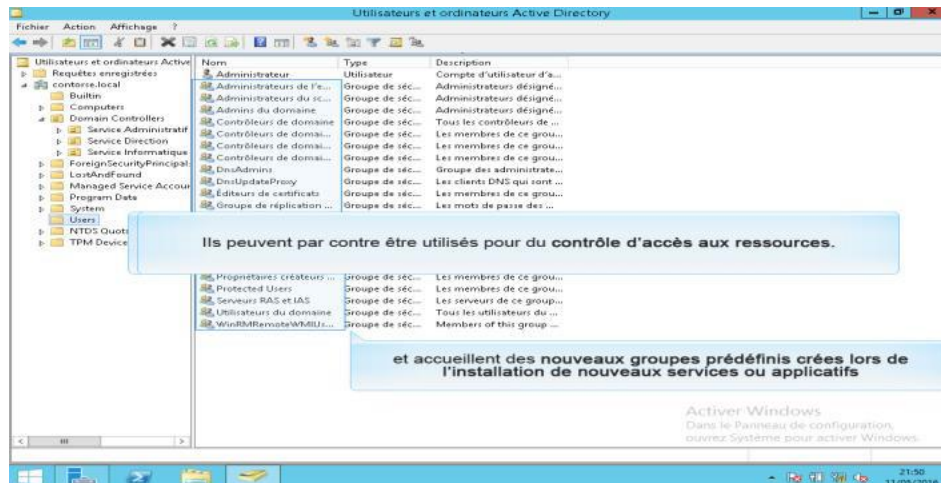


Les groupes intégrés ou Builtin sont des groupes permettant d'assigner des permissions aux utilisateurs nécessitant des droits d'administrations sur le domaine.

Par exemple pour la réalisation de sauvegarde ou de restauration.

Les groupes intégrés sont stockés dans le dossier Builtin.

L'étendue de ces groupes est toujours de type Domaine local.



Les groupes prédéfinis complètent les groupes intégrés à la différence qu'ils proposent en plus, des étendues de type global voir universel et accueillent des nouveaux groupes prédéfinis créés lors de l'installation de nouveaux services ou applicatifs.

Et enfin, il existe un dernier groupe nommé groupes spéciaux.

Ils sont gérés exclusivement par le système et regroupent différents utilisateurs en fonction des circonstances (par exemple le groupe Tout le monde).

Ils ne sont en aucun cas gérables depuis le console d'administration et ne peuvent être ajoutés dans un groupe.

Ils peuvent par contre être utilisés pour du contrôle d'accès aux ressources.

Conclusion

Nous avons pu voir que pour structurer son AD en fonction de l'organisation de l'entreprise, il est préférable de créer des OU car elles peuvent être soumises à des stratégies.

Nous savons également que plusieurs rôles sont hébergés sur le contrôleur de domaine et que parmi ces rôles, celui du catalogue global est particulièrement important.

Enfin, nous sommes maintenant en mesure d'identifier le rôle joué par certains groupes. On peut ainsi identifier les groupes intégrés, prédéfinis et spéciaux.