Guédon Rémi

Session 2014-2015

**BTS SIO**

**Option SISR**

**Sisr3**  **Services orientés utilisateurs et notament les services stratégiques pour l’organisation**

**Compte-Rendu d'Activité n° 1**

**Intitulé de l'Activité :**

**Active directory (ldap) Windows Server 2012**

**Objectifs de l’activité**

**Cette activité vise à montrer :**

1. Création d’un active directory avec des utilisateurs

2) Création de profils et de répertoires partagés

3) Mise en place d’un serveur AD secondaire

**Déroulement de l'Activité :**

1) Création d’un contrôleur de domaine

2) Création des répertoires partagés

3) Création des profils utilisateurs

4) Création des GPO

5) Avoir accès à internet sur les machines clientes

6) Ajout d’un contrôleur de domaine secondaire (réplication)

**Matériels et Logiciels utilisés :**

Serveur contrôleur de domaine Windows server 2012 R2

Station clientes Windows 8.1



**I – Introduction**

L’étude de l’Active Directory est une activité très intéressante car dans chaque société, il y a un LDAP de présent et dans de très nombreux cas il est gérer par Windows server, il est donc nécessaire de maitriser un active directory.

**II – Présentation**

Notre structure est une ESN (Entreprise de Services du Numérique) du nom de Rézocean, l’entreprise est composé de trois parties : la direction, la partie commercial ainsi que les techniciens. L’administrateur réseaux a mis en place un contrôleur de domaine (active directory sous Windows Server 2012). Il a opté pour un serveur sous Windows pour faciliter la gestion des utilisateurs, des répertoires …

Toute la société se repose sur ce seul serveur, en cas de panne tout est perdu, l’activité s’arrête. Conscient de cela, le responsable informatique a décidé de mettre en place un second contrôleur de domaine en réplication avec le serveur principal. Grâce à ce système, en cas de panne du serveur principal le second prendra le relais de manière autonome, le seul défaut sera que les dossiers partagés, les profils ainsi que les lecteurs réseaux ne seront pas répliquer sur le contrôleur de domaine secondaire mais cela n’empêchera pas les salariés de continuer leurs travails en attendant que le serveur principal soit de nouveau fonctionnel.

Le contrôleur de domaine est composé d’un active directory (utilisateurs, groupes et unités d’organisation), il y a également un dns, un dhcp, des dossiers partagés, des profils (itinérants et obligatoires), des GPO liées à une unité d’organisation, et un accès à internet pour les clients grâce à une deuxième carte (NAT) sur le serveur et grâce au service routage.

**III – Déroulement de l’activité**

1. La création du contrôleur de domaine

Les deux premières choses à faire après l’installation de Windows Server 2012 sont de lui mettre une adresse ip fixe et de changer le nom du serveur. Il faut maintenant ajouter le rôle AD DS, quand ce rôle est ajouté il faut promouvoir le serveur en contrôleur de domaine (choix du nom de domaine …).

Une fois cela fait il faut ajouter le service DHCP et par la suite il faudra se rendre dans le service DHCP pour créer une nouvelle étendue, dans cette étendue il faut préciser les options suivantes : adresses ip à distribuer, la passerelle ainsi que le dns.

Ensuite, il faut créer les utilisateurs et les groupes dans l’active directory pour cela il suffit de se rendre dans « outils d’administration » puis dans « Utilisateurs et ordinateurs » et enfin de créer l’utilisateur comme nous le montre la capture suivante :



1. Création des répertoires partagés

Dans notre cas, avec la société Rézocean, nous avons décidé d’ajouter un 2ème disque dur sur le serveur principal, son rôle sera dédié à contenir les répertoires partagés ainsi que les profils.

Sur ce disque dur on créer d’abord des dossiers (des groupes) « Commercial », « Direction » et « technicien ». Chaque dossier contient un dossier par utilisateurs correspondant à leurs rôles dans la société. Il faut maintenant partager les dossiers aux utilisateurs légitimes. Pour cela il faut aller dans « Partage avancé » et supprimer « tout le monde » et ajouter l’utilisateur ou le groupe propriétaire du dossier. Il ne reste plus qu’à faire pareil pour tous les dossiers.

Une fois tous les dossiers créés et les droits attribués il faut créer un script pour chaque groupe qui activera les lecteurs réseaux des utilisateurs, ces différents scripts seront stockés dans le dossier SYSVOL :

C:\Windows\SYSVOL\sysvol\REZOCEAN.lab\scripts



Le script pour l’utilisateur David membre du groupe direction est le suivant :



Ce script est enregistrer sous le nom « script\_direction.bat », une fois que le script est créer il faut se rendre sur le profil de l’utilisateur concerné, puis dans les options du compte (script d’ouverture de session) mettre le nom du script, dans notre cas : script\_direction.bat

 

Dorénavant, quand l’utilisateur « David » ouvrira sa session il possèdera trois lecteurs réseaux (Commun, Direction et david).



1. Création des profils utilisateurs

Pour mettre en place des profils, on va créer sur le deuxième disque dur un dossier « profils\_itinérant$ » qui servira à stockés tous les profils. Il est absolument indispensable de partager ce dossier en mettant « utilisateurs authentifiés ».

Ensuite il faut se rendre dans les propriétés de l’utilisateur et mettre en chemin du profil le chemin de partage de dossier « profils\_itinerant$ » et il faut rajouter %username% à la fin.



Pour vérifier que le profil itinérant à bien été créer il faut se rendre dans le dossier profils\_itinérant$ et vérifier qu’un dossier david.V2 s’est créer.

Maintenant nous allons créer un profil obligatoire, avec cette fois ci l’utilisateur « Rémi ».

Pour cela il faut créer un dossier profil\_obligatoire$ et le partagé avec seulement « utilisateurs authentifiés ». Ensuite il faut copier le dossier Default qui se situe dans « C:\Users » et le coller dans le dossier profils\_obligatoire$ et le renommer Default.V2

Une fois cela fait, on rentre dans le dossier Default.V2 et on affiche les dossiers et fichiers cachés et décocher « masquer les fichiers protégés par le système d’exploitation ». Puis renommer le fichier NUSER.DAT en NTUSER.MAN.

Et pour finir il ne reste plus qu’à indiquer le chemin de profils a l’utilisateur en question.



Et l’utilisateur dispose maintenant d’un profil obligatoire.

1. Création des GPO (Stratégies de groupe)

Création d’une ou plusieurs OU (Unité d’organisation) dans notre cas une unités d’organisation qui se nomme « groupes » puis déplacer dans cette OU tous les groupes, utilisateur, les utilisateurs et les ordinateurs présent dans l’active directory.



Ensuite il faut se rendre dans « gestion des stratégies de groupe » puis créer une gpo au niveau de l’OU que l’on a créé précédemment puis choisir les groupes sur lequel la stratégie doit s’appliquer. Et pour finir il faut modifier la stratégie en empechant l’accès au cmd, en désactivant l’accès au panneau de configuration…

Si on veut que la gpo s’applique immédiatement on peut taper la commande suivante dans un cmd : « gpupdate /force ».

1. Accès à internet sur les machines clientes

Nous travaillons sur un environnement virtuel (VmWare) en host-only pour bénéficier d’internet sur les machines cliente il nous faut rajouter une carte réseau NAT sur le serveur. Dès que la carte est ajouter le contrôleur de domaine à internet.

Pour que les postes clients bénéficient d’un accès à internet il faut installer le rôle routage sur le serveur principal. Quand le rôle est installé il faut le configurer en accès NAT et le diriger vers la carte réseau que l’on a rajouté précédemment.



Une fois que le paramétrage est fini les clients pourront bénéficier d’un accès à internet.

1. Ajout d’un contrôleur de domaine secondaire (réplication)

Nous allons installer un deuxième serveur Windows server 2012, le paramétrer en lui mettant une adresse ip statique différente de celle du premier serveur mais qui est sur la même plage ip, en dns on lui mettra celle du premier serveur et pour finir il faut modifier le nom du serveur. Maintenant il faut rentrer le deuxième serveur dans le domaine REZOCEAN.lab. Une fois que le serveur est dans le domaine il faut comme pour le premier serveur installer le rôle « AD DS », une fois cela fait il faut le promouvoir en contrôleur de domaine il faut ajouter un contrôleur de domaine à un domaine existant.

Puis il faut ensuite préciser que le serveur doit répliquer depuis le serveur principal.

Une fois la configuration terminé il y a un second contrôleur de domaine présent si l’on créer un utilisateur sur le premier il sera automatiquement répliqué sur le deuxième.

Dès que l’active directory est répliqué il faut maintenant répliquer le DHCP pour cela il faut ajouter le rôle DHCP sur le serveur secondaire.

Ensuite il faut le configurer pour cela clic droit sur « ipv4 » puis sur configurer un basculement ensuite il faut spécifier que le basculement se fera avec le premier DHCP.

Le DHCP est maintenant répliqué.



**IV- Conclusion**

Pour conclure, les objectifs ont tous été atteints, le domaine est bien organiser avec la réplication qui fonctionne bien quand le serveur principal s’éteint ou est en panne, le serveur secondaire prend le relais sans qui est le moindre désagrément pour les utilisateurs. Le seul problème est que les dossiers partagés ainsi que les profils qui ne sont plus accessible car ils ne sont pas répliquer. Mais c’est un moindre mal car sinon l’activité de l’entreprise s’arrêterai nette.

Et pour terminer, j’ai rencontré un seul problème avec le service routage mais sinon tous les autres activités ont été réalisé avec succès.

Ce TP était très enrichissant car c’était un cas très proche d’un cas d’entreprise.