Restreindre le droit d'intégration à un domaine Windows

Introduction :

Peu de personne savent que n'importe quel utilisateur authentifié sur un domaine Windows peut joindre un ordinateur à ce même domaine.

Nous allons donc voir comment procéder pour fermer cette brèche et par la même occasion déléguer à un groupe d'utilisateur le droit de joindre un ordinateur au domaine.

Pré requis :

Un domaine : taz.com

Une OU (Unité d'organisation) : ordinateur

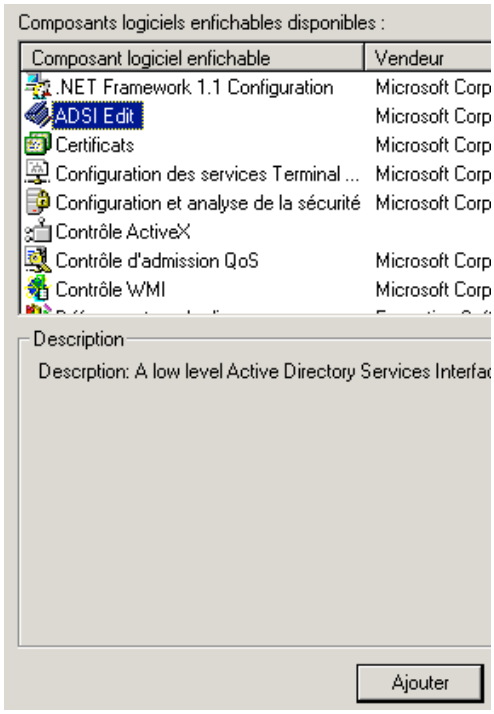
Un groupe : technique

Empêcher un utilisateur authentifié sur le domaine à joindre un objet ordinateur au domaine.

Commençons par bloquer la brèche afin d'empêcher les utilisateurs authentifier sur le domaine à pouvoir joindre des ordinateurs dans celui-ci.

Pour cela ouvrez une console MMC « Démarrer > exécuter > mmc » + « Ok », puis appuyer simultanément sur les touches « Ctrl » + « m » , appuyer alors simultanément sur les touches « Alt » + « o »

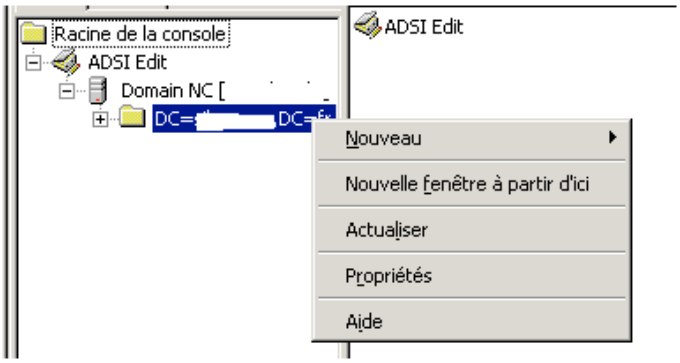
Sélectionnez alors le composant logiciel enfichable « ADSI Edit » puis cliquer sur « Ajouter », « Fermer » et « Ok ».



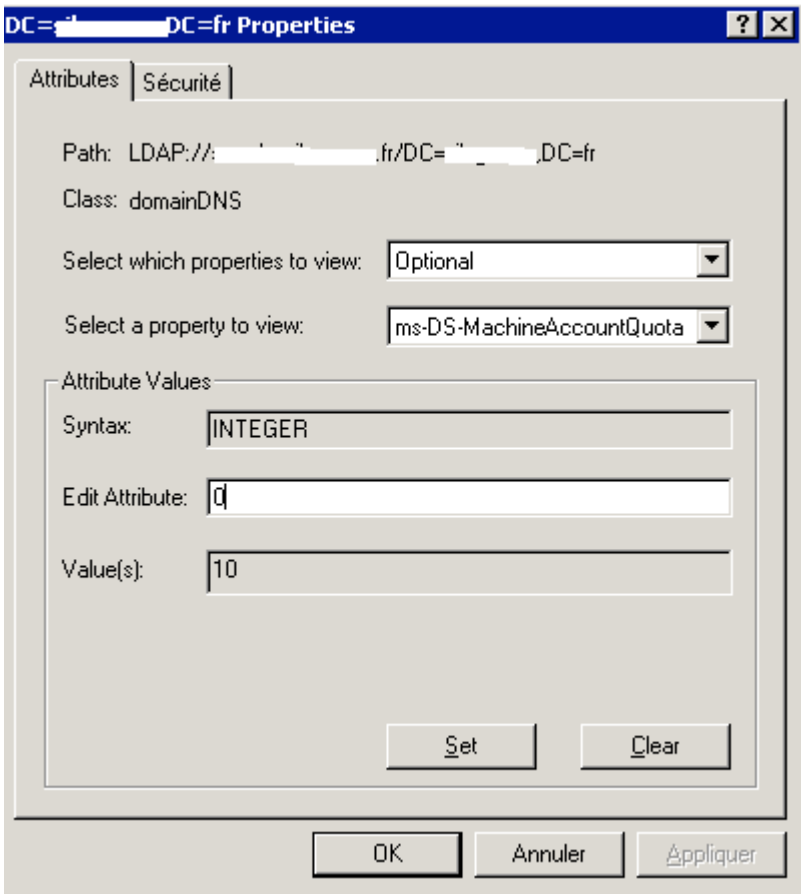
Faîtes alors un clic droit sur le composant « ADSI Edit » et cliquez sur « Connect to… ».

Si vous avez plusieurs domaines vous serez obligé de sélectionner celui sur lequel vous souhaitez faire l'opération.

Sélectionnez alors votre domaine et faîte un clic droit + propriétés sur celui-ci.



Sélectionnez alors l'attribut « ms-DS-MachineAccountQuota », puis saisissez la valeur 0 et cliquez sur « appliquer », vous remarquerez que par défaut chaque utilisateur authentifié sur le domaine peut joindre 10 ordinateurs au domaine.



A partir de ce moment là, seul les administrateurs du domaine pourront joindre des ordinateurs au domaine.

Rediriger les ordinateurs joint au domaine dans une OU définit.

Par défaut un ordinateur joint au domaine arrivent dans l'OU crée à l'installation de l'AD « Computers ».

Le problème et qu'il n'est pas possible de créer des GPO (http://fr.wikipedia.org/wiki/GPO) sur cette OU ni de créer des OU enfant.

Nous allons donc spécifier que les ordinateur joint au domaine arriverons pas défaut dans l'OU : ordinateur.

Pour cela sur le contrôleur de domaine allez dans démarrer exécuter puis saisissez cette commande :

Redircmp « OU=ordinateur,DC=taz,dc=com »

Puis cliquez sur Ok

A partir de ce moment, les ordinateurs joint au domaine seront automatiquement mis dans cette OU.

Déléguer la gestion de l'intégration des ordinateurs au domaine à un groupe d'utilisateurs

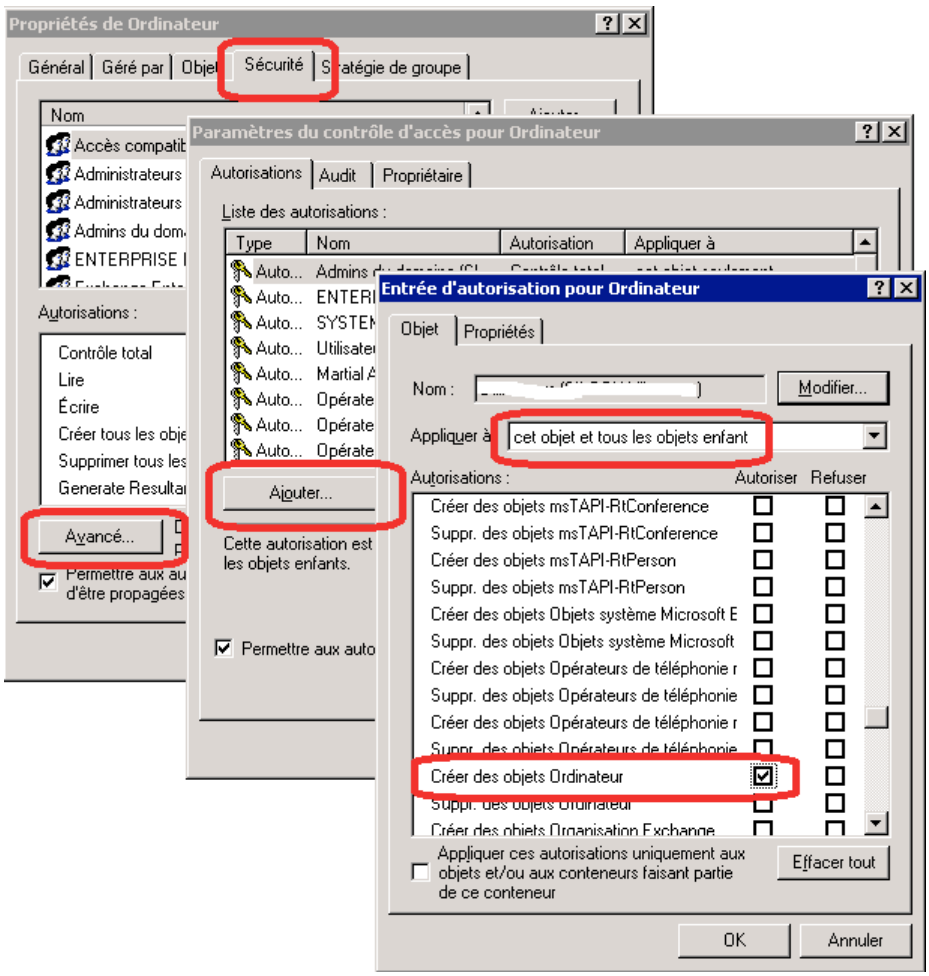
Nous allons maintenant déléguer au groupe technique le droit de créer des objets ordinateur est donc de joindre des ordinateurs au domaine.

Pour cela, depuis votre contrôleur de domaine, allez dans : démarrer > programmes > outils d'administration > Utilisateurs et Ordinateurs Active Directory.

Allez dans le menu affichage et cochez « Fonctionnalités avancées », puis faîtes un clic droit + propriétés sur l'OU « ordinateur », allez dans l'onglet Sécurité et cliquez sur Avancés puis sur Ajouter.

Sélectionnez le groupe « technicien ».

Dans le champ « Appliquer à » sélectionnez « cet objet et tous les objets enfant » puis cochez « Autoriser » sur l'autorisation « Créer des objets Ordinateurs »



A partir de ce moment, seuls les membres du groupe « technicien » pourront intégrer des ordinateurs au domaine.