BTS Informatique de gestion
2e année
Option administrateur de réseaux locaux d'entreprise

Isabelle Ufarte

Architecture logicielle des systèmes informatiques

Autocorrection

Directrice de publication : Valérie Brard-Trigo

Sommaire

Correction des exercices du cours

Correction des ateliers

Séquence 1

Vocabulons

Cette séquence prépare le lecteur quant au contenu de cet ouvrage.

Exercice récapitulatif 

Ce petit questionnaire vous permet de vérifier vos connaissances. Suivant le nombre de OUF gagné vous pourrez rebûcher cette séquence ou passer à la suite.

Question 1

La réponse **d** est vraie. Aucun OUF, c'était juste pour savoir si votre esprit n'était pas en veille.

Question 2

Les réponses **a** et **b** un OUF par bonne réponse. La réponse **c** est fausse car on ne parle de coopératif que parce les applications attendent que le processeur soit libre pour l'utiliser.

La réponse **d** est fausse car les thread étant le découpage d'un programme en morceaux afin de les exécuter en même temps n'a de commun avec le multitâche que l'apparence de parallélisme.

Question 3

La réponse **d** un OUF. Les réponses **a** et **b** correspondent à la définition d'une architecture SMP.

Question 4

La réponse **a** oui, le partitionnement (MBR et GPT) ne dépendant pas uniquement du système d'exploitation mais aussi du processeur, un OUF. **b**, oui, mais son nom change et certains composants ne sont pas encore compatibles 64 bits, un OUF. **c**, Windows 2003 server fonctionne avec des partitions MBR ou des partitions GPT, pas les 2 à la fois. **d**, Comme pour a, ce qui est plus cher c'est le nouveau processeur.

Rappel AMSI : Tous les ordinateurs x86 utilisent un style de partition appelé MBR (Master Boot Record). MBR contient une table de partition qui décrit l'emplacement des partitions sur le disque. On ne peut créer que 4 partitions principales. Aussi, pour pallier le problème, la 4e pouvait être une partition étendue sur laquelle un nombre illimité de lecteurs logiques pouvait être créé.

Les Itanium eux, sont des ordinateurs qui utilisent un nouveau style de partition appelé GPT (GUID Partition Table). Avec cette technologie on peut créer jusqu'à 128 partitions principales. On peut également installer des disques MBR sur les systèmes Itanium, mais on ne peut pas démarrer un système à partir de ces disques.

Question 5

Réponse **a** les deux, **b**, nom netbios, **c** nom d'hôte, d les deux. Un OUF par bonne réponse.

Quel OUF êtes vous ?

0 – 2 C'est plus facile de faire les exercices quand on a lu le cours.

3 – 5 Il vaut mieux commencer avec de bonnes bases, pour l'instant c'est simple, une relecture ne vous ferait pas de mal.

6 – 9 Tournez la page de votre livre de cours.

10 C'est pas possible, vous avez triché, il n'y a que 9 bonnes réponses !

Séquence 2

Les systèmes multi-utilisateurs

Cette séquence trace les grandes lignes de l'administration d'un réseau. Elle donne des notions de multi-utilisateurs et du multitâche.

Exercice 2

Donner un autre exemple.

La vente de fleurs par correspondance sur Internet par exemple.

Exercice 3

Donner un exemple.

Une société de fret d'un port à un progiciel qui permet de gérer informatiquement les divers départements de sa société :

- Chargement /déchargement,
- Gains/ pertes de temps et d'argent
- Arrivée / départ des camions
- Gestion du personnel

Exercice 4

Donnez un autre exemple.

Météo France utilise des supercalculateurs pour travailler sur un seul élément : le temps.

Exercice 5

Parmi les propositions suivantes indiquez celles qui impliquent un système multitâche ou un système multi-traitements.

a. Un grand club de loisirs met en place une application informatique (utilisée par les agences de voyages connectées) destinée à indiquer le nombre de places disponibles dans les centres de vacances du club.

b. Un comptable utilise un micro-ordinateur pour tenir ses dossiers clients en utilisant un logiciel comptable multi-sociétés.

c. L'organe central d'une banque propose à ses agences un accès télématique à son système informatique. Elles pourront ainsi exploiter les différents logiciels de gestion de la banque.

Proposition a : ni l'un, ni l'autre, c'est un programme qui est mis en commun.

Proposition b : Ni l'un, ni l'autre, on travaille dans un milieu multi-utilisateurs, ici il y a une seule personne.

Proposition c : L'un ou l'autre, cela dépend s'il y a un seul serveur, plusieurs serveurs spécialisés, le multitâche a ma préférence.

Exercice 6

Donner des exemples pour chacune des actions de l'administrateur.

Centralisation : Administration centralisée par un serveur de données, et d'accès au domaine, administration à distance des postes des utilisateurs.

Contrôler : Mots de passe, lecture du journal des événements qui rapporte toutes les opérations effectuées.

Sécuriser : droits, permissions, comptes d'utilisateurs.

Informer : communiquer avec les utilisateurs sur les changements avec des mails...

Optimiser : n'effectuer qu'une seule fois une opération et l'appliquer sur plusieurs utilisateurs à la fois grâce à des stratégies, cloner des machines.

Réparer : Antivirus, scanner un disque, restaurer une image.

Planifier : organiser les sauvegardes sur la semaine et sur des supports différents.

Déléguer : créer des console d'administration à distance : MMC qui donne des petits pouvoirs aux utilisateurs comme gérer le pool d'impression d'une imprimante.

Exercice 7

Donner des exemples d'outils.

Console MMC, Antivirus, Antispam, Intranet, logiciel de prise en main à distance ...

Exercice 8

Puisque c'est si évident expliquez pourquoi un serveur WEB ne doit pas être contrôleur de domaine.

Un serveur WEB est accessible directement de l'extérieur par une adresse IP fixe par exemple. On le trouve dans une zone dite démilitarisée, c'est-à-dire sans protection. Tout le monde ou presque doit pouvoir y accéder. C'est une porte ouverte.

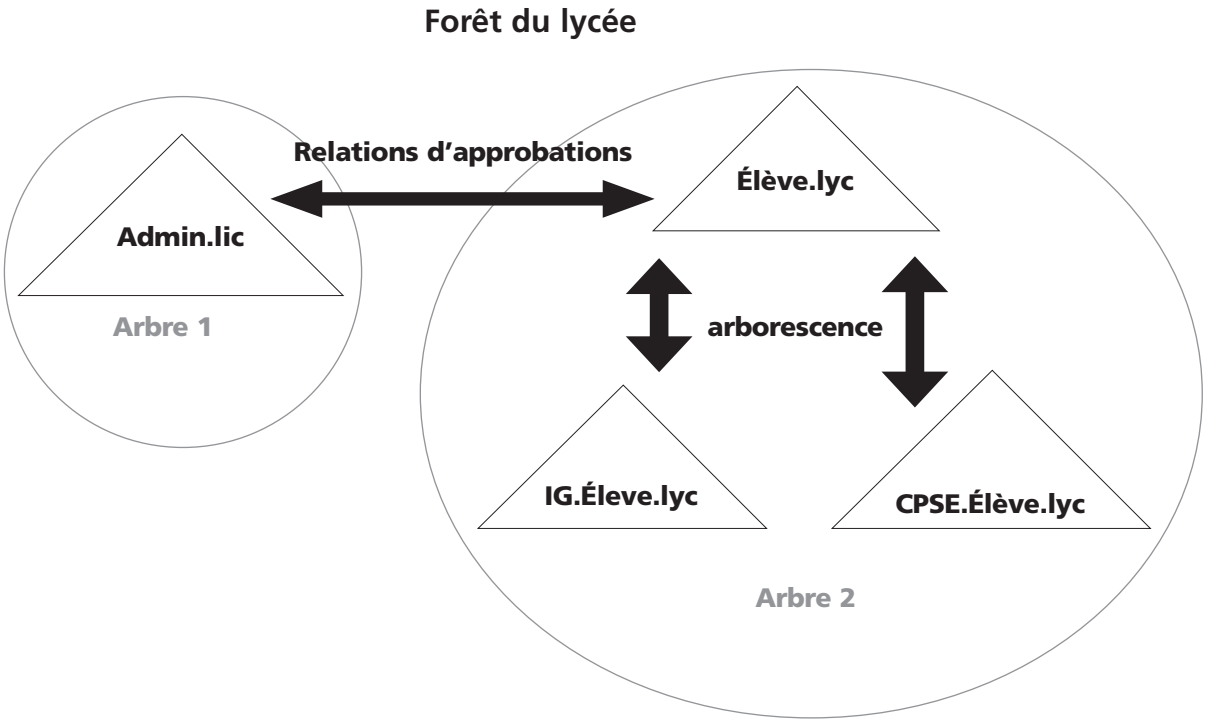
Le contrôleur de domaine est le cœur d'un réseau, il contient les « modes d'accès » au domaine. Il ne doit être accessible que par les administrateurs d'un domaine. Dans le réseau il est souvent protégé par des routeurs, enfermé physiquement dans des salles réservées. Deux mondes différents.

Séquence 3

Introduction à Active Directory

Cette séquence présente un système d'exploitation de type réseau 2003 Server.

Exercice 9



Rajoutez sur le schéma les relations d'approbation. Entourez les arbres de la forêt.

Exercice 10

Combien y a-t-il d'arbres ?

Il y a deux arbres.

Exercice 11

Admi.lic pourrait-il être un site différent ?

Non un site implique une certaine distance, dans un lycée 800 m est une distance considérable. Bon peut être qu'à Paris...

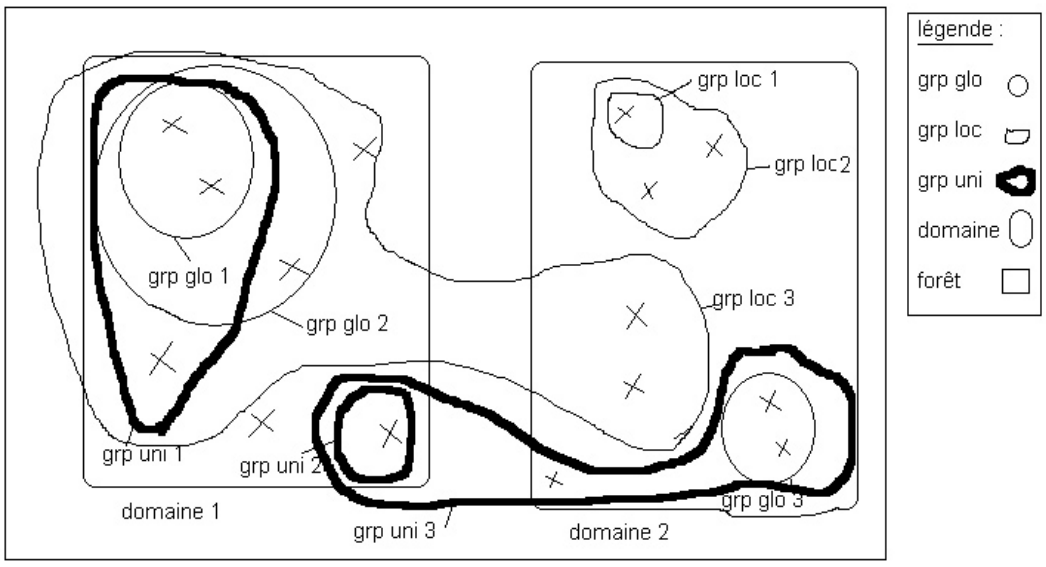
Exercice 12

Un compte utilisateur d'utilisateur intégré est-il un objet ou une classe ?

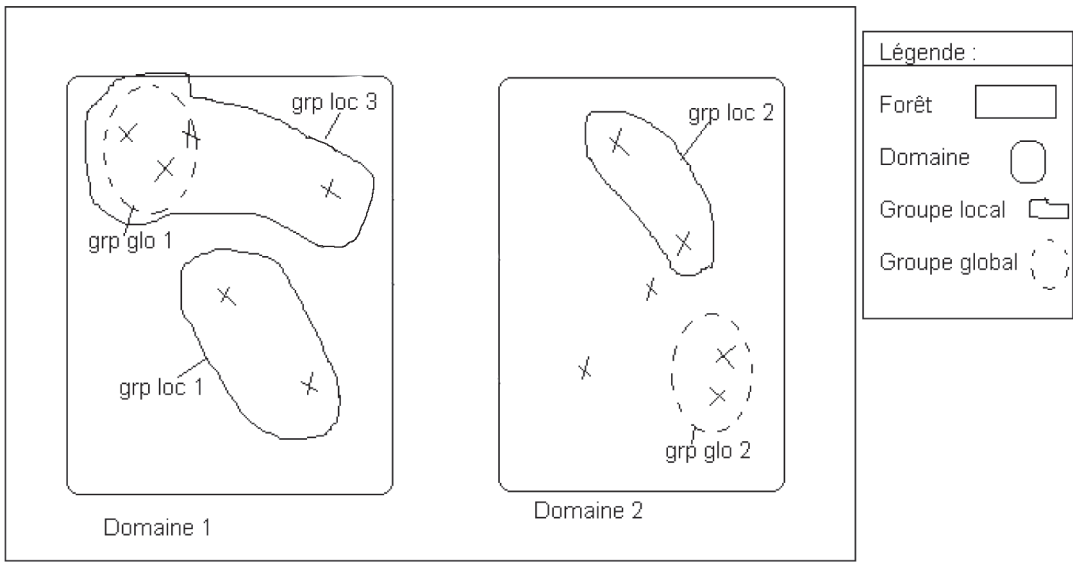
Un compte d'ordinateur ou d'utilisateur est une classe puisqu'il définit des attributs. Mais ici on parle d'un compte d'utilisateur intégré, quelque chose de particulier puis des valeurs définissent certains de ses attributs, donc la réponse est un objet.

Exercice 13

Faites un tableau récapitulatif ou un schéma permettant d'indiquer quels sont les membres de ces groupes dans les différents modes.



Voici un schéma pour le mode natif.



Voici un schéma pour le mode mixte. Il y a moins de possibilités.

Séquence 4

Gestion des authentifications

Cette séquence présente en détail le contrôle d'accès via la création de comptes et la création de groupes.

Exercice 14

Créez l'unité d'organisation Trouvetout qui vous servira pour l'atelier 3.

- Ouvrez votre console *MMC*.
- Dans la console *Utilisateurs et Ordinateurs d'Active Directory*, dans votre domaine, cliquez droit sur nouvelle *Unité d'organisation.*
- Nommez-la Trouvetout.

Exercice 15

Nous allons créer un compte pour le superintendant de l'équipe d'investigation. Marcel Dupin (descendant du célèbre Arsène Lupin) doit pouvoir enregistrer le résultat de ses recherches sur son répertoire personnel du serveur.

1. *Vous commencerez par créer le compte pour ce monsieur.*
   Ceci est effectué en plusieurs étapes : Création des unités, création du compte, création des dossiers, les partager et modification du compte.
   - Dans la console ***Utilisateurs et Ordinateurs d'Active Directory***, dans votre domaine, et dans l'unité Trouvetout, cliquez droit et créez l'unité d'organisation investigation.
   - Dans investigation, cliquez droit, ***Nouveau, Utilisateur.***
   - Entrez le nom Marcel Dupin et MaDupin comme nom ***d'ouverture de session***.
   - Suivre les différentes étapes de mot de passe.
   - Validez.
2. *Puis vous créez si ce n'est déjà fait le dossier RepPerso sur le disque dur C du serveur Balou2003 dans le dossier Trouvetout. C'est dans ce dossier que l'on retrouve tous les autres sous-dossiers de la société.*
   - Ouvrir ***l'explorateur Windows.***
   - Créez un dossier Trouvetout à la racine.
   - Créez un sous-dossier RepPerso.
   - Partagez le dossier RepPerso.
3. *La troisième étape consiste à donner l'accès à l'utilisateur sur la ressource (avec des droits et des permissions).*
   - Donnez les autorisations de modification sur RepPerso en cliquant sur le bouton ***autorisations.***
   - Donnez les droits de modification à MaDupin sur RepPerso dans l'onglet ***Sécurité***.
   - Validez.
   - Créez un sous-dossier investigation dans RepPerso.

4. Enfin vous modifierez l'attribut du répertoire personnel de Marcel dans Active directory.

- Retournez sur le compte utilisateur de Marcel Dupin avec la console ***Utilisateurs et Ordinateurs Active Directory***.
- Cliquez sur l'onglet ***Profils*** et complétez la ***zone dossier de base*** en rajoutant se connecter Z : sur \\Balou2003\Trouvetout\RepPerso\investigation\%username% dans la partie ***Dossier de base***.

Exercice 16

Pour comprendre le principe du profil errant, nous allons mettre en place plusieurs cas de figure. Dessinez un serveur dans une colonne, un poste client 1 dans une deuxième colonne et un poste client 2 dans une troisième colonne. Vous noterez chaque étape dans les bonnes colonnes et vous incrémenterez le numéro du profil à chaque changement.

Cas 1

Événements	Serveur	Client 1	Client 2	Remarques
Lundi				
9 h 10	P1 →	P1		À la connexion le profil est copié du serveur au poste client si sur le poste client la version du profil est différente de celle du serveur.
matin	P1	~~P1~~ P2		Nouveau fond d'écran avec photo de Cécilia. Profil local modifié, il devient P2.
Fin matinée	P1	~~P2~~ P3		Nouveau raccourci. Profil local modifié, il devient P3.
17 h 30	~~P1~~ P3 ←	P3		Déconnexion, le profil est copié du poste client sur le serveur où il remplace la version présente.

Le profil du serveur en fin de journée est P3 : C'est P1 auquel on a rajouté la photo de Cécilia, et le raccourci vers le dossier de travail.

Cas 2 : À 8 h 50 le profil du client 1 est P3.
À 17 h 30 le profil du serveur est P3.

Événements	Serveur	Client 1	Client 2	Remarques
Mardi				
8 h 50	P3	P3		À la connexion comparaison entre la version du profil du serveur et du client. Ici identique, donc pas de copie.
10 h	P3 →	P3	P3	Nouvelle connexion sur le poste 2. Le profil est copié du serveur au poste client 2.
Fin matinée	P3	P3	~~P3~~ P4	Nouveau fond d'écran avec photo de Martine. Profil local modifié, il devient P4.
Fin de matinée suite	~~P3~~ P4 ←	P3	P4	Déconnexion, le profil est copié du client sur le serveur où il remplace la version présente.
17 h 30	~~P4~~ P3 ←	P3	P4	Déconnexion, le profil est copié du client sur le serveur où il remplace la version présente.

Cas 3

Événements	Serveur	Client 1	Client 2	Remarques
Mercredi				
9 h 02	P3	P3	~~P4~~ P3	À la connexion le profil est copié du serveur au poste client si sur le poste client la version du profil est différente de celle du serveur. C'est le cas ici.
9 h 07	P3	P3	P3	À la connexion comparaison entre la version du profil du serveur et du client. Ici identique, donc pas de copie.
Matin	P3	~~P3~~ P5	P3	Nouveau fond d'écran avec photo de Nathalie et nouveau raccourci. Profil local modifié, il devient P5.
10 h	~~P3~~ P5	P5	P3	Déconnexion, le profil est copié du poste client sur le serveur où il remplace la version présente.
	P5	P5	~~P3~~ P6	Modification du paramètre d'affichage. Profil local modifié, il devient P6.
15 h	P5	P5	P6	Panne électrique.
16 h	P5	P5	~~P6~~ P5	À la connexion le profil est copié du serveur au poste client si sur le poste client la version du profil est différente de celle du serveur. C'est le cas ici.

Sur le poste 2 à 9 h 02 la photo en fond d'écran est celle de Cécilia.

Sur le poste 2 à 9 h 07 la photo en fond d'écran est la même que celle de Cécilia puisque les profils sont les mêmes.

À 10 h sur le poste 2 la photo est celle de Cécilia, il n'y a pas eu de demande de mise à jour par le client.

À 16 h le profil du poste 2 est P5.

Exercice 17

Dsadd ou "OU=administratif,OU=Trouvetout,DC=dom51,DC=loc"
Dsadd ou "OU=comptabilité,OU=Trouvetout,DC=dom51,DC=loc"
Dsadd ou "OU=investigation,OU=Trouvetout,DC=dom51,DC=loc"t
Dsadd ou "OU=informatique,OU=Trouvetout,DC=dom51,DC=loc"

Exercice 18

Ne pas oublier de créer un sous-dossier administratif dans RepPerso avec l'explorateur.

Seul Paul Bigout a été créé dans l'unité administratif, il manque les 4 autres membres.

Remarque

Avec 2003 Server pour des raisons de sécurité on crée un compte désactivé sinon, il faut écrire un mot de passe qui vérifie la stratégie 2003 Server et ce mot de passe serait en clair dans le fichier.

dsadd user *"CN=Pauline Hujier,OU=administratif,OU=Trouvetout,DC=dom51,DC=loc" -samid PaHujiet* ***-upn*** *PaHujiet@dom51.loc* ***-fn*** *Pauline* ***-ln*** *Hujier* ***-display*** *Pauline Hujier* ***-pwd * -hmdir*** *\\\\balou2003\\RepPerso\administratif\\%username%* ***-hmdrv*** *z :* ***-profile*** *\\\\balou2003\\Profils\\model*

dsadd user *"CN=Jean Duhamel, OU=administratif, OU=Trouvetout,DC=dom51, DC=loc"-samid JeDuhamelt* ***-upn*** *JeDuhamel@dom51.loc****-display*** *Jean Duhamel* ***pwd * -hmdir*** *\\\\balou2003\\RepPerso\\administratif\\%username%* ***-hmdrv*** *z :* ***-profile*** *\\\\balou2003\\Profils\\model*

dsadd user *"CN=Jeanine Guerelle, OU=administratif, OU=Trouvetout, DC=dom51,DC=loc"* ***-samid*** *JeGuerelle* ***-upn*** *JeGuerelle@dom51.loc* ***-display*** *Jeanine Guerelle* ***pwd * -hmdir*** *\\\\balou2003\\RepPerso\\administratif\\%username%* ***-hmdrv*** *z :* ***-profile*** *\\\\balou2003\\Profils\\model*

dsadd user *"CN=Julie Kernel, OU=administratif,OU=Trouvetout,DC=dom51,DC=loc"****-samid*** *JuKernel* ***-upn*** *JuKernel@dom51.loc* ***-display*** *Julie Kernel* ***pwd * -hmdir*** *\\\\balou2003\\RepPerso\\administratif\\%username%* ***-hmdrv*** *z :* ***-profile*** *\\\\balou2003\\Profils\\model*

Remarques

- En vous déplaçant dans la console Utilisateurs et Ordinateurs Active Directory vous pouvez voir les 4 utilisateurs. En ouvrant les onglets Profils vous aurez la désagréable surprise de remarquer que %username% n'a pas été remplacé par le vrai nom de l'utilisateur dans la zone dossier de base.
- Il est préférable de créer un fichier batch avec une boucle FOR et des paramètres pour faire un vrai script.

Exercice 19

dsadd user *"CN=Zinzin Reporteur,OU=investigation,OU=Trouvetout,DC=dom51,DC=loc"*

-samid *ZiReporteur*

-upn *ZiReporteur@dom51.loc* ***-display*** *Zinzin Reporteur* ***pwd * -hmdir*** *:\\\\balou2003\\RepPerso\\investigation\\%username%*

-hmdrv *z :*

dsadd user *"Milou Lechien,OU=investigation,OU=Trouvetout,DC=dom51,DC=loc"****-samid*** *MiLechien*

-upn *MiLechien@dom51.loc* ***-display*** *Milou Lechien*

pwd * -hmdir :*\\\\balou2003\\RepPerso\\investigation\\%username%*

-hmdrv *z :*

Remarque

Il est préférable de créer un fichier batch avec une boucle FOR et des paramètres pour faire un vrai script.

Exercice 20

Créez L'unité d'organisation Bandit dans Trouvetout et rajoutez y l'individu Raspoutine Charles en utilisant des commandes LDAP.

En mode console tapez directement les commandes suivantes :
Dsadd ou ''ou=bandit,OU=Trouvetout,DC=dom51,DC=loc"
Dsadd user "cn= Charles Raspoutine,ou=bandit,ou=Trouvetout,dc=dom51,dc=loc,"–samid ChRaspoutine, -upn ChRaspoutine@dom51.loc, -display CharlesRaspoutine,

Vous pouvez aussi les enregistrer dans un fichier dont l'extension est bat.

Exercice 21

Voici une partie du contenu du fichier **creergrploc** :

dsadd group "CN=admess_loc,OU=administratif,OU=Trouvetout,DC=dom51,DC=loc"**-secgrp yes -scope l -samid** admess_loc

Voici une partie du contenu du fichier **creergrpglo** :

dsadd group "CN=admess_glo,OU=administratif,OU=Trouvetout,DC=dom51,DC=loc"**-secgrp yes -scope g -samid** admess_glo

Exercice 22

Supprimez Bandit et tout ce qui s'y trouve en LDAP.

Suppression de l'unité d'organisation bandit et de tout ce qu'elle contient
Dsrm -subtree "ou=bandit,ou=Trouvetout,dc=dom51,dc=loc"

Séquence 6

Les stratégies d'AD

Cette séquence termine la liste des objets gérés dans la base de données d'Active directory : les stratégies et la sécurité qu'elles apportent.

Exercice 23

Quels sont les paramètres de stratégie de groupes résultants pour les objets utilisateurs dans l'unité et pourquoi ?

Les stratégies s'appliquent dans l'ordre du plus grand au plus petit niveau.

Vont s'appliquer dans l'ordre : GPO1, GPO2, GPO3 puis quand GPO4 arrive il y a un conflit avec la première et la troisième des stratégies. C'est la dernière mise en place qui gagne. En fin de compte, ne seront appliquées que les stratégies GPO2 et GPO4.

Exercice 24

On souhaite qu'une application antivirus soit installée sur tous les postes du domaine. On souhaite qu'office ne soit installé que sur l'unité d'organisation administrative, et que le logiciel de comptabilité ne soit installé que sur l'unité Comptabilité à l'exception de celui de Michael Junit, que faire ?

L'objet GPO1 est une stratégie qui s'applique au niveau du domaine, elle permet d'installer à distance l'antivirus.

L'objet GPO2 est une stratégie qui s'applique au niveau de l'unité d'organisation Administratif et qui permet d'installer à distance Office.

L'objet GPO3 est une stratégie qui s'applique au niveau de l'unité d'organisation Comptabilité pour installer à distance le logiciel de Compta. On y applique un filtre dans l'onglet Sécurité : pour le groupe créé pour l'occasion contenant Michael Junit, on refuse d'appliquer la stratégie de groupe.

Séquence 7

Le DNS ou tout ce que vous n'avez jamais voulu savoir sur le DNS

Cette séquence vous permettra de connaître et de maîtriser le DNS.

Exercice 25

Que fait la commande ping monpremier ?

Si le DNS du poste d'où a été lancé le ping est bien configuré, c'est l'adresse IP du poste monpremier qui est rendue. Le mappage est effectué par le serveur DNS. Puis on voit les 4 paquets envoyés et bien reçus.

Exercice 26

Pour les 4 cas de figure ci-dessous vous expliquerez le circuit des demandes de résolution de nom des machines via un schéma.

1. *Monpremier, via son logiciel navigateur Internet Explorer, veut communiquer avec Mondernier mais il ne connaît pas son adresse IP.*

Monpremier regarde dans son fichier host, comme il n'y est pas il envoie la demande à son serveur DNS. Le serveur DNS regarde s'il fait autorité sur la zone concernée. C'est le cas, donc il connaît la réponse, il renvoie la réponse positive au client DNS en faisant autorité.

2. *Même question à l'identique que la une, Monpremier refait exactement la même demande (votre réponse sera différente elle !).*

Il a de la mémoire Monpremier, plus exactement un cache, c'est son solveur local qui va lui transmettre l'adresse IP, puisqu'il l'a déjà demandé.

3. *Monpremier, via son logiciel de navigation, veut communiquer avec Monpépère (il n'y a pas d'erreur dans le nom de la machine !).*

Après avoir regardé sans grand succès dans son cache local, le client DNS envoie sa requête à son serveur DNS. Le serveur pense qu'il y n'y a pas de suffixe que Monpépére fait partie de sa zone d'autorité. Il ne trouve pas Monpépère et comme il fait autorité sur cette zone il ne transmet pas la demande à un autre serveur DNS et renvoie une réponse négative au client.

4. *Monpremier, via son navigateur, veut communiquer avec le serveur du site : www.binome.recherche.fr.*

Monpremier commence par regarder dans son cache local au cas où il aurait déjà la réponse. Ce n'est pas le cas donc, il demande à son serveur DNS. Le serveur DNS ne fait pas autorité sur la zone aussi va-t-il lancer une requête récursive pour connaître la réponse en demandant à un de ses serveurs racine de faire la recherche pour lui. Il obtiendra l'adresse de chaque serveur de chaque niveau, jusqu'à obtenir le serveur faisant autorité sur la zone (réponses de références). Il pourra ainsi indiquer à son client l'adresse IP lors d'une requête positive.

Exercice 27

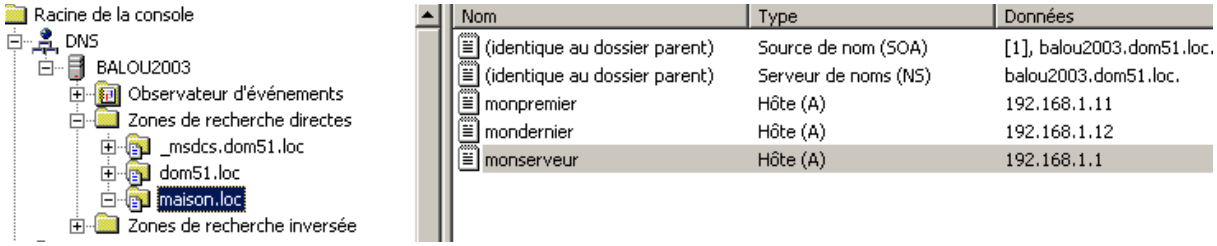
Sur votre serveur essayez de créer les zones, les domaines et les hôtes du premier schéma.

On va utiliser la console magique et lancer le service DNS.

Étape 1 créer une nouvelle zone maison.loc sur notre serveur.

Étape 2 créer les hôtes dans la nouvelle zone.

Voici le résultat a obtenir.



Exercice 28

Voici que votre réseau s'agrandit. Il contient des sous-domaines et plusieurs zones. Pour vous aider à répondre aux questions suivantes, vous disposez de l'arborescence des noms de domaines du réseau et des machines qui s'y trouvent, ainsi que des fichiers de configurations des zones.

1. Puisque monpremier.maison.loc demande à son serveur DNS Monserveur.chambre1.appart1.maison.loc sans regarder dans son cache voici les requêtes :

Expéditeur	Destinataire	Objet
Monpremier.maison.loc	Monserveur.chambre1.appart1.maison.loc	Req1 : quelle est l'adresse IP de postelili.chambre1.appart1.maison.loc
Postelili.chambre1.appart1.maison.loc ne fait pas parti de la zone de Monserveur.chambre1.appart1.maison.loc. Le serveur ne fait autorité que sur maison.loc mais il a délégué la zone en question à un autre serveur dont il a le nom dans son fichier..		
Monserveur.chambre1.appart1.maison.loc	postejojo.appart1.maison.loc	Req2 : quelle est l'adresse IP de postelili.chambre1.appart1.maison.loc
postejojo.appart1.maison.loc fait autorité sur la zone appart1.maison.loc et connaît la réponse		
postejojo.appart1.maison.loc	Monserveur.chambre1.appart1.maison.loc	Réponse faisant autorité : 192.168.1.15
Monserveur.chambre1.appart1.maison.loc	Monpremier.maison.loc	Réponse positive : 192.168.1.15

2. Pour une recherche itérative, c'est au client de faire ses recherche en fonction des aides des serveurs.

Expéditeur	Destinataire	Objet
Monpremier.maison.loc	Monserveur.chambre1.appart1.maison.loc	Req1 : quelle est l'adresse IP de postelili.chambre1.appart1.maison.loc
Postelili.chambre1.appart1.maison.loc ne fait pas parti de la zone de Monserveur.chambre1.appart1.maison.loc. Le serveur ne fait autorité que sur maison.loc mais il a délégué la zone en question à un autre serveur dont il a le nom dans son fichier.		
Monserveur.chambre1.appart1.maison.loc	Monpremier.maison.loc	Réponse par référence adresse toi au serveur postejojo.appart1.maison.loc dont l'adresse IP est 192.168.1.16
Monserveur.chambre1.appart1.maison.loc	postejojo.appart1.maison.loc	Req2 : quelle est l'adresse IP de postelili.chambre1.appart1.maison.loc
postejojo.appart1.maison.loc fait autorité sur la zone appart1.maison.loc et connaît la réponse		
postejojo.appart1.maison.loc	Monpremier.maison.loc	Réponse positive faisant autorité : 192.168.1.15

3. Si tu ne le sais pas encore c'est que les réponses précédentes étaient fausses : postejojo.appart1.maison.loc bien sur !

4. C'est écrit dans le fichier : serveursécure.maison.loc.

5. NON

6. Voici comment est modifié le fichier de la **zone appart1.maison.loc** :

Contenu du fichier de configuration de la zone appart1.maison.loc.

```
appart1.maison.loc.  IN        SOA    postejojo.appart1.maison.loc.  admi.maison.loc.
                                      (20 18000 3600 72000  86400)

                       NS   postejojo.appart1.maison.loc.
                       NS   postecoco.appart1.maison.loc.
                       NS   serveursécure.maison.loc.

postelili.chambre1.appart1.maison.loc.        IN      A       192.168.1.15
postefred.appart1.maison.loc.  IN      A       192.168.1.13
postejojo.appart1.maison.loc.  IN      A       192.168.1.16
```

Ainsi que la zone **maison.loc**

Contenu du fichier de configuration de la zone maison.loc

```
maison.loc.  IN        SOA    monserveur.chambre1.appart1.maison.loc.  admi.maison.loc.
                              (3 36000 3600 360000 86400)
; deux serveurs de noms de la zone
                       NS   monserveur.chambre1.appart1.maison.loc.
                       NS   serveursécure.maison.loc.

; délégation de la zone appart1.maison.fr avec ses deux serveurs de noms
appart1.maison.loc. IN         NS   postejojo.appart1.maison.loc.
                       NS   postecoco.appart1.maison.loc.
                       NS   serveursécure.maison.loc.
```

; et délégation de la zone appart2.maison.fr avec deux serveurs de noms

```
appart2.maison.loc. IN NS   sonserveur.appart2.maison.loc.
                       NS   serveursécure.maison.loc.
```

; déclaration des adresses des hôtes faisant autorité

```
monpremier.maison.loc.          IN      A       192.168.1.11
mondernier.maison.loc.          IN      A       192.168.1.12
routeur.maison.loc.             IN      A       192.168.1.8
routeur.maison.loc.             IN      A       192.168.2.8
```

; déclaration des adresses des serveurs des sous-domaines

```
monserveur.chambre1.appart1.maison.loc  IN      A       192.168.1.1
postejojo.appart1.maison.loc.           IN      A       192.168.1.16
sonserveur.appart2.maison.loc.          IN      A       192.168.2.1
serveursécure.maison.loc.               IN      A       192.168.1.10
postecoco.appart1.maison.loc.           IN      A       192.168.1.14
```

Séquence 8

Le DHCP

Cette séquence montre l'utilité du DHCP et à travers différents exemples, les multiples configurations.

Exercice 29

Où va une trame ayant comme adresse destinataire 255.255.255.255 ? Quel nom donne t-on à une trame ayant comme adresse destinataire 255.255.255.255 ?

Une trame ayant pour adresse 255.255.255.255 n'a pas de direction précise elle est diffusée à travers tout le réseau. Tous les postes la lisent et ceux qui peuvent répondre le font. Cette trame est un broadcast.

Exercice 30

Complétez les trames en rajoutant les adresses des expéditeurs et des destinataires.

Étape	Nom trame	Ad MAC source	Ad IP source	Ad IP destinataire
1	DHCPDISCOVER	client	0.0.0.0	255.255.255.255
2	DHCPOFFER	serveur	Ip serveur	Nvelle IP client
3	DHCPREQUEST	client	Nvelle IP client	255.255.255.255
4	DHCPNACK	serveur	IPmserveur	IPclient

Exercice 31

Décrivez les trames circulant lors de la première demande de connexion d'un poste du sous-réseau B.

Le client ne connaît pas l'adresse d'un serveur DHCP donc il effectue un broadcast. Il n'y a pas de serveur sur son sous-réseau donc il n'obtient pas de réponse aux 4 demandes qu'il effectue, donc il prend une adresse dans la plage réservée de Microsoft.

Si vous avez dit qu'un serveur DHCP du sous-réseau répondait, honte à vous 2 fois.

UN BROADCAST ne passe pas les routeurs !!!

Pour pallier ce premier obstacle il faut mettre en place un agent relais sur le routeur et c'est facile, cochez la case indiquée sur l'image écran.

Honte à vous une deuxième fois car en plus de dire des bêtises vous n'êtes pas observateur. Un routeur indique qu'il y a deux 2 réseaux différents à faire communiquer. Sur le serveur DHCP on a créé qu'une seule étendue pour un sous-réseau, donc le serveur n'a pas d'adresse IP correspondant à ce sous-réseau.

Il faut rajouter une nouvelle plage réseau sur un serveur DHCP.

Exercice 32

Si on rajoute un serveur DHCP dans le sous-réseau B, comment cela fonctionnera-t-il pour les clients du sous-réseau A et du sous-réseau B ?

Si on relie le sujet il n'est pas question d'une nouvelle étendue sur le serveur DHCP du sous-réseau B, donc si on considère que suite à l'exercice 3, on a configuré l'agent relais sur le routeur et une nouvelle étendue sur un serveur DHCP de la zone A, les clients du sous-réseau B obtiendront une adresse IP via le routeur du serveur DHCP du sous-réseau A.

Si on configure une zone dans dans le sous-réseau B, il faudra qu'elle soit différente de celle définit dans le sous-réseau A. Car les serveurs DHCP ne communiquant pas on ne peut pas savoir qu'une adresse a déjà été donnée.

Exercice 33

Quand un poste client renouvelle-t-il son bail ?

Un client renouvelle son bail à 50% du temps de son bail directement à son serveur DHCP.
Puis au 87,5% du temps via un broadcast.
À chaque fois que le poste client redémarre.
À chaque fois que le poste client effectue un renew.
Si un idiot a supprimé l'allocation sur le serveur par inadvertance.

Exercice 34

Dans une classe de cours de BTS IG réseaux chaque élève dispose d'un serveur et d'un client qu'il partage avec son binôme. Tous sont sur le même sous-réseau. Que se passe-t-il pour les clients s'ils mettent tous en place un serveur DHCP ?

Et si tous les élèves sont sur des sous-réseaux différents ?

Il y a plusieurs cas de figures. De toute façon c'est le premier serveur qui a répondu qui gagne un nouveau client et non pas le serveur DHCP le plus proche du client. Si chaque élève propose une plage d'adresse différente, pas de conflit à l'horizon pour les postes clients, sinon bonjour la pagaille, car même pour l'exercice 34, les serveurs DHCP ne communiquent pas entre eux.

Si chacun est sur un sous-réseau différent, ça marche mais espérons qu'il n'y est pas d'agent relais !

Séquence 9

Les protocoles

Cette séquence présente une série de protocoles utilisés à travers les différents services d'un réseau.

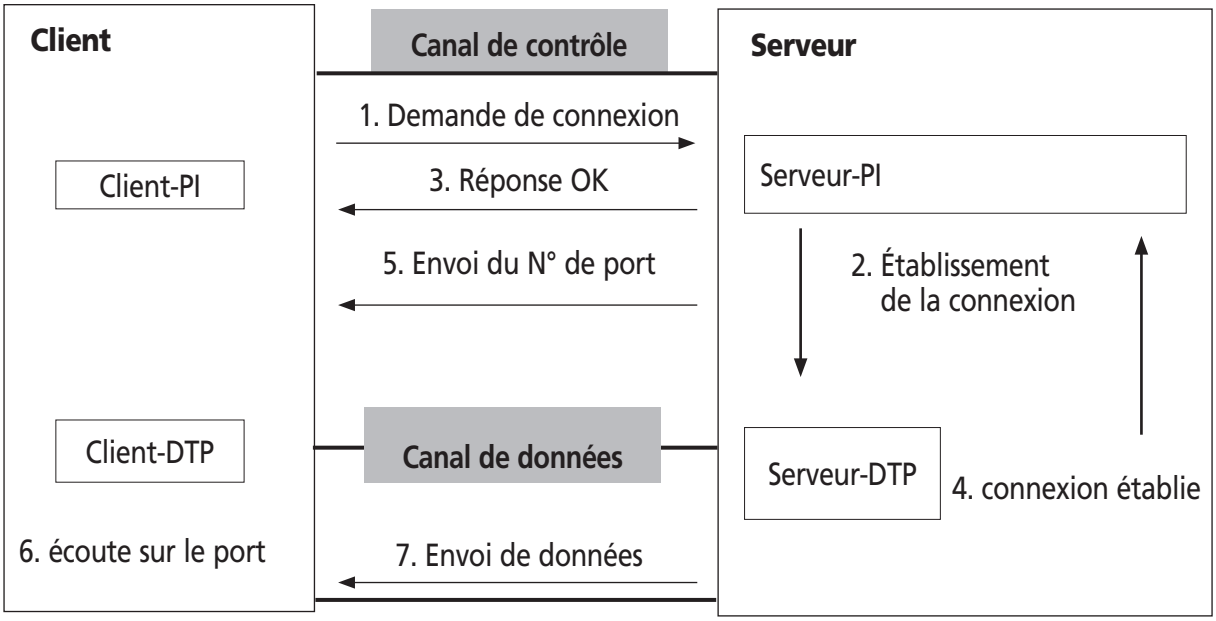
Exercice 36

Quel processus agit sur quel canal ?

DTP gère le canal des données et établit la connexion. Le PI exécute les commandes reçues sur le canal de contrôle et les applique sur le canal des données.

Exercice 37

Faites un schéma d'un tel échange de flux en représentant les canaux et les différents process.



Exercice 38

En faisant un telnet du client sur le port 25 envoyez un mail sur le serveur.

Client : Telnet 25
MAIL yoyo@ici.fr
Serveur : OK
Client : RCPT Toto@okmag.fr
Serveur : OK
Client : DATA Salut, tu vas bien ?
Serveur : OK

Exercice 39

Quand on est client DNS en quel mode est-on ?

Dans une console DOS, tapez la commande IPCONFIG /ALL
La réponse est hybride. D'abord le client interroge son serveur DNS puis il fait un broadcast.
Il n'a pas été trouvé de nouveau nom pour le DNS, puisque celui-ci « remplace le WINS ».

Exercice 40

Comment un ordinateur en b-node recherche t-il un ordinateur du réseau ?

utilisation du fichier hosts
utilisation du fichier lmhosts
diffusion UDP

Exercice 41

Comment un ordinateur en h-node client WINS recherche-t-il un ordinateur sur le réseau ?

requête au serveur WINS
utilisation du fichier lmhosts
diffusion UDP

Exercice 42

Comment un ordinateur en h-node client DNS recherche-t-il un ordinateur sur le réseau ?

utilisation du fichier hosts
requête au serveur DNS
diffusion UDP

Exercice 43

Vous allez installer une autorité de certificat sur un contrôleur de domaine. Il faut que le serveur IIS soit présent et qu'il accepte de gérer la technologie ASP.

C'est un composant qu'il vous faut installer.

Pour vérifier le bon fonctionnement vous rajouterez sur votre client un composant enfichable certificat, dans une console MMC que vous créerez pour l'occasion.

Pour installer une autorité de certificat sur votre serveur Balou :
le serveur IIS ainsi que la structure ASP.NET doivent être installés.

- Dans *le panneau de configuration* cliquez sur *Ajouter/Suppression de composants Windows.*
- Sélectionnez *Services de certificats.*
- Au message d'erreur, il vous faudra accepter ceci comment une information coulant de source. Cliquez sur *OK.* Pour des raisons de sécurité vous ne changerez pas de nom de machine ni l'appartenance au domaine.

- Vous n'avez qu'un seul serveur il est donc *Autorité racine d'entreprise* (comme pour le domaine).
- Votre nom d'autorité est certificat-balou
  DC=Dom51,DC=loc
  Rien de très inconnu.
- Paramétrez le lieu d'enregistrement des bases de données.
- Pour la durée 6 mois suffiront.
- Vous activerez les pages ASP.

Bravo l'installation de votre serveur est terminée !

Pour effectuer une demande certificat auprès d'une autorité de certification :

- Connectez-vous en tant qu'administrateur du domaine sur le client.
- Créez sur le client une console MMC.
- Ajoutez le composant logiciel enfichable *certificat* et choisissez *mon compte d'utilisateur* par exemple.
- Développez le composant enfichable de la console.
- Cliquez droit sur le dossier *Personnel*.
- Choisissez *Toutes les tâches*, puis *Demander un nouveau certificat...*
- Choisissez le type de certificat.
- Et en fonction de la sécurité choisissez de protéger la clé privée par un mot de passe.
- Choisissez Balou comme Autorité de certificat.
- Saisissez le nom du nouveau certificat.

On peut aussi créer un certificat via une page WEB (vous avez installé un serveur IIS) *http://balou2003/certsrv*

Séquence 12

Un Serveur de bases de données

Dans cette séquence vous rajouterez la notion de serveur de bases de données avec l'exemple de SQL Server.

Exercice 44

Dans la société Trouvetout, seuls les membres de l'unité d'organisation Investigateurs pourront accéder à la base de données Disparus. De plus ils n'auront pas tous les mêmes droits. Quel genre d'accès faut-il prévoir ? Doit-on utiliser un seul accès commun pour plusieurs utilisateurs où chaque utilisateur existera ?

Les informations sont sensibles. Il faudra aussi créer des administrateurs de SQL server. On préférera une sécurité SQL Server et Windows pour l'installation du serveur de BDD. Chaque personne aura sa propre identification sur SQL, ce qui nous permettra de tracer ces opérations. Faut-il reprendre les utilisateurs AD ou créer de nouveaux accès ? Ces personnes sont habituées au secret et sont capables de se rappeler un nouveau mot de passe !

Séquence 13

La sécurité

Cette séquence est un petit récapitulatif sur la sécurité en informatique.

Exercice 45

Voici un tableau récapitulatif sur la sécurité. À vous de le remplir !

Tableau récapitulatif sur la sécurité.

Environnement Besoins	Poste de travail	Réseau local	Réseau local connecté à Internet
Matériel	Outils de sauvegarde : – Disquette – CD onduleur	1 serveur centralise la gestion des : – utilisateurs – fichiers – impressions – sauvegarde bandes K7 Raid 1 ..5 Routeur pour sous réseau	1 serveur : – proxy – routeur – pare feu
Logiciel, SE Windows 2003 SQL Server	Protection du micro par mot de passe : – Bios – Système Verrouiller le clavier NTFS : fichiers antivirus	Active directory : – Unité – Groupe – Utilisateur (mp, profils) – Stratégie – Utilisateurs avec des droits spéciaux Gestionnaires de fichiers : – Répertoires partagés – Droits d'accès Raid 1..5 Création de sous réseau Passerelle pour sous réseau	Proxy Pare feu routeur

Correction des ateliers

Atelier 1
Mise en domaine

Exercice 1 

Avec l'utilisateur Lambda, sous Windows XP Pro, lancez la commande MMC et rajoutez le composant enfichable 'service sur le poste serveur'. Puis essayez de lancer ce composant dans la console MMC de l'utilisateur Lambda.

Et cela ne marche pas, il fallait me croire. Ce composant donne un accès au serveur, mais Lambda n'étant pas un membre du groupe administrateur, ne peut pas utiliser le serveur.

Merci les stratégies Windows.

Atelier 2

Les droits et permissions

Exercice 2

Création des comptes utilisateurs Tif et ptiAnnie, puis testez-les.

Dans votre console MMC que vous avez enregistré sous le nom de ma console à l'atelier précédent, vous utilisez l'utilitaire Utilisateurs et Ordinateurs Active Directory.

- Dans l'unité d'organisation Users, cliquez droit dans la fenêtre de droite.
- Sélectionnez *Nouveau* puis *Utilisateur*.
- Nommez le Tif dans les zones : Prénom, UPN et nom d'ouverture de session antérieur à Windows 2000.
- Cliquez sur le bouton *suivant*. Entrez votre mot de passe 2 fois.
- Cochez seulement le mot de passe n'expire jamais.
- Cliquez sur le bouton *Suivant*
- Cliquez sur le bouton *Terminer*

Même chose pour ptiAnnie.

Exercice 3

Création du groupe local explorateur qui contient le groupe Voyageurs et ptiAnnie.

- Sur le container *Users*, cliquez droit sur *Nouveau* puis sur *groupe*.
- Modifiez les attributs de groupe en sélectionnant local, nommez-le explorateur.
- Cliquez droit Propriétés sur le groupe explorateur, Dans l'onglet Membre rajoutez le groupe Voyageurs et l'utilisateur ptiAnnie.
- Cliquez sur OK.

Exercice 4

Laissez les droits tels quels dans chacun des onglets. Qu'observez-vous pour Tif et pour ptiAnnie, peuvent-ils faire les mêmes choses ? Est-ce normal ?

Les 2 utilisateurs font partie du groupe Tout le monde et ont la possibilité de voir le dossier partagé dans le voisinage réseau.

Au niveau de la sécurité ils font partie du groupe Utilisateurs du domaine donc ils peuvent lire le contenu du dossier partagé. Aucun des 2 n'a plus de permissions ou de droits que l'autre.

Exercice 5

Si l'on donne la permission de modifier au groupe Tout le monde à l'aide du bouton Autorisations, que se passe-t-il pour les mêmes lascars ?

Les 2 utilisateurs ne peuvent rien faire de plus, car les droits du groupe Utilisateurs n'ont pas changé.

Exercice 6

Supprimez le groupe Utilisateurs et rajoutez le groupe Explorateurs dans l'onglet Sécurité et donnez lui le droit de modification, que se passe-t-il pour les mêmes lascars ?

On vient de permettre à Tif de créer des fichiers des répertoires à l'intérieur du dossier partagé. ptiAnnie ne fait pas partie de ce groupe et donc ne peut rien faire de plus que de voir le partage, elle n'y rentre plus.

Exercice 7

On enlève le groupe Tout le monde dans les autorisations que l'on remplace par le groupe Explorateur en lecture, que se passe- t-il pour les mêmes lascars ?

Tif voit le partage, rentre dans le partage et lit les fichiers mais ne peut rien modifier.

PtiAnnie ne sait même pas que le partage existe, elle ne le voit plus dans le voisinage réseau.

Exercice 8

On donne le droit de modifier à ce groupe Explorateur à l'aide du bouton Autorisations, que se passe-t-il pour les mêmes lascars ?

Rien de neuf pour ptiAnnie et Tif peut modifier des fichiers et créer des dossiers.

Exercice 9

On donne le droit de lecture au groupe Explorateurs dans l'onglet Sécurité, que se passe-t-il pour les mêmes lascars ?

Rien de neuf pour ptiAnnie et Tif ne peut que lire les informations.

Exercice 10

À quoi sert le bouton Autorisations et à quoi sert l'onglet Sécurité ?

On a remarqué qu'il faut laisser le partage ouvert pour les utilisateurs qui ont besoin d'y accéder en leur donnant l'autorisation de modification. On affine avec les droits suivant les besoins. Il y a 2 filtres l'un après l'autre. Si le premier ne laisse rien passer, le second ne sert à rien. C'est la notion de passoire à tamis successif de plus en plus fin.

Si les autorisations n'existent pas on ne voit même pas le partage.

Ainsi si les autorisations sont en lecture ou même modification et qu'il n'y a pas de droit, on peut voir le partage mais pas son contenu.

Si on rajoute des droits de lecture, on voit le contenu du partage.

Si on rajoute des droits de modification, on peut rajouter des informations par exemple.

Exercice 11

Voici une série d'utilisateurs, de groupes et un dossier partagé, vous indiquerez pour les utilisateurs et chacun des groupes leurs droits finaux après héritage.

On suppose que les permissions sont ouvertes en mode modification au moins pour tout le monde.

Le groupe Arc En ciel n'étant membre d'aucun autre groupe, il garde son contrôle total.

L'utilisateur Indigo est membre de tous les groupes, il obtient donc le plus gros droit, le contrôle total qu'il hérite du groupe Arc En Ciel.

Le groupe Pastels n'hérite de personne, il garde son droit de lecture sur Cadeaux

Le groupe Huile n'hérite de personne, il garde son droit d'écriture sur Cadeaux.

Le groupe Couleurs hérite des 2 groupes précédents. C'est le droit d'écriture qui l'emporte, ce qui ne change rien pour lui.

Exercice 12

Expliquez en détail ce que fait chaque ligne et rajoutez les commandes manquantes pour venir à bout de l'exercice.

On crée un dossier Voyages qui contient 5 sous dossiers. Puis on le partage.

On donne le droit d'écriture à Tif au dossier partagé Voyages et donc à tous les sous dossiers qu'il contient, par héritage. Cette commande n'enlève pas les droits des Administrateurs.

Pour que cela marche, il faut en plus :

- Ouvrir les autorisations au groupe explorateur.
- On doit modifier les droits et les appliquer au groupe explorateur et non pas seulement à Tif.

Atelier 3

Gestion des utilisateurs

Remarques

Comment faire pour connaître les attributs ?

Exporter les objets d'Active Directory dans un fichier texte et le lire (pensez CSVDE, pensez LDIFDE)

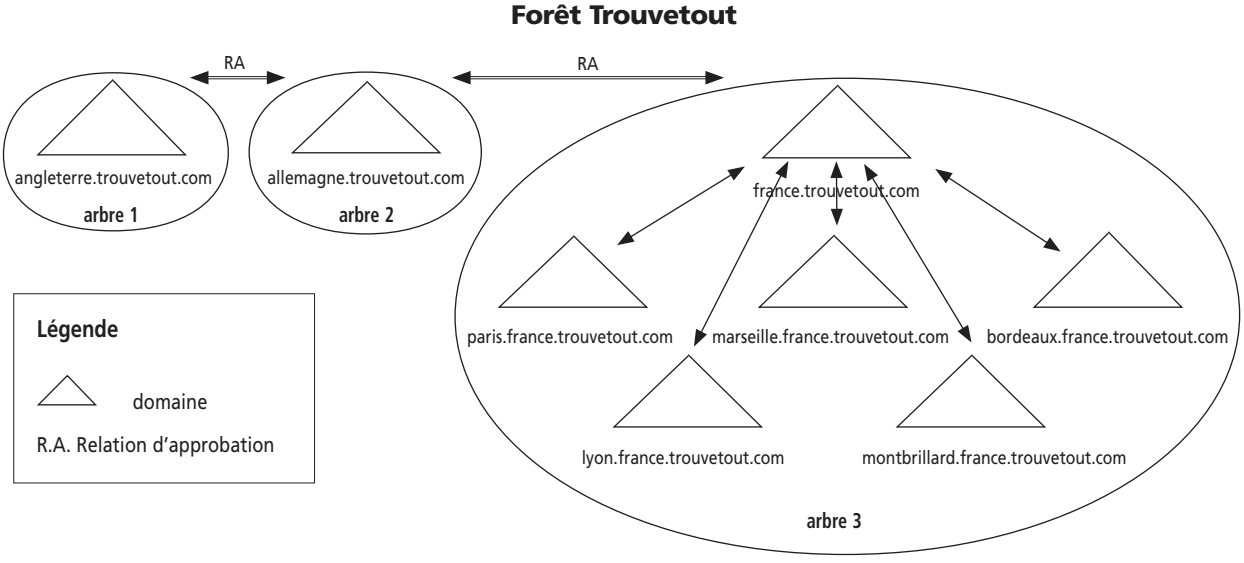
Votre script ne marche pas ?

J'ai bien précisé qu'il fallait être à 300 % dans cet atelier. Ici les erreurs de frappe ne pardonnent pas. Quand vous créez un objet, les unités les dossiers dont il fait référence existent-ils ? Attention à la casse ! Ne mettez pas d'espace dans le nom entier de l'objet (le DN).

Exercice 13

Proposez un schéma de la forêt Trouvetout.

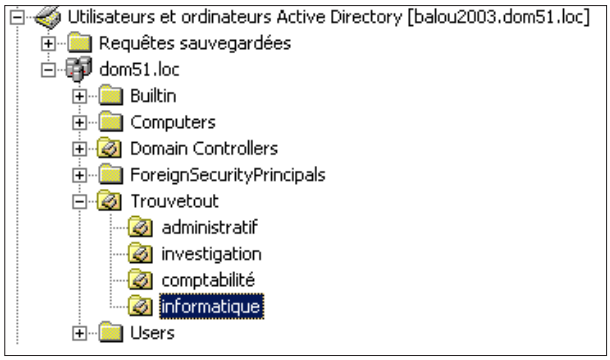
Les 3 sites formeront des arbres différents en relation d'approbation. Le site de la France est une arborescence. Il y a 8 domaines. Le domaine France.trouvetout.com a une relation père-fils avec 5 autres domaines : Paris.france.trouvetout.com, Marseille.france.trouvetout.com, Montbrilland. france.trouvetout.com, Bordeaux.france.trouvetout.com et Lyons.france.trouvetout.com.



Exercice 14

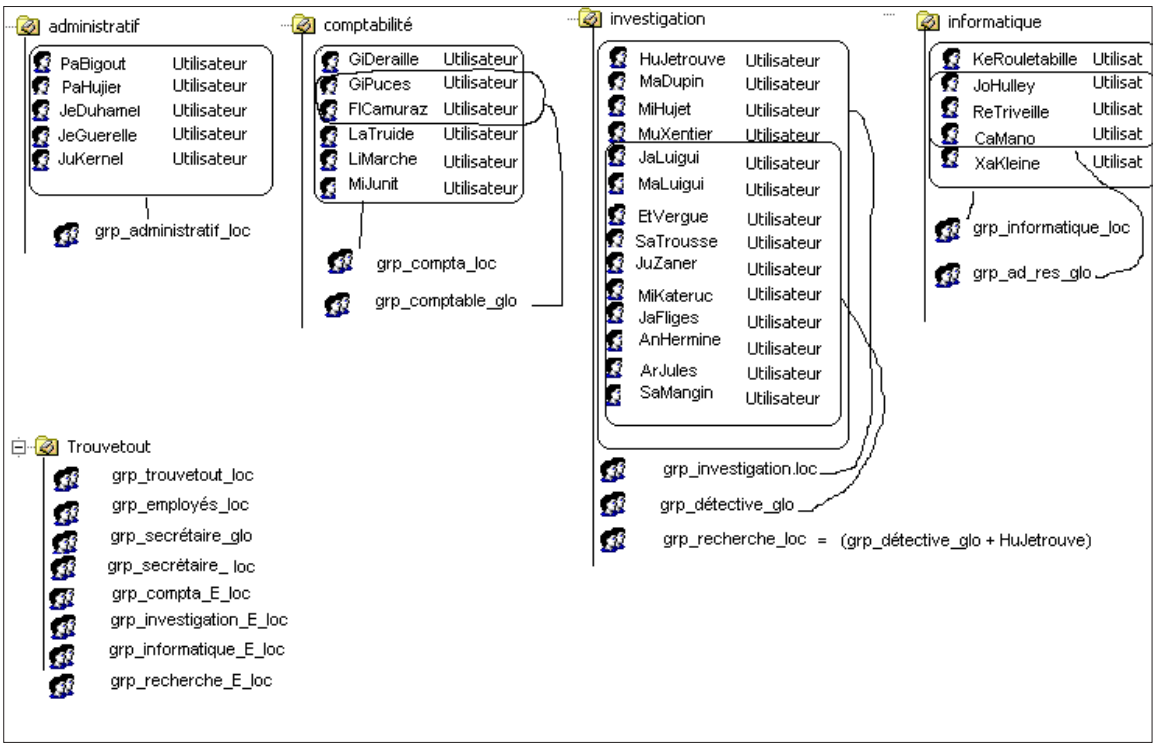
Proposez un schéma récapitulant les différentes unités d'organisations, les différents groupes, locaux, globaux et universels, les utilisateurs, les permissions, les ressources partagées.

Notre politique de nom de compte est ici de prendre les 2 premières lettres du prénom auxquelles on rajoute le nom de la Personne. Ne seront en majuscule dans ce nouveau nom que la première et troisième lettre. On évite ainsi les doublons en choisissant seulement les prénoms ou les noms.



Il y a 4 unités d'organisations. Il y a 12 groupes locaux et 4 groupes globaux.

Les deux premiers schémas nous servent de base pour travailler dans la console *Utilisateurs* et *Ordinateurs Active Directory* et le troisième liste les ressources utilisées avec les droits et permissions.



Les groupes locaux et globaux qui se trouvent dans l'unité Trouvetout, c'est-à-dire au niveau supérieur des 4 sous unités regroupent des personnes se trouvant dans différentes unités.

Sur le schéma il était difficile d'en montrer les membres avec des ensembles aussi le contenu est détaillé ci-dessous :

grp_trouvetout_loc = grp_administratif_loc + grp_compta_loc + grp_investigation_loc + grp_informatique_loc

grp_employés_non_info_loc = grp_compta_loc + grp_investigation_loc + PaHujier + JeDuhamel + JeGuerelle + JuKernel

grp_employés_loc = grp_employés_non_info_loc + grp_informatique_loc

grp_secrétaire_glo = PaHujier + Mihujet + MuXentier
grp_secrétaire_loc = grp_secrétaire_glo
grp_compta_E_loc = grp_compta_ loc + PaBigout
grp_investigation_E_loc = grp_investigation_loc + PaBigout
grp_recherche_E_loc = grp_recherche_loc + PaBigout
grp_informatique_E_loc = grp_informatique_loc + PaBigout

Lorsque l'on créera les comptes utilisateurs, il ne faudra pas oublier de faire en sorte que :

- Les utilisateurs des unités Administratif et Comptabilité n'aient accès qu'à un seul poste qui peut être nommé (impossible à mettre en place si vous n'avez pas plusieurs clients pour vérifier).
- Les utilisateurs des unités Administratif, Comptabilité et Investigation aient un profil obligatoire.
- Les utilisateurs du groupe recherche_loc aient la possibilité de se connecter au réseau de l'extérieur.

Ressources	Permissions de Partage	Droits NTFS
Trouvetout		
Echange	grp_trouvetout_loc *modif*	grp_trouvetout_loc *lecture*
Administratif		grp_administratif_loc *modif*
Communication		Pabigout *modif* grp_employés_loc *lecture*
Comptabilité		grp_comptabilité_E_loc *modif*
Informatique		grp_informatique_loc *modif*
Investigation		grp_investigation_E_loc *modif*
Recherche		grp_recherche_E_loc *modif*
Monttouve		PaBigout, GiDeRaille, HuJetrouve KeRouletabille *lecture*
Monttouveadmi		GiDeraille, HuJetrouve, KeRouletabille PaBigout *lecture modif*
Monttouvecompta		HuJetrouve, KeRouletabille PaBigout GiDeraille *lecture modif*
Monttouveinfo		PaBigout, GiDeRaille, HuJetrouve KeRouletabille *lecture modif*
Monttouveinvesti		PaBigout, GiDeRaille, KeRouletabille HuJetrouve *lecture modif*
Profils	grp_trouvetout_loc *modif*	grp_employé_non_info_loc *lecture* grp_informatique_loc *modif*
RepPerso		
Administratif		*Seul l'utilisateur du compte a les droits de modifications sur son répertoire personnel.*
Comptabilité		
Informatique		*RepPerso est innaccessible du voisinage réseau, on y accède par le poste de travail.*
Investigation		

Ressources	Permissions de Partage	Droits NTFS
Imprimante_reprographie		grp_secrétaire_ loc modif
Imprimante_compta		grp_comptabilité_loc modif
Imprimante_Tous		grp_trouvetout_loc modif

Dans l'image qui précède sur les ressources, on remarque que seuls 3 dossiers sont partagés. Par héritage les dossiers fils sont partagés. J'aurais pu partager directement Trouvetout, mais ce dossier est 'artificiel' il n'existe que parce que l'exercice existe, il n'est pas utile dans la réalité. De plus il n'a pas besoin d'être visible à travers le réseau.

Pour que tout fonctionne correctement et que vous, administrateur, ait accès aux dossiers pour en modifier les droits et permissions, il ne faut pas oublier de rajouter l'utilisateur *Administrateur*, et enlever les autres groupes et utilisateurs non cités sur le schéma.

Pensez à bloquer l'héritage au niveau du parent en appliquant les autorisations au dossier seulement pour vous simplifier le travail.

Personne n'a le contrôle total hormis le compte Administrateur.

Exercice 15

Créez les différentes ressources partagées.

Pour créer des ressources, utilisez *l'explorateur* ou le *poste de travail*. Cliquez droits sur les dossiers pour les partager. Pour appliquer des permissions cliquez sur le bouton *Autorisation* dans l'onglet *Partage* et pour les droits sélectionnez l'onglet *Sécurité*.

Les ressources qui sont des imprimantes ne peuvent êtres créées, elles apparaissent seulement dans le schéma de l'exercice 2. Toutefois si vous avez une imprimante réseau ou non vous pouvez la déclarer sous les 3 noms et lui appliquer la sécurité adéquate.

Rappel sur les droits NTFS et les permissions de partage

Imaginons que les permissions et les droits soient des portes. Un utilisateur pour accéder à un objet doit passer 2 portes. Si la première est fermée, il n'a aucune chance d'ouvrir la seconde.

Donc si un utilisateur a la permission de modification sur le partage il peut passer la première porte. On affine les possibilités de l'utilisateur lors de la mise en place des droits : lecture, modification...

Les permissions NTFS sont cumulatives, la moins restrictive s'applique, sauf la permission ***aucun accès***. Quand un utilisateur fait partie de groupe attention au résultat.

Rappel sur le profil et le répertoire personnel

Un profil ne se crée sur le serveur que lorsque l'utilisateur se connecte sur un poste. A ce moment le dossier sur le serveur contenant son profil est vide ; il se remplit dès qu'il se déconnecte.

Contrairement, un répertoire personnel est créé sur le serveur dès la création du compte utilisateur.

Très important

Depuis la version W2003 Server, une multitude de protections a été mise en place.

- **Pour les profils**

  Quand on crée un utilisateur avec la console AD, si l'administrateur veut regarder le contenu du profil d'un utilisateur pour le rendre obligatoire par exemple, il n'en a pas la possibilité, il faut qu'il se l'approprie.

  Une autre solution consiste à créer les dossiers Profils des utilisateurs sur l'explorateur avant que l'utilisateur ne se connecte et les droits NTFS seront corrects.

  On peut également en cas de profil obligatoire, le créer au préalable puis rediriger tous les utilisateurs sur ce profil particulier, ce qui nous permet de ne pas écrire de fichiers batch pour créer autant de dossier profils que d'utilisateurs.

  Si on crée un profil obligatoire, il serait bon de le protéger, aussi les utilisateurs n'auront pas les droits NTFS de ***Modification*** sur ce dossier mais seulement la ***Lecture***.

- **Pour le répertoire personnel**

  Celui-ci étant créé avec la création du compte utilisateur, le dossier hérite des droits NTFS du dossier parent. L'administrateur a tous les droits ainsi que l'utilisateur. On se rappelle combien il est dangereux de laisser le contrôle total à un utilisateur et il faut le lui supprimer immédiatement !

En fonction de ces informations, voici un modus vivendi.

Création des 3 dossiers partagés et mise en place des droits et permissions une fois tous les comptes créés et les groupes aussi. Il est important d'avoir une vision de l'ensemble, car les groupes seront créés avant les utilisateurs.

Le dossier Echange

On doit ouvrir au maximum les permissions de partage et restreindre par les droits NTFS.

Le dossier RepPerso

Il est partagé il y a des permissions de *contrôle total* de partage et NTFS pour l'Administrateur. On ne peut pas y accéder par le réseau, donc il n'y a pas de modification possible à distance. Les utilisateurs ont un accès en mode modification via leur poste de travail avec l'unité z.

Lorsque vous créerez les comptes utilisateurs, pas besoin d'attendre qu'ils soient membres de groupes pour créer les répertoires personnel.

La valeur de l'attribut du répertoire Personnel est :

\\Baloo2003\RepPerso*l'unitédu compte*\%username%

Le dossier Profils

Il doit permettre la création du profil par l'utilisateur du groupe informatique. Les autres employés n'ont un accès qu'en *lecture* seule.

Au niveau du partage les permissions *modif* pour le groupe grp_trouvetout_loc. Les droits NTFS sont : *modif* pour le groupe grp_informatique_loc et *lecture* pour le groupe grp_employés_non_informatique.

Profil pour tous les employés non informaticiens

Ils ont tous le même profil et il est obligatoire.

- On crée un utilisateur model avec *Active Directory*
- Avec *l'explorateur* cliquez droit sur le dossier partagé Profils, dans l'onglet *Partage*, cliquez sur le bouton *Autorisations*. Rajoutez l'utilisateur model en mode *modification*.
- Rajoutez le aussi dans l'onglet *Sécurité*.
- Avec la console *Active Directory*, cliquez droit *Propriétés* sur le compte utilisateur model.
- Dans l'onglet *Profil* rajoutez le chemin suivant : \\Baloo2003\Profils\%username%
- Quand vous cliquez sur le bouton Appliquer, %username% est remplacé par model.
- Connectez-vous et déconnectez-vous avec l'utilisateur model sur le poste client.
- Avec *l'explorateur* cliquez droit sur le dossier Model dans le dossier Profils pour afficher les *propriétés*.
- Un message vous dit que vous n'en avez pas le droit sauf si vous en devenez propriétaire. On va le faire.
- Cliquez sur le bouton *Paramètres avancés* puis dans l'onglet *Propriétaire*.
- Cochez la case *Remplacer le propriétaire des sous-conteneurs et des objets*.
- Vous pouvez maintenant voir le contenu du dossier model.
- Renommez le fichier NTuser.dat en NTuser.man afin de rendre ce profil obligatoire.
- Dans la vraie vie, vous auriez avant rajouté les raccourcis sur le bureau...
- À chaque fois que vous créerez des comptes utilisateurs non informaticiens, le chemin du profil sera : \\Baloo2003\Profils\model

Profil pour les informaticiens

Créez les comptes des utilisateurs.

Rendez-les membres du groupe grp_informaticien_loc

Donnez les droits NTFS de modification à ce groupe sur le dossier partagé Profils.

Modifiez les comptes des informaticiens et rajoutez la valeur de l'attribut profil avec pour chemin : \\Baloo2003\Profils\%username%

L'administrateur n'y aura aucun accès, mais qu'importe maintenant !

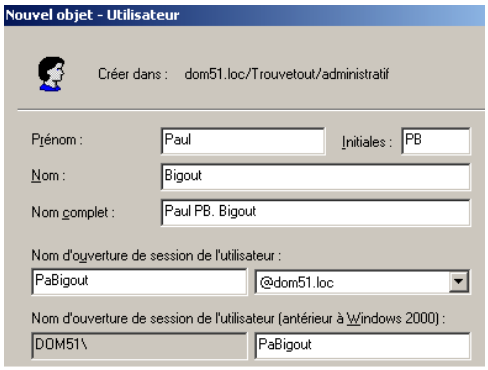
Exercice 16

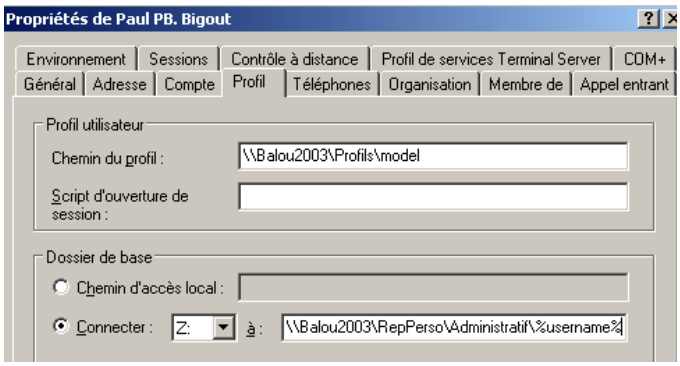
Créer les comptes de Paul Bigout et de James Luigui en fonction des différentes exigences.

Remarque : ***Les groupes ne seront créés que dans le dernier exercice, aussi tout ne fonctionnera qu'une fois la séquence terminée.***

- Ouvrez la console *Utilisateurs* et *Ordinateurs Active Directory*.
- Placez-vous dans l'unité Trouvetout et sa sous unité administratif.
- Cliquez droit *Nouveau Utilisateur*.
- Nom de compte: PaBigout.

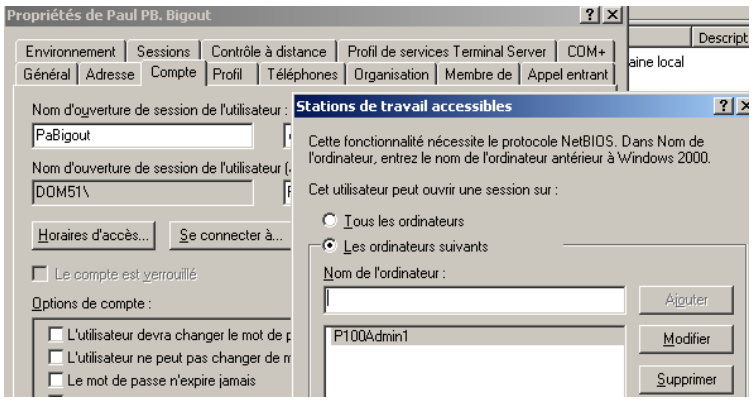
Une fois le compte créé, on va le modifier pour lui rajouter un profil, un dossier personnel et faire en sorte qu'il ait un poste attribué.





Son profil est de type obligatoire. Il doit avoir été créé au préalable avec un model comme indiqué dans le modus vivendi ou comme le model.

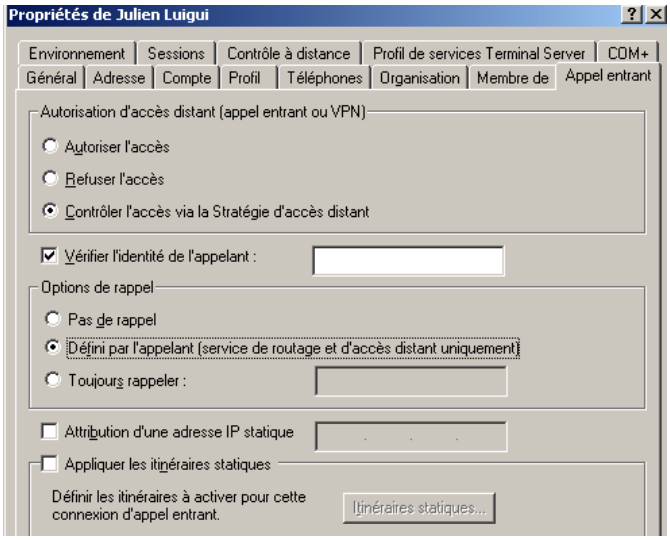
- Pour attribuer un poste précis à un utilisateur, configurez l'onglet *Compte* puis cliquez sur le bouton *Se connecter à...*



Dans l'image écran suivant le nom du poste dépend d'une numérotation et d'un service. Si vous souhaitez que cela marche sur votre réseau, n'utilisez pas ce nom mais le nom de votre poste client !

Autre méthode

Si vous avez suivi le modus vivendi vous pouvez faire une copie du model utilisateur, le modifier en conséquence et le déplacer dans la bonne unité.



Pour créer James Luigui vous procéderez de la même manière en remarquant que son répertoire personnel se trouve dans le dossier Investigation et non pas Administratif.

De plus, Paul Luigui n'est pas restreint dans l'utilisation d'ordinateur, donc la dernière étape n'est pas à reproduire et il doit pouvoir ouvrir une session via internet.

Cela nécessite une série d'autres manipulations qui configure un VPN. Cette étape peut faire l'objet d'une activité et nécessite d'autres connaissances et plus de matériel.

Exercice 17

Avec un script LDIF créez les 9 détectives restants.

Problème : Ceci ne peut marcher que si, le profil model a déjà été créé et pour les permissions sur le dossier RepPerso, il faudra attendre la fin de l'exercice 7.

Exercice 18

Écrire le fichier contenant des commandes active directory (LDAP) pour créer l'ensemble des comptes de Montbillard manquants.

dsadd user «CN=RémiTreville,OU=informatique,OU=Trouvetout,DC=dom51,DC=loc» -samid ReTriveille -upn ReTriveille@dom51.loc -fn Rémi -mi RT -ln Triveille -display Rémi Triveille -pwd * -hmdir \\Baloo2003\RepPerso\Informatique\%username% -hmdrv z: -mustchpwd yes

Exercice 19

Faites en sorte que chacun ait accès aux ressources partagées voulues. (Membres de groupes attribution des droits et permissions...)

- Avec la console *Utilisateurs* et *Ordinateurs Active Directory*, remplir les groupes locaux et globaux en fonction du tableau de l'exercice 24.
- Utilisez *l'Explorateur* et placez-vous sur les dossiers partagés pour appliquer les permissions et droits aux groupes en fonction du tableau de l'exercice 24.

Atelier 4

Exercice 20

Empêchez tous les utilisateurs exceptés ceux du service Informatique de :

- *– modifier leur menu Démarrer ;*
- *– modifier leurs paramètres Réseau ;*
- *– modifier les paramètres d'Internet Explorer.*

Soit on applique la stratégie sur l'unité Trouvetout et on bloque l'héritage pour l'unité Informatique, soit on applique la stratégie sur l'unité Trouvetout et on filtre pour le groupe Informatique qu'il faudra créer, soit on applique la stratégie sur les 3 unités concernées. Le plus propre est la deuxième solution qui sera explicitée ici.

1. Dans la console *Utilisateurs* et ordinateurs *Active Directory*, sur l'unité Trouvetout, créer une nouvelle stratégie. Appelée protection.

Dans *Configuration utilisateur*, choisir *Modèles d'administration*, puis *Menu Démarrer* et *Bureau*.

Activer l'option : *désactiver le glisser déplacer des menus contextuels* dans le Menu Démarrer

On vient d'empêcher la modification du menu Démarrer. Voyons le reste.

Dans *Configuration utilisateur* choisir *Modèles d'administration* puis *Réseau*, enfin *Connexion réseau* et *accès distant*

Activer l'option : *interdire l'accès aux propriétés d'une connexion au réseau local.*

Mais il faut l'interdire aussi à partir du panneau de configuration.

Dans *Configuration utilisateur* choisir *Modèles d'administration* puis *Panneau de configuration* enfin *Connexion réseau et accès distant* et *Masquer les applications du panneau de configuration* spécifié : la liste comprenant des éléments ayant l'extension .cpl.

Dans *Configuration utilisateur*, choisir *Modèles d'administration* puis *Composants Windows et Internet Explorer* cliquer sur *panneau de configuration*

Désactiver *l'onglet connexion.*

2. Application du filtre : on sélectionne notre stratégie, on clique sur le bouton *Propriétés*, dans l'onglet *sécurité* on rajoute le groupe local informatique et on coche *refuser d'appliquer la stratégie de groupe.*

Le groupe local informatique contient tous les utilisateurs de l'unité informatique.

Exercice 21

Créez une stratégie qui configure les postes de l'entreprise Trouvetout avec les paramètres indiqués ci-dessus.

Dans la console *Utilisateurs et ordinateurs Active Directory*, sur l'unité Trouvetout, créer une nouvelle stratégie, appelée proxy.

Dans Configuration *utilisateur* cliquer sur *Paramètre Windows* puis sur *Maintenance d'Internet* choisir *Connexion* et enfin *paramètres du proxy*

- Activer *paramètre proxy* et choisir Parici 8081
- Ne pas utiliser Parici pour l'intranet.

Remarque : cette stratégie s'applique car elle est placée avant la stratégie empêchant de modifier les paramètres d'Internet Exploreur. Stratégie lancée par la connexion de l'utilisateur.

Exercice 22

Écrivez le fichier batch qui crée ce raccourci vers la ressource CE et créez la stratégie qui permettra de rajouter ce raccourci.

1. Avec le bloc note écrire le fichier suivant :

Fichier batch **rac.bat**

net use x : \\balou2003\CE

2. Pour le retrouver facilement le copier sur le bureau avant de le copier dans le bon dossier stratégie.

3. Dans la console *Utilisateurs et ordinateurs Active Directory*, sur l'unité Trouvetout, créer une nouvelle stratégie nommée virtuel.

Dans *Configuration utilisateurs*, *Paramètres Windows*, *scripts*, double cliquer sur *scripts d'ouverture de session.*

Cliquer sur le bouton *ajouter* puis sur le bouton *Parcourir.*

4. Vous voyez le nom tarabiscoté de la stratégie, alors avec votre explorateur copiez-y le fichier rac.bat. C'est fait ?

5. Revenez sur votre stratégie pour ouvrir votre fichier et le lier à la stratégie.

Remarque : la ressource CE a été partagée et les utilisateurs ont les permissions et les droits adéquats.

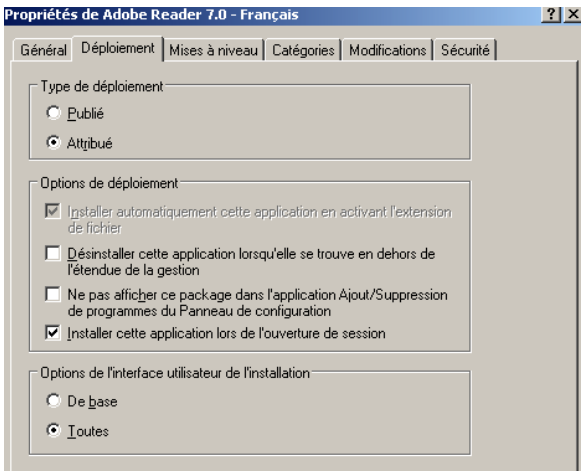
Exercice 23

Écrivez la stratégie qui permet d'installer à distance ce logiciel au démarrage de la session des utilisateurs.

Avant toute chose, le logiciel que l'on veut installer est particulier puisqu'il a une extension .msi. Donc il vous faut en trouver un sur un CD ou sur internet. Acrobat Reader est distribué en msi. On peut appliquer cette opération à une machine, comme à un utilisateur aussi on choisit en fonction.

On commence par copier le fichier dans un dossier partagé accessible par tous les membres de l'unité comptabilité en lecture.

- Dans la console *Utilisateurs et ordinateurs Active Directory*, sur l'unité comptabilité, créer une nouvelle stratégie.
- Choisir *configuration de l'utilisateur.*
- Double-cliquez sur *Paramètres du logiciel*, puis sur *Installation de logiciel.*
- Cliquez droit sur *Installation de logiciels*, pointez sur *Nouveau*, puis cliquez sur *Package*.
- Cliquez sur le package Windows Installer à attribuer, puis cliquez sur *Ouvrir.*



- Dans la boîte de dialogue *Déploiement du logiciel*, on doit choisir entre 3 options.
- Cliquez sur *Attribué* puisque vous voulez que cela soit fait automatiquement lors de l'ouverture de session de l'utilisateur.
- Attendez un instant c'est assez long.
- Vous allez maintenant modifier les options pour que l'installation se lance bien à l'ouverture de session. Bouton droit, *propriété sur votre package*.

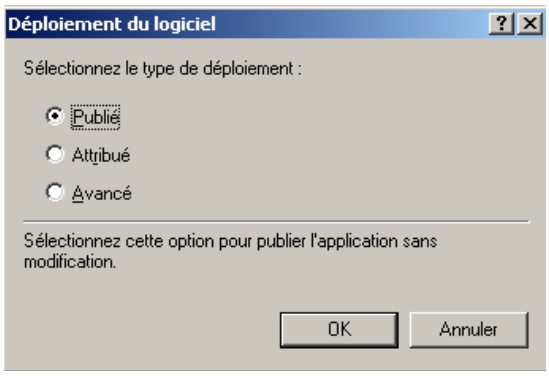
Remarque : Cochez comme sur l'image écran *Installer cette application lors de l'ouverture de session*.

Exercice 24

Écrivez la stratégie qui permet aux utilisateurs d'installer ce logiciel enregistré sur le serveur à partir du Panneau de Configuration Ajout/Suppression de Programmes.

Dans la console *Utilisateurs et ordinateurs Active Directory*, sur l'unité informatique, créer une nouvelle stratégie.

On commence par copier le fichier dans un dossier partagé accessible par tous les membres de l'unité comptabilité en lecture.



- Choisissez *configuration de l'utilisateur*.
- Double-cliquez sur *Paramètres du logiciel*, puis sur *Installation de logiciel*.
- Cliquez droit sur *Installation de logiciels*, pointez sur *Nouveau*, puis cliquez sur *Package*.
- Cliquez sur le *package Windows Installer à attribuer*, puis cliquez sur *Ouvrir*.
- Cliquez sur *Publier* pour l'avoir dans ajout/suppression de programme.

Atelier 5

Mise en place d'un serveur de sites : IIS

Exercice 25

Avec quoi testez-vous le site ? à partir de quelle machine ? Et qu'obtenez-vous ?

À partir du poste client, c'est-à-dire la machine sous XP Pro, on lance un navigateur, comme Internet Explorer, Modzila ...

Dans la barre de navigation on tapera l'adresse IP 192.168.5.1 du serveur de site.

La belle page que vous avez réalisée, ne s'affiche pas, au lieu de ça, le message d'erreur « impossible d'afficher la page » apparaît.

Si vous obtenez un autre message d'erreur c'est que vos connexions réseau, ou que vos configurations ne sont pas correctes.

Pensez à arrêter le site par défaut.

Le gestionnaire de service IIS affiche bien la page monprem.hrml dans la partie droite lorsque la sélection est sur premier alors ?

Alors quand on utilise un assistant on utilise un outil programmé pour des sites classiques et d'habitude la page de démarrage d'un site s'appelle index.htm ou default.htm ou default.asp. Ce n'est pas le cas chez nous.

Pour modifier la page de démarrage, dans les propriétés du site, choisir l'onglet document, supprimer les 3 entrées par défaut et rajouter monprem.html.

Retournez sur votre client, effacez l'historique et le cache et relancez la recherche. C'est mieux non ?

Exercice 26

Créez un deuxième site que vous appellerez deuxième, ouvrant lançant la page madeux.html du site Deux sur le serveur. Testez-le, que se passe-t-il ?

C'est la première page qui s'affiche et non pas la deuxième. Une solution serait d'arrêter le premier site, mais un serveur de site peut lancer plusieurs sites à la fois !

Exercice 27

Configurez le deuxième site sur le port 81. Comment testez-vous le site ? Que se passe t- il ?

Dans la barre de navigation, on rajoute sans espace, le numéro du port précédé de deux points.

Ça marche.

Exercice 28

Testez vos 2 sites en les appelant avec les noms DNS.

Si le deuxième site ne s'affiche pas c'est peut être que vous avez oublié de modifier le port en remettant le port par défaut 80 !

Exercice 29

Créez un troisième site qui appelle la page matr.html du dossier Trois sur Innetpub\wwwroot. On accède à ce site en tapant simplement http://troisieme dans la barre de navigation. Testez ce site à partir du serveur, du client connecté au domaine et non connecté. Expliquez vos choix et les résultats.

Dans la console DNS il n'est pas utile de créer un nouveau domaine. Mais doit on créer un Alias ou un nom d'hôte troisième ?

Si on crée un Alias dans notre domaine qui sera mappé sur notre serveur :

- Appel du site du serveur : OK
- Appel du site du poste client connecté au domaine : OK
- Appel du site du poste client non connecté au domaine : OK

Le client connecté ou non a comme serveur DNS celui qui sait mappé l'alias avec le nom d'hôte, donc il n'y a pas de problème.

Si on crée un nom d'hôte qui sera mappé sur l'adresse IP :

- Appel du site du serveur : OK
- Appel du site du poste client connecté au domaine : OK
- Appel du site du poste client non connecté au domaine : OK

Le serveur DNS mappe le nom DNS avec la bonne adresse IP.

Donc avec la console IIS on configure le site avec un nom d'hôte ou d'alias sans indiquer qu'il s'agit du domaine courant.

Exercice 30

Et si maintenant vous utilisez l'adresse IP du serveur dans votre navigateur, que se passe-t-il ?

C'est le premier site qui sera lancé, c'est-à-dire le premier qui a été relié avec l'adresse Ip.

Exercice 31

Que faire pour interdire au poste client d'accéder à tous nos sites en une seule modification d'autorisation ?

On peut obtenir le même onglet de sécurité du répertoire en se positionnant non pas sur un site mais sur le dossier sites Web qui englobe tous les sites. Et donc restreindre pour tous les sites web en une seule fois l'accès au poste client. On remarque que si l'on observe les propriétés de tous les sites dans la console IIS, il a rajouté la restriction sur chacun d'eux.

Exercice 32

Et si on interdit l'accès à tous les sites par la méthode précédente et qu'on l'autorise expressément sur le site premier, que se passe-t-il ?

C'est encore un problème de cumul de droits qui l'emportera ? Dans notre cas les droits ont la même « force », mais sont-ils appliqués en même temps ? Dites avez-vous lu la réponse à la question précédente ? Si oui c'est quoi encore que ce délire ? Il n'est pas question de cumul de droit puisque il rajoute à tous les sites la restriction, il faut supprimer cette restriction. Un point c'est tout.

Exercice 33

Comment faire pour que votre client accède à la première page du site mais ne puisse pas voir la seconde ?

Comme on peut restreindre l'accès sur tous les sites, sur un seul site, on peut le restreindre sur une page de la même manière. Donc dans la console IIS, après avoir sélectionné la page suite.html dans le site premier, on supprime l'accès pour le poste client. Tout simple !

Atelier 6

Exercice 34

Quelle est la différence entre un alias et un nom d'hôte ?

Un nom d'hôte permet d'associer un nom DNS à une adresse IP.

Un alias est un autre nom donné à une machine qui sert de serveur IIS ou serveur FTP.

Par exemple votre serveur a comme nom d'hôte Balou2003.dom53.loc et pour les besoins, il peut être serveur FTP et porter le nom d'alias www pour mon domaine premier.mfr.

Dans un Intranet, si on utilise des noms d'hôtes pour serveur, seuls les clients du domaine pourront accéder à l'intranet. En effet le serveur DNS sait faire la traduction. Pour que l'intranet soit visible de l'extérieur, son serveur doit être un alias. Question de zone d'autorité.

Exercice 35

Vous créerez en mode graphique la zone maison.loc et vous rajouterez les enregistrements qui vont bien.

On ne peut pas vraiment reproduire le schéma avec toutes les machines qui font autorité sur les zones, on peut simuler avec notre serveur en créant 3 zones et les hôtes de chacune des zones. On ne peut pas les imbriquer les unes dans les autres.

Vous pouvez faire le même exercice sous Linux en modifiant les bons fichiers.

Atelier 7

Le DHCP

Exercice 36

Comment savoir que c'est effectivement le serveur DHCP qui a fourni une adresse au client ?

En regardant sur la console DHCP du serveur dans Baux d'adresse on remarque qu'une adresse a été utilisée par un poste dont l'adresse MAC correspond à celle de votre poste client.

Exercice 37

Comment le serveur attribue-t-il les adresses IP aux postes clients ?

Le serveur n'attribue pas les adresses au hasard il prend la première de libre dans sa plage. Donc notre client étant le seul il a toujours l'adresse 192.168.5.3

Exercice 38

Comment vérifier qu'un client garde toujours la même adresse à chaque renouvellement du bail ?

On peut raccourcir le bail à 1 minute et sur le poste client taper ipconfig/.all toutes les minutes on remarque que le bail est différent mais que l'adresse est la même.

Exercice 39

Réservez l'adresse 192.168.5.5 pour votre client et vérifiez.

Placez vous dans la console DHCP et cliquez droit sur *Réservations* et rajoutez la réservation comme dans l'exemple en rajoutant l'adresse MAC.

Regardez dans les baux d'adresses après un release et un renew sur le client pour vérifier.

Exercice 40

Que se passe-t-il si vous créez une autre étendue dont la plage est : 192.168.5.7 à 192.168.5.10 ?

C'est impossible il y a un conflit.

Exercice 41

Mettez en place le routeur pour le sous réseau 192.168.7.0 donnez à votre client une adresse statique 192.168.7.7 et testez votre réseau avec des ping. Faites en sorte que votre client ait une adresse dynamique. Rajoutez une étendue sur le serveur 192.168.7.1 à 192.168.7.5 en excluant l'adresse IP 192.168.7.1 qui est réservée au routeur. Testez. Quelle est l'adresse du client. ?

Le client n'obtient pas d'adresse comprise dans la plage d'étendue du serveur DHCP mais il en prend une dans la plage réservée de Microsoft.

Exercice 42

Mettez en place un logiciel de capture de trames sur le routeur. Capturez les trames sur la patte du routeur du réseau 192.168.7.0 et faites un release et un renew sur le client. Analysez les trames.

Dans la capture de trame on remarque 4 demandes (suivant le logiciel en clair) DHCPDISCOVER qui sont des broadcast et donc qui n'obtiennent aucune réponse.

Exercice 43

Sur le client faites une demande de renouvellement de bail tout en capturant les trames. Qu'observez-vous sur le client et sur le routeur ?

Le client obtient la première adresse disponible 192.168.7.2 pour lui dans la plage de son sous réseau car comme le montre la capture de trame la demande passe le routeur ainsi qu'une réponse.

Exercice 44

Soit 2 sous-réseaux A et B, sur chacun on trouve, un routeur, un client et un serveur. Ce qui fait un total de 6 machines. On peut se poser la question du pourquoi 2 routeurs ? Facile il y a en fait 3 sous réseaux dans cet exemple avec un sous réseau qui ne contient pas de poste. Il y a un seul serveur DHCP pour distribuer des adresses dynamiques dans les sous réseaux A et B. Sur quel routeur doit-on installer l'agent relais ?

On installe l'agent relais sur le routeur du réseau sans DHCP, donc sur le réseau B.

Atelier 8

Le routage

Exercice 45

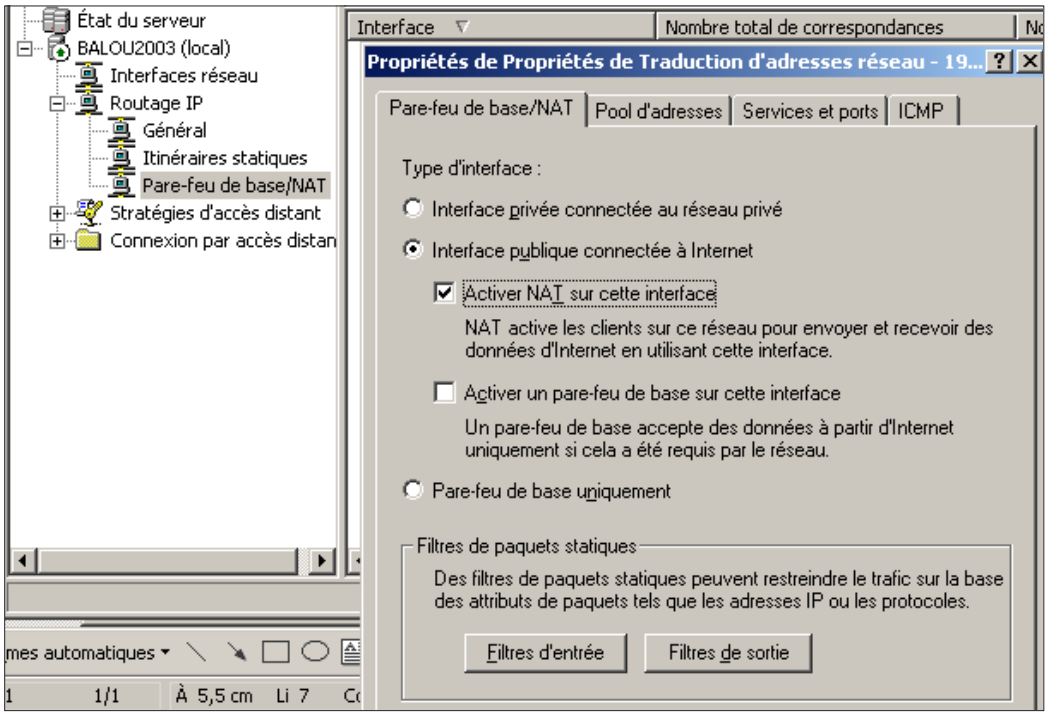
Pourquoi ?

Le serveur communique avec ses 2 cartes réseaux mais les réseaux ne communiquent pas entre eux il manque le routage entre les 2 réseaux.

Exercice 46

Comme vous connaissez l'utilité d'un routeur NAT, vous allez reconfigurer votre routeur en routeur NAT.

Dans notre console développer Routage IP, puis pare-feu de base et NAT puis rajouter une nouvelle interface sur la carte qui va vers l'extérieur et cocher pour obtenir du nat.



Exercice 47

Vous allez appliquer des filtres pour que votre client puisse communiquer avec la deuxième carte réseau du routeur mais ne puisse pas sortir sur internet.

Utiliser les filtres au même endroit. Ici des filtres de sortis.

Exercice 48

Créez un filtre pour que votre client ne reçoive pas les réponses de certains sites de votre choix.

Utiliser les filtres au même endroit. Ici des filtres d'entrée.

Atelier 9

Exercice 49

Dans une entreprise pourquoi installer utiliser Terminal serveur pour des utilisateurs ?

Il a été vu plus en avant dans le cours que certains systèmes multi-utilisateurs, n'avaient recours qu'à une seule application et que installer X fois cette application n'était pas amusant, mais que la mettre à jour non plus. Aussi pourquoi ne pas l'installer qu'une seule et en offrir l'accès à plusieurs utilisateurs ? N'est-ce pas là le principe même du client-serveur ?

Si cette pratique est avantageuse pour l'administrateur réseau qui n'a pas besoin d'effectuer X fois la maintenance des postes, X fois de mettre à jour les applications (même avec une stratégie !), elle est aussi moins coûteuse. Les postes clients n'ont pas besoin d'évoluer avec l'application. Mais attention à ne pas lésiner sur le serveur, il doit supporter la charge de plusieurs personnes travaillant sur lui.

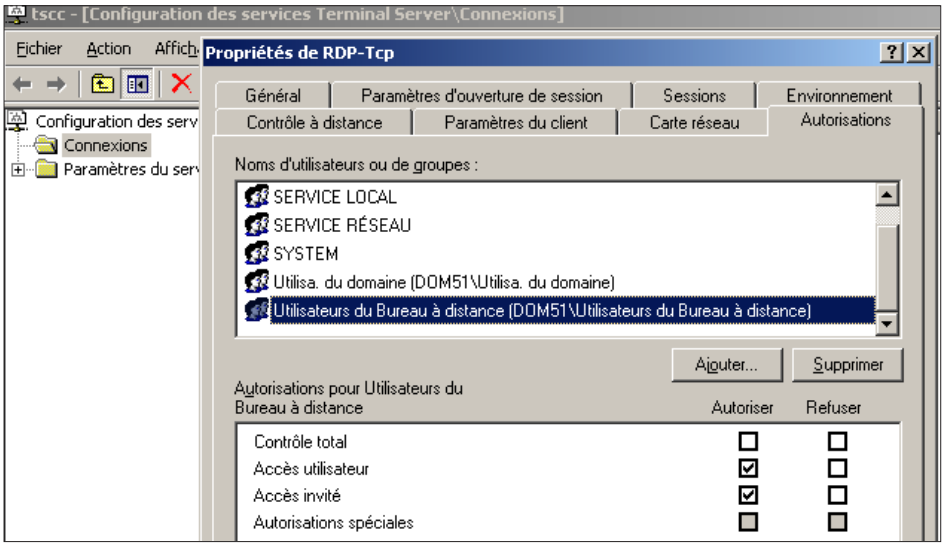
Exercice 50

Quelle précaution faut-il prendre pour installer le logiciel de connexion au serveur terminal serveur sur les clients ?

Pour qu'un client puisse se connecter à Terminal serveur il lui faut une application particulaire : msrdpcli.msi Si un client veut ce fichier pas de problème avec XP, c'est automatique, pour les autres il leurs faut récupérer ce fichier sur le serveur. On recommande donc de copier ce fichier dans un dossier partagé avec un accès pour les utilisateurs concernés. Mais nous pouvons faire mieux ! L'extension ne vous rappelle rien ? Si l'installation à distance via une stratégie. Mais vous y aviez pensé !

Exercice 51

Lorsque vous créez un utilisateur Terminal serveur, quels sont les paramètres à spécifier dans la console Utilisateur et Ordinateurs Actives Directory ?



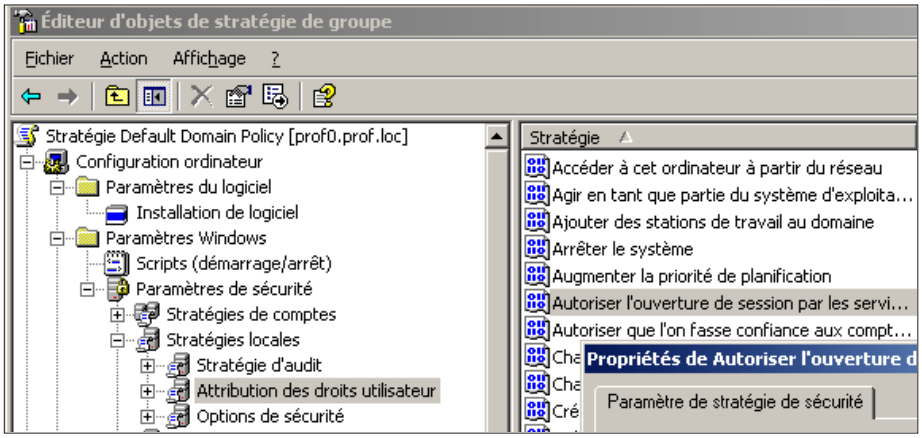
Si on met en place Terminal Serveur qui est un outil qui nécessite beaucoup de puissance (mémoire et processeur) sur le serveur, ce n'est certes pas pour un seul utilisateur ! Donc il nous faudra utiliser un groupe pour autoriser les

utilisateurs à se connecter au serveur. Windows a déjà ce groupe en stock, Utilisateurs du bureau à distance. Ne pas oublier avec la Console Utilisateurs et Ordinateurs Active Directory de rendre membre l'utilisateur à ce fameux groupe. Car :

- Un utilisateur peut accéder au service Terminal serveur de plusieurs manières. En fait deux suffisent.
- Soit il fait partie du groupe Utilisateurs du bureau à distance et lorsque Terminal serveur est installé grâce à la connexion RDP-TCP il accède naturellement au service.

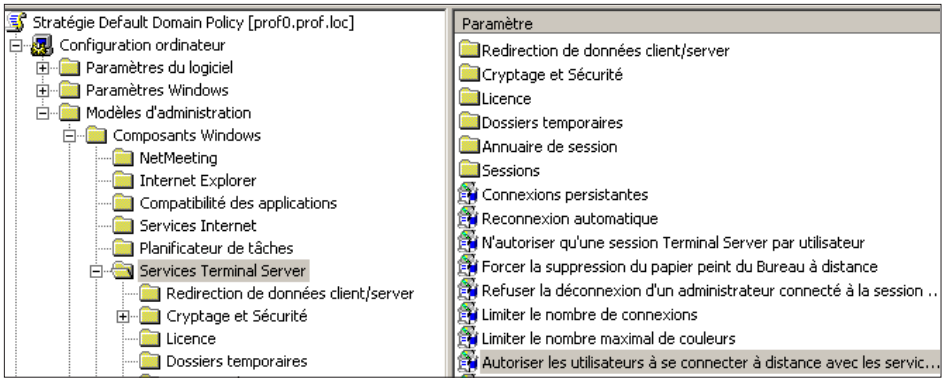
Cette fenêtre provient de la console Configurations des Services Terminal Serveur. On y accède via les outils d' administration.

Soit il fait partie du groupe Utilisateurs du bureau à distance et après la mise en place de 2 stratégies il accède au service de Terminal Serveur. Et ces stratégies utilisent ce fameux groupe.



Stratégie 1 : on doit rajouter le groupe autoriser à ouvrir une session.

Stratégie 2 : bien sûr cela marche aussi avec des noms d'utilisateurs ou tout autre groupe.



Exercice 52

Créez un utilisateur Terminal serveur qui de son poste client accède à Word uniquement.

On peut n'autoriser l'accès à des utilisateurs qu'à une seule application de 3 manières différentes.

- Propre à un individu : dans la console Utilisateurs et Ordinateurs Active Directory dans les Propriétés on trouve un onglet Environnement très intéressant. Quand on coche démarrer le programme suivant lors de l'ouverture de session et que l'on y rajoute le chemin de l'exécutable, l'utilisateur ne peut rien utiliser hormis cette application.

- Pour une unité d'organisation : Il existe une stratégie qui porte le doux nom de Démarrer un programme à la connexion. On peut le trouver dans Configurations utilisateur, modèles d'administration, Service Terminal Serveur.
- Pour toute connexion à Terminal Serveur, dans les propriétés de la connexion RDP-TCP, on retrouve l'onglet Environnement

Exercice 53

Créez un utilisateur Terminal serveur de type administrateur qui accède au serveur d'un poste client.

Par défaut si on n'applique aucune restriction tout utilisateur ayant une connexion Terminal Serveur peut tout faire sur le serveur. Attention le danger !

Exercice 54

Créez un utilisateur terminal serveur qui peut accéder à toutes les applications sur le serveur mais qui ne peut pas administrer le serveur ou le réseau.

On doit se concentrer sur les autorisations qu'ont les utilisateurs sur la connexion, on a un accès utilisateur, et un accès invité (pour le contrôle total pas de problème !). L'accès invité ne permet qu'un accès réduit aux applications sur le serveur comme on le souhaite.

On peut également travailler avec la stratégie : définit les règles pour le contrôle à distance des sessions Terminal Serveur.

Remarque : utiliser d'autres stratégies qui ne sont pas sous la hiérarchie Terminal serveur implique que l'utilisateur sera certes limité dans sa session Terminal serveur, mais aussi dans sa session normale.

Exercice 55

Quelle est la différence entre l'utilisation des propriétés dans la connexion RTD-TCP et les stratégies Terminal serveur ?

On a bien compris qu'il y a plusieurs niveaux et que ce sont les paramètres de la connexion qui priment sur les autres.

Exercice 56

À quoi sert le gestionnaire de licence terminal serveur ?

Si on n'installe qu'une seule fois un logiciel, cela ne veut pas dire qu'un seul utilisateur l'utilise. La preuve dans ce dossier. Aussi pour rester dans la légalité on achètera des licences par serveurs et non pas postes et ces licences seront gérées par le serveur à la connexion des utilisateurs.

Atelier 10

Exercice 57

À quoi cela sert ?

La plupart du temps à réparer à distance, ou a faire une démonstration à l'utilisateur sur l'utilisation d'un outil.

Exercice 58

Sur quels protocoles se base cette prise en main ?

En général les protocoles comme telnet, http, SSL pour la sécurité et TCP/IP bien sur.

Atelier 12

Les utilisateurs SQL

Exercice 59

Créez la procédure stockée ajout_personne qui permet de rajouter des instances dans la table personne. N'oubliez pas de paramétrer la procédure et de vérifier la syntaxe.

Une variable est toujours précédée du signe @

La première ligne indique les paramètres.

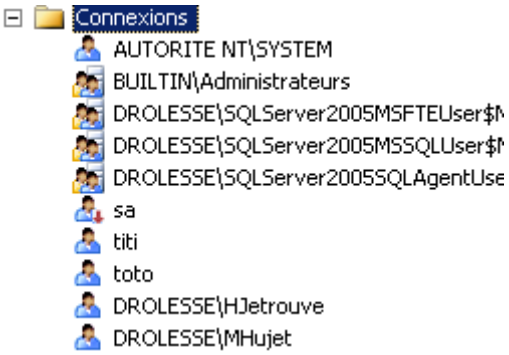
La dernière ligne est la commande SQL qui permet d'ajouter une instance en fonction des paramètres en entrée.

```
CREATE PROCEDURE ajout_personne
    -- Add the parameters for the stored procedure here
    @num nchar(5), @nom nchar(25), @prenom nchar(25), @naiss datetime, @datec
AS
BEGIN
insert into personne values (@num, @nom, @prenom, @naiss, @dateid)
END
GO
```

Exercice 60

Créez les accès pour les chercheurs de Trouvetout et les utilisateurs pour la base Disparus

Il n'y a ici qu'un extrait des accès pour Trouvetout.



Comme vous avez bien utilisé tous les onglets de l'accès les utilisateurs se sont rajoutés d'eux-même dans la base de données Disparus.

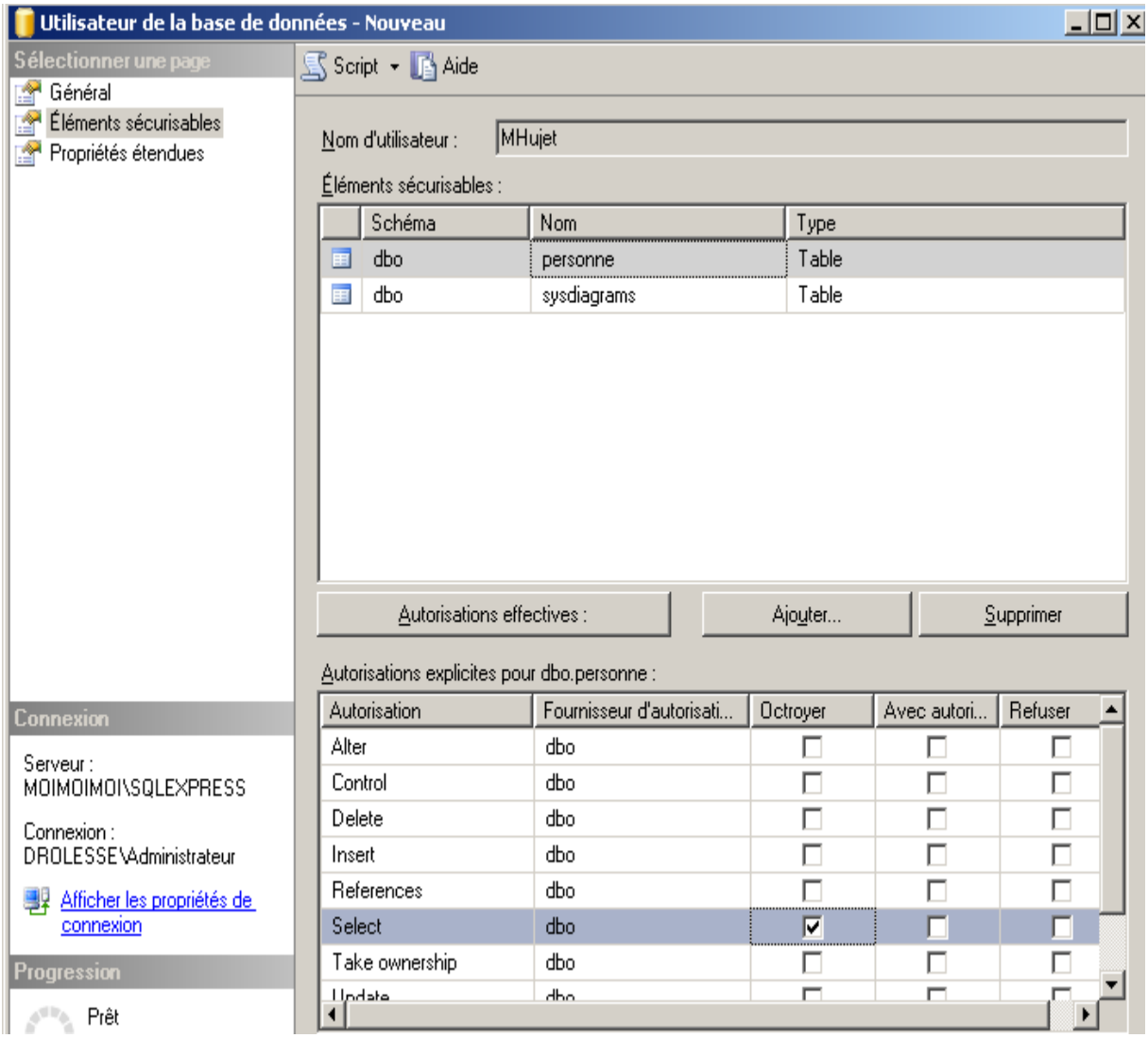
Exercice 61

Y-a-t-il une contradiction dans nos permissions ?

Le fait d'autoriser l'utilisation d'une procédure n'est pas en contradiction avec le fait d'utiliser une instruction. C'est même une protection qu'il faut mettre en place. De toutes manières les utilisateurs qu'ils proviennent de la société Trouvetout ou d'ailleurs ne sont pas des spécialistes en SQL aussi doit-on leur proposer des procédures.

Exercice 62

MHujet ne doit pouvoir que visualiser le contenu de la table Personne.



Exercice 63

Que font ces lignes de commandes ?

La première ligne rajoute une personne dans la table personne.

La deuxième ligne affiche cette même personne, puisque la table était vide avant.

L'utilisateur n'a pas l'autorisation d'utiliser l'instruction Insert into, il y a un refus.

Exercice 64

Pour se connecter avec l'utilisateur MHujet faut-il fermer la session Windows de HJetrouve ?

Non inutile, il suffit de fermer la connexion SQL et d'en ouvrir un autre avec un autre utilisateur.

Exercice 65

Connectez-vous avec l'analyseur de requête avec MHujet. Que font les lignes de commandes de l'exercice 63 ?

MHujet n'a que le droit SELECT aussi seule la deuxième ligne fonctionnera. De plus s'il avait le droit d'exécuter la procédure il y aurait un conflit puisque l'instance existe déjà dans la table personne.

Exercice 66

Connectez-vous avec l'analyseur de requête avec Jluigui. Que font les lignes de commandes de l'exercice 63 ?

L'utilisateur existe bien mais il n'a aucune permission.

Atelier 13

Serveurs SQL suite et fin

Exercice 67

Rajoutez Disparus_2 comme fichier à votre base de données, ce fichier est un fichier secondaire. Question subsidiaire : qu'est-ce qu'un fichier secondaire et comment le reconnaît-on en le regardant ?

- Cliquez droit sur la base de données Disparus, *Propriétés*.
- Sélectionnez la page *Fichiers*.
- Cliquez sur le bouton *Ajouter.*
- Dans la zone *fichiers de la base de données* entrez dans la première colonne Disparus_2.
- Cliquez sur le bouton ... de la dernière colonne et choisir le fichier Disparus.ndf.
- Dans la deuxième colonne entrez *secondary*.

Un fichier secondaire se reconnaît à son extension ndf.

Exercice 68

Tous les dimanches matin à 1 heure, vous allez vérifier la base de données Disparus pour que l'espace disque ne dépasse pas 3 Mo et effectuez une réparation si besoin.

- Cliquez droit sur *Plans de maintenance du dossier gestion.*
- Lancez l'*Assistant.*
- Dans la première fenêtre on vous demande de sélectionner la base de données, c'est *Disparus*.
- Cliquez sur *Suivant*.

- Vous allez optimiser une fois par semaine, le dimanche à une heure du matin, l'espace utilisé par la base de données pour qu'elle ne dépasse pas les 3 Mo que vous considérez comme nécessaire.
- Cliquez sur *Suivant.*
- Puis dans la fenêtre suivante vérifier l'intégrité de la base de données et réparez les erreurs tous les dimanches à 1 heure du matin.
- Cliquez sur *Suivant.*
- N'effectuez pas de sauvegarde de la base comme du journal.
- Enregistrez le rapport sur le bureau et nommez votre plan de maintenance Vérif-et-répare-dimanche.

Exercice 69

Effectuez une sauvegarde complète de la base de données Disparus.

- Cliquez droit sur Disparus.
- Dans le menu *Tâches*, choisir *Sauvegarder la base de données*.
- Sélectionnez une *sauvegarde complète.*
- Comme il n'existe pas d'unité cliquez sur le bouton *Ajouter* Dans la zone *Destination*.
- Cochez *Unité de sauvegarde*.
- Sélectionnez *unit-Disparus.*
- Cliquez sur *OK.*
- Ne rien modifier d'autre dans la première fenêtre de sauvegarde.
- Comme vous n'avez pas planifié la sauvegarde, elle s'effectue sous vos yeux.
- Pour vérification, allez dans le dossier *Gestion et Sauvegarde* pour voir que l'unité a été créée.
- Avec *l'explorateur* vous vérifiez qu'il y a bien une sauvegarde dans cette unité.

Exercice 70

Détruisez la base de données Disparus.

Sélectionnez la base de données Disparus et Supprimez la. Cliquez sur le bouton *réactualiser* pour vérifier votre manipulation.

Exercice 71

Restaurez la base de données Disparus.

Pour restaurer une base de données, il faut faire attention à bien sélectionner l'unité de sauvegarde.

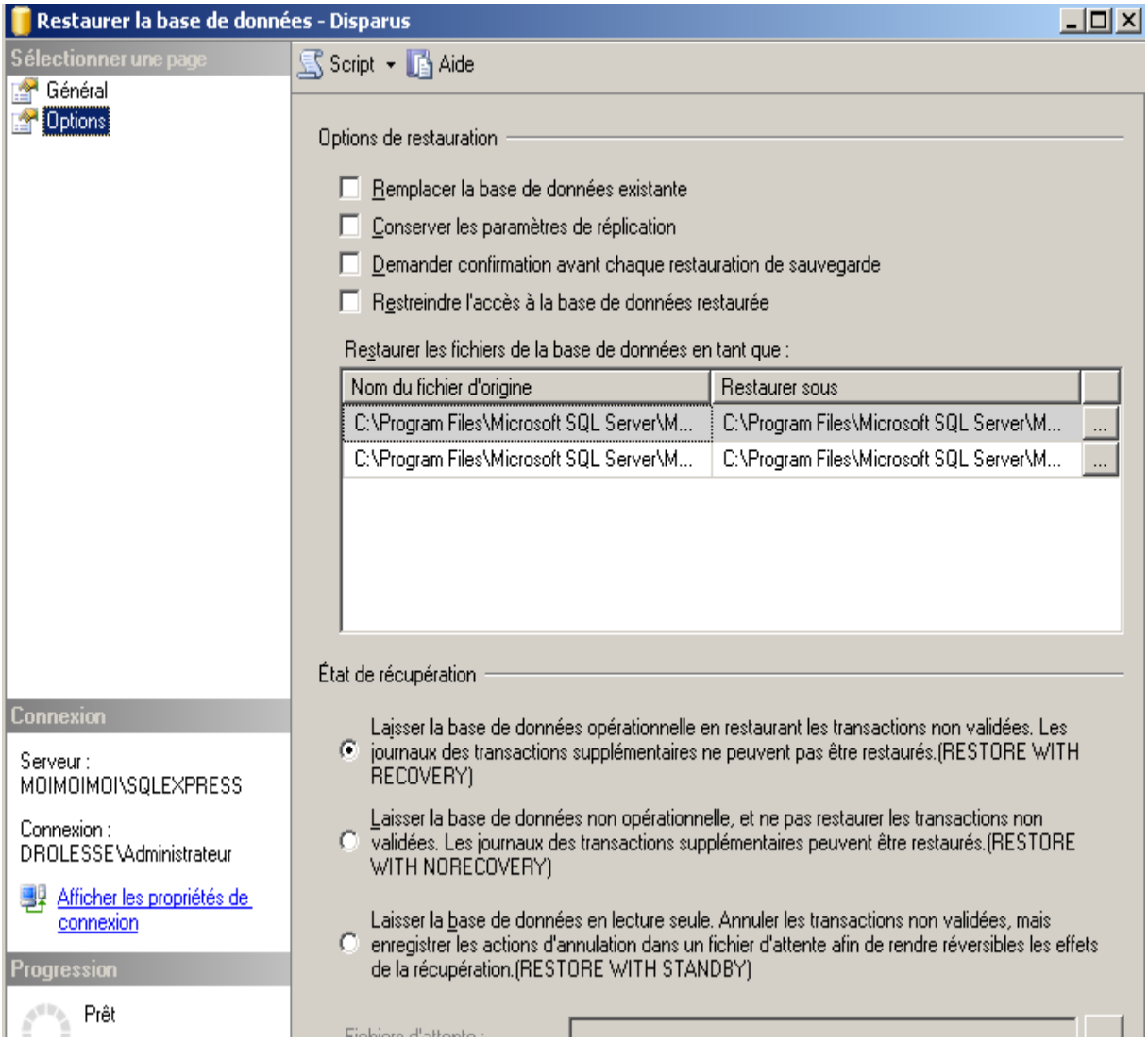
Exercice 72

Dans la base de données disparus rajoutez une personne. Quels genres de sauvegarde et de restauration faut-il effectuer lors de la suppression de la base de données Disparus.

Inutile de refaire une sauvegarde complète. On préfère effectuer une sauvegarde **différentielle** qui ne contiendra que ce qui a été ajouté. C'est plus rapide et tient moins de place sur le disque.

Pour la restauration on devra en effectuer 2, la complète et la différentielle. Pour que celles-ci fonctionnent on doit modifier des options dans la première restauration : Il faut laisser la base non opérationnelle mais permettre la restauration d'autres journaux de transaction. Option 2

Pour la deuxième restauration re-cochez la première option.


Restaurer la base de données - Disparus
Sélectionner une page
Général
Options
Script
Aide
Options de restauration
Remplacer la base de données existante
Conserver les paramètres de réplication
Demander confirmation avant chaque restauration de sauvegarde
Restreindre l'accès à la base de données restaurée
Restaurer les fichiers de la base de données en tant que :
Nom du fichier d'origine
Restaurer sous
C:\Program Files\Microsoft SQL Server\M...
C:\Program Files\Microsoft SQL Server\M...
C:\Program Files\Microsoft SQL Server\M...
C:\Program Files\Microsoft SQL Server\M...
État de récupération
Laisser la base de données opérationnelle en restaurant les transactions non validées. Les journaux des transactions supplémentaires ne peuvent pas être restaurés.(RESTORE WITH RECOVERY)
Laisser la base de données non opérationnelle, et ne pas restaurer les transactions non validées. Les journaux des transactions supplémentaires peuvent être restaurés.(RESTORE WITH NORECOVERY)
Laisser la base de données en lecture seule. Annuler les transactions non validées, mais enregistrer les actions d'annulation dans un fichier d'attente afin de rendre réversibles les effets de la récupération.(RESTORE WITH STANDBY)
Connexion
Serveur :
MOIMOIMOI\SQLEXPRESS
Connexion :
DROLESSE\Administrateur
Afficher les propriétés de connexion
Progression
Prêt