

TP : Active Directory (Services Annuaire)

Public(s)	Section de BTS SIO option : SISR
Savoir(s)	C21 Installer et configurer un microordinateur C22 Installer et configurer un réseau
Capacité(s)	C22 Installer et configurer un réseau C26 Installer un routeur
Objectif(s)	<ul style="list-style-type: none">• Créer un contrôleur de domaine.• Joindre les PC clients au domaine.• Créer les comptes utilisateurs dans un domaine.• Les mêmes utilisateurs feront parti des groupes adéquats, qui possèdent un profil itinérant, permettant ainsi à ces utilisateurs à se connecter avec leurs profils propres.
Professeur	Christophe CHITTARATH

Un groupe de travail réseau est relativement facile à mettre en place, l'inconvénient est qu'il n'y ait pas de règle commune à tous afin de gérer d'une façon cohérente les tâches d'administration réseau, par exemple les mots de passe, les partages...etc.

Microsoft version serveur dispose un service appelé Active Directory, qui permet de centraliser la gestion de l'administration réseau, et ce à travers des objets tels que les comptes utilisateurs, les profils, GPO (Group Policy Objects) ...etc.

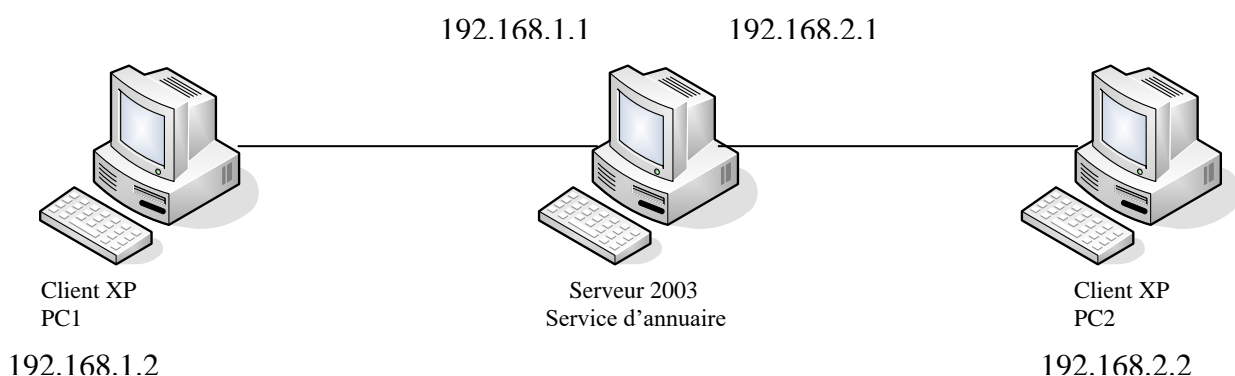
L'installation du service AD promeut un serveur en contrôleur de domaine qui centralise les échanges, les authentifications, les applications des règles prédéfinies au sein du domaine.

Cette PTI consiste à étudier et à mettre en évidence le rôle joué par les profils :

- Default Users
- All Users
- Local
- Itinérant
- Obligatoire

Elle a pour but de déployer les stratégies de groupe afin de centraliser et optimiser l'administration des objets (machines, compte d'utilisateurs...) dans un domaine.

Configuration du réseau : à compléter les adresses IP



Configuration requise :

Vous créez un team contenant trois postes (1 serveur 2003 et 2 PC client XP)

Configurer vos postes selon le tableau ci-dessous :

Hostname	IP	Masque	Passerelle	DNS
PC1	192.168.1.2	255.255.255.0	192.168.1.1	192.168.1.1
PC2	192.168.2.2	255.255.255.0	192.168.2.1	192.168.2.1
serveur	192.168.1.1	255.255.255.0	néant	127.0.0.1
	192.168.2.1	255.255.255.0		127.0.0.1

Deuxième partie : GPO

GPO Group Policy Object

Stratégie Redirection des dossiers Mes document du profil

- L'inconvénient d'un profil local est que l'utilisateur ne retrouve pas son environnement de travail, lors qu'il change de PC.
- L'avantage d'un profil itinérant est que l'utilisateur retrouve son environnement de travail quelque soit le PC avec lequel il travaille, du moment que le PC en question, fasse parti du domaine.

Ceci étant, le profil itinérant peut s'enrichir des dossiers avec le temps, et grossit en taille mémoire, par conséquence, le temps de téléchargement du profil du serveur vers le PC devient plus long voire impossible.

- La solution est de créer une stratégie de groupe, qui redirige certains dossiers utilisateur dans le profil vers un dossier appelé par exemple **redirection** indépendant du profil utilisateur. On extrait en quelque sorte, ces dossiers du profil, qui conserve simplement un pointeur dans le profil, assurant la liaison entre ce profil itinérant et les dossiers "retirés" du profil.

Ainsi, l'utilisateur n'a pas besoin de tout télécharger les dossiers dans son profil itinérant mais simplement quelques éléments de base : papier peint, raccourci... il retrouve cependant les dossiers liés au profil d'une façon transparent grâce au pointeur.

Démonstration

- 1) Se connecter au nom d'un utilisateur dont le profil est itinérant.
- 2) Surcharger artificiellement le profil de l'utilisateur, en copiant les fichiers (300 méga octets environ) dans le dossier **Mes documents** du profil de l'utilisateur.
- 3) Fermer la session. Que constatez-vous ?
- 4) Se reconnecter de nouveau du même poste. Que constatez-vous ?

Remédiation

Créer un dossier dans la racine appelé par exemple **redirection**, puis le partager avec la permission lecture, écriture, modification...

- 1) Sous **redirection**, créer un 2^{ème} dossier au nom de l'utilisateur.
- 2) Création d'une **unité organisatinelle**, appelé **UO1**, pour ce faire, aller dans **Outil administration, utilisateur_active Directory, clic droit sur le nom du domaine...etc**
- 3) Placer l'utilisateur en question dans **UO1**.

- 4) Clic droit sur l'**UO1**, **propriété**, puis **stratégie de groupes**, donner un nom à votre stratégie comme par exemple **stratégie_redirection**, puis cliquer sur **modifier**.
- 5) Développer onglet **Configuration Utilisateur**, puis **Paramètre de Windows**, puis **Redirection du dossier**.
- 6) Cliquez droit sur **Mes Documents**, choisir **propriété**.
- 7) Dans Paramètre, choisir **De base – Rediriger les dossiers....**
- 8) Dans emplacement du dossier cible, choisir **Créer un dossier pour un utilisateur....**
- 9) Dans Chemin d'accès de la racine : saisir le chemin UNC
\\nom_du_serveur\redirection
- 10) Pour actualiser la stratégie de groupe aller dans une fenêtre de DOS, puis taper **gpupdate/force** puis valider.
- 11) Tester la stratégie en se connectant puis déconnectant au nom de cet utilisateur.
- 12) Que constatez-vous au niveau du temps de connexion – déconnexion ?
- 13) Que trouvez-vous dans le sous dossier **Redirection** ?

A tester les autres stratégies :

- **Interdire l'utilisation de l'invite de commande**
Configuration utilisateur - Modèle d'administration – Système
- **Empêcher l'Accès au panneau de configuration**
Configuration utilisateur - Modèle d'administration – Panneau de configuration
- **Masquer les lecteurs logiques : A, B , C...etc**
Configuration utilisateur - Modèle d'administration – Explorateur Windows - Dans poste de travail masquer... ;
- **Créer une sous unité organisationnelle UO2**, placer les nouveaux utilisateurs puis montrer que les stratégies activées dans **UO1** (parent) hérite sur **UO2**.
- **Démontrer que les utilisateur de UO2 peut bloquer l'héritage venant de UO1** (c'est-à-dire de ne pas subir stratégie de parent).

- **Imaginer une situation conflictuelle** dans l'application d'une stratégie au niveau d'un utilisateur. Démontrer la logique dans l'application de celles-ci dans une telle situation.

- A)** – Créer un compte toto puis le placer dans UO_A
 – Créer un compte titi dans UO_B qui se trouve en dessous de UO_A
 - Appliquer la stratégie qui autorise l'accès à l'invite de commande sur OU_A
 - Appliquer la stratégie qui refuse l'accès l'invite de commande sur OU_B

Question :

- titi peut-il accéder à l'invite de commande et pourquoi ?

B) Stratégie par rapport au groupe

Créer un compte tutu dans le conteneur USER, créer une UO_C à la racine

Créer un groupe C dans UO_C, déclarer l'appartenance de titi et tutu dans le groupe C.

- Appliquer la stratégie qui refuse l'accès au panneau de configuration sur UO_C
- Appliquer la stratégie qui refuse l'accès au panneau de configuration sur UO_B

Question :

- titi et tutu peuvent-ils accéder au panneau de configuration et pourquoi ?

C) stratégie plus haute ou plus basse:

- Appliquer une deuxième stratégie qui autorise l'accès au panneau de configuration sur UO_C.

Question

- tutu peut-il accéder au panneau de configuration et pourquoi ?

Permuter les deux stratégies, que constatez-vous ? Conclusion.

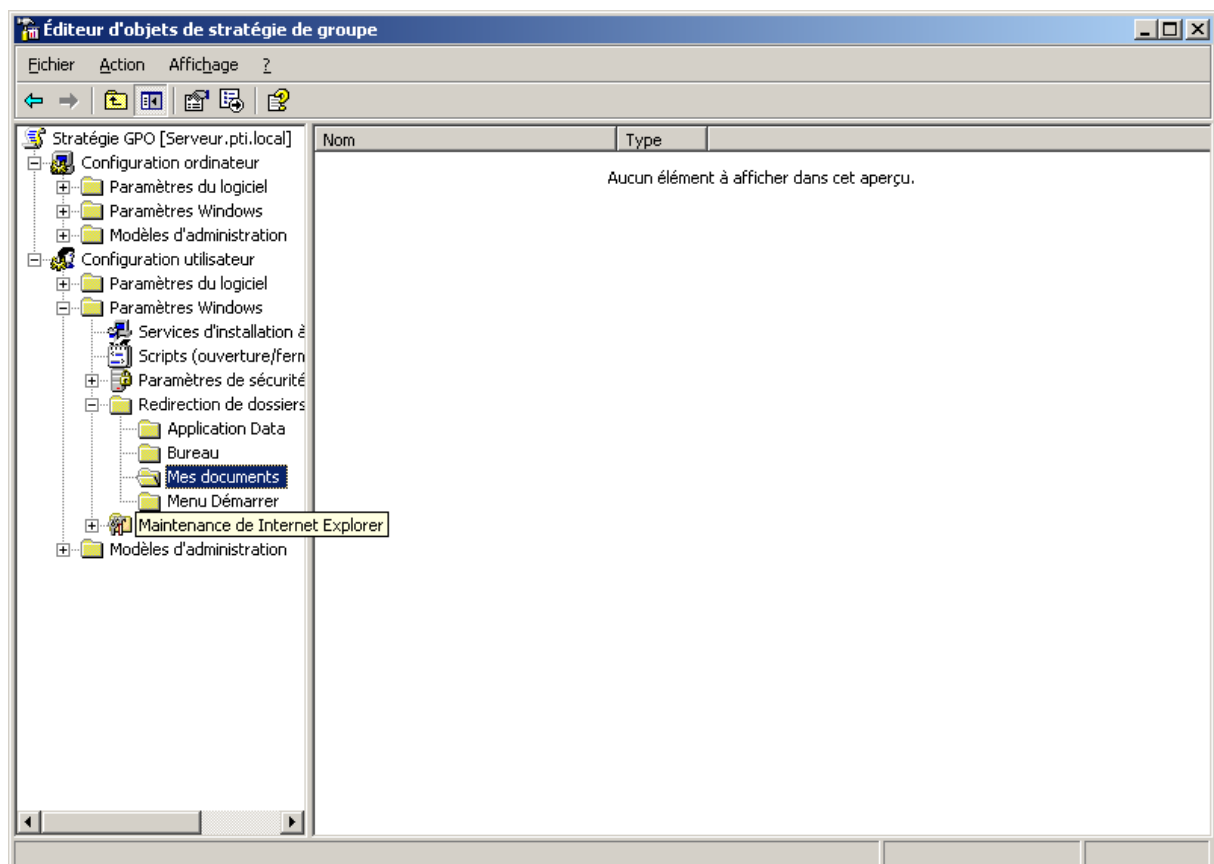
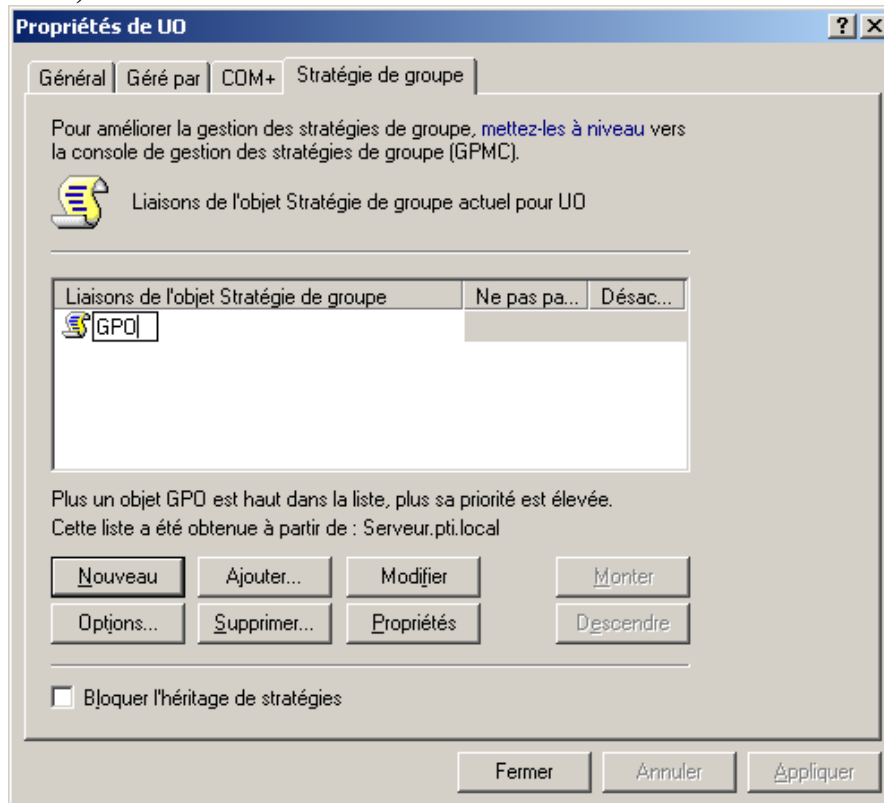
D) stratégie la plus restrictive

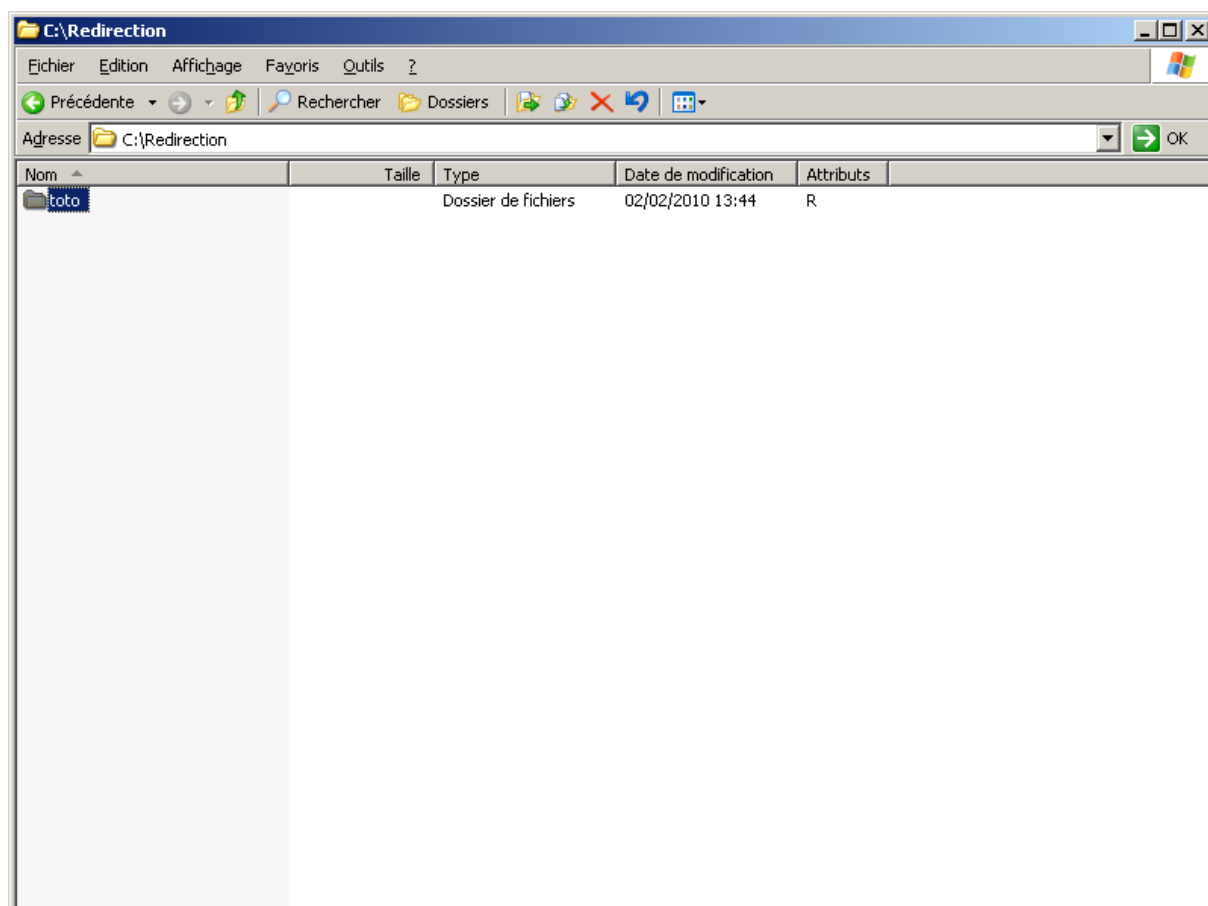
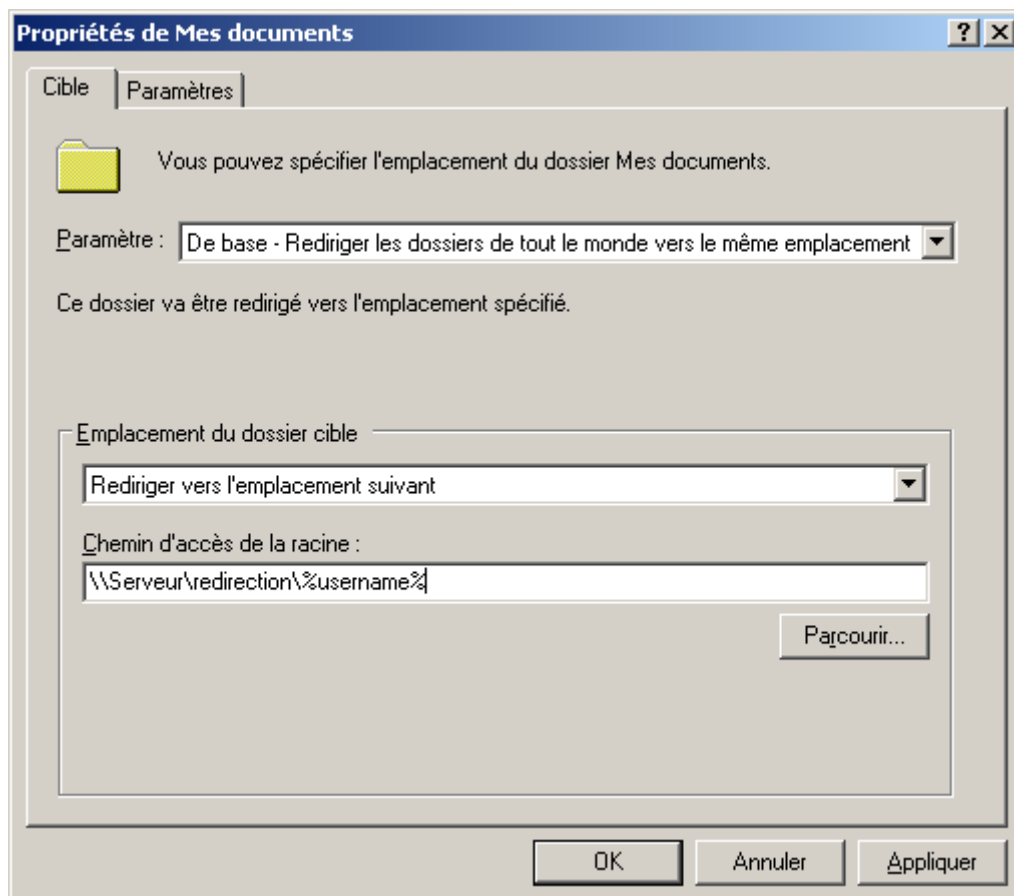
En cas de conflit de stratégie entre deux groupes dans deux U.O différentes, laquelle des deux stratégies emporte sur l'autre.

E) par rapport au poste

En cas de conflit de stratégie entre celle s'applique sur le poste, et celle qui s'applique sur un compte utilisateur, laquelle des deux stratégies emporte sur l'autre.

F)





```

C:\ Invite de commandes
Microsoft Windows [version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrateur>gpupdate /force
Actualisation de la stratégie...

L'actualisation de la stratégie utilisateur s'est terminée.
L'actualisation de la stratégie ordinateur s'est terminée.

Pour vérifier des erreurs dans le traitement de la stratégie, consultez
l'Observateur d'événements.

C:\Documents and Settings\Administrateur>_

```

