الجمهورية الجزائرية الديمقراطيـــة الشعبية

République Algérienne Démocratique et Populaire

وزارة التكوين و التعليم المهنيين

Ministère de la Formation et de l'enseignement Professionnelle

معهد التكوين و التعليم المهنيين – بئر خادم-

Institut de la formation et de l'enseignement Professionnels

- Bir Khadem -

MANUEL TECHNIQUE ET PEDAGOGIQUE

ADMINISTRATION ET SECURITE DES RESEAUX INFORMATIQUES

MODULE

Gestion des clients et administration des permissions

NIV : 5

2014

I.F.E.P

WWW.DZPEN.COM | قلم الجزائر

PREAMBULE :

Le manuel du stagiaire est un ouvrage didactique. Il fournit aux stagiaires des supports d'enseignement et d'apprentissage pour l'acquisition de la compétence (connaissances, habiletés et attitudes) visée par le programme d'étude.

La spécialité Administration et sécurité des réseaux informatiques comporte de modules qualifiants et des modules complémentaires, parmi ces modules est celui de la **gestion des clients et administration des permissions** qui fait l'objet de notre Manuel.

La durée d'enseignement du module est de 102heures. La répartition initiale de ce module a été faite sur quinze (15) chapitres. Après une étude approfondie du contenu de ce module, il a été réduit en sept (07) chapitres (voir détail en annexe C) pour les raisons suivantes.

Le chapitre 1 qui est intitulé: **création et modification d'un compte utilisateur locale** est le résultat de la fusion des chapitres 1et 2, la fusion a été faite parce que le contenu des deux chapitres est basé sur le compte utilisateur local.

Le chapitre 2 qui est intitulé: **gestion et configuration des comptes utilisateurs dans** un domaine c'est le chapitre 3 dont son contenu est le même.

Le chapitre 3 qui est intitulé: **définition d'un profil utilisateur** est le résultat de la fusion des chapitres 4,5et 6 car nous avons constatés que dans les propriétés d'un compte utilisateur dans l'onglet Profil il existe le profil, le dossier de base et le script d'ouverture de session.

Le chapitre 4 qui est intitulé **gestion des groupes d'utilisateurs** est le résultat de la fusion des chapitres 7, 8, 9,10 et 11 parce que le contenu des cinq chapitres est basé sur les groupes d'utilisateurs local et de domaine avec les types et les étendus d groupes.

Le chapitre 5 qui est intitulé: **gestion des permissions (autorisations et droits)** nous avons ajoutés des s/sous sections pour plus de précisions.
Le chapitre 6 qui est intitulé: **Attribution des permissions et des autorisations NTFS pour les utilisateurs** reste le même.

Le chapitre 7 qui est intitulé: **partage des ressources et des dossiers** est le résultat de la fusion des chapitres 14 et 15 parce que le système de fichier a été abordé dans le chapitre 14.

Ce manuel contient des éléments bien détaillés en théorie avec des exercices théoriques, pratiques et de synthèses ainsi que les corrigés types.

WWW.DZPEN.COM | قلم الجزائر

I.1- Présentation de la profession :

BRANCHE PROFESSIONNELLE : INFORMATIQUE

DENOMINATION DE LA SPECIALITE : Administration et Sécurité des réseaux informatiques

---

Description de la spécialité :

Le technicien Supérieur en Administration et Sécurité des Réseaux informatiques est un professionnel capable d'assurer : la configuration, l'installation, l'administration, la sécurité et la maintenance du premier niveau d'un réseau d'équipements et d'applications informatiques, centralisés ou répartis, caractérisés par :

- Un couplage étroit entre le matériel et le logiciel,
- Une sécurité accrue des données et système d'information
- Une interaction avec un environnement productif et/ou technique.

Tâches essentielles:

- Installer et configurer un réseau de machines hétérogènes,
- Configurer les équipements matériels ou logiciels du réseau (Nœud, Switch, Routeur, Serveur)
- Installer et configurer des services clients,
- Installer des logiciels répartis, et mettre en place des bases de données centralisées,
- Gérer des espaces disques communs, et configurer le partage des périphériques sur le réseau et pouvoir établir les connexions sur un réseau extérieur.
- Gérer le réseau et son évolution,
- Assurer la sécurité des systèmes,
- Assurer la sécurité du réseau,
- Assurer la sauvegarde des données,
- Superviser le fonctionnement des réseaux,
- Assurer le soutien aux clients des réseaux,
- Résoudre les problèmes liés aux réseaux,
- Réparer et configurer des systèmes d'ordinateurs.

I.2-Conditions de travail :

- Lieu de travail :

- Salle machines, bureaux…

- Caractéristiques physiques

Eclairage :

Eclairage normal avec apport artificiel (tube fluorescent).

Température :

Température ambiante et/ou avec climatisation.

Humidité :
Selon le milieu ambiant.

Poussière :
Milieu aussi dépoussiérer que possible.

Bruits et vibrations :
Environnement non bruyant.

- Risques et maladies professionnels :

- Risques liés aux rayonnements des tubes cathodiques,
- Fatigue des yeux
- Déformations de la colonne vertébrale

-**Contacts sociaux :**
Le BTS en administration et sécurité des réseaux informatiques travaille avec autonomie eten équipe.
Dans la plupart des cas, il intervient avec d'autres professionnels des réseaux informatiques
(Installateur réseau, administrateur BDD…).
Il est parfois en rapport direct avec les clients, notamment lorsqu'il opère sur Des réseaux informatiques d'entreprises.
Sa ponctualité et son sens de communication lui permettent de fidéliser sa clientèle.

I.3-Exigences de la profession :

Physiques :
- Ce métier exige souvent de bonnes conditions physiques
- Avoir une bonne vision avec ou sans verres correcteurs
- Avoir une ouïe assez fine

Intellectuelles :
- Esprit Scientifique.
- Esprit d'Initiative
- Esprit méthodique
- Esprit de Synthèse.
- Faculté développée de raisonnement logique.
- Sens de responsabilité.
- Sens de l'organisation
- La résistance au stress et le dynamisme sont également nécessaire à cette fonction

Contre-indications :
- Présenter un handicap physique
- Avoir une excessive déficiente sensibilité oculaire ou une ouïe déficiente
- Stress
- Présenter une hernie discale ou déformation de la colonne vertébrale

I.4- Responsabilité de l'administrateur réseau:

Responsabilité Matérielle :
echnicien supérieur administrateur de réseau est responsable des équipements sur lesquels il intervient, des informations stockées, de leur protection et leur confidentialité.

WWW.DZPEN.COM | قلم الجزائر

- **Responsabilité Décisionnelle :**

En général l'administrateur exerce son activité au sein d'une hiérarchie qui est le principal responsable sur les décisions relevant de son domaine technique ou administratif. Néanmoins il est entièrement responsable quant aux décisions opérationnelles qu'il engage.

- **Responsabilité Morale :**

L'administrateur réseau à une responsabilité morale sur la qualité du service effectué, sur la confidentialité des informations pertinentes de l'organisation ou de l'entreprise qui l'emploi.

- **Responsabilité Sécuritaire :**

L'administrateur doit veiller et respecter les consignes de sécurité des personnes, matériels, applications et informations stratégiques.

I.5- Possibilité de Promotion :

Selon le cadre Règlementaire, et conformément au statut de l'entreprise, Le BTS en administration et sécurité des réseaux a une perspective de carrière intéressante dans un marché du travail en constante évolution.

I.6- Formation :

Condition d'admission :

- 3ième Année secondaire (maths, science, technique).

Durée de la Formation :

- 30 Mois dont 24 semaines de stage pratique.

I.7- Niveau de qualification :

- Niveau (5) V

- **Diplôme :** Brevet de Technicien Supérieur en administration et sécurité des réseaux informatiques.

FICHE DE PRESENTATION DU MODULE QUALIFIANT

MODULE : Gestion des clients et administration des permissions

CODE : M.Q.4

DUREE : 102 HEURES

OBJECTIF MODULAIRE

COMPORTEMENT ATTENDU :

A l'issue de ce module qualifiant le stagiaire doit être capable de :

Gérer les clients (comptes d'utilisateurs et les comptes d'ordinateurs) et administrer les permissions,

Selon les critères, les conditions et les précisions suivantes :

CONDITION D'EVALUATION :

A l'aide de :

- Systèmes d'exploitation Windows
- Systèmes d'exploitation Linux
- Equipements informatiques

A partir de :

- Orientations et consignes.

CRITERES GENERAUX DE PERFORMANCE :

- Gestion correcte des comptes d'utilisateurs et de groupes
- Détermination juste des droits et permissions d'accès aux ressources
- Respect des normes et consignes techniques.
- Conformité des comptes avec les consignes et orientations.
- Respect d'une politique rigoureuse de sécurité.
- Respect des temps alloués aux interventions.

WWW.DZPEN.COM | قلم الجزائر

OBJECTIFS INTERMEDIAIRES	CRITERES PARTICULIERS DE PERFORMANCE	ELEMENTS DE CONTENU
▪ Définir un Compte utilisateur	▪ Définition correcte d'un Compte utilisateur	▪ Utilisateurs locaux ▪ Utilisateurs prédéfinis (Administrateur, Invité)
▪ Créer et modifier un compte utilisateur	▪ Création correcte d'un compte ▪ Modification correcte d'un compte	▪ Création d'un compte d'utilisateur sur un ordinateur local ▪ Modifier un compte sur un ordinateur local
▪ Gérer et configurer des comptes utilisateurs dans un domaine	▪ Caractéristique exactes des comptes utilisateur	▪ Gestion et configuration des comptes utilisateurs dans un domaine : -Définition d'Active Directory Compte d'utilisateur de domaine - Création d'un compte utilisateur de domaine - Intégration d'un client dans un domaine - Propriétés d'un compte utilisateur - Rechercher des personnes ou ordinateurs ou objets dans Active Directory - Options de compte (Heure de disponibilité ou restrictions d'horaires, Ordinateurs autorisés, Expiration de compte, Copie d'un compte utilisateur).
▪ Définir un profil utilisateur	▪ Définition exacte du profil utilisateur	▪ Profil par défaut et Profil Utilisateur ▪ Profils d'utilisateurs itinérants - Profils obligatoires - Configuration d'un profil d'utilisateur itinérant - Création d'un profil itinérant personnalisé -Profil itinérant personnalisé Obligatoire
▪ Création de dossier de base	▪ Création correcte de dossier de base	▪ Dossier de base
▪ Créer un script d'ouverture de session	▪ Création correcte de scripts	▪ Scripts d'ouverture de session dans Windows Server 2003/2008/2012 ▪

OBJECTIFS INTERMEDIAIRES	CRITERES PARTICULIERS DE PERFORMANCE	ELEMENTS DE CONTENU
▪ Définir un groupe	▪ Définition correcte d'un groupe	▪ Qu'est-ce qu'un groupe ▪ Groupes prédéfinis sur un ordinateur local ▪ Groupes prédéfinis standards ▪ Groupes prédéfinis Spéciaux ou Groupes dits Systèmes. ▪ Création d'un groupe. ▪ Stratégie d'utilisation de groupes locaux dans un groupe de travail
▪ Gérer les Groupes dans un Domaine	▪ Gestion correcte des groupes	▪ Groupes d'utilisateur dans un Domaine
▪ Enumérer les types de groupes	▪ Enumération exacte des types de groupes	▪ Les types de groupes -Groupes de sécurité -Groupes de distributions
▪ Définition des étendues de groupes	▪ Définition juste des étendues	▪ Les étendues de groupes - Groupe global - Groupe de domaine local - Groupes Universels - Imbrication de groupes (en mode natif, En mode mixte)
	▪ Définition correcte de Groupe par défaut	▪ Méthodologies d'utilisation des groupes
▪ Définir Groupes par défaut		▪ Définir les groupes par défaut 1-Sur les serveurs Contrôleurs de Domaine - Groupes prédéfinis - Groupes intégrés à étendue de domaine locale -Schéma d'imbrication des groupes et comptes utilisateurs dans un domaine 2-Sur tous les ordinateurs -Groupes spéciaux 3-Création de groupes

OBJECTIFS	CRITERES PARTICULIERS DE	ELEMENTS DE CONTENU

INTERMEDIAIRES	PERFORMANCE	
▪ Gérer les permissions (autorisations et droits)	▪ Attribution juste des droits et permissions ▪ Gestion correcte des permissions	▪ Gestion d'accès aux ressources - Contrôle d'accès - Administration des accès aux dossiers locaux partagés - Mise en place des fichiers hors connexion
▪ Attribuer les permissions et les autorisations NTFS pour les utilisateurs	▪ Attribution adéquate des permissions	▪ Les permissions et les autorisations pour les utilisateurs -Règles concernant les Autorisations
▪ Partager les ressources et les dossiers.	▪ Opérabilité du partage	▪ Partage des ressources et des dossiers. 1-Partager un dossier - Partage à partir de l'Explorateur - A partir de la console de gestion de l'ordinateur - Supprimer un partage - Se connecter à une ressource partagée - Contrôler les partages 2-Système de fichiers (Windows/Linux) - Structure du système de fichiers NTFS - Système de fichiers CDFS - Système de fichiers UDF
▪ Sécuriser les systèmes de fichiers	▪ Sécurisation juste des fichiers	▪ Sécurité des systèmes de fichiers -Autorisations simples de partage (Autorisations simples et autorisations de Sécurité)

Chapitre1 : Création et modification d'un compte utilisateur local

Introduction :

Les comptes d'utilisateur personnalisent Windows pour chacune des personnes qui partagent un ordinateur. Un compte d'utilisateur vous offre une vue personnalisée de vos propres fichiers, une liste de vos sites Web favoris et une liste des pages Web que vous avez consultées récemment. Grâce au compte d'utilisateur, les documents que vous créez ou enregistrez sont stockés dans votre dossier Mes documents personnel et sont donc séparés des documents des autres utilisateurs de l'ordinateur.

Il existe deux types de comptes d'utilisateurs :

1.1 Utilisateurs locaux :

Un compte d'utilisateur local (c'est-à-dire un utilisateur qui travaille directement sur la machine sans passer par le réseau) permet d'ouvrir une session uniquement sur l'ordinateur qui contient le compte de l'utilisateur crée. Le compte est contenu dans une base de données locale et n'est pas dupliqué sur d'autres ordinateurs.

1.2 Utilisateur prédéfinis :

Un compte utilisateur prédéfinis permet à un utilisateur d'effectuer des tâches administratives ou d'accéder provisoirement aux ressources réseau.

Windows Server2003, 2008 et windows7crées par défaut deux comptes intégrés Administrateur et Invité lors de son installation :

1.2.1 Administrateur :

Le compte administrateur permet de gérer l'ensemble de la configuration des ordinateurs et du domaine et en particulier la création, la modification et la suppression des comptes d'utilisateurs et de groupes. Ce compte ne peut être désactivé, sauf si vous avez au préalable créé un utilisateur équivalent.

C'est donc la personne qui possède le plus de privilèges sur l'ordinateur.

Le résumé de ses fonctions est :

- La gestion des comptes d'utilisateurs et des comptes de groupes.
- La gestion des stratégies de groupes.
- La création de dossiers et l'installation de fichiers ou d'applications sur le disque dur.

WWW.DZPEN.COM | قلم الجزائر

- La modification logicielle du système d'exploitation.
- L'installation et la configuration de l'imprimante.
- La gestion des ressources partagées (création, droits).
- La sauvegarde et restauration des données …

Remarque :

Il est vivement conseillé de renommer l'Administrateur car il sera plus difficile à une personne malveillante de trouver le mot de passe d'un compte lorsqu'on ne connaît pas le nom du compte. Il est possible à partir des stratégies de groupe ou du registre de ne pas afficher le nom du dernier utilisateur ayant ouvert une session.

1.2.2 Invité :

Le compte invité est réservé aux utilisateurs qui ne possèdent pas de compte sur l'ordinateur. Aucun mot de passe ne lui est associé, ce qui permet aux utilisateurs d'ouvrir rapidement une session pour consulter leurs courriers électroniques ou surfer sur Internet. Ce compte utilisateur ne peut apporter aucune modification au système.

Remarque :

- Le nom du compte utilisateur doit être unique sur l'ordinateur sur lequel il est crée.
- La taille de nom d'ouverture de session est de 20 caractères alphanumérique, la saisie de plus de 20 caractères est tolérable mais Windows reconnaît que les 20 premiers caractères.
- Les caractères suivants ne sont pas autorisés : " / \ [ ] :; | = , + * ? <>
- Les noms d'ouverture de session ne sont pas soumis à la casse.
- La taille du mot de passe doit être supérieure ou égale à 8 caractères.
- Le mot de passe doit contenir des caractères de chacun des groupes suivants (Voir tableau 01) :

Groupes	Exemples
Lettres minuscules	a, b, c ….
Chiffres	0,1 2, 3, 4, 5, …..
Caractères qui ne sont pas des lettres ou des chiffres	! ? <> * - + / [ ] ( ) { }= ; , . %

Tableau 01

WWW.DZPEN.COM | قلم الجزائر

1.3 Création d'un compte d'utilisateur sur un ordinateur local :

La création d'un compte d'utilisateur local se fait par le composant **Utilisateur** et **groupes locaux**, avec les privilèges d'un **administrateur**, en suivant ces étapes :

-Allez dans **Démarrer**, sur **Panneau de configuration** puis sur **Outils d'administration** et enfin cliquer sur **Gestion de l'ordinateur** (figure 02).

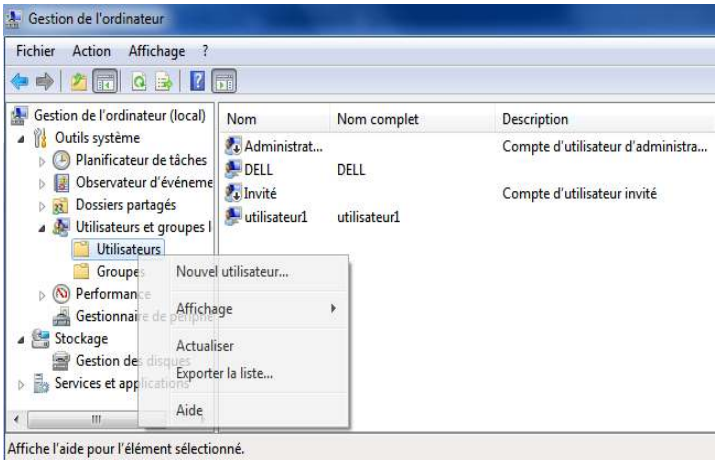


Figure 02

-Dans la fenêtre de **Gestion** de **l'Ordinateur** cliquez sur "**Utilisateur et groupes locaux**". Deux dossiers se présentent devant vous :

- Utilisateurs : Contient la liste des utilisateurs.
- Groupes : Contient la liste des groupes.

-Développez le dossier utilisateur, cliquez avec le bouton droit sur le volet détail.

-Un menu contextuel s'affiche puis exécuter la commande de création d'un **nouvel utilisateur**. La boite de dialogue ci-dessous apparaît (figure 03).

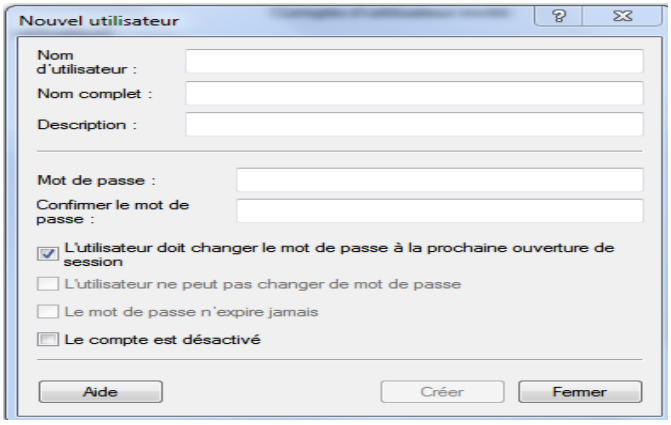


Figure 03

WWW.DZPEN.COM | قلم الجزائر

La boite de dialogue Figure 03 vous permet d'introduire les informations suivantes :

- Nom utilisateur : Nom unique choisi par l'utilisateur.
- Nom détaillé : Nom complet de l'utilisateur reflète celui qui détient l'ordinateur.
- Description c'est une donnée facultative qui identifie les utilisateurs.
- L'utilisateur doit changer de mot de passe à la prochaine ouverture : Dés la

Première ouverture de session on demande à changer un mot de passe.

- L'utilisateur ne peut pas changer de mot de passe.
- Le mot de passe n'expire jamais.
- Le compte est désactivé : Empêche l'utilisation du compte (voir figure 04).

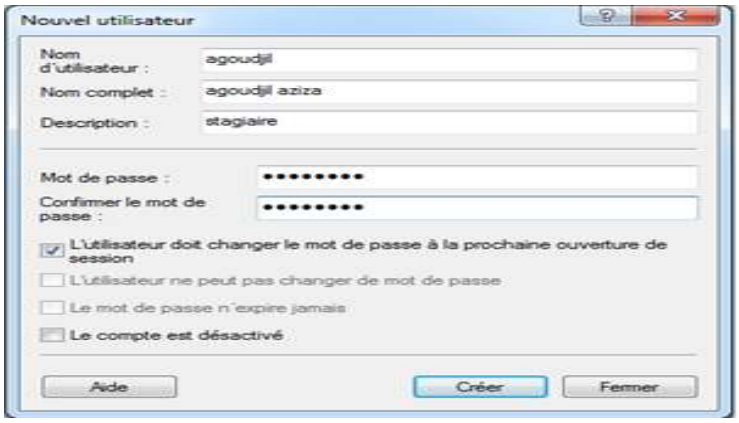


Figure 04

1.4 Modifier un compte utilisateur local :

Une fois le compte local crée il sera visible dans la liste des utilisateurs de la console **Gestion de l'ordinateur** dans la rubrique **Utilisateur** (voir figure 05).

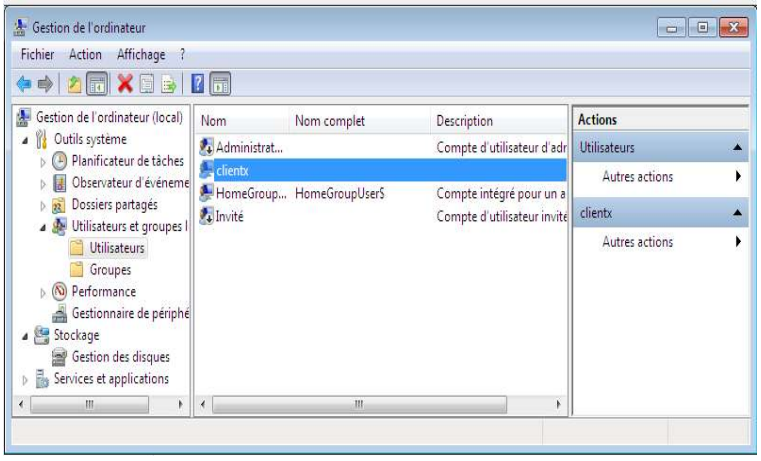


Figure 05

WWW.DZPEN.COM | قلم الجزائر

La modification d'un compte d'utilisateur local sefait par un double-clique sur le nom d'utilisateur .La fenêtre **Propriétés** de cet utilisateur affiche trois onglets (voir figure 06) :

- Onglet "**Général**" :

Vous pouvez définir la gestion du mot de passe tel que le droit à l'utilisateur de changer son mot de passe et aussi activer ou désactiver le compte.



Figure 6

- Onglet "**Membre de**" :

Ajouter l'utilisateur en tant que membre d'un autre groupe, et si vous ne connaissez pas le nom du groupe vous pouvez faire une recherche avancé en cliquant sur avancé.

- Dans l'onglet "**Profil**": Vous pouvez définir le profil d'un utilisateur

Parmi ces modifications nous pouvons supprimer, renommer ou initialiser le mot de passe d'un compte utilisateur local. Pour cela il suffit de cliquer avec le bouton droit sur cet objet, un menu contextuel affiche ces commandes (voir figure07).

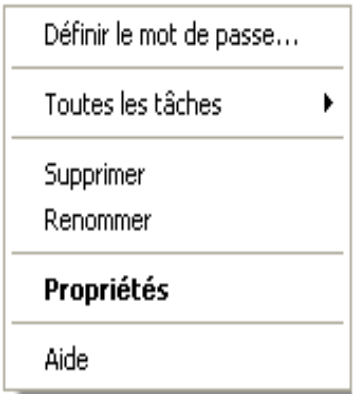


Figure 7

WWW.DZPEN.COM | قلم الجزائر

1.5 Exercices théoriques :

Exercice N°01 :

1. Quel est le rôle d'un compte utilisateur local ?

2. Quel est le rôle d'un compte administrateur ?

3. Qu'est ce qu'un compte invité ?

4. Qui peut créer un compte utilisateur local, invite ou administrateur ?

Exercice N°02:

1. Qu'est ce qu'un compte prédéfini ?

2. Est-il possible de supprimer le compte prédéfini Administrateur ?

3. Est-il possible de renommer le compte prédéfini Administrateur ?

4. Est-ce que le compte prédéfini Invité est activé par défaut ?

5. Lorsque vous renommez un compte d'utilisateur, est-ce que vous perdez toutes les permissions qui ont été associées à ce compte sur des partages ?

6. Lorsque vous supprimez un compte et que vous le recréez à l'identique, perdez vous les permissions qui ont été associées à ce compte sur des partages ?

7. Vous souhaitez laisser libre choix des mots de passe pour vos utilisateurs. Comment allez- vous procéder lors de la création de leur compte d'utilisateur ?

1.6 Exercice pratique:

2. Ouvrer une session Administrateur sur votre ordinateur local.

3. Créer un Compte d'utilisateur local portant votre nom.

4. Ouvrer une session avec votre nom.

5. Que constatez – vous ?

WWW.DZPEN.COM | قلم الجزائر

1.7 Résumé :

Les comptes d'utilisateurs servent à authentifier, autoriser ou refuser l'accès aux ressources et à auditer l'activité des utilisateurs individuels de votre réseau.

Lors de L'installation de Windows par défaut deux comptes intégrés Administrateur et Invité sont crées. Une fois le compte utilisateur local est crée chaque personne accède à son compte d'utilisateur à l'aide d'un nom d'utilisateur et d'un mot de passe. Des modifications peuvent être apportées sur un compte utilisateur local, comme la suppression, la réinitialisation du mot de passe et la renomination.

1.8 Exercice de synthèse :

1. Ouvrir une session en tant qu'administrateur sur le poste client avec localpw

2. Créer un compte utilisateur avec les renseignements suivants :

Utilisateur : localuser1

Description : mon compte d'utilisateur

Mot de passe : Passe01.

3. Désactiver la case à cocher l'utilisateur doit changer de mot de passe à la prochaine ouverture de session, puis cliquer sur Créer.

4. Fermer la boite de dialogue Nouvel utilisateur.

5. Fermer la console Gestion de l'ordinateur, puis la session.

6. Modifier le nom, le mot de passe et l'image du compte utilisateur.

Tester :

1. Ouvrir une session avec localuser1 et son mot de passe sur serveurx, Que ce passe t-il et Pourquoi?

2. Ouvrir une session sur poste client avec localuser1.

3. Créer un autre compte utilisateur localuser2.

4. Modifier l'heure système.

5. Accéder au serveurx via voisinage réseau, que ce passe t-il?

Comment pouvez vous interprétez ce fait?

WWW.DZPEN.COM | قلم الجزائر

Chapitre2 : Gestion et configuration des comptes utilisateurs dans un domaine

Introduction :

Les comptes utilisateurs permettent aux utilisateurs d'accéder aux ressources du domaine : Les informations de comptes sont centralisées sur un serveur, dans l'annuaire des objets du réseau. Si une modification doit être apportée à un compte, elle doit être effectuée uniquement sur le serveur qui la diffusera à l'ensemble du domaine. Ils sont associés à un mot de passe, et fonctionnent dans un environnement définit (local ou domaine). Un utilisateur possédant un compte sur le domaine pourra donc s'identifier sur toutes les machines de ce domaine, sauf si l'administrateur met une restriction en place.

2.1 Définition d'Active Directory :

Active Directory est le nom du service d'annuaire (au sens informatique) de Microsoft. Active Directory permet de regrouper toutes les informations concernant le réseau, que ce soient les utilisateurs, les machines ou les applications. L'utilisateur peut ainsi trouver facilement des ressources partagées, et les administrateurs peuvent contrôler leurs utilisations grâce à des fonctionnalités de sécurisation des accès aux ressources répertoriées.

Active Directory a pour objectif de permettre la gestion des comptes, des ordinateurs, des ressources et de la sécurité de façon centralisée, dans le cadre d'un domaine. Un domaine constitue un ensemble d'utilisateurs et de machines dont le contrôle est centralisé.

2.1.1 Installation d'Active Directory :

L'installation d'Active Directory se fait à partir du gestionnaire de serveur en choisissant (ADD ROLES) ou Exécuter puis taper la commande DC PROM (voir figure 08).

WWW.DZPEN.COM | قلم الجزائر

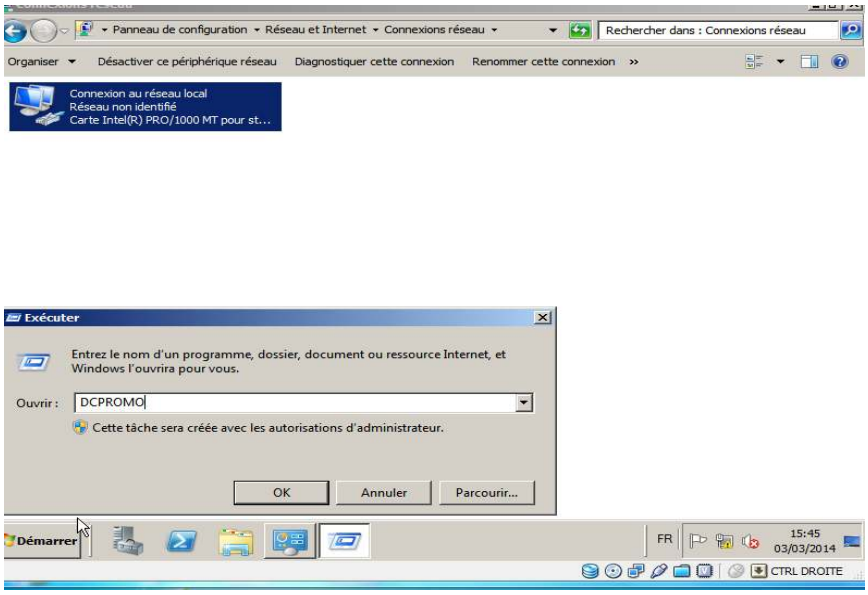


Figure 08

➢ La nomination du Domaine (voir figure 09):

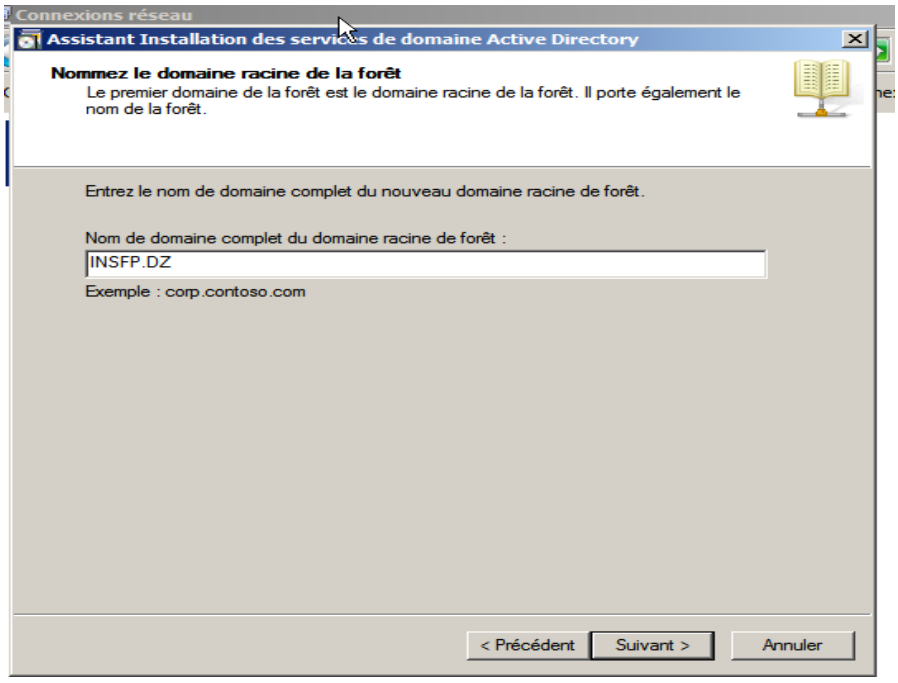


Figure 09

➢ Spécification de l'emplacement d'Active Directory (voir figure 10):

WWW.DZPEN.COM | قلم الجزائر

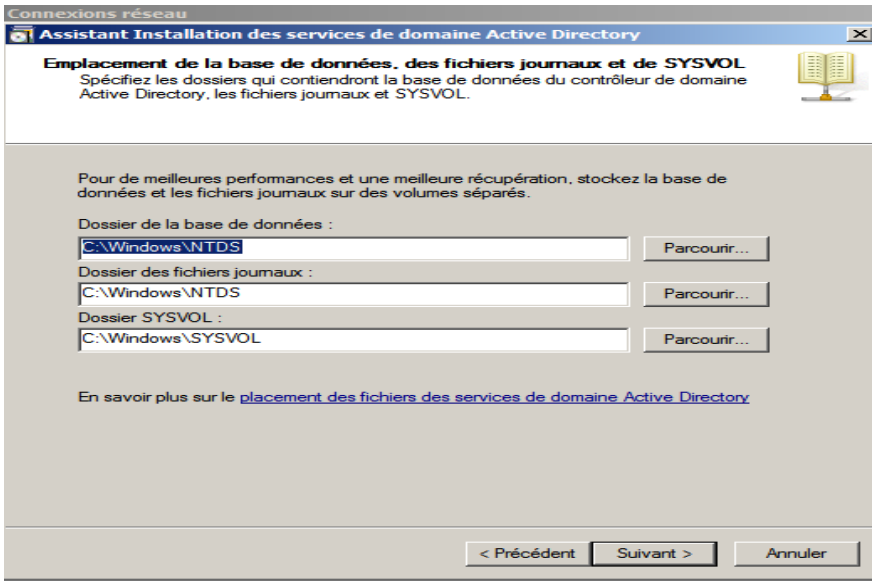


Figure 10

- L'installation d'Active Directory est en cours (voir figure 11) :

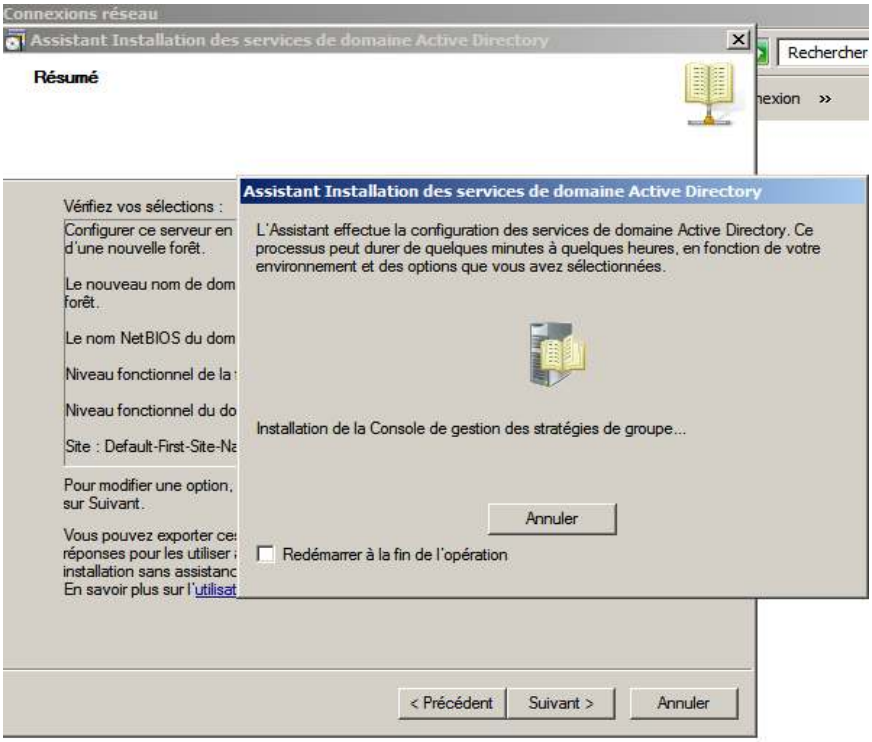


Figure 11

WWW.DZPEN.COM | قلم الجزائر

➢ La fin de l'assistant d'installation des services de domaine Active Directory (voir figure 12):

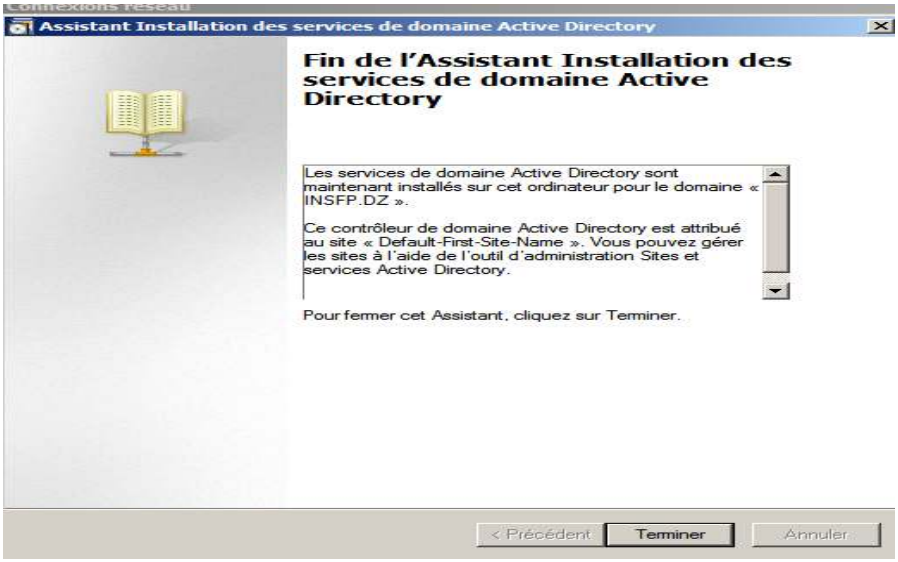


Figure 12

➢ Le service de domaine d'Active Directory est installé (voir figure 13):

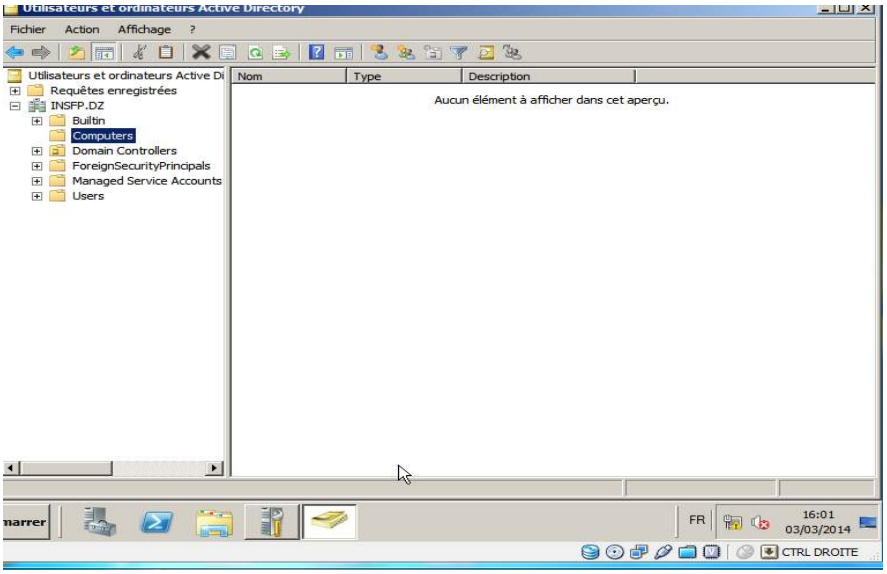


Figure 13

WWW.DZPEN.COM | قلم الجزائر

2.2 Compte utilisateur de domaine :

Les comptes d'utilisateurs de domaine résident dans Active Directory, sur des contrôleurs de domaine et peuvent accéder à toutes les ressources sur le réseau, à condition d'avoir les privilèges nécessaires.

2.3 Création d'un compte utilisateur de domaine :

Etant administrateur sur un ordinateur contrôleur de domaine, la création de compte d'utilisateur de domaine se fait par la console **Utilisateurs et ordinateurs Active Directory**. Tout en suivant les étapes suivantes :

- Cliquez sur **Démarrer**, puis sur **Programme**, pointez sur **Outil d'administration** et enfin choisir **Utilisateurs et ordinateurs Active Directory**.

-Déployez domaine, avec le bouton droit de la souris cliquez sur **Users** puis pointez sur **Nouveau** et choisir **Utilisateur (voir figure 14)**.

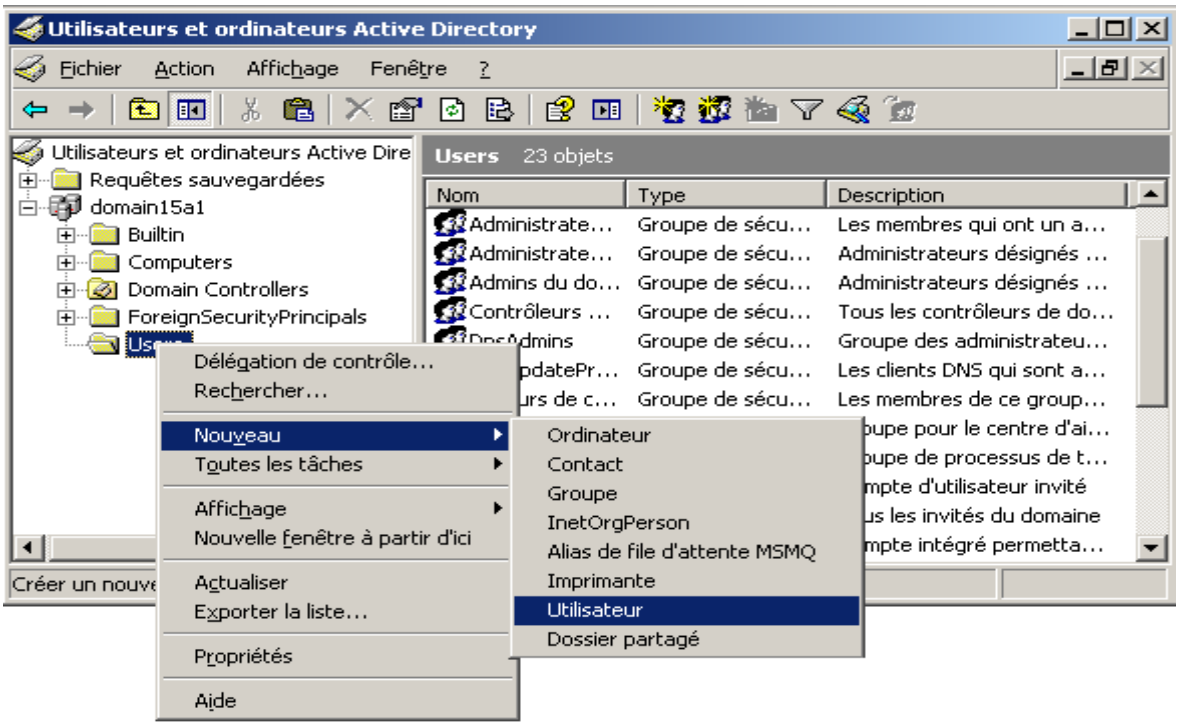


Figure 14

WWW.DZPEN.COM | قلم الجزائر

- La boite **Nouvel objet – utilisateur** vous offre la possibilité d'introduire les informations suivantes (voir figure 15) :

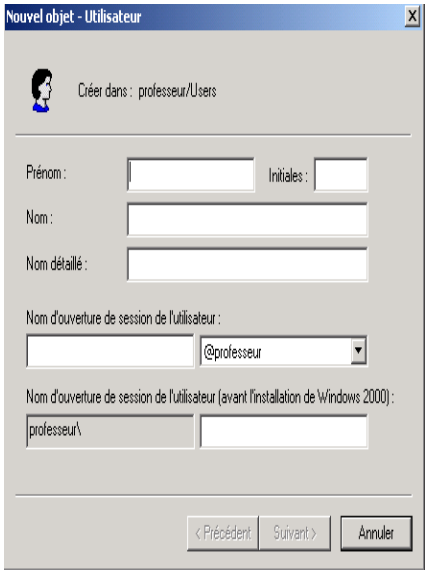


Figure 15

- Prénom : prénom de l'utilisateur qui est obligatoirement introduit.
- Initiales : initiales de l'utilisateur.
- Nom : nom de l'utilisateur, qui est aussi obligatoirement introduit.
- Nom détaillé : nom complet de l'utilisateur. Windows2003-2008 rempli automatiquement cette zone si vous fournissez les informations dans les zones Prénom, Initiales et Nom
- Nom d'ouverture de session de l'utilisateur : nom d'ouverture de session propre à l'utilisateur. Cette option comporte une liste qui identifie de façon unique l'utilisateur sur le réseau.
- Nom d'ouverture de session de l'utilisateur (avant l'installation de Windows 2000) : Nom d'ouverture de session dont l'utilisateur se servait les versions ultérieures de Windows 2003.

- Cliquer sur suivant une boite de dialogue s'affiche pour définir les options du mot de passe (voir la figure 16)

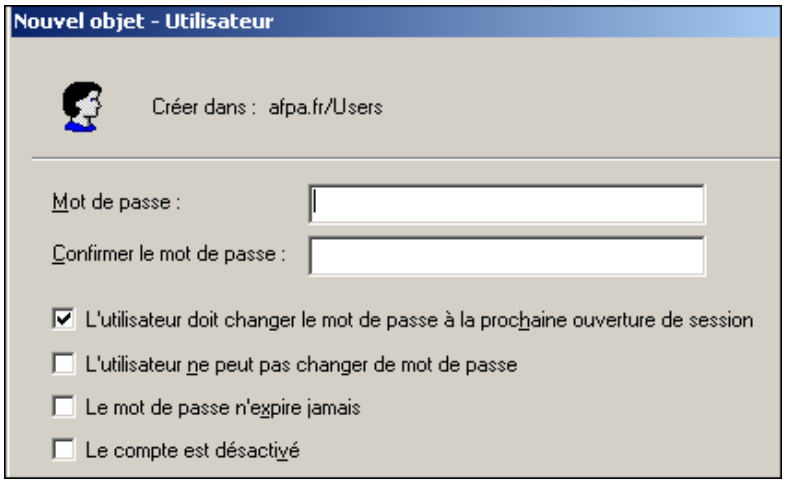


Figure 16

WWW.DZPEN.COM | قلم الجزائر

- **Mot de passe et Confirmer le mot de passe :** L'administrateur peut donner un mot de passe à l'utilisateur.
- **L'utilisateur doit changer le mot de passe à la prochaine ouverture de session:**

Concerne la majorité des utilisateurs. Lorsque le compte est crée par l'administrateur, ce dernier force le mot de passe d'ouverture de session. Cela oblige l'utilisateur à le changer immédiatement. Cela garantit que l'administrateur n'en aura plus connaissance et ne pourra pas utiliser l'identité de l'utilisateur.

- **L'utilisateur ne peut pas changer le mot de passe (compte sensible..) :** Utilisé pour les comptes partagés par plusieurs utilisateurs. Cela garanti qu'un utilisateur ne peut pas changer le mot de passe, et c'est s'assurer que les autres auront toujours accès à ce compte.
- **Le mot de passe n'expire jamais :** Option qui outrepasse les paramètres de la stratégie de compte, utilisé pour certains comptes qui ne sont pas souvent utilisés. (compte système ou compte de secours pour l'administrateur).
- **Le compte est désactivé :** Permet d'interdire l'accès aux ressources pour un compte particulier. Les comptes des utilisateurs momentanément absents doivent être désactivés.

2.4 Intégration d'un client dans un domaine :

Pour connecter un client à un domaine, nous devons connaître le nom du domaine et posséder un compte d'utilisateur valide sur le domaine, pour cela nous devons configurer le DNS dans les paramètres TCP/IP de l'ordinateur client tout en suivant les étapes suivantes :

- Ouvrez les propriétés de **Connexion au réseau** local (voir figure 17).

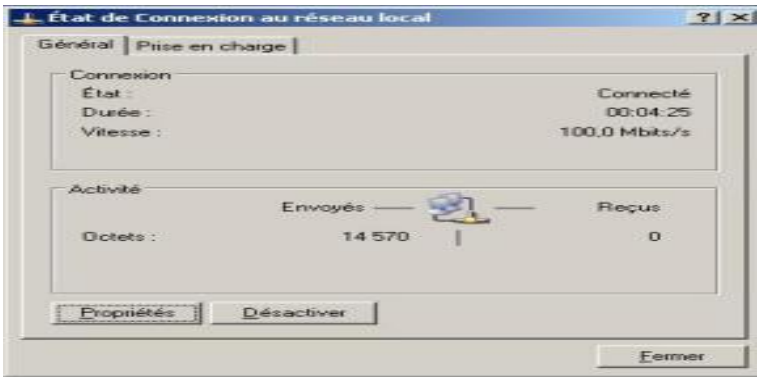


Figure 17

WWW.DZPEN.COM | قلم الجزائر

- Dans la liste, sélectionnez Protocole Internet (TCP/IP) puis cliquez sur Propriétés (voir figure 18).

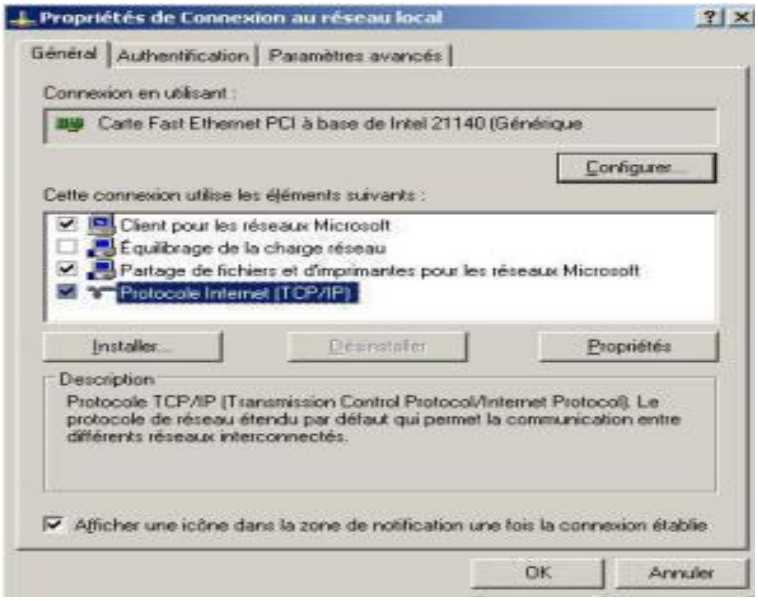


Figure 18

- Attribuer une adresse IP statique à votre ordinateur ainsi que le masque de sous-réseau et la passerelle par défaut (voir figure 19).

Remarque :

Dans la zone Serveur DNS préféré, l'adresse IP que vous devez entrer doit être celle du serveur DNS.



Figure 19

WWW.DZPEN.COM | قلم الجزائر

- Validez la modification puis redémarrez votre ordinateur. Tester la connectivité du poste client avec le serveur avec la commande **Ping** dans l'invité de commande .Après la configuration des paramètres TCP/IP de l'ordinateur client nous passons à l'intégration du client au domaine tout en suivant les étapes suivantes :

- Cliquez sur le bouton **Démarrer** , puis sur **Panneau de configuration** faites un double clic sur **Système**, puis cliquez sur **Modifier les paramètres.** (Voir la figure 20).



Figure 20

-Sous Paramètres de nom d'ordinateur, de domaine et de groupe de travail, cliquez sur Modifier.

- Si vous êtes invité à fournir un mot de passe administrateur ou une confirmation, fournissez le mot de passe ou la confirmation.

- Sous l'onglet Nom de l'ordinateur, cliquez sur **Modifier** (voir figure 21).

Vous pouvez également cliquer sur ID réseau pour utiliser **l'Assistant** Joindre un domaine ou un groupe de travail afin d'automatiser le processus de connexion à un domaine et la création d'un compte d'utilisateur de domaine sur votre ordinateur.

WWW.DZPEN.COM | قلم الجزائر

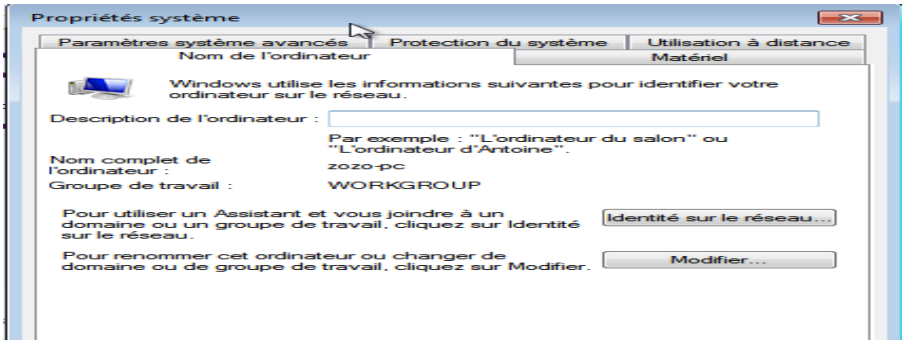


Figure 21

-Sous **Membre d'un**, cliquez sur **Domaine.** . Sous l'onglet Nom de l'ordinateur, taper le nom de l'ordinateur.

Tapez le nom du domaine que vous souhaitez rejoindre, puis cliquez sur **OK**

(Voir figure 22).

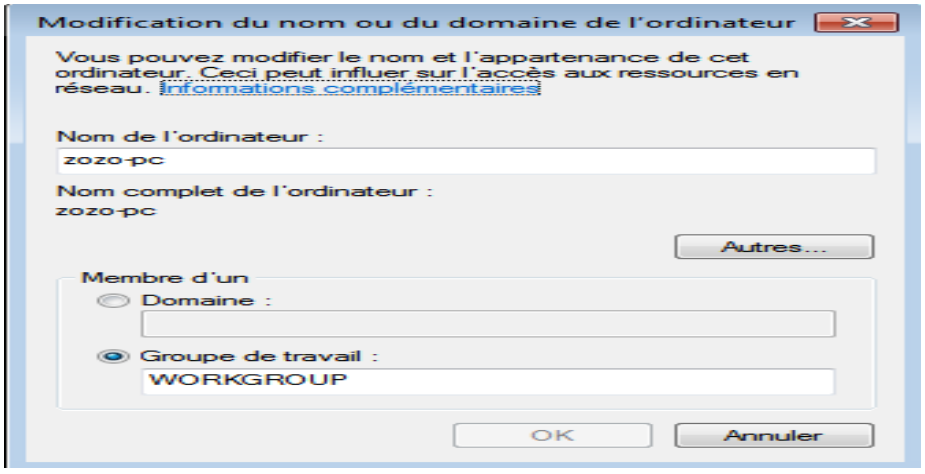


Figure 22

Remarque :

Vous serez invité à taper votre nom d'utilisateur et mot de passe pour le domaine.

Une fois que vous avez rejoint le domaine, vous êtes invité à redémarrer votre ordinateur.

Vous devez redémarrer votre ordinateur pour que les modifications prennent effet.

WWW.DZPEN.COM | قلم الجزائر

Test :

Pour tester la connexion de poste client au domaine nous devons procéder comme suit:

Cliquer sur le menu **démarrer** puis **outil d'administration**, utilisateur **et ordinateur active directory** et on clique sur **ordinateur** (computer) le nom de l'ordinateur s'affiche (voir figure 23).

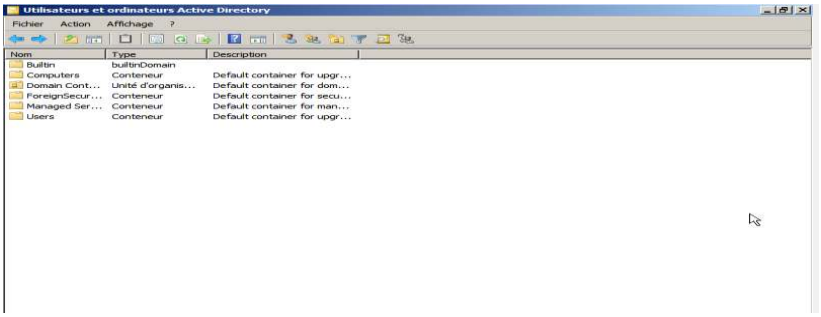


Figure 23

2.5 Propriétés d'un compte utilisateur :

La boîte de dialogue des propriétés d'un compte utilisateur du domaine peut accueillir jusqu'à treize onglets, selon la configuration du domaine (voir figure 24). Toutes les données saisies dans la boîte de dialogue des propriétés peuvent servir de critères de recherche dans **Active Directory**. Par exemple, vous pouvez trouver le numéro de téléphone ou le service d'un utilisateur en faisant une recherche sur le nom de cet utilisateur.

La boite de dialogue **Propriétés** contient les informations sur chaque compte d'utilisateur. Quatre onglets **Général**, **Adresse**, **Compte et Profil** contiennent des données personnelles .

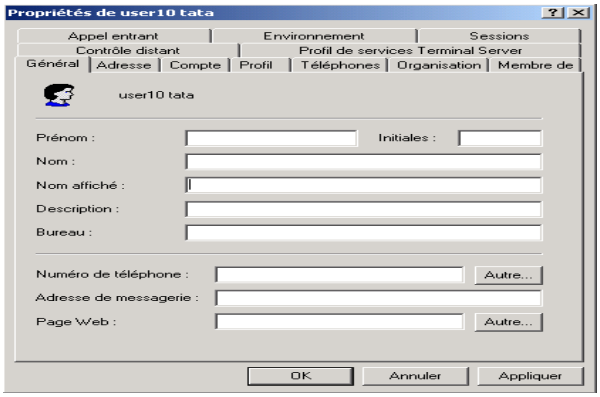


Figure 24

WWW.DZPEN.COM | قلم الجزائر

La configuration des propriétés d'un compte utilisateur de domaine se fait comme suit:

-Dans le menu **Outils d'administration**, choisissez **Utilisateurs et ordinateurs Active Directory.**

- Ouvrez le compte utilisateur du domaine concerné.

- Double cliquez sur le compte utilisateur pour ouvrir la boîte de dialogue **Propriétés**.

Cliquez sur l'onglet des propriétés à définir, effectuez les modifications de votre choix et cliquez sur **OK** lorsque vous avez terminé. (Voir figure 25)

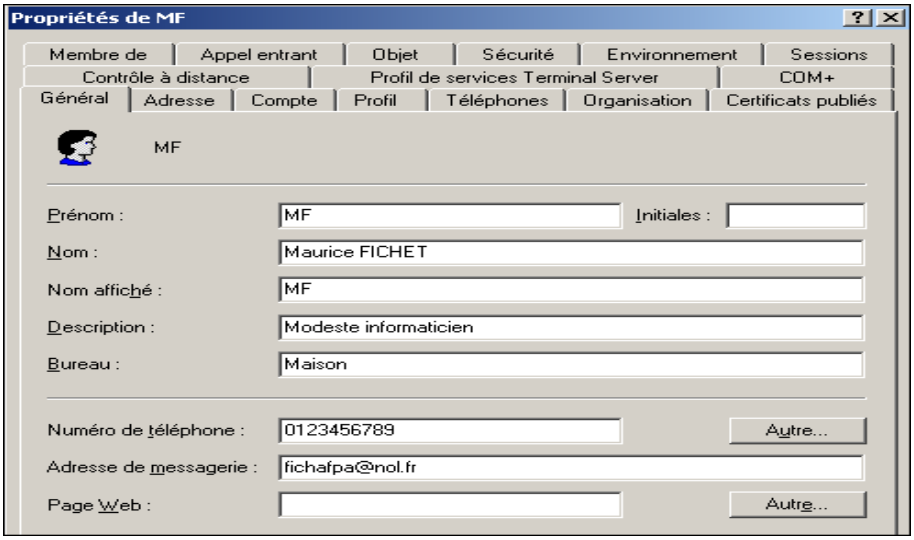


Figure 25

Les différentes propriétés sont :

- **Propriétés personnelles** sont les attributs des utilisateurs : (@dresse, n° Téléphone Émail …). Ces Informations sont stockées dans la Base d'annuaire. Elles permettent de localiser un utilisateur dans **Active Directory**.
- **Environnement**, **Sessions**, Contrôles **à Distance, profiles de services Terminal Server :** sont utilisés pour le service Terminal Server.
- **Certificats publiés**: gère les certificats de l'utilisateur
- **Membre de** : Groupe auquel appartient l'utilisateur.
- **Appel entrant** : Paramétrage de l'utilisateur d'accès distant.
- **Objet**: Informations sur les dates de création, modification de l'objet et affichage du N° USN.

WWW.DZPEN.COM | قلم الجزائر

- **Sécurité**: droits d'accès sur l'objet utilisateur.
- **Général**: infos générales de type nom, prénom….
- **Adresse**, **Téléphone**, **Organisations**: Infos de types générales sur l'utilisateur
- **COM+** : Appartenance de l'utilisateur dans les groupes de partitions COM+.
- **Compte** : Nom d'ouverture de session, horaires d'accès, options de mot de passe et date d'expiration du compte
- **Profil** : Chemin d'accès du profil utilisateur, chemin d'accès du script d'ouverture de session, chemin d'accès du répertoire personnel de l'utilisateur et toute connexion automatique à des lecteurs réseau.

2.6 Rechercher des personnes ou ordinateurs ou objets dans Active Directory :

A l'aide des renseignements que vous venez d'introduire dans la saisie du compte utilisateur par exemple, vous pouvez retrouver un utilisateur dans tout Active Directory.

Menu Action – **Rechercher** de la console **Utilisateurs et ordinateurs Active Directory**.

Validez le menu **Action** – recherché (voir la figure 26).

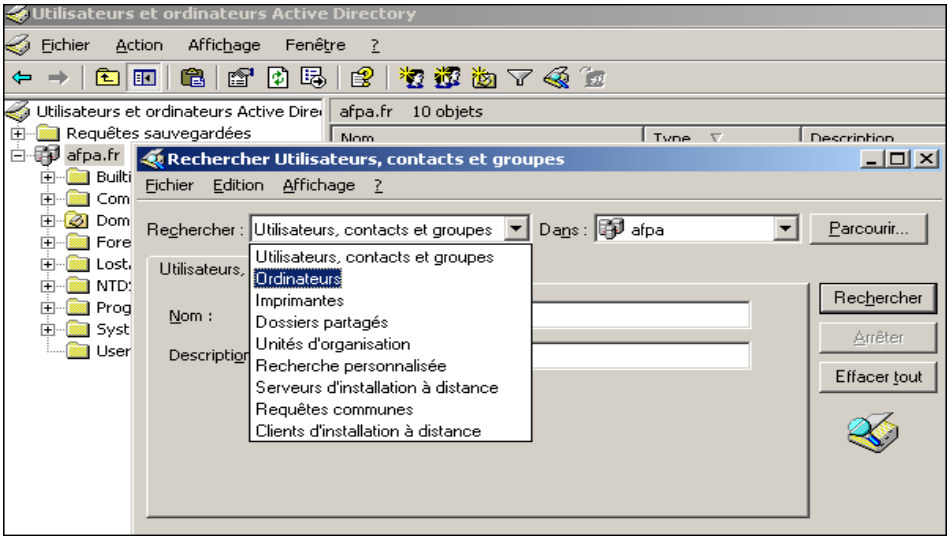


Figure 26

Après la sélection d'une personne ou ordinateur ou objet dans Active Directory, nous cliquons sur rechercher (voir figure 27)

WWW.DZPEN.COM | قلم الجزائر



Figure 27

2.7 Options de compte:

Des options peuvent être attribuées au compte de chaque utilisateur comme :

2.7.1 Heure de disponibilité ou restrictions d'horaires :

Les heures d'accès à l'ordinateur peuvent être restreintes de manière à ce que des intrus ne puissent utiliser l'ordinateur pendant l'absence de l'utilisateur autorisé. C'est utilisé pour la sécurité. Il vous suffit de définir des heures d'ouverture de session (horaire d'accès) (Voir figure 28).

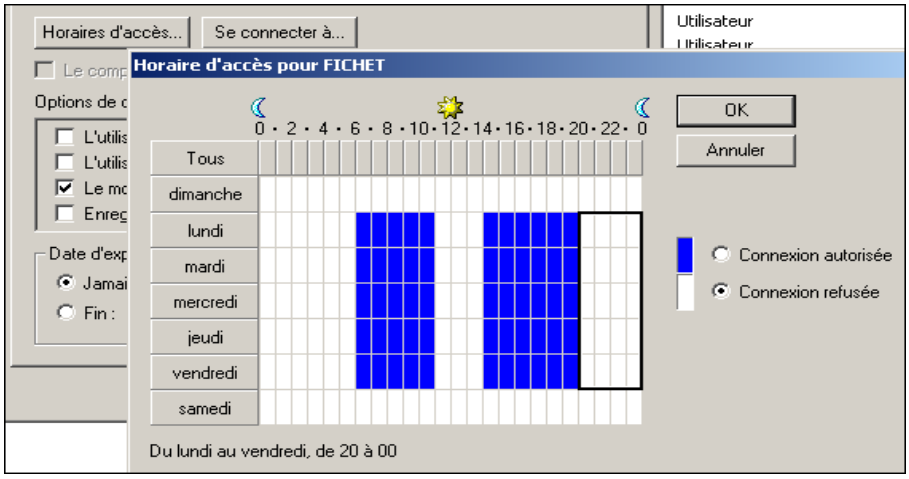


Figure 28

2.7.2 Ordinateurs autorisés :

La connexion au réseau à certains utilisateurs peut être autorisée qu'à partir d'un seul ou de plusieurs ordinateurs. Cette fonction nécessite que le protocole NetBIOS sur TCP/IP soit

WWW.DZPEN.COM | قلم الجزائر

activé. (Onglet Propriétés avancées de TCP/IP). C'est ce protocole qui permet d'identifier les ordinateurs par leurs noms.

Par défaut, les utilisateurs peuvent travailler en réseau à partir de n'importe quel ordinateur du domaine (voir figure 29).

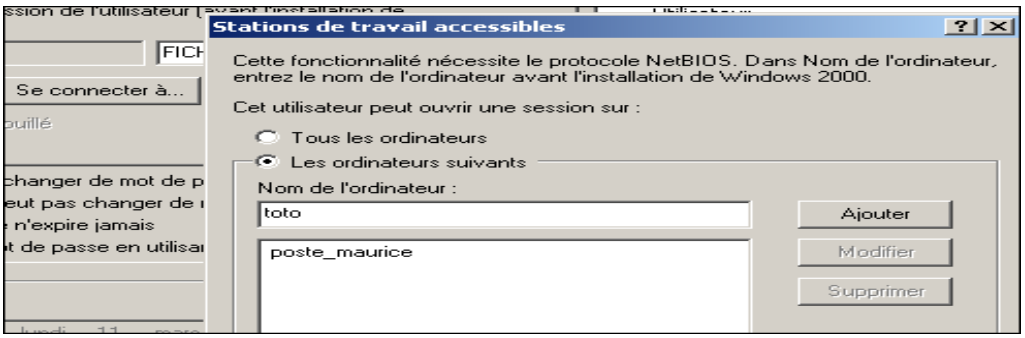


Figure 29

2.7.3 Expiration de compte :

L'option "**Date d'expiration de compte**" peut être rajoutée pour la désactivation automatique du compte (voir figure 30).

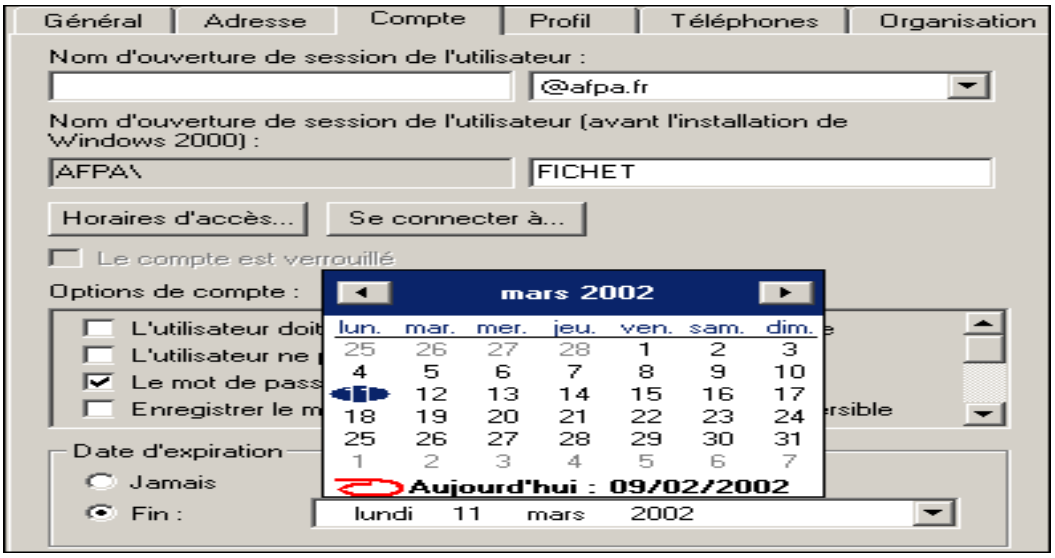


Figure 30

WWW.DZPEN.COM | قلم الجزائر

2.7.4 Copie d'un compte utilisateur :

La copie d'un compte utilisateur est utile si vous avez de nombreux utilisateurs identiques à créer, vous devez choisir un compte modèle puis à partir du menu **Action – Copier,** avec une copie les éléments suivants sont conservés (voir figure 31) :

- Restrictions horaires.
- Majorité des Options de comptes sur le mot de passe.
- Restriction d'accès.
- Date d'expiration.
- Appartenance aux groupes.
- Options de profil et de dossier de base.

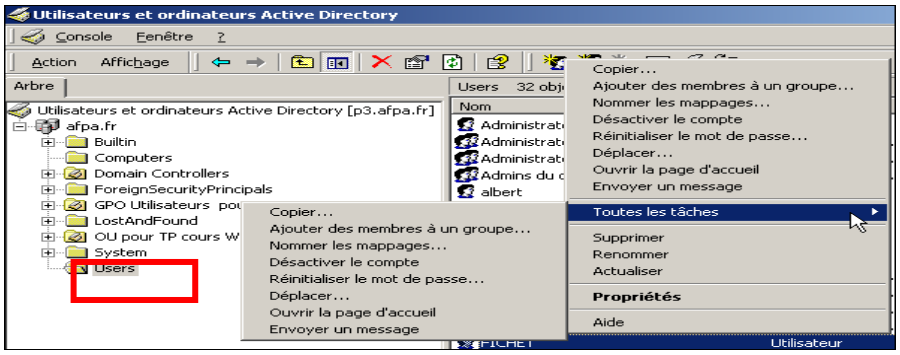


Figure 31

2.8 Exercice d'application :

1. Créer deux comptes utilisateurs de domaine section1, section2 avec les données suivantes:
   - Prénom : sect1, sec2.
   - Nom d'ouverture de session : section1, section2.
   - Le mot de passesection1, section2

2. Activer la case à cocher l'utilisateur doit changer de mot de passe à la prochaine ouverture de session.

WWW.DZPEN.COM | قلم الجزائر

2.9 Résumé :

Ce chapitre a défini la création et la configuration des comptes utilisateurs dans un domaine.ces dernier nous permettent de déterminer les caractéristiques exactes des comptes utilisateurs de domaine, à savoir les propriétés et les options des comptes.

2.10 Exercice de synthèse :

1. Créer deux comptes utilisateurs de domaine serveur1, serveur2 avec les données suivantes:

Prénom : user1, user2.

Nom d'ouverture de session : serveur1, serveur2.

Le mot de passe user1, user2.

Activer la case à cocher l'utilisateur doit changer de mot de passe à la prochaine ouverture de session.

2. Adhérer le poste clients au domaine serveurx.

3. Définir les propriétés du compte serveur1 avec les horaires d'accès du samedi à Jeudi de 8:00 à 16:00

4. Pour **serveur2** définir les horaires d'accès entre **12:00 et 20:00**, le reste des propriétés est le même que serveur1.

5. Tester :

6. Ouvrir une session avec serveur1 à partir de serveur que constater vous ?

7. Ouvrir une session avec serveur1 à partir de poste client.

8. Modifier l'heure système que constater vous?

9. Ouvrir une session avec serveur2 que constater vous?

WWW.DZPEN.COM | قلم الجزائر

Chapitre 3 : Le profil et le dossier de base d'un utilisateur

Introduction :

Un profil peut être relatif à une personne seule, ou à un groupe de personnes ayant des points communs, tels que par exemple les membres d'un groupe de travail. Il s'agit d'un ensemble de paramètres associé à un compte utilisateur. Ces paramètres rassemblent un grand nombre d'informations sur l'utilisateur, comme son identifiant, son adresse e-mail...

3.1 Profil par défaut et Profil Utilisateur :

Un profil d'utilisateur est crée à la première ouverture de session de l'utilisateur sur un ordinateur. Tous les paramètres propres à l'utilisateur sont automatiquement enregistrés dans le sous-dossier de cet utilisateur. Lorsque l'utilisateur ferme la session, son profil d'utilisateur est mis à jour sur l'ordinateur sur lequel il avait ouvert la session. Le profil d'utilisateur conserve donc les paramètres de bureau de l'environnement de travail de chaque utilisateur sur l'ordinateur local. Les types de profils d'utilisateur sont :

3.1.1 Profil d'utilisateur par défaut :

Le Profil d'utilisateur par défaut est la base de tous les profils d'utilisateur. A l'origine, chaque profil d'utilisateur est une copie du profil d'utilisateur par défaut, qui est stocké sur tous les ordinateurs exécutant Windows 2000 Professionnel ou Windows 2000,2008 server.

3.1.2 Profil d'utilisateur local :

Le Profil d'utilisateur local est crée à la première fois qu'un utilisateur ouvre une session sur un ordinateur, et est stocké sur l'ordinateur local. Toutes les modifications apportées au profil d'utilisateur local sont propres à l'ordinateur sur lequel les changements ont été effectués. Plusieurs profils d'utilisateurs locaux peuvent exister sur un ordinateur (voir figure 32)

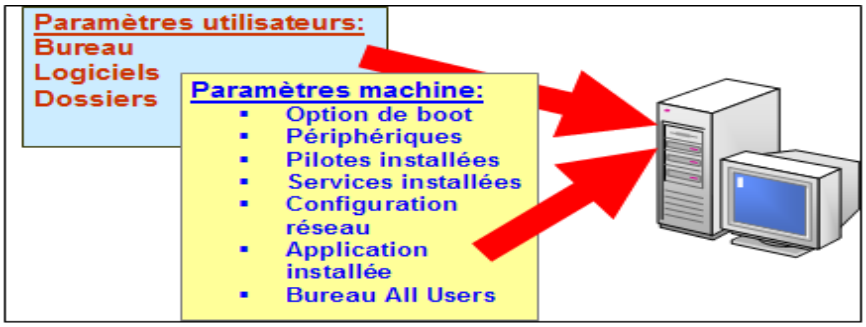


Figure 32

WWW.DZPEN.COM | قلم الجزائر

Remarque 1 :

Le dossier "**Mes Documents"** contient tous les fichiers créés par un utilisateur. En effet, par défaut, les commandes "**Ouvrir**" et "**Enregistrer sous…**" des applications Microsoft pointent vers le dossier "**Mes Documents"**. Pour chaque profil, il y a douze dossiers dont sept cachés et quelques fichiers dont **ntuser.dat (voir figure 33).**

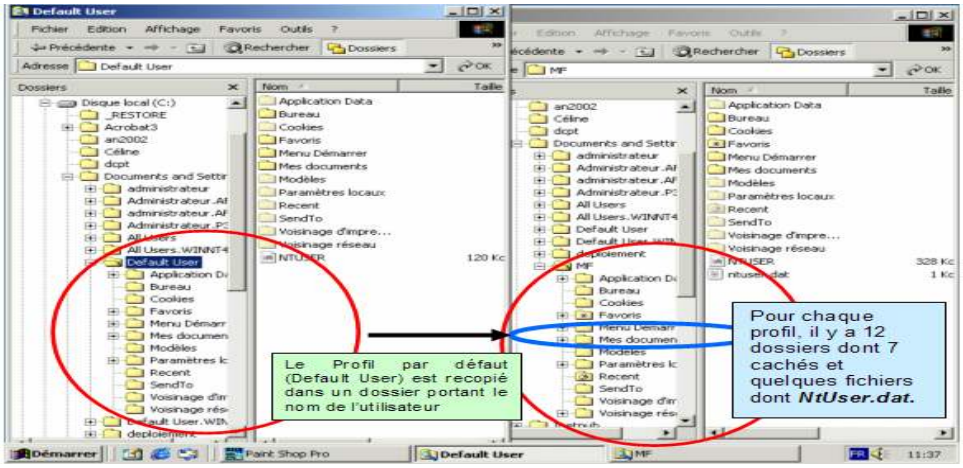
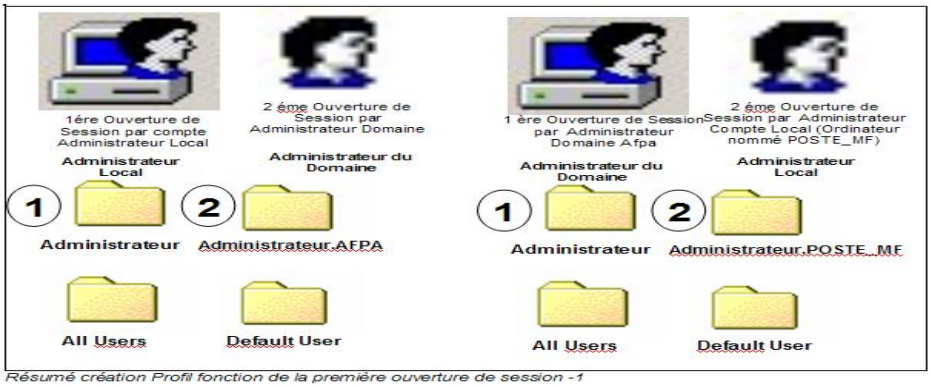


Figure 33

Remarque 2 :

Nous avons vu qu'un utilisateur retrouve son environnement de travail à chaque ouverture de session. Par contre si un utilisateur dispose d'un même nom pour se connecter en local et sur un domaine, deux dossiers différents seront crées. En fait lors de l'ouverture de session le système va essayer de créer un dossier portant le nom de l'utilisateur, mais si un dossier portant le même nom existe déjà, Windows2003- 2008 va automatiquement ajouter le nom du fournisseur de sécurité (domaine ou local en tant qu'extension **(voir figure 34).**



Résumé création Profil fonction de la première ouverture de session -1

Figure 34

WWW.DZPEN.COM | قلم الجزائر

3.2 Profils d'utilisateurs itinérants :

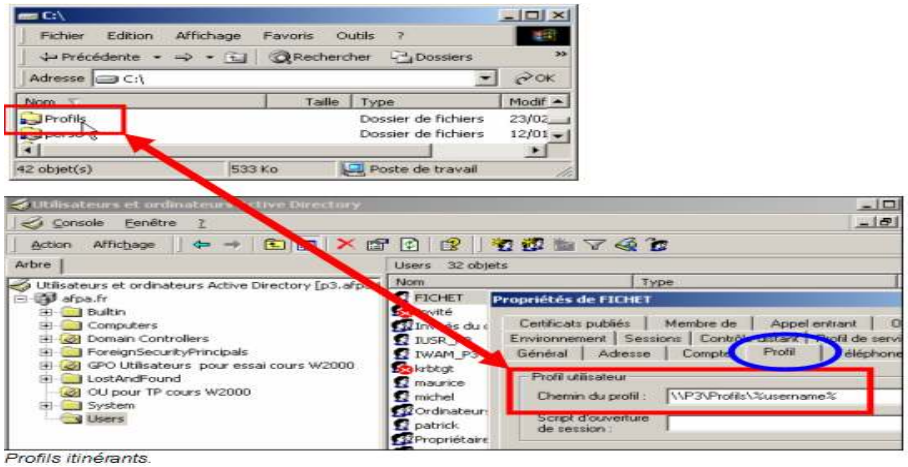
Le profil d'utilisateur itinérant est crée par l'administrateur système et stocké sur un serveur. Ce profil est disponible à chaque fois qu'un utilisateur ouvre une session sur un ordinateur sur le réseau. Si un utilisateur apporte des modifications aux paramètres de bureau, son profil d'utilisateur est mis à jour sur le serveur lorsqu'il ferme la session.

3.2.1 Profils obligatoires :

Le profil obligatoire est crée par l'administrateur pour indiquer les paramètres particuliers d'un utilisateur ou des utilisateurs, et peut être de type local ou itinérant. Un profil d'utilisateur obligatoire ne permet pas à un utilisateur d'enregistrer des modifications apportées aux paramètres de son bureau. L'utilisateur peut modifier les paramètres du bureau de l'ordinateur sur lequel il a ouvert une session, mais ces modifications ne sont pas enregistrées lorsqu'il la ferme.

3.2.2 Configuration d'un profil d'utilisateur itinérant :

Pour configurer un profil utilisateur itinérant aller dans la console **Utilisateurs** et **ordinateurs Active Directory**, créez un utilisateur, indiquez comme chemin d'accès le dossier qui contient son profil, puis configurez ce profil. Par exemple, créez un utilisateur appelé utilisateur1, puis indiquez comme chemin d'accès du profil **\\serveur\Profils\Utilisateur1**. Pour configurer le profil, ouvrez une session sur le domaine en tant qu'utilisateur1, modifiez selon les besoins les paramètres de bureau, puis fermez la session. (Voir figure 35).



Profils itinérants.

Figure 35

WWW.DZPEN.COM | قلم الجزائر

3.2.3 Création d'un profil itinérant personnalisé :

Pour créer un profil d'utilisateur itinérant, suivez la procédure ci-dessous.

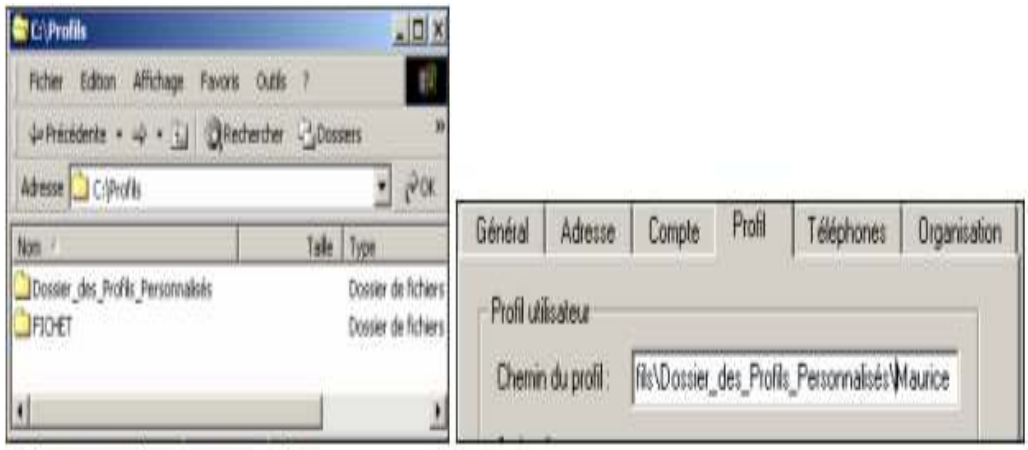
- Créez un dossier partagé sur le serveur, et donnez aux utilisateurs l'autorisation **Contrôle total** sur ce dossier.

- Indiquez le chemin d'accès du dossier partagé.

-Ouvrez la console **Utilisateurs et ordinateurs Active Directory**.

-Dans le volet de détails, cliquez avec le bouton droit sur le compte d'utilisateur approprié, puis cliquez sur **Propriétés**.

-Dans l'onglet **Profil**, sous **Profil utilisateur**, tapez le chemin du dossier partagé dans la zone **Chemin du profil**. Le chemin d'accès doit s'afficher de la façon suivante :**\\serveur\dossier_partagé\utilisateur**Vous pouvez utiliser la variable %**username**% au lieu d'indiquer le nom de l'utilisateur. Windows 2000 remplace alors automatiquement %**username**%par le nom du compte d'utilisateur du profil d'utilisateur itinérant. Seul un administrateur peut modifier un profil d'utilisateur itinérant une fois qu'il a été créé (voir figure 36).



Créer Profil itinérant personnalisé.

Figure 36

Remarque :

Le fichier Ntuser.dat contient la section du registre qui s'applique au compte d'utilisateur, et contient les paramètres du profil d'utilisateur. Ce fichier se trouve dans le dossier de profil de l'utilisateur.

WWW.DZPEN.COM | قلم الجزائر

3.2.4 Profil itinérant personnalisé obligatoire :

Si vous voulez toujours utiliser le même profil utilisateurs itinérant et que vous désirez qu'il ne soit pas modifié, vous devez mettre ce profil en mode lecture seule. Dans ce cas, les utilisateurs travailleront dans l'environnement qui leur a été assigné. Le fichier **Ntuser.dat** stocke les paramètres d'environnement de l'utilisateur. Si l'accès de ce fichier sur le serveur est en lecture seule, l'utilisateur recharge toujours le même environnement.

Le fichier sur le serveur ne pourra jamais être modifié, même si l'utilisateur a opéré des modifications en cours de session.

Sur le serveur, pour éviter les modifications du profil personnalisé obligatoire, modifiez le nom du fichier caché **NtUser.dat** en **NtUser.man.**

3.3 Création de Dossier de base :

L'emplacement par défaut ou l'utilisateur enregistre leur documents personnels est le dossier **Mes document**. Windows 2003-2008 offre un emplacement supplémentaire qui est le **dossier de base**. Ce dernier peut résider sur un ordinateur client ou dans un dossier partagé sur le serveur. Tous les dossiers de bases des utilisateurs peuvent être rassemblés dans un même emplacement réseau. La création de dossier de base se déroule comme suit :

- Dans un emplacement que vous réservez pour le dossier de base, créez et partager un dossier.
- Retirez l'autorisation **Contrôle total** au groupe **Tout le monde** et affectez le au groupe utilisateurs possédant les comptes.
- Dans l'onglet **Profil** et sous **Dossier de base**, cliquez sur **Connecter** et choisir une lettre de lecteur pour la connexion. Dans **A** entrez le chemin du dossier de base qui est de la forme **\\nom-serveur\nom-dossier-partagé\nom-de-session** (voir figure 37).

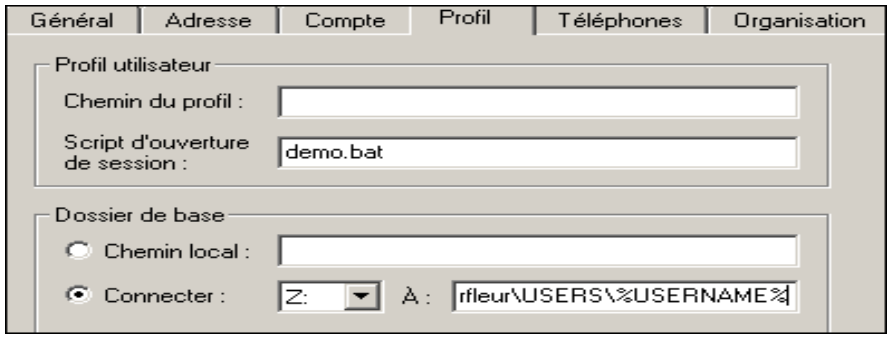


Figure 37

WWW.DZPEN.COM | قلم الجزائر

3.4 Création d'un script d'ouverture de session :

Les scripts d'ouverture de session définissent des commandes à exécuter à chaque ouverture de session. On s'en sert pour régler l'horloge du système, définir les chemins d'accès des lecteurs du réseau, des imprimantes, etc. Même s'il est possible de les exploiter pour exécuter des commandes ponctuelles, il est préférable de ne pas le faire pour définir des variables d'environnement. Tous les paramètres d'environnement utilisés par les scripts ne seront pas pris en compte par les processus utilisateurs ultérieurs. De même, ne les employez pas pour spécifier des applications à exécuter au démarrage. Placez plutôt les raccourcis appropriés dans le dossier démarrage de l'utilisateur. Les scripts d'ouverture de session contiennent généralement des commandes Windows. Toutefois, ils peuvent se présenter sous la forme suivante :

- Fichiers de l'environnement d'exécution de scripts Windows portant l'extension .vbs,js, ou toute autre extension de script valide.
- Fichiers batch portant l'extension .bat.
- Fichiers de commandes portant l'extension .cmd.
- Programmes exécutables portant l'extension .exe.

Plusieurs utilisateurs peuvent employer le même script d'ouverture de session et en tant qu'administrateur, vous contrôlez quel utilisateur exploite tel script. Comme leur nom l'indique, ces scripts d'ouverture de session s'exécutent lorsque les utilisateurs se connectent à leur compte.

Voici comment spécifier un script d'ouverture de session :

- Ouvrez la boîte de dialogue **Propriétés** de l'utilisateur dans **Utilisateurs et ordinateurs Active Directory**, puis sélectionnez l'onglet **Profil**.

- Tapez le chemin d'accès du **script** d'ouverture de session dans le champ du même nom. Assurez-vous de saisir le chemin d'accès complet, comme**\\Zeta\jdupont\eng.vbs.**

La création de scripts d'ouverture de session est plus simple qu'il n'y parait, surtout si vous exploitez le langage de commandes Windows. Presque toutes les commandes à taper à l'invite de commandes peuvent être exécutées dans un script d'ouverture de session. Les tâches les plus courantes de ces scripts sont la définition des imprimantes par défaut et des chemins d'accès réseau. Vous pouvez spécifier ces informations à l'aide de la commande NET USE. Les commandes NET USE suivantes définissent une imprimante réseau et un lecteur réseau :

WWW.DZPEN.COM | قلم الجزائر

net use lpt1: \\zeta\deskjet , net use g: \\gamma\corp\fichiers

Si vous placez ces commandes dans le script d'ouverture de session d'un utilisateur, celui-ci dispose d'une imprimante réseau sur LPT1 et d'un lecteur réseau sur G. Vous êtes libre de créer des connexions similaires dans un script. Avec VBScript, vous devez initialiser les variables et les objets que vous prévoyez d'utiliser puis invoquer les méthodes appropriées de l'objet Network pour ajouter les connexions.

Voici un exemple :

```
Option Explicit
Dim wNetwork, printerPath
Set wNetwork = WScript. CreateObject ("WScript.Network")
PrinterPath = "\\zeta\deskjet"
wNetwork.AddWindowsPrinterConnection printerPath
wNetwork.SetDefaultPrinter printerPath
wNetwork.MapNetworkDrive "G:", "\\gamma\corpfiles"
Set wNetwork = vbEmpty

Set printerPath = vbEmpty
```

On fait appel à la méthode AddWindowsPrinterConnectpour ajouter une connexionà l'imprimante Deskjet sur Zeta et à la méthode SetDefaultPrinterpour définirl'imprimante comme imprimante par défaut de l'utilisateur. On peut ensuiteinvoquer la méthode MapNetworkDrivepour définir un lecteur réseau sur G.

Quand vous tapez le nom d'un script dans la zone **Script d'ouverture de session** de la rubrique **Profil utilisateur** vous n'avez pas besoin de taper le chemin du dossier (voir figure 38).

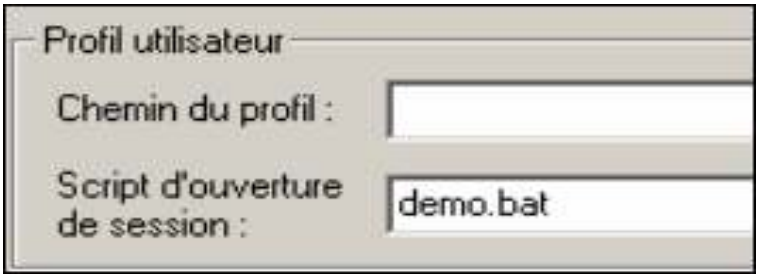


Figure 38

WWW.DZPEN.COM | قلم الجزائر

Les principales variables d'environnement utilisables dans un script d'ouverture de session sont :

- %HOMEDRIVE% Lecteur du répertoire de base (disque local ou unité réseau)
- %HOMEPATH% Répertoire de base.
- %HOMESHARE% Nom de partage contenant le répertoire de base.
- %OS% Système d'exploitation
- %PROCESSOR_ ARCHITECTURE% Type de processeur (par exemple x86)
- %USERDOMAIN% Domaine contenant le compte de l'utilisateur.
- %USERNAME% Nom de l'utilisateur

3.5 Exercice théorique :

1. Qu'est ce qu'un profil itinérant?

2. Quelle est la différence entre le profil itinérant et le profil obligatoire ?

3. Quel est le rôle d'un dossier de base ?

4. Qu'est ce qu'un script d'ouverture de session ?

3.6 Exercice pratique :

1. Créer un dossier sur le serveur appelé Profils et le partager avec un nom Profil.

2. Créer un profil itinérant pour l'utilisateur serveur1

3. Créer un profil itinérant obligatoire pour serveur2.

4. Ouvrer une session avec le compte serveur2et personnalisé votre bureau en créant des raccourcis (un raccourci vers le C par exemple) et un fichier texte.

WWW.DZPEN.COM | قلم الجزائر

3.7 Résumé :

Un profil est un environnement spécifiquement conçu pour un utilisateur.
Du point de vue de l'administrateur, le profil est un outil précieux qui permet de créer des profils par défaut pour tous les utilisateurs du réseau ou de créer des profils adaptés aux différents services ou postes de l'entreprise. Il est également possible de créer des profils obligatoires qui permettent aux utilisateurs de modifier la configuration du bureau alors qu'ils ont ouvert une session, sans que celle-ci soit enregistrée lors de la fermeture de la session. Un profil obligatoire présente toujours la même apparence à chaque fois qu'un utilisateur ouvre une session.

3.8 Exercice de synthèse :

1. Créer un dossier Profil sur le lecteur C.

2. Partager ce dossier avec le nom de partage par défaut «Profils».

3. Cocher la case Contrôle total.

4. Créer un compte utilisateur qui servira à créer des modèles de profils

Utiliser les informations suivantes :

- Prénom Profil.
- Nom Compte.
- Nom d'ouverture de session de l'utilisateur Profil.
- Nom d'ouverture de session de l'utilisateur (antérieur à 2000) Profil.
- Mot de passe Password001.

5. Déconnectez-vous de votre serveur.

6. Ouvrer une session avec le compte Profil.

7. Personnalisez votre bureau grâce à l'application affichage du panneau de configuration, ajouter sur le bureau les icônes Mes Documents, Poste de travail, Favoris Réseaux.

8. Créer un profil itinérant pour l'utilisateur Profil.

9. Tester le bon fonctionnement du profil.

10. Créer un dossier de base nommé base.

WWW.DZPEN.COM | قلم الجزائر

Chapitre 4: Gestion des groupes utilisateurs

Introduction :

Les groupes permettent de simplifier la gestion de l'accès des utilisateurs aux ressources du réseau. Les groupes permettent d'affecter en une seule action une ressource à un ensemble d'utilisateurs au lieu de répéter l'action pour chaque utilisateur. Un utilisateur peut être membre de plusieurs groupes.

4.1 Qu'est-ce qu'un groupe :

Un groupe est un ensemble de comptes d'utilisateur qui nous permet de gérer l'accès des utilisateurs aux ressources partagées, telles que les dossiers, les fichiers, les répertoires et les imprimantes réseaux partagés et d'accorder à ses membres des autorisations sur les ressources partagées en une seule fois (voir figure 39).

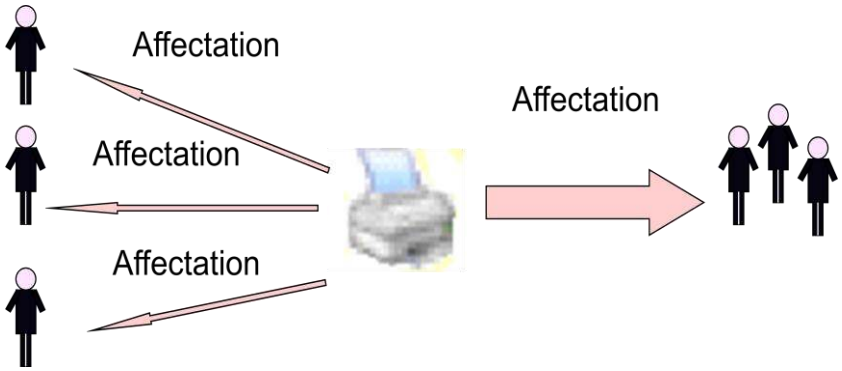


Figure 39

4.2 Groupes prédéfinis sur un ordinateur local :

Ils permettent d'accorder des permissions uniquement au niveau de la machine. Dans le cas d'une machine non-reliée à un domaine, il est possible d'inclure uniquement les comptes locaux. L'appartenance à un groupe permet d'hériter de ses « pouvoirs ». Certains groupes locaux sont prédéfinis et ne peuvent être supprimés mais seulement renommés (Voir figure 40).

Les groupes prédéfinis sur un ordinateur local sont :

- **Groupe administrateur :** contrôle total sur l'ordinateur.
- **Groupe Opérateurs de sauvegarde :** sauvegarde et restauration du système entier peut ouvrir une session locale et arrêté l'ordinateur ne peut pas modifier la

WWW.DZPEN.COM | قلم الجزائر

stratégie de sécurité.

- **Groupe opérateurs de configuration réseau :** paramétrage TCP/IP par exemple. Ne peut pas ajouter un périphérique.
- **Groupe utilisateur avec pouvoir :** Ils peuvent modifier l'heure, créer un compte, des partages, accéder à certaines parties du registre et donc installer certains programmes.
- **Groupe invités :** pas d'ouverture de session sur la machine pour le compte invité prédéfini mais autorisée aux membres du groupe,les tâches de gestion sont interdites.
- **Groupe duplicateurs :** réplication des fichiers entre serveurs dans un domaine. Le groupe existe en prévision de l'adhésion à un domaine (gestion par un serveur).
- **Groupe utilisateurs du bureau à distance :** utilisation de son bureau depuis un autreordinateur.
- **Groupe utilisateurs :** Ils ont très peu de pouvoir sur la gestion de la machine. Ils peuvent créer des imprimantes en tant que clients mais ne peuvent pas partager leurspropres répertoires.
- **Groupe help services group :** associé avec le compte utilisateur permet de lancer des outils de diagnostic.

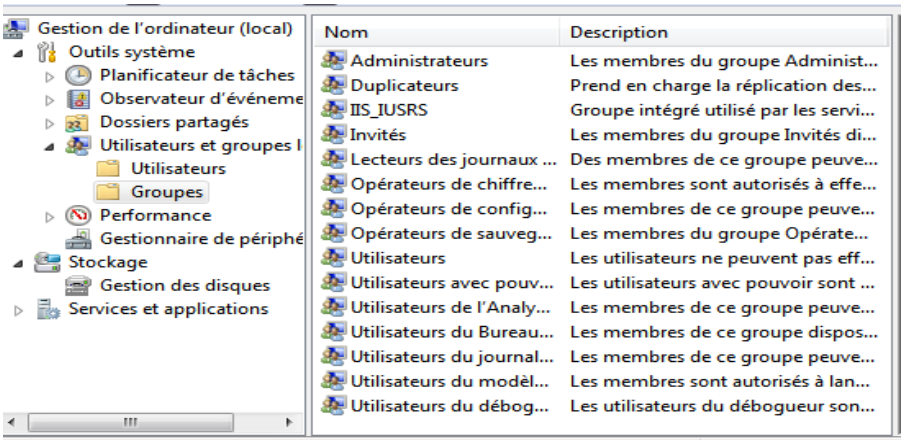
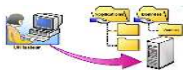


Figure 40

WWW.DZPEN.COM | قلم الجزائر



4.3 Groupes prédéfinis standards :

Les membres de ce groupe ne possèdent pas davantage d'autorisations ou de droits d'utilisateur qu'un compte d'utilisateur standard.

Dans les versions antérieures de Windows, le groupe prédéfinis standards (utilisateurs avec pouvoir) était conçu de manière à accorder aux utilisateurs des autorisations, et des droits d'administrateur spécifiques pour réaliser des tâches système courantes.

Dans cette version de Windows, les comptes d'utilisateurs standards peuvent par défaut réaliser la plupart des tâches de configuration courantes, telles que la modification des fuseaux horaires.

Pour les applications héritées qui exigent les mêmes autorisations et droits d'utilisateur avec pouvoir, que ceux définis dans les versions antérieures de Windows.

Les administrateurs peuvent appliquer un modèle de sécurité qui autorise le groupe utilisateurs avec pouvoir à assumer les mêmes droits et autorisations que ceux configurés dans les versions antérieures de Windows.

4.4 Groupe prédéfinis spéciaux ou groupes dits système :

Ils ne sont pas visibles pendant la gestion des groupes, ils apparaissent lors des affectations de permissions ou de droits. Les administrateurs ne peuvent leurs affecter des membres mais l'appartenance à ces groupes est réalisée par certaines actions de l'utilisateur ou de manière automatique. Ils sont appelés « **entités de sécurité intégrée ».**

- **Groupe tout le monde** : Ce groupe englobe toutes personnes connus ou non de la base SAM. Dès qu'un partage est créé, ce groupe y possède par défaut la permission« Contrôle total ». Pour les imprimantes il ne possède que le droit d'imprimer.
- **Groupe créateur propriétaire :** Avant qu'un utilisateur ne crée un objet, il n'appartient pas à ce groupe, juste après il en fait partie. Cela permet par exemple de créer un répertoire où tout le monde peut déposer un message et seuls les propriétaires ont la permission de modifier le leurs, les autres ne peuvent que les lire

WWW.DZPEN.COM | قلم الجزائر

Groupe interactif : Ce groupe intègre toutes personnes « logées » physiquement sur l'ordinateur.

- **Groupe utilisateurs authentifiés :** contient toute personne authentifiée en local ou à distance.
- **Groupe réseau :** contient les personnes authentifiées depuis le réseau.

4.5 Création d'un groupe :

La création d'un groupe local s'effectue à partir du composant logiciel enfichable **Utilisateurs et groupes locaux** accessible depuis la console **Gestion de l'ordinateur**.

Pour créer un groupe local suivez les étapes suivantes :

-Ouvrez **Gestion de l'ordinateur** depuis **Outils d'administration** du menu **Programmes**.

-Dans la partie gauche Arbre, sélectionnez **Groupes** du composant **Utilisateurs et groupes locaux**.

- Activez le menu **Action** ou le menu contextuel (clic droit) sur le dossier « **Groupes**» ou le menu contextuel (clic droit) dans la partie droite de la fenêtre.

-Sélectionnez **Nouvel groupe**.

-Complétez les rubriques de la boîte de dialogue **Nouveau groupe**.

-Ajoutez ou supprimez des membres.

-Cliquez sur le bouton « **Créer** » (Figure 41).

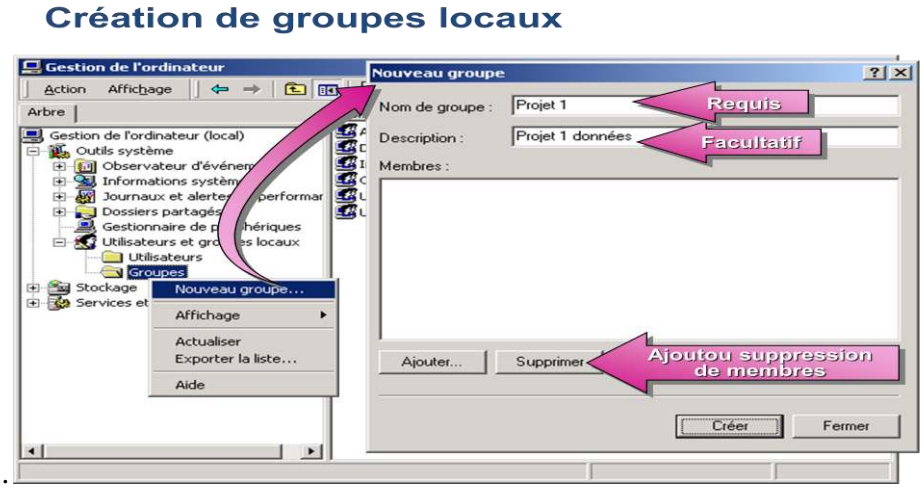
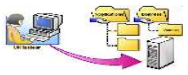


Figure 41

WWW.DZPEN.COM | قلم الجزائر



Les rubriques de la boîte de dialogue « Nouveau groupe » sont décrites ci-après (Tableau42):

Rubrique Description	Rubrique Description
Nom de groupe	Nom unique du groupe local, ce nom doit être différent de tout autre nom de groupe ou nom d'utilisateur contenu dans la base de données locale de sécurité de l'ordinateur. Il peut contenir jusqu'à 256 caractères. Cette zone est obligatoire.
Description	Zone permettant la saisie d'un texte descriptif sur le groupe local.
Ajouter	Permet d'ajouter un utilisateur dans la liste des membres du groupe local.
Supprimer	Permet de supprimer l'utilisateur sélectionné dans la liste des membres du groupe local.
Créer	Valide la création d'un nouveau groupe.
Fermer	Ferme la boite de dialogue Nouveau groupe mais ne valide pas la création en cours d'un nouveau groupe.

Tableau 42

4.6 Stratégie d'utilisation de groupes locaux dans un groupe de travail :

Dans un environnement de groupe de travail, la stratégie utilisée pour accorder des autorisations est simple. Tout d'abord, vous pouvez uniquement les utiliser pour l'ordinateur local.

Tout utilisateur qui souhaite accéder à une ressource partagée ou réalisé une tâche système sur un ordinateur, doit disposer d'un compte utilisateur sur cet ordinateur.

Si plusieurs utilisateurs d'un ordinateur doivent accéder à la même ressource ou réaliser la même tâche système, vous devez utiliser un groupe local pour accorder les autorisations ou les droits, puis ajouter les comptes d'utilisateurs appropriés en tant que membres.

Cette méthode s'appelle la stratégie **ALP** :

Placer des comptes utilisateurs (**A**) dans un groupe local (**L**) de l'ordinateur qui héberge les ressources, ou sur laquelle vous souhaitez que les utilisateurs réalisent des tâches système.

Accordez des autorisations (**P**) ou des droits au groupe local de l'ordinateur qui héberge la ressource réseau, ou sur lequel les tâches systèmes doivent être réalisées.

WWW.DZPEN.COM | قلم الجزائر

Si vous le pouvez accordez des droits aux comptes utilisateurs en les incorporant dans un groupe intégré, au lieu de créer un groupe local (figure 43).

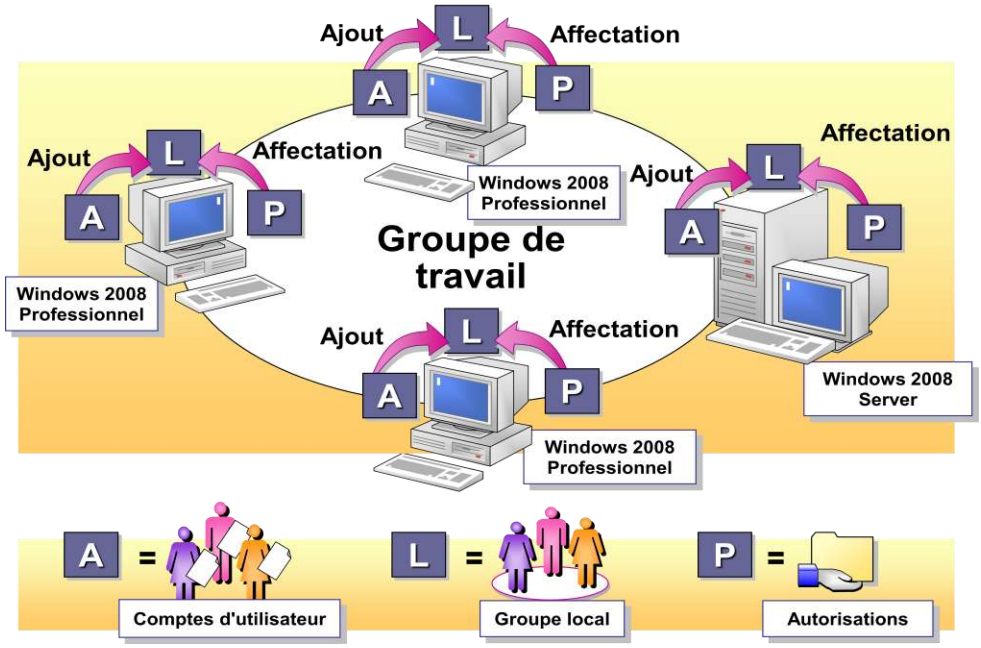


Figure 43

4.7 Groupe d'utilisateur dans un domaine :

Les groupes de Windows 2003-2008 sont utilisés pour gérer les comptes d'utilisateurs dans le but d'accéder à des ressources. Tout ceci dans un souci de simplifier l'administration.

Il est en effet plus aisé d'utiliser un groupe en fonction du besoin, plutôt que de sélectionner plusieurs utilisateurs éparpillés dans une liste de comptes.

Les groupes peuvent bénéficier de droits particuliers (comme par exemple le droit de sauvegarder, de gérer les imprimantes, etc. ...) ou hériter des droits par imbrication du groupe dans un autre groupe (voir figure 44).

WWW.DZPEN.COM | قلم الجزائر

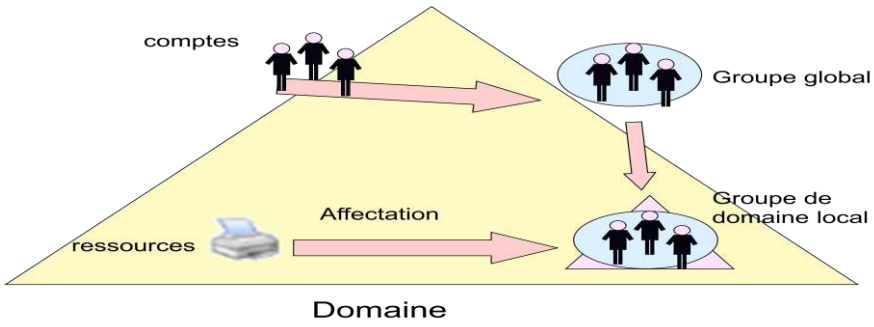


Figure 44

- Puisqu'un objet hérite automatiquement des droits de son parent, il est intéressant de former des groupes, d'y placer des objets, et d'attribuer des permissions aux groupes. Cela évite de traiter chaque objet séparément (voir figure 45).

Sur les ressources, on définit les autorisations (droits Lecture, Ecriture, Modifier, …) que l'on veut affecter à certains utilisateurs ou groupes.

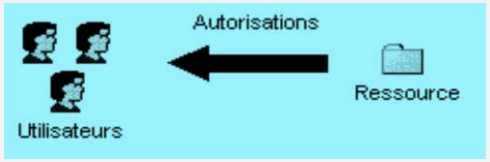


Figure 45

- Les groupes simplifient l'affectation d'autorisations à des ressources (voir figure 46) :

On peut ainsi former un groupe « Tle_5 » qui est le seul à avoir accès à un dossier défini. Il suffit de placer dans ce groupe tous les élèves de cette classe.

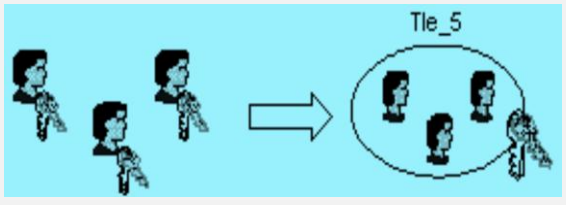


Figure 46

WWW.DZPEN.COM | قلم الجزائر

- Les utilisateurs peuvent être membres de plusieurs groupes (voir figure 47):

On peut ainsi placer les mêmes utilisateurs dans des groupes différents. L'élève Ali est dans le groupe Tle_5, mais il est également dans le groupe TPE.

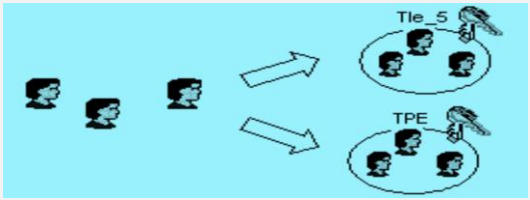


Figure 47

- Les groupes peuvent être imbriqués dans d'autres groupes (voir figure48):

On peut même imbriquer des groupes (les groupes Tle_1, Tle_2, etc… appartiennent à un même groupe appelé « Terminales » qui est seul à avoir accès à un dossier « Terminales »)

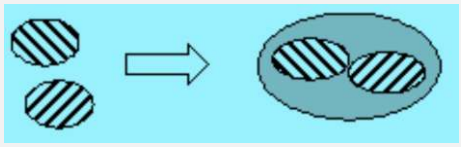


Figure 48

- L'attribution des autorisations d'une même ressource à plusieurs groupes (voir figure 49).

On peut attribuer des autorisations d'une même ressource à plusieurs groupes (ex : l'imprimante est accessible aux groupes Tle_1, Tle_2, … Tle_5, mais pas aux autres élèves.

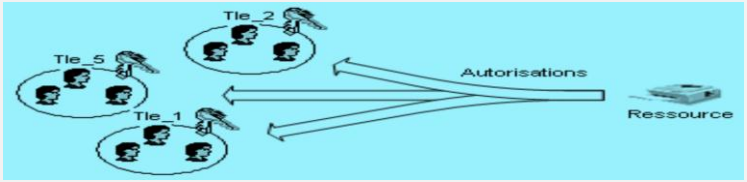
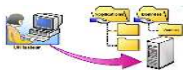


Figure 49

WWW.DZPEN.COM | قلم الجزائر



4.8 Les types de groupes:

Deux types de groupes sont disponibles :

4.8.1 Groupe de sécurité :

Les groupes de sécurité permettent d'affecter des utilisateurs et des ordinateurs à des ressources. Peuvent aussi être utilisés comme groupes de distribution.

4.8.2 Groupe de distribution :

Les groupes de distribution exploitables entre autres via un logiciel de messagerie. Ils ne permettent pas d'affecter des permissions sur des ressources aux utilisateurs.

Les applications utilisent des groupes de distribution comme listes pour des fonctions non liées à la sécurité, t'elle que l'envoi de messages électroniques a des groupes d'utilisateurs.

4.9 Les étendues de groupes :

L'étendue d'un groupe définit les restrictions d'appartenance et d'utilisation du groupe. Il existe trois étendues différentes :

4.9.1 Groupe global :

Le groupe global peut être utilisé pour accorder un accès à des ressources dans n'importe quel domaine de la forêt et il sert généralement à regrouper des utilisateurs ayant des besoins similaires en termes d'accès aux ressources.

4.9.2 Groupe de domaine local :

Le groupe de domaine local ne peut être utilisé que pour un accès à des ressources du domaine local. Il est utilisé pour accorder des autorisations sur des ressources de domaine situées dans le même domaine que celui dans lequel nous avons crée le groupe de domaine local. La ressource peut résider ailleurs que sur un contrôleur de domaine.

4.9.3 Les groupes universels :

Les groupes universels peuvent être utilisés pour accéder à des ressources dans n'importe quel domaine de la forêt. Ils diffèrent des groupes globaux par le fait qu'ils ne sont disponibles que dans les domaines WS2003, 2008 s'exécutant en mode natif.

WWW.DZPEN.COM | قلم الجزائر

De plus leurs membres peuvent provenir de n'importe quel domaine, alors que ceux des groupes globaux ne peuvent provenir que du propre domaine du groupe. Les groupes universels sont nouveaux dans WS2003, 2008 et n'ont pas d'équivalence sous NT.

4.9.4 Imbrication de groupes :

L'imbrication permet d'ajouter un groupe en tant que membre d'un autre groupe.

L'imbrication des groupes permet de consolider leur gestion.

L'imbrication augmente les comptes membres affectés par une action unique, et réduit la fréquence de réplication provoquée par la réplication de modifications dans l'appartenance aux groupes.

Les options d'imbrication sont variables selon que le niveau de fonctionnalité de votre domaine Windows Server 2003, 2008 et Windows 2000 en mode natif ou Windows 2000 en mode mixte.

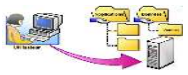
Un groupe imbriqué hérite automatiquement les permissions de son groupe parent et peut également disposer de permissions spécifiques.

L'imbrication de groupes peut faciliter leur gestion à condition qu'elle soit planifiée avec soin. Pour imbriquer des groupes, il suffit de sélectionnez le groupe qui deviendra le groupe enfant, et de l'ajouter en tant que membre du groupe choisit comme groupe parent. Le groupe enfant apparaît dans l'onglet Membres (voir figure 50).



Figure 50

WWW.DZPEN.COM | قلم الجزائر



- En mode mixte :

- Un groupe **Local de domaine** peut contenir des utilisateurs et groupes globaux de n'importe quel domaine.
- Un groupe **Global** peut contenir uniquement des utilisateurs du même domaine que le sien. II n'existe pas de groupe **Universel** en mode mixte.

- En mode natif :

- Un groupe **Local de domaine** peut contenir des comptes d'utilisateurs, des groupes globaux et des groupes universels de n'importe quel domaine de la forêt ainsi que des domaines locaux de son propre domaine. Mais il ne peut être membre d'un autre groupe.
- Un groupe **Global** peut contenir des comptes d'utilisateurs et des groupes globaux uniquement du même domaine.
- Un groupe **Universel** peut contenir des comptes d'utilisateurs, des groupes globaux et des groupes universels de n'importe quel domaine de la forêt.

Remarque :

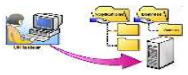
Le groupe local de domaine peut être utilisé pour mettre des permissions sur des ressources de son domaine, il n'est visible que dans son propre domaine.

Les groupes **g**lobaux et universels peuvent être utilisés pour définir des permissions sur des ressources à partir de n'importe quel domaine de la forêt. Ils sont visibles dans tous les domaines de la forêt (voir tableau 51).

Étendue	**Peut être imbriqué dans**		
	Global	**Domaine local**	**Universel**
Global	Oui (uniquement depuis le même domaine)	Oui	Oui
Domaine local	Non	Non	Non
Universel	Non	Oui	Oui

Tableau 51

WWW.DZPEN.COM | قلم الجزائر



4.10 Méthodologies d'utilisation des groupes :

Pour utiliser les groupes de manière efficace, il vous faut des stratégies permettant d'appliquer les différentes étendues de groupes. Le choix de la stratégie dépend de l'environnement réseau Windows de votre organisation. En présence d'un domaine unique, des groupes globaux et des groupes locaux de domaine sont généralement utilisés pour accorder des autorisations d'accès aux ressources réseau.

Afin de choisir les étendues de groupe les plus adaptées à vos besoins, nous allons présenter quelques méthodes d'implémentation basées sur des règles mnémotechniques.

Ainsi nous désignerons chaque élément par un symbole :

A (Account) Compte d'utilisateur

L (Local Group) Groupe Local

G (Global Group) Groupe Global

DL (Domain Local Group) Groupe Local de domaine

U(Universel Group) groupe universel

P(Permission) droit et autorisation

-La stratégie A. G. P :

La stratégie **A G P** permet de placer des comptes d'utilisateurs (**A**) dans des groupes globaux (**G**) et d'accorder des autorisations (**P**) aux groupes globaux. Cette stratégie a une limite : elle complique l'administration dans le cas de plusieurs domaines. Si des groupes globaux de plusieurs domaines requièrent des autorisations identiques, vous devez accorder ces autorisations à chaque groupe global individuellement. Vous pouvez appliquer la stratégie **A G P** aux forêts incluant un seul domaine et très peu d'utilisateurs, et auxquelles vous n'allez jamais ajouter d'autres domaines.

- La stratégie **A G P** présente les avantages suivants :
  - Les groupes ne sont pas imbriqués et peuvent donc faciliter le dépannage.
  - Les comptes appartiennent à une seule étendue de groupe.
- La stratégie **A G P** présente les inconvénients suivants :

WWW.DZPEN.COM | قلم الجزائر

- Chaque fois qu'un utilisateur s'authentifie pour accéder à une ressource, le serveur doit contrôler l'appartenance au groupe global pour vérifier si l'utilisateur est toujours membre du groupe.
- Elle a un impact négatif sur les performances car un groupe global n'est pas mis en cache.

-La stratégie A G DLP :

La stratégie **A G DLP** permet de placer des comptes d'utilisateurs (**A**) dans des groupes globaux (**G**), puis d'insérer les groupes globaux dans des groupes locaux de domaine (**DL**) et d'accorder des autorisations (**P**) aux groupes locaux de domaine. Cette stratégie offre davantage de souplesse pour la croissance du réseau, et limite le nombre de fois où vous devez définir des autorisations. La stratégie **A G DL P** peut être appliquée à une forêt comportant un ou plusieurs domaine(s) et à laquelle vous pourriez ajouter d'autres domaines (voir figure 52).

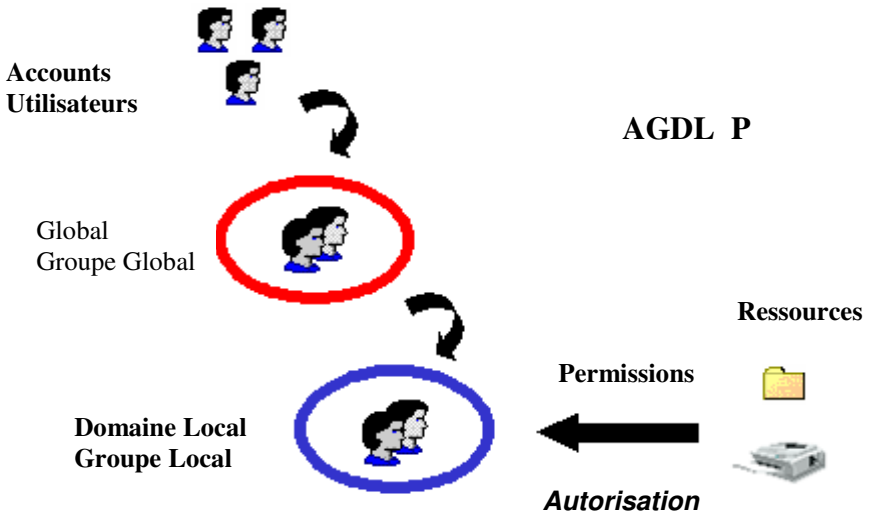
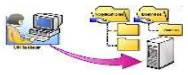


Figure 52

➢ La stratégie **A G DL P** présente les avantages suivants :

- Les domaines sont flexibles.
- Les propriétaires de ressources requièrent moins d'accès à Active Directory pour sécuriser de manière souple leurs ressources.

WWW.DZPEN.COM | قلم الجزائر



➢ La stratégie **A G DL P** présente les inconvénients suivants :

▪ Une structure de gestion à plusieurs niveaux est plus complexe à configurer au départ mais plus facile à gérer à long terme.

- La stratégie A G U DL P :

La stratégie **A G U DL P** vous permet de placer des comptes d'utilisateurs (**A**) dans des groupes globaux (**G**), d'insérer les groupes globaux dans des groupes universels (**U**), puis de placer les groupes universels dans des groupes locaux de domaine (**DL**) et d'accorder des autorisations (**P**) aux groupes locaux de domaine.

Utilisez **A G U DL P** pour une forêt possédant plusieurs domaines afin que les administrateurs puissent consolider des groupes globaux de plusieurs domaines dans un seul groupe universel. Ce groupe universel peut ensuite être placé dans tout groupe local de domaine, dans tout domaine d'approbation, et ainsi accorder des droits ou des autorisations à de nombreux groupes globaux de plusieurs domaines en une seule action.

➢ La stratégie A G U DL P présente les avantages suivants :

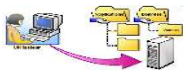
▪ Flexibilité au niveau de la forêt.

▪ Possibilité de gestion centralisée.

- la stratégie A G L P :

- La stratégie **A G L P est** appliquée pour placer des comptes d'utilisateurs dans un groupe global, et accorder des autorisations au groupe local. Cette stratégie à une limite, elle ne permet pas d'octroyer des autorisations d'accès à des ressources situées hors de l'ordinateur local. Veillez donc à placer des comptes d'utilisateurs dans un groupe global, à ajouter le groupe global au groupe local, et à accorder des autorisations au groupe local.

WWW.DZPEN.COM | قلم الجزائر



Cette stratégie vous permet d'utiliser un même groupe global sur plusieurs ordinateurs locaux. Utilisez autant que possible des groupes locaux de domaine. Utilisez des groupes locaux uniquement si aucun groupe local de domaine n'a été crée à cette fin.
Vous pouvez utiliser la stratégie **A G L P** si votre domaine présente les caractéristiques suivantes :

- Mise à niveau de Microsoft Windows NT4.0 vers Windows Server 2003 -2008.
- Maintien d'une stratégie de groupe Windows NT 4.0.
- Maintien d'une gestion centralisée des utilisateurs avec gestion décentralisée des ressources.

➢ La stratégie A G L P présente les avantages suivants :

- Elle maintient la stratégie de groupe Windows NT 4.0.
- Les propriétaires de ressources appartiennent à chaque groupe nécessitant un accès.

➢ La stratégie **A G L P** présente les inconvénients suivants :

- Active Directory ne contrôle pas l'accès.
- Vous devez créer des groupes redondants au niveau des serveurs membres.
- Elle n'autorise pas la gestion centralisée des ressources.
- L'appartenance au groupe local n'est pas dupliquée.

4.11 Les groupes par défaut sur les serveurs contrôleurs de domaine:

Les groupes par défaut possèdent des droits, et des autorisations prédéfinis qui permettent de faciliter la mise en place d'un environnement sécurisé. Ainsi un certain nombre de rôle courant sont directement applicable, en faisant membre du groupe par défaut adéquat l'utilisateur à qui l'on souhaite donner des droits ou autorisations.
Ces groupes et les droits qui leurs sont associés sont crées automatiquement.

WWW.DZPEN.COM | قلم الجزائر

4.11.1 Les groupes prédéfinis :

Sur tous les ordinateurs fonctionnant sous Windows 2003-2008 un certain nombre de groupes prédéfinis sont crées lors de l'installation de Windows 2003-2008 :

- Les groupes locaux prédéfinis qui se trouvent dans le conteneur **Builtin**.

- Les groupes globaux prédéfinis ainsi que certains groupes de domaine local qui se créent dans le conteneur **Users**.

➢ **Le conteneur Builtin :** réunit les groupes prédéfinis du domaine avec une étendue de domaine local. Ce conteneur s'est enrichi de seize objets supplémentaires sous Windows 2003-2008 (voir figure 53).

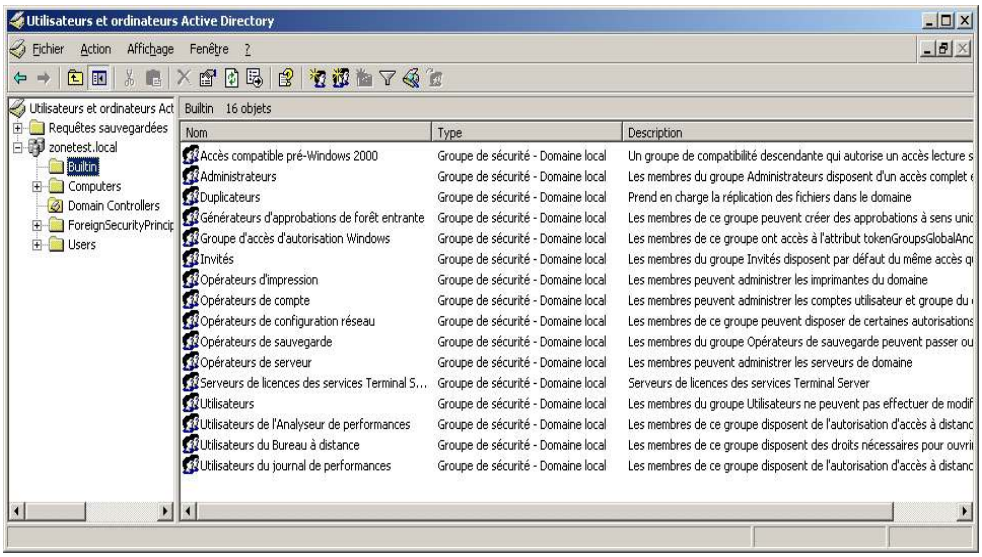


Figure 53

Ces groupes disposent de droits et de permissions implicites, aussi en insérant un membre dans un de ces groupes vous lui octroyez des droits supplémentaires
(voir tableau 54).

WWW.DZPEN.COM | قلم الجزائر

Opérateurs de compte	Les membres de ce groupe peuvent administrer les comptes d'utilisateurs et groupes (ajouter, supprimer et modifier). Ils ne peuvent cependant pas toucher au compte Administrateur ni aux autres membres du groupe opérateurs de compte.
Opérateurs de serveur	Les membres de ce groupe peuvent partager des ressources ainsi qu'effectuer des sauvegardes et des restaurations sur des contrôleurs de domaine.
Opérateurs d'impression	Les membres de ce groupe peuvent gérer les imprimantes réseau des contrôleurs de domaine.
Administrateurs	Les membres de ce groupe peuvent administrer les contrôleurs de domaine ainsi que toute station ayant intégrée le domaine. Par défaut, le groupe global Administrateurs de domaine ainsi que le compte Administrateur font partie du groupe local Administrateurs.
Invité	Le groupe global Invités du domaine ainsi que le compte d'utilisateur Invité sont intégrés dans ce groupe. Les membres de ce dernier disposent de peu de droits.
Utilisateurs	Le groupe global du domaine utilisateur est intégré dans ce groupe. Ce groupe peut être utilisé pour affecter des droits et permissions à toute personne disposant d'un compte dans le domaine.
Duplicateurs	Le groupe local Duplicateurs effectue les réplications de répertoires. Le compte d'utilisateur de ce groupe est configuré afin de se connecter au service Duplicateur du contrôleur de domaine
Accès compatible Pré-Windows 2000	Ce groupe permet de faire fonctionner les applications avec un niveau de sécurité Windows 2000 ou de version antérieure à Windows 2000.
Opérateurs de sauvegarde	Les membres de ce groupe peuvent effectuer des sauvegardes et restaurations sur tout contrôleur de domaine.

Tableau 54

WWW.DZPEN.COM | قلم الجزائر

➢ **Le conteneur Users** liste les groupes prédéfinis du domaine avec une étendue globale ainsi que quelques groupes prédéfinis du domaine avec une étendue de domaine local (voir figure 55).

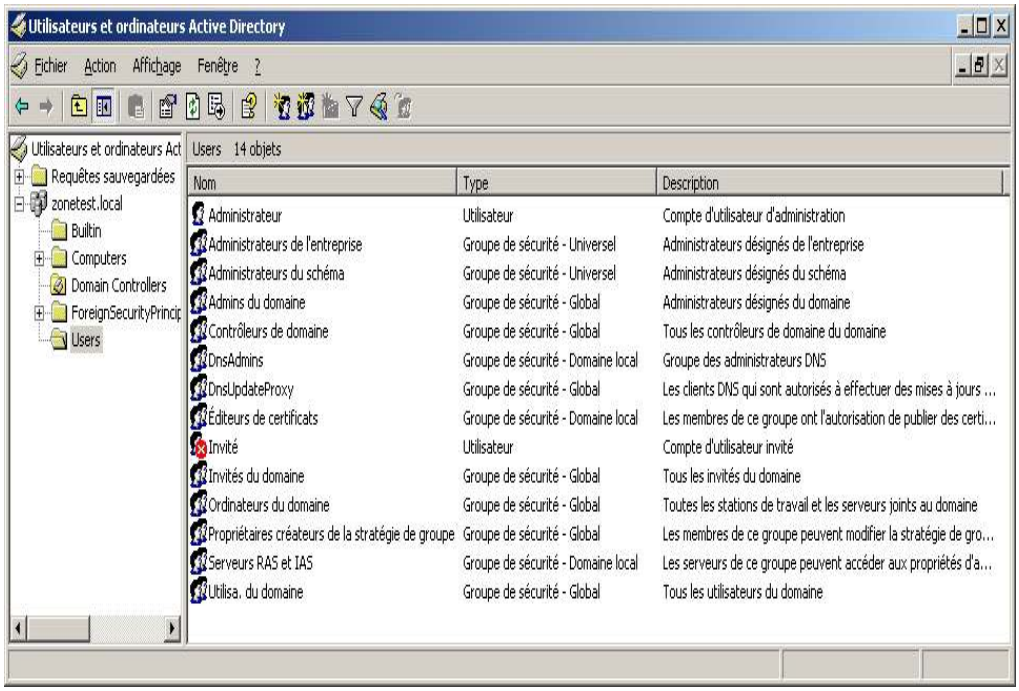


Figure 55

4.11.2 Les groupes intégrés à étendue de domaine local :

Ces groupes procurent aux utilisateurs des droits et autorisations prédéfinis, leur permettant de réaliser des tâches sur des contrôleurs de domaine et dans active directory. Les groupes de domaine local intégrés sont uniquement situés sur des contrôleurs de domaine. Nous ne pouvons pas supprimer ces groupes.

WWW.DZPEN.COM | قلم الجزائر

4.11.3 Schéma d'imbrication des groupes et comptes utilisateurs dans un domaine (voir figure 56).

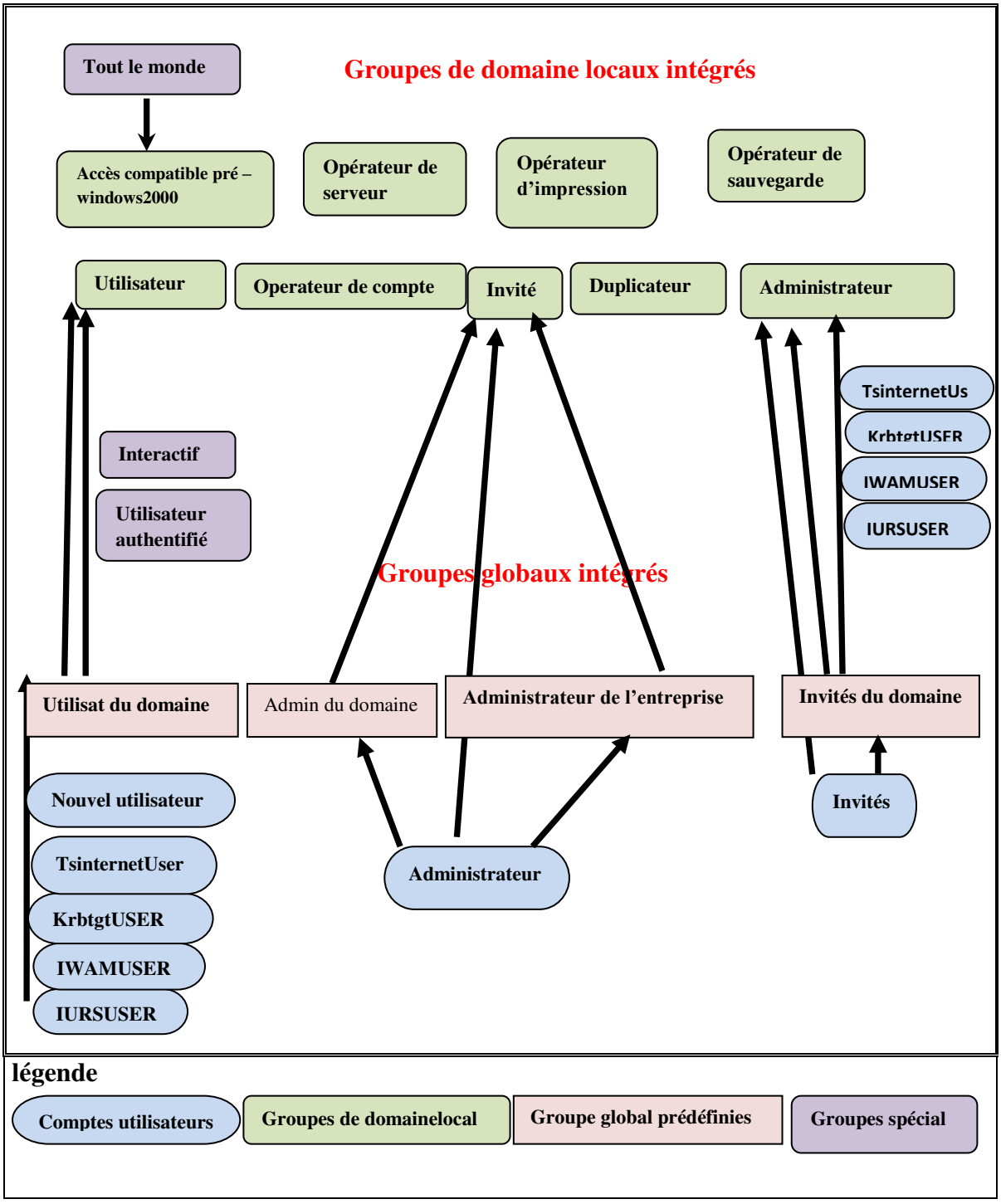
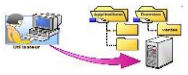


Figure 56

WWW.DZPEN.COM | قلم الجزائر



4.12 Les groupes par défaut sur tous les ordinateurs :

Windows XP Professionnel comporte trois groupes essentiels dont l'appartenance est contrôlée par l'administrateur : **Utilisateurs**, **Utilisateurs avec pouvoir** et **Administrateurs**. Il y en a cependant beaucoup d'autres que l'on a rarement besoin de manipuler, certains sont même invisibles. Sous XP ce groupe est identique au groupe Tout le monde, excepté le fait qu'il ne contient pas d'utilisateurs ou d'invité anonyme. Contrairement au groupe Tout le monde de Windows NT 4.0, le groupe utilisateurs authentifié n'est pas utilisé pour affecter des autorisations. Seuls les groupes contrôlés par l'administrateur (principalement Utilisateurs, Utilisateurs avec pouvoir et les membres du groupe Administrateur), servent à attribuer les permissions sur les partages.

- **Le groupe Administrateurs :**

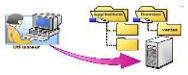
Le groupe Administrateurs contient tous les comptes à qui on a donné tous les pouvoirs sur le poste de travail. Idéalement l'accès administratif ne doit être utilisé que pour :

- Installer le système d'exploitation et ses composants (comme les pilotes de matériel, les périphériques du système et ainsi de suite).
- Installer Service Packs et Windows Packs.
- Mettre à niveau le système d'exploitation.
- Réparer le système d'exploitation.
- Configurer des paramètres critiques du système d'exploitation (tels que la stratégie de mot de passe, le contrôle d'accès, la stratégie d'audit, la configuration du pilote en mode noyau et ainsi de suite).
- S'approprier des fichiers devenus inaccessibles.
- Gérer les journaux d'audit et de sécurité.
- Sauvegarder et restaurer le système.

- **Le groupe Utilisateurs.**

L'ajout d'utilisateurs au groupe utilisateurs est l'option la plus sécurisée, parce que les autorisations par défaut allouées à ce groupe n'autorisent pas les membres à modifier les paramètres du système d'exploitation, ou d'autres données utilisateur.

WWW.DZPEN.COM | قلم الجزائر



Toutefois les autorisations de niveau utilisateur ne permettent pas toujours aux utilisateurs d'exécuter correctement des applications héritées, ni des programmes écrits pour les versions de Windows antérieures à Windows 2000. Seuls les membres du groupe utilisateurs ont l'assurance de pouvoir exécuter des applications certifiées pour Windows.

- **Le groupe Utilisateurs avec pouvoir :**

Le groupe Utilisateurs avec pouvoir fournit principalement une compatibilité ascendante pour l'exécution d'applications non certifiées Microsoft. Les autorisations par défaut allouées à ce groupe permettent à ses membres de modifier les paramètres d'ordinateur. Si des applications non certifiées doivent être prises en charge, les utilisateurs finaux doivent faire partie du groupe Utilisateurs avec pouvoir.

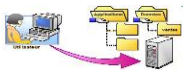
Les Utilisateurs avec pouvoir peuvent :

- Exécuter des applications héritées, en plus des applications certifiées Windows 2000 ou Windows XP Professionnel.
- Installer des programmes qui ne modifient pas les fichiers du système d'exploitation ou installer des services système.
- Personnaliser des ressources système, telles que les imprimantes, l'heure, la date, les options d'énergie et d'autres ressources du panneau de configuration.
- Créer et gérer des comptes d'utilisateurs et des groupes locaux.
- Arrêter et démarrer les services système qui ne sont pas démarrés par défaut.

- **Le groupe opérateurs de sauvegarde**

Les membres du groupe opérateurs de sauvegarde peuvent sauvegarder et restaurer des fichiers sur l'ordinateur, indépendamment des autorisations protégeant ces fichiers. Ils peuvent également ouvrir une session sur l'ordinateur et arrêter celui-ci, mais ils n'ont pas la possibilité de modifier les paramètres de sécurité.

WWW.DZPEN.COM | قلم الجزائر



4.12.1 Groupes spéciaux :

II existe aussi les groupes spéciaux sous Windows 2003-2008 qui ne peuvent pas se manipuler. En effet la qualité de membre de ces groupes ne peut pas être modifiée, et fait référence à l'état de votre système à un instant donné.

Ce sont les groupes Tout le monde, Utilisateurs authentifiés, Créateur propriétaire, Réseau, Interactif qui sont interprétés comme suit :

- **Le groupe Tout le monde :** comprend tous les utilisateurs ceux que vous avez crée le compte Invité ainsi que tous les utilisateurs des autres domaines.
  Attention car lorsque vous partagez une ressource, ce groupe dispose par défaut de la permission Lecture sur le partage (et Contrôle total sous Windows 2000).

- **Le groupe Utilisateurs authentifiés :** comprend tout utilisateur possédant un compte d'utilisateur et un mot de passe pour la machine locale ou Active Directory. Affectez des permissions à ce groupe plutôt qu'au groupe Tout le monde**.**
- **Le groupe Créateur propriétaire :** toute personne ayant crée ou pris possession d'une ressource, fait partie de ce groupe pour la ressource concernée. Le propriétaire d'une ressource dispose des pleins pouvoirs sur cette dernière.
- **Le groupe Réseau:** comprend toute personne accédant via le réseau à une ressource.
- **Le groupe Interactif :** comprend tous les utilisateurs qui ont ouvert une session localement (dans le cas où vous utilisez Terminal Server, ce groupe comporte tous les utilisateurs ayant ouvert une session sur le serveur de terminal).

4.13 Création de groupes :

Pour créer un groupe d'utilisateurs dans un domaine il faut suivre les étapes suivantes :

-Dans le menu **Outils d'administration**, choisissez **Utilisateurs et ordinateurs Active Directory**.

WWW.DZPEN.COM | قلم الجزائر

- Développez le domaine dans lequel vous créez le groupe.

-Faire un clic droit sur le **conteneur**, pointez sur **Nouveau** et choisissez **Groupe** dans le menu contextuel pour ouvrir la boîte de dialogue de la figure 57

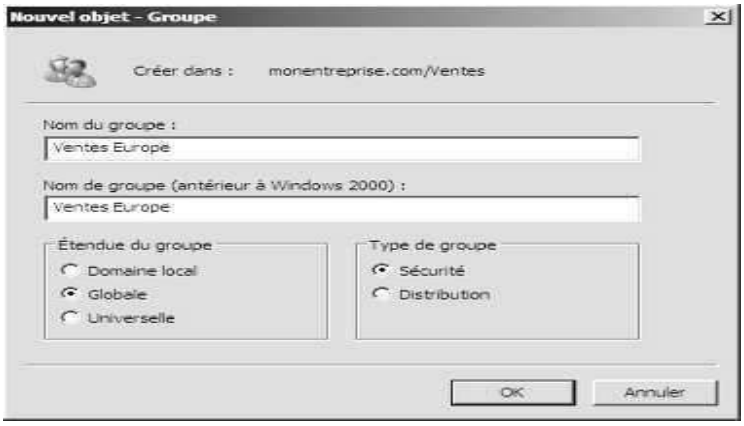


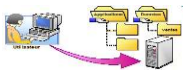
Figure 57

- Complétez les informations demandées :

- Le nom du groupe doit être unique dans le domaine.
- Le nom de groupe tel qu'il apparaît aux systèmes d'exploitation antérieurs à Windows2000 est complété automatiquement. Ces systèmes d'exploitation ne sont plus pris en charge, mais peuvent toujours exister en cas de situation d'héritage.
- Dans la section **Étendue de groupe**, choisissez **Domaine local**, **Globale** ou **Universelle**.
- Dans la section **Type de groupe**, choisissez **Sécurité** ou **Distribution.**

-Lorsque vous avez terminé, cliquez sur **OK**. Le nouveau groupe apparaît. Vous devrez éventuellement patienter quelques minutes que le groupe se réplique sur le catalogue global avant d'ajouter des membres.

WWW.DZPEN.COM | قلم الجزائر



4.14 Exercice théorique :

1. Qu'est-ce qu'un groupe de distribution ?
2. Qu'est ce qu'un groupe de sécurité ?
3. Quelle est la différence entre un groupe global, un groupe de domaine Local et un groupe Universel ?

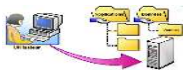
4.15 Exercice pratique:

1. Créer un groupe global sous le nom GRETA.
2. Inclure le compte utilisateur Service dans le groupe Global GRETA.
3. Inclure GRETA dans un Groupe de Domaine Local CHAMPLAIN.
4. Insérez l'ordinateur client dans le groupe GRETA.

4.16 Résumé :

Ce chapitre a exploré les options à la disposition de l'administrateur pour configurer les groupes, type de groupe, et l'étendue des groupes avec Windows Server 2008.
Les groupes sous Windows Server 2008 sont des objets des Services de domaine Active Directory ou des objets locaux, lesquels contiennent des utilisateurs, des contacts, des ordinateurs ou d'autres groupes. En général un groupe contient des comptes utilisateurs.
Les groupes simplifient l'administration, au lieu d'affecter des droits et des autorisations à chaque utilisateur individuel, l'administrateur les affecte à des groupes.

WWW.DZPEN.COM | قلم الجزائر



4.17 Exercice de synthèse :

1. Créer deux groupes d'utilisateur globaux Gchefservice, Gpersonnel sur le serveur.

2. Donner l'étendue et le type des deux groupes.

3. Créer les utilisateurs suivants : ChefS1, ChefS2, Employer1, Employer2.

4. Ajouter les utilisateurs ChefS1, ChefS2 au groupe global Gchefservice.

5. Ajouter les utilisateurs Employer1 et Employer2 dans le groupe Gpersonnel.

6. Créer un nouvel utilisateur Usertest.

7. Ajouter cet utilisateur dans le groupe prédéfini Administrateurs.

8. Ouvrir une session avec Usertest sur le contrôleur de domaine. Que constatez-vous ?

WWW.DZPEN.COM | قلم الجزائر

Chapitre 5 : Gestion des permissions (autorisations et droits)

Introduction :

Les permissions désignent ce que les diverses catégories d'utilisateurs (propriétaire d'un fichier, membres du groupe propriétaire d'un fichier et le reste du monde) ont l'autorisation d'effectuer sur un fichier donné. Par exemple, une catégorie d'utilisateurs peut avoir accès en lecture et écriture à un fichier, alors qu'une autre catégorie a accès en lecture seulement à ce même fichier.

5.1 Gestion d'accès aux ressources :

L'accès aux ressources se configure en trois étapes Le partage, la publication et la permission :

- **Le partage** *:* Pour réaliser un partage, il suffit de cliquer sur **Propriétés** et d'aller dans l'onglet partage. Vous pouvez bien entendu créer des partages invisibles par les utilisateurs en ajoutant le signe $ à la fin du nom de partage. Ce genre de partage est très utile pour créer des répertoires contenant des sources, des packages d'installations, etc. (voir figure 58).

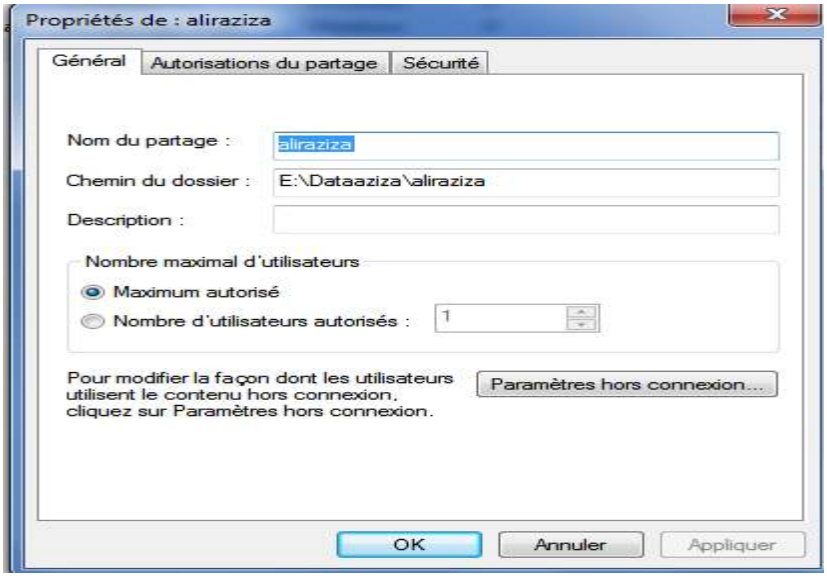
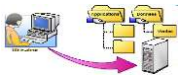


Figure 58

- **La publication** *:* La publication représente la possibilité de rendre facilement un partage accessible à un utilisateur. Soit via une correspondance, soit via un raccourci. Cette procédure se réalise souvent via un script de démarrage ou via une stratégie.

WWW.DZPEN.COM | قلم الجزائر



- **Les permissions *:*** L'utilisateur reçoit une série de clé ticket lors de son identification sur le réseau. Ses clés sont représentées par des SID. Exemple : User test : SID …..-1307, global compta : SID …..-1334. Quand on demande une ressource, il y a vérification via les ACL (Access control List) ou sont vérifié les permissions (grant).

5.1.1 Contrôle d'accès :

Le contrôle d'accès est le processus autorisant des utilisateurs, des groupes et des ordinateurs à accéder à des objets sur le réseau au moyen d'autorisations, de droits d'utilisateur et d'audit d'objets.

Le système de contrôle d'accès dans Windows 2003-2008 est basé sur trois composants qui permettent la définition du contexte de sécurité des éléments du système.

Ces trois éléments sont :

- Les entités de sécurité
- Le SID
- DACL – Discretionary Access Control List

1. Les entités de sécurité : Les entités de sécurité peuvent être un compte utilisateur, d'ordinateur ou un groupe. Ils permettent d'affecter l'accès à un objet en le représentant dans le système informatique.

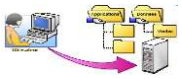
Le SID : Toutes les entités de sécurité sont identifiées dans le système par un numéro unique appelé **SID**. Ce SID est lié à la vie de l'objet, ainsi si l'on supprime un groupe et qu'on le recrée ce même groupe juste après (même nom, même propriétés), celui-ci se verra attribuer un nouveau SID. L'ensemble des définitions de sécurité étant basé sur ce SID, les accès donnés au groupe supprimé ne seront pas transférées au nouveau groupe.

DACL - Discretionary Access Control List : Les **DACL** sont associées à chaque objet sur lequel on va définir un contrôle d'accès. Les DACL sont composées d'ACE (Access Control Entry) qui définit les accès à l'objet.

Les ACE se composent de la façon suivante :

- Le SID de l'entité à qui l'on va donner ou refuser un accès.
- Les informations sur l'accès (ex : Lecture, Ecriture, …)
- Les informations d'héritages.
- L'indicateur de type d'ACE (Autoriser ou refuser).

WWW.DZPEN.COM | قلم الجزائر



A chaque tentative d'accès à une ressource, cette liste sera parcourue afin de déterminer si l'action voulue peut être réalisée.

5.1.2 Administration des accès aux dossiers locaux partagés :

Le partage d'un dossier permet de rendre disponible l'ensemble de son contenu via le réseau. Par défaut lors de la création d'un partage, le groupe « **Tout le monde** » bénéficie de l'autorisation« **Lecture** ».Il est possible de cacher le partage d'un dossier en ajoutant le caractère « **$** » à la fin du nom. Pour pouvoir y accéder il sera obligatoire de spécifier le chemin complet (**\\nom_du_serveur\nom_du_partage$**):

➢ Partage administratif

Windows 2003-2008 crées automatiquement des partages administratifs.

Les noms de ces partages se terminent avec un caractère $ qui permet de cacher le partage lors de l'exploration par le réseau.

Le dossier système (Admin$), la localisation des pilotes d'impression (Print$) ainsi que la racine de chaque volume (c$, d$, …) constituent autant de partages administratifs.

Seuls les membres du groupe « Administrateurs » peuvent accéder à ces partages en accès Contrôle Total. Le partage IPC$ permet l'affichage des ressources partagées (dossiers partagés, imprimantes partagés).

➢ Création de dossiers partagés

Sur des machines Windows 2003-2008 Serveur en mode autonome ou serveur membre, seul les membres des groupes « Administrateurs » et « Utilisateurs avec pouvoirs » peuvent créer des dossiers partagés. Pour pouvoir créer un partage vous avez trois possibilités :

• **L'outil d'administration - Gestion de l'ordinateur** à l'aide du composant logiciel enfichable. « Dossier partagés » (voir figure 59).

WWW.DZPEN.COM | قلم الجزائر

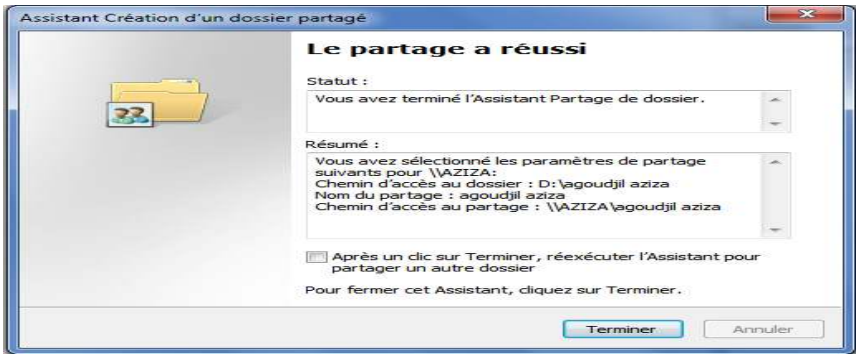


Figure 59

• **L'explorateur** par le biais du menu contextuel de tous les dossiers de l'arborescence.

• La commande **NET SHARE** (net share Nom Dossier Partagé=Unité: Chemin).

➢ Autorisations sur les dossiers partagés

Chaque dossier partagé peut être protégé par une ACL qui va restreindre son accès spécifiquement aux utilisateurs, groupes ou ordinateurs qui y accèdent via le réseau.
Il existe trois niveaux d'autorisations affectables :

• **Lecture** : Permet d'afficher les données et d'exécuter les logiciels.

• **Modifier** : Comprend toutes les propriétés de l'autorisation lecture avec la possibilité de créer des fichiers et dossiers, modifier leurs contenus et supprimer leurs contenus.

• **Contrôle total** : Comprend toutes les propriétés de l'autorisation Modifier.

Les trois niveaux d'autorisations sont disponibles en « Autoriser » ou en «Refuser » en sachant que les autorisations de refus sont prioritaires.
Pour affecter des autorisations de partage, vous avez deux solutions :

• A l'aide de l'outil d'administration « **Gestion de l'ordinateur** » et du composant enfichable« **Dossier Partagé** ».

• A l'aide de l'explorateur dans les propriétés du dossier partagé.

WWW.DZPEN.COM | قلم الجزائر

➢ Connexion à un dossier partagé

Afin qu'un client puisse accéder à un dossier partagé, plusieurs moyens sont disponible

• Favoris réseau : Permet de créer des raccourcis vers les partages désiré.

• Lecteur réseau : Permet d'ajouter le dossier partagé directement dans le poste de travail en lui attribuant une lettre.

• Exécuter : Permet d'accéder ponctuellement à la ressource en spécifiant simplementle chemin UNC d'accès à la ressource.

5.1.3 Mise en place des fichiers hors connexion :

Grâce aux Fichiers hors connexion, vous pouvez continuer à travailler avec des fichiers ou des programmes réseau, même lorsque vous êtes déconnectés. La mise en place des fichiers hors connexion se fait comme suit :

- ✓ Ouvrez le Poste de travail.
- ✓ Dans le menu outils, cliquez sur options des dossiers.
- ✓ Sous l'onglet fichiers hors connexion, vérifiez que la case à cocher autoriser l'utilisation de fichiers hors connexion est activée.
- ✓ Activez synchroniser tous les fichiers hors connexion avant de terminer la session pour obtenir une synchronisation complète. Pour une synchronisation rapide, laissez cette case à cocher désactivée (voir figure 60).

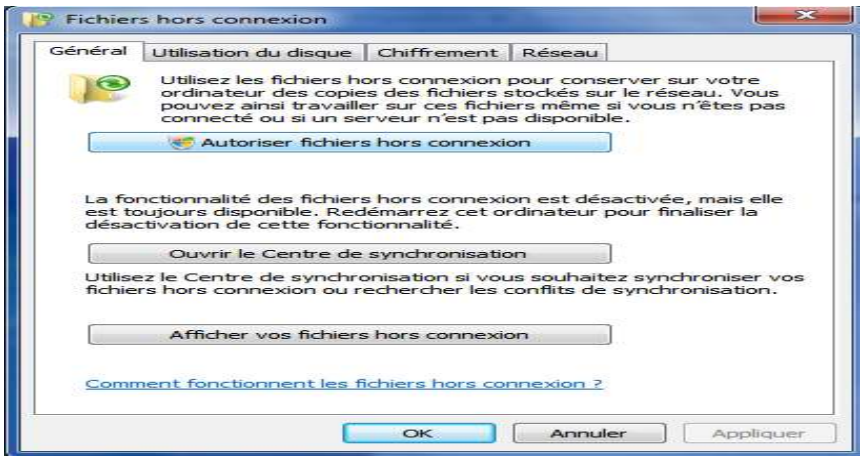
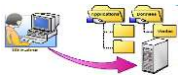


Figure 60

WWW.DZPEN.COM | قلم الجزائر



5.2 Exercice théorique:

1. L'accès aux ressources se configure en trois étapes lesquelles ?

2. Qu'est ce qu'il faut faire pour créer un partage invisible ?

3. Quel est le rôle des ACL ?

4. Quel est le rôle du contrôle d'accès ?

5. Quels sont les composants du contrôle d'accès ?

6. Quel est l'utilité des fichiers mis hors connexion ?

5.3 Exercice pratique :

1. Créer deux utilisateurs locaux test1 et test2.

2. Créer un dossier à la racine de C:\ avec la création d'un fichier texte et le partager avec les propriétés suivantes :

- test1 y a accès en lecture/écriture.
- administrateur y a accès en contrôle total.
- test2y a accès en lecture.

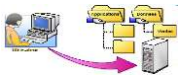
3. Ouvrez une session en tant que test2.

4. Accéder au dossier partagé et modifier le fichier texte que constatez-vous ?

5.4 Résumé :

Windows Server 2008 propose de nombreuses manières de gérer l'administration des accès aux ressources, de les sécuriser et de les rendre accessibles avec une attribution juste des droits et des permissions.

WWW.DZPEN.COM | قلم الجزائر



5.5 Exercice de synthèse :

1. Créer quatre utilisateurs sur chaque poste :

Poste1 : utilisateur1, mot de passe : Passe01 et utilisateur2 : mot de passe Passe02, utilisateur3, mot de passe : Passe03, utilisateur4, mot de passe : Passe04

Poste2 : user1, mot de passe : Passe01 et user2, mot de passe : Passe02, user3, mot de passe : Passe03, user4, mot de passe : Passe04.

L'utilisateur ne doit pas changer son mot de passe à la première ouverture de session.

2. Créer deux groupes, nommés Groupe1 et Groupe2.

3. Insérer les deux premiers utilisateurs (utilisateur1, utilisateur2) dans le groupe Groupe1 et les deux autres (utilisateur3, utilisateur4) dans le groupe Groupe2.

4. Créer un dossier sur le lecteur D: ayant le nom : Data avec votre nom.et créer dedans un fichier texte appelé MonTexte.txt contenant : votre nom, et un dossier Alir, placer un fichier texte dans le dossier Alir.

5. Partager ce dossier en conservant le nom du dossier.

6. Vérifier que dans voisinage réseau vous voyez l'autre ordinateur du groupe de travail.

7. Créer un lecteur réseau nommé T, vers le dossier partagé de votre binôme tester la connexion sur ce lecteur réseau.

8. Afficher les autorisations d'accès sur le partage du dossier.

9. Quelles sont les autorisations d'accès sur le partage possibles ? Partager le dossier Alire en n'autorisant que la lecture pour tous.

10. Comment apparaît le dossier Alire par rapport au dossier DATA dans Favoris réseau (sur votre poste et sur le poste de votre binôme) ?

11. Ajouter un nouveau nom de partage sur le dossier DATA, sans supprimer l'ancien.

12. Peut-on définir des autorisations différentes sur ce nouveau partage ?

13. Vérifier l'accès sur le nouveau partage dans Favoris réseau.

14. A partir d'une session ouverte avec un compte utilisateur, ajouter et supprimer des fichiers dans le dossier 'Alire' de votre poste (via le poste de travail), essayer de faire la même chose dans le dossier partagé du poste de votre binôme. Expliquer les différences ?

WWW.DZPEN.COM | قلم الجزائر

Chapitre 6 : Attribution des permissions et des autorisations NTFS pour Les utilisateurs

Introduction :

Le système de fichier NTFS (Windows NT File System) permet de stocker très efficacement des données sur une partition. Ainsi vous pouvez accorder des autorisations sur des dossiers et les fichiers, afin de contrôler le niveau d'accès aux ressources dont bénéficient les utilisateurs. Le système NTFS optimise par ailleurs l'espace disque en permettant la compression de données et la configuration de quotas de disque.

6.1 Les permissions et les autorisations NTFS pour les utilisateurs :

Les autorisations NTFS ne sont disponibles que sur les partitions NTFS. Pour sécuriser des fichiers et des dossiers sur des partitions NTFS, vous accordez des autorisations NTFS pour chaque compte d'utilisateur ou groupe d'utilisateurs qui doit accéder à la ressource.
Le système NTFS stocke une liste de contrôle d'accès (ACL, Access Control List) associée à chaque fichier et dossier contenus dans une partition NTFS. La liste ACL contient tous les comptes d'utilisateurs, groupe d'utilisateurs et ordinateurs bénéficiant de l'accès au fichier ou au dossier, ainsi que le type d'accès qui leur est accordé
(voir figure 61).

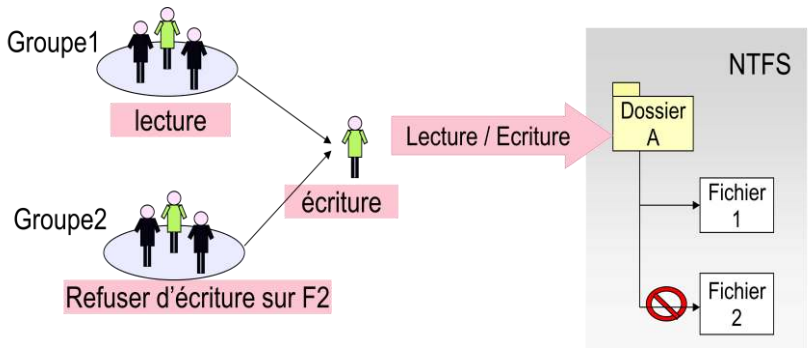
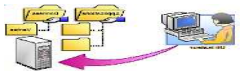


Figure 61

6.1.1 Autorisation sur un dossier :

L'autorisation sur un dossier est accordée pour contrôler l'accès à ces dossiers ainsi qu'aux fichiers et sous dossiers qu'ils contiennent. Le tableau suivant énumère les autorisations NTFS standard que vous pouvez accorder sur les dossiers et le type d'accès offert par chaque autorisation (voir tableau 62).

WWW.DZPEN.COM | قلم الجزائر



Autorisation NTFS sur les dossiers	Possibilités offertes à l'utilisateur
Lecture	Afficher les fichiers et les sous-dossiers contenus dans le dossier ainsi que les attributs, l'appropriation et les autorisations associés au dossier.
Ecriture	Créer des fichiers et des sous-dossiers dans le dossier, modifier les attributs du dossier et afficher, l'appropriation et les autorisations associées au dossier.
Afficher le contenu du dossier	Afficher les fichiers et les sous-dossiers contenus dans le dossier
Lecture et exécution	Parcourir les dossiers et effectuer les opérations permises par les autorisations Lecture et Ecriture et Afficher le contenu du dossier.
Modifier	Supprimer le dossier et effectuer les opérations permises par les autorisations Ecriture et Lecture et exécution.
Contrôle total	Modifier les autorisations, prendre possession d'un dossier, supprimer des sous-dossiers et des fichiers et effectuer les opérations permises par toutes les autres autorisations NTFS sur les dossiers.

Tableau 62

Les autorisations de dossiers NTFS, sont accordées soit dans le panneau "**Partage**», onglet "**Sécurité**, soit dans le panneau" **Propriétés**" du dossier, onglet "**Sécurité**" (Voir figure 63).

WWW.DZPEN.COM | قلم الجزائر

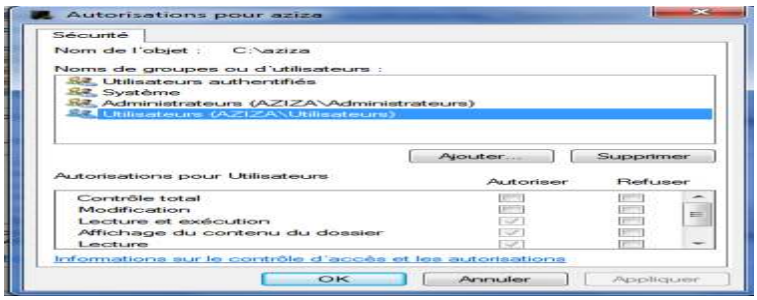


Figure 63

6.1.2 Autorisations NTFS sur les fichiers :

Vous accordez des autorisations sur des fichiers pour contrôler l'accès aux fichiers. Le tableau suivant énumère les autorisations NTFS standard que vous pouvez accorder sur les fichiers et le type d'accès offert par chaque autorisation (voir tableau 64) :

Autorisation NTFS sur les dossiers	**Possibilités offertes à l'utilisateur**
Lecture	Lire le fichier, les attributs, l'appropriation et les autorisations associés au fichier.
Ecriture	Remplacer le fichier, modifier les attributs du fichier et afficher l'appropriation et les autorisations associées au dossier
Lecture et exécution	Exécuter des applications et effectuer les opérations permises par l'autorisation Lecture.
Modifier	Modifier et supprimer le fichier et effectuer les opérations permises par les autorisations Ecriture et Lecture et exécution.
Contrôle total	Modifier les autorisations, prendre possession d'un fichier et effectuer les opérations permises par toutes les autres autorisations NTFS sur les fichiers.

Tableau 64

Les autorisations de dossiers NTFS sont accordées soit dans le panneau "Partage", onglet "Sécurité, soit dans le panneau" Propriétés" du dossier, onglet "Sécurité «Voir figure 65).

WWW.DZPEN.COM | قلم الجزائر

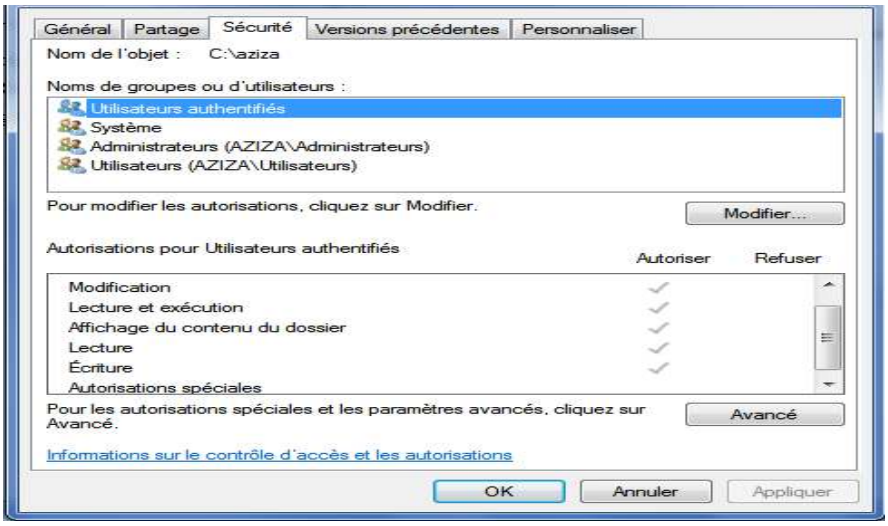


Figure 65

Remarque :

Parmi les autorisations NTFS sur les dossiers et les fichiers, il existe une autorisation spéciale qui n'est pas une autorisation standard. Cela correspond à une combinaison spéciale d'attributs NTFS, chacunedecesautorisations résultedela combinaisonstandardd'attributs NTFS. Si vous voulez connaître la liste des attributs utiliséspouruneautorisation, affectez une autorisation à l'utilisateur puis cliquez sur le bouton **avancé** (voir figure 66).

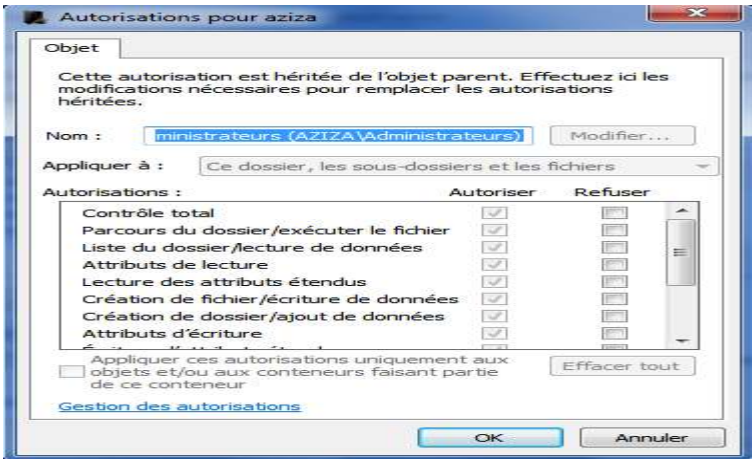


Figure 66

WWW.DZPEN.COM | قلم الجزائر

6.1.3 Présentation de l'héritage NTFS :

Sur le système de fichier NTFS de Windows 2003-2008, les autorisations que vous accordez à un dossier parent sont héritées et propagées à tous les sous-dossiers, et les fichiers qu'il contient. Tous les nouveaux fichiers et dossiers créés dans ce dossier hériteront aussi de ces permissions.

Par définition, toutes les autorisations NTFS d'un dossier créé seront héritées par les dossiers et fichiers qu'il contiendra.

Il est possible de bloquer cet héritage (pour des raisons de sécurité) afin que les permissions ne soient pas propagées aux dossiers, et aux fichiers contenus dans le dossier parent.

Pour bloquer l'héritage des permissions, afficher les propriétés du dossier, allez dans l'onglet **Sécurité**, puis cliquez sur le bouton «**avancés** » désactiver la case à cocher « **Permettre aux autorisations héritées du parent de se propager à cet objet et aux objets enfants**. Cela inclut les objets dont les entrées sont spécifiquement définies ici» (voir figure 67).

Dans la nouvelle fenêtre, cliquer **Copier** si vous souhaitez garder les autorisations précédemment héritées sur cet objet, ou alors cliquer **Supprimer** afin de supprimer les autorisations héritées et ne conserver que les autorisations explicitement spécifiées.

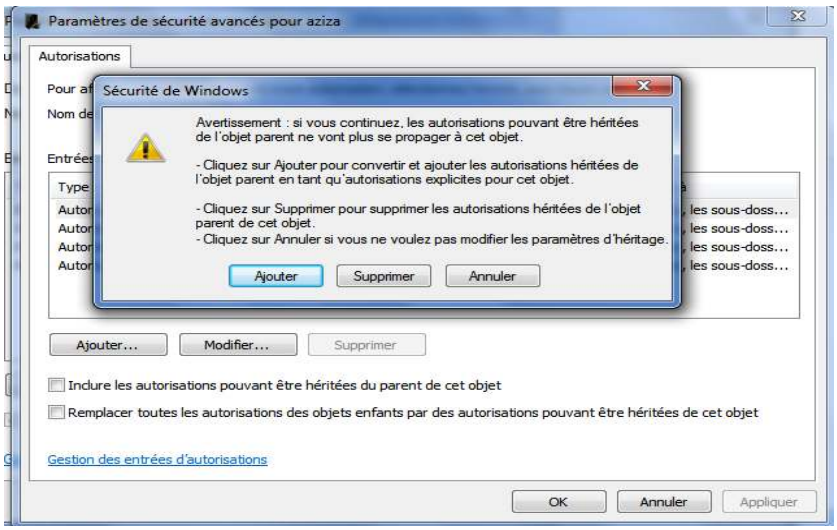
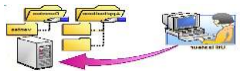


Figure 67

WWW.DZPEN.COM | قلم الجزائر



6.2 Règles concernant les autorisations NTFS :

Règle 01 : Un fichier ou un dossier **hérite** des permissions du dossier dans lequel il a été créé. Exception : un fichier n'hérite pas de la permission « Afficher le contenu du dossier ».

Règle 02 : Si un utilisateur appartient à plusieurs groupes, les autorisations s'additionnent, sauf s'il y a refus explicite.

Règle 03 : L'autorisation Refuser est prioritaire sur les autres.

Règle 04 : Les autorisations sur les fichiers sont prioritaires sur celles du dossier.

Règle 05 : Changer les autorisations d'un dossier provoque la modification des permissions des fichiers et sous-dossiers de ce dossier, selon le même mécanisme d'héritage que lors de la création d'un nouveau fichier, il est possible de bloquer cet héritage.

Règle 06 : Au formatage d'un disque dur : Contrôle total à tout le monde.

- **Le propriétaire d'un fichier :** Le créateur d'un fichier ou d'un répertoire en est le propriétaire, attention il ne possède pas tous les droits sur son fichier, mais il a le privilège d'obtenir la permission (changer les permissions), ce qui lui permet finalement d'avoir **contrôle total** sur son Fichier.
- **Le cas particulier des administrateurs :** Tout administrateur possède le droit (appropriation) sur n'importe quel fichier.

6.3 Exercice théorique :

1. Soit un dossier D ayant les permissions :

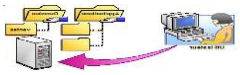
Comptabilité Afficher le contenu du dossier

Commercial Modifier

Fabrication Lecture.

Quelles sont les permissions d'un fichier F créé dans D par un commercial ?

WWW.DZPEN.COM | قلم الجزائر



2. Soit un dossier D1 ayant les permissions:

Tout le monde Modifier

Chefs1 Lecture

Chefs1 peut-il supprimer D1 ?

3. Soit un dossier D2 ayant les permissions :

Tout le monde Contrôle total

ChefS1 Lecture refusée

ChefS1 peut-il voir le contenu de D2 ?

4. Soit un dossier D3 ayant les permissions :

ChefS1 Lecture

Soit un fichier F contenu dans D3 :

ChefS1 Modifier

ChefS1 peut-il supprimer F ?

5. Soit un dossier D4 ayant les permissions :

ChefS1 Lecture et exécution

Et un fichier F contenu dans D4 :

ChefS1 Lecture et exécution

On positionne le droit Modifier sur D4 pour ChefS1.

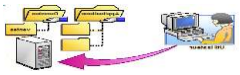
Que deviennent les droits de F ?

6.4 Exercice pratique :

Attribuer les autorisations suivantes sur le dossier travaux aux utilisateurs sur le contrôleur de domaine.

Utilisateurs	Partage	NTFS
Serveur1	contrôle total	lecture
Serveur1	Lecture	contrôle total
Serveur1	contrôle total	contrôle total

WWW.DZPEN.COM | قلم الجزائر



6.5 Résumé :

Windows Server 2003-2008 dispose des autorisations NTFS inscrite dans la liste de control d'accès (ACL) de chaque volume. Ainsi chaque utilisateur verra son Sid accompagné des droits d'accès aux ressources. Ce mode d'autorisation d'accès aux dossiers, garantissent un degré de sécurité maximal.

6.6 Exercice de synthèse :

Les utilisateurs chefs1, chefs2,employer1, employer2 ainsi que les groupes Gchefservice et Gpersonnel ont été déjà crée dans le chapitre 4.

1. Ouvrir une session avec le compte administrateur sur le contrôleur de domaine.

2. Créer un dossier appelé travaux dans la partition C:\,et créer un fichier texte dans ce dossier.

3. Partager le dossier travaux.

4. Accorder au groupe administrateur et le groupe tout le monde l'autorisation de partage contrôle total.

5. Afficher les autorisations NTFS par défaut sur le dossier travaux.

6. Quelles sont les autorisations actuellement accordées sur le dossier, et pourquoi sont-elles grisées ?

7. Supprimer le groupe de tout le monde.

8. Bloquer l'héritage des autorisations et supprimer toutes les autorisations accordées sur le dossier travaux.

9. Accorder des autorisations sur le dossier travaux comme suit:

L'autorisation contrôle total au compte administrateur.

L'autorisation modifiée au groupe Gchefservive.

L'autorisation lecture au groupe Gpersonnel.

10. Tester :

1. Se connecter en tant qu'utilisateur chefs1, et essayer de modifier le fichier dans le dossier travaux. Que constatez-vous ?

2. Se connecter en tant qu'utilisateur employer, et essayer de modifier le fichier dans le dossier travaux Que constatez-vous ?

WWW.DZPEN.COM | قلم الجزائر

Chapitre 7 : Partage des ressources et des dossiers

Introduction :

L'objectif principal d'un réseau est bien évidemment de pouvoir utiliser les fichiers ou dossiers situés sur un autre micro (station ou serveur). Pour cela l'Administrateur ou son équivalent devra mettre en place le partage des ressources
afin delesrendre accessibles via le réseau auxutilisateurs. Il mettra ces ressources disponibles avec des droits différents (lecture, Control total …) en fonction des profils des utilisateurs.

7.1 Partage d'un dossier :

Les dossiers partagés permettent aux utilisateurs d'accéder aux fichiers et aux dossiers d'un réseau. Les dossiers partagés peuvent contenir des applications, partagés, des données ou les données personnelles d'un utilisateur. Les dossiers de données partagés constituent un emplacement central à partir duquel les utilisateurs peuvent accéder aux fichiers et qui vous permet de sauvegarder plus facilement les données contenues dans les fichiers (voir figure 68).

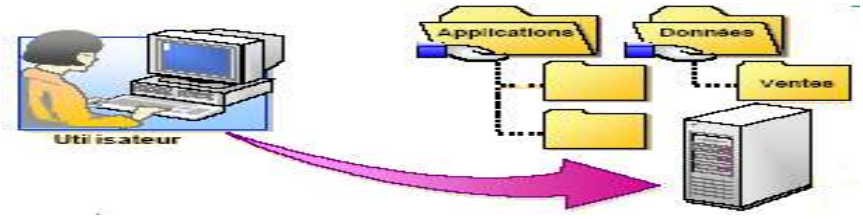


Figure 68

7.1.1 Partage à partir de l'Explorateur :

- Sélectionnez le dossier à partager, puis menu **Fichier partage et sécurité** ou à partir du menu contextuel clic droit dossier à partager option **Partager- partage - autorisation**.
- Cochez Partager ce dossier (voir figure 69). Possibilité de changer le nom du partage commentaire éventuel. Possibilité de restreindre ou non le nombre de connexions simultanées sur ce partage. Par défaut la limite est égale à 10 connexions simultanées ce qui correspond au **Maximum autorisé** pour Windows XP ou jusqu'à concurrence des licences pour un serveur W2003.Possibilité de plusieurs noms partage différents pour un même dossier.

WWW.DZPEN.COM | قلم الجزائر

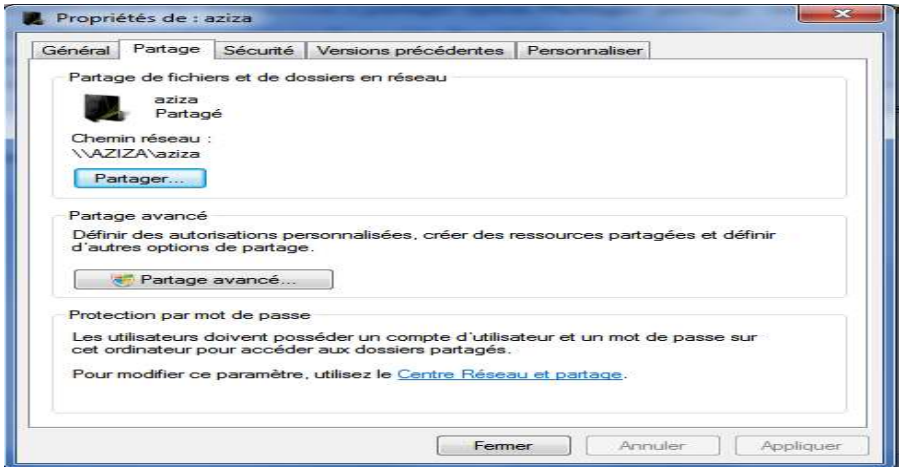


Figure 69

Pour Modifier les **Autorisations** d'accès à travers le réseau cliquez sur le bouton **Autorisations.** Par défaut **Lecture** pour le groupe **Tout le Monde** est appliqué (voir figure 70).

- **Permissions de dossier partagé:**

  - **Lecture**: l'utilisateur peut lire les fichiers, exécuter des programmes et parcourir les sous- dossiers.
  - **Modifier:** Lecture, créer, modifier ou supprimer des dossiers et fichiers.
  - **Contrôle total:** Modifier c'est le droit de changer les permissions possibilité **d'Autoriser** ou **Refuser** une permission, si appartenance à plusieurs groupes combinaison des permissions, la permission finale pour l'utilisateur sera une combinaison de ces permissions(en résumé la plus élevée), avec pour exception le cas ou une permission est positionnée sur la colonne **Refuser**. Dans ce cas **Refuser** est prioritaire. Vous avez pour u même dossier le droit de créer plusieurs noms de partage différents. Il vous suffit de cliquer sur le bouton **Nouveau Partage.** Possibilité **d'Ajouter** de nouveaux **Utilisateurs** ou groupe d'utilisateurs.

WWW.DZPEN.COM | قلم الجزائر

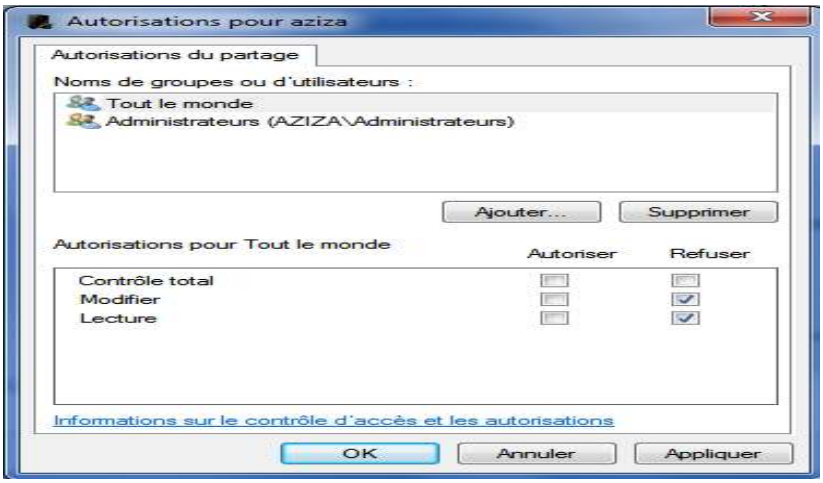


Figure 70

7.1.2 A partir de la console Gestion de l'ordinateur :

➢ Allez dans la fenêtre **Gestion de l'ordinateur**, puis dans la rubrique **Dossiers partagés** sélectionnez **Partages**. Allez dans le menu **Action –Nouveau partages de fichiers** pour démarrer l'assistant de création d'un partage (voir figure 71).

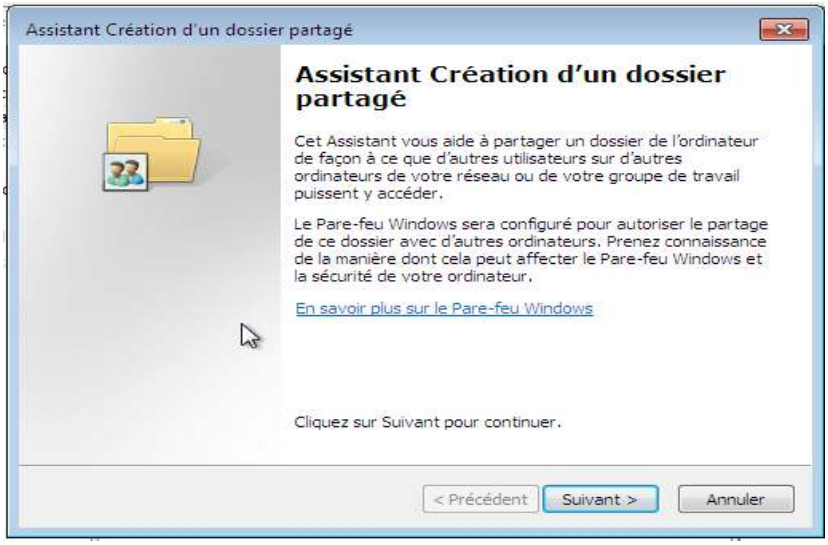


Figure 71

WWW.DZPEN.COM | قلم الجزائر

➢ Dans l'écran suivant vous devez saisir le chemin local à partager ou via le bouton Parcourir afin d'entrer un dossier existant ou en créer un nouveau (voir figure 72).

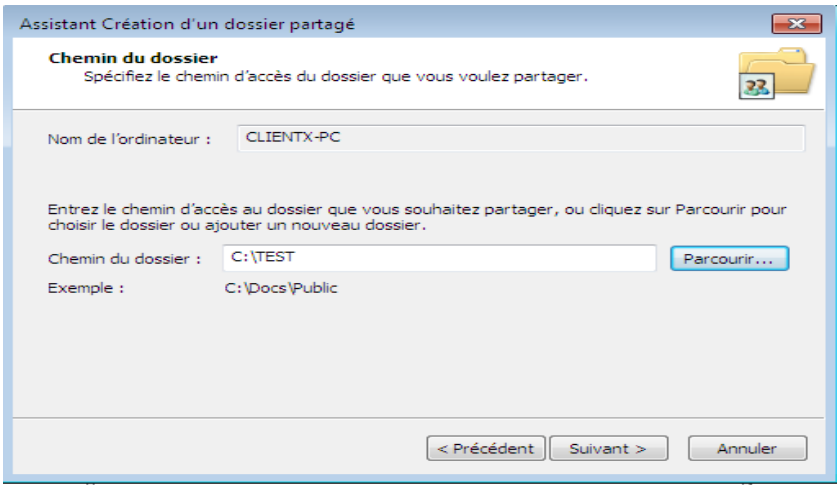


Figure 72

➢ Ensuite vous devez entrer ou modifier les autorisations à apporter au dossier. Vous pouvez choisir l'un des trois réglages prédéfinis ou personnaliser (Modifier) selon vos souhaits cliquer sur suivant (voir figure 73).

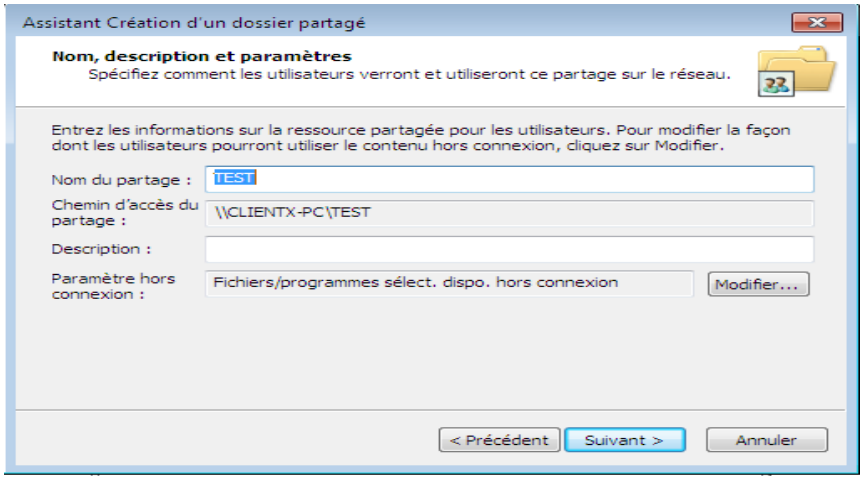


Figure 73

WWW.DZPEN.COM | قلم الجزائر

➢ Cliquer sur suivant pour déterminer les autorisations de partage (voir figure 74)

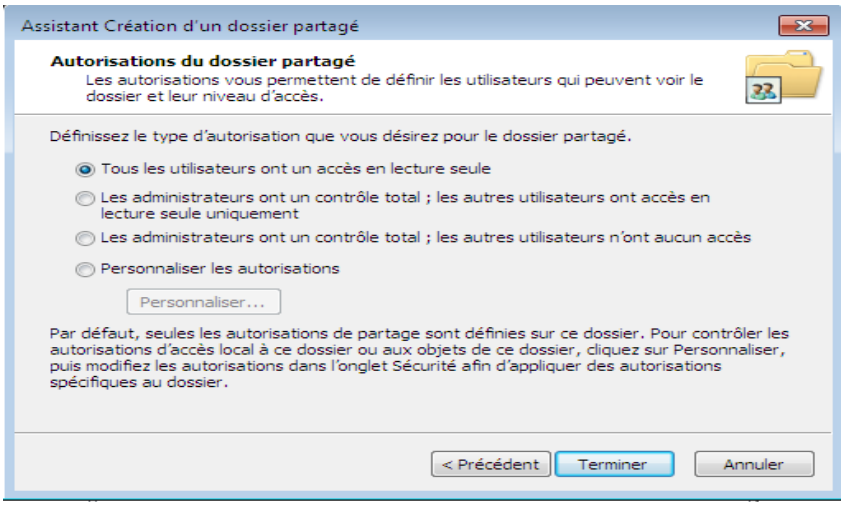


Figure 74

➢ En final une fenêtre récapitule l'opération de création du partage (voir figure 75).



Figure 75

7.1.3 Supprimer un partage :

Cette opération est équivalente à en supprimer l'accès à travers le réseau ainsi que toutes les permissions associées. Vous pouvez réaliser cette cessation de partage soit à partir de **L'Explorateur** ou via la console précédente de **Gestion de l'ordinateur.**

A partir de l'explorateur sélectionnez le **dossier partagé**. Puis à partir du menu contextuel sélectionnez **Propriétés**. Sélectionnez le partage puis cliquez sur le bouton **Supprimer le**

WWW.DZPEN.COM | قلم الجزائر

partage. Vous pouvez aussi réaliser cette opération à partir de la fenêtre **Gestion de l'ordinateur**. Dans la rubrique **Outils système, Dossiers partagés**, **Partage** Sélectionnez le nom du partage à supprimer puis à partir du menu contextuel validez **Arrêter le partage (voir la figure 76)**.

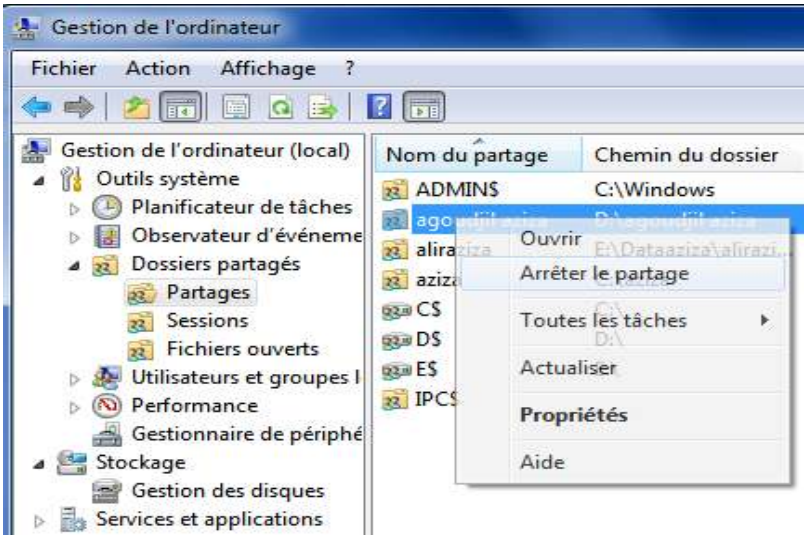


Figure 76

7.1.4 Se connecté à une ressource partagée :

Plusieurs possibilités s'offrent à vous pour vous connecter à une ressource partagée sur le réseau. Vous pouvez par exemple utiliser à partir de **l'Explorateur** la navigation directe avec les noms **UNC**. Sélectionnez **Favoris réseaux, Tout le réseau, Réseau Microsoft Windows**- puis l'endroit ou se situe la ressource partagée (domaine ou groupe de travail, puis le nom de machine) (voir figure 77).

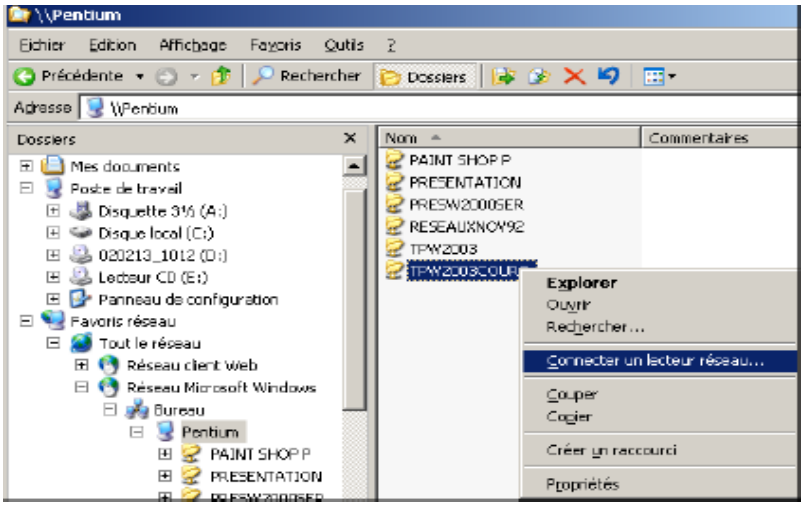


Figure 77

WWW.DZPEN.COM | قلم الجزائر

Les ressources mémorisées et déjà partagées apparaissent. Sélectionnez la ressource apparaissant comme déjà partagée. Puis faire un clic droit afin de faire apparaître le menu contextuel. Validez **Connecter un lecteur réseau**. Ensuite vous devez choisir une lettre de lecteur, choisir le **Chemin de la ressource partagée de type UNC**(\\ serveur\partage)Cocher Se reconnecter à l'ouverture de session. La Possibilité de se connecter sur un Nom d'utilisateur différent. Le répertoire que vous venez de partager est maintenant accessible par un double clic sur l'icône **Favoris réseau**. L'ajout de favoris réseaux peut se réaliser directement à partir de l'icône **Ajout d'un Favori réseau (voir figure 78).**

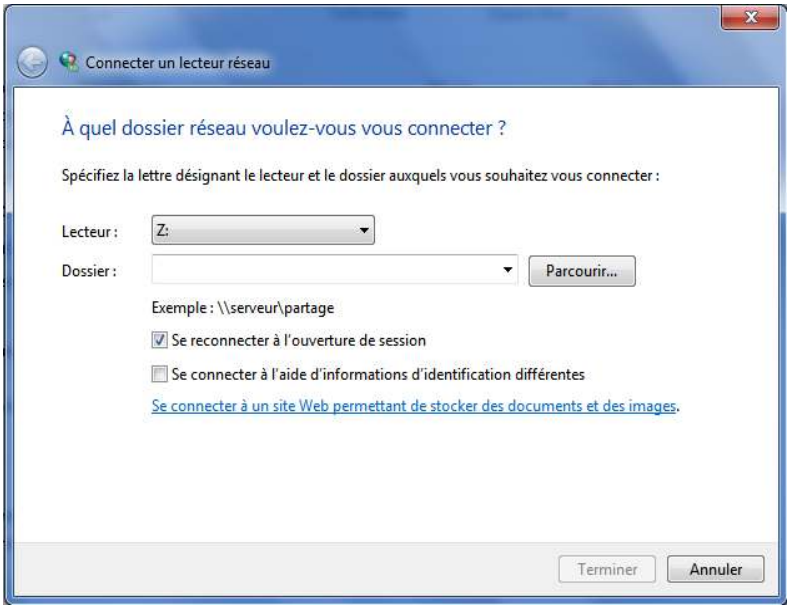


Figure 78

7.1.5 Contrôler les partages :

Le contrôle de partages se fait à partir de la console **Gestion de l'ordinateur.**

Ce contrôle de partages permet à l'utilisateur ou àl'administrateur d'afficherlesutilisateursdu réseau accédant à une ressource partagée et permet aussi de contrôler l'accès à cette ressource. Le dossier **Fichiers ouverts** donne la liste de tous les fichiers ouverts sur le serveur. Vous pouvez directement à partir de cette fenêtre fermer certains fichiers. Avec cette action si le fichier était ouvert en lecture/écriture toutes les modifications seront perdues. Par contre cette connexion ne peut être que temporaire car s'il veut, l'utilisateur peut réutiliser la ressource dès qu'il le veut (voir figure 79).

WWW.DZPEN.COM | قلم الجزائر



Figure 79

La rubrique **Sessions** permet la visualisation de toutes les sessions ouvertes sur l'ordinateur. En fait vous visualisez toutes les personnes effectuant des connexions sur l'ordinateur.La rubrique**Partage**permet de partager ou cesser le partage deressources (voir figure 80).



Figure 80

7.2 Partage d'une imprimante :

L'imprimante est une interface logicielle entre le système d'exploitation et le périphérique d'impression. L'imprimante représente tout le logiciel nécessaire pour assurer le lien entre l'application qui envoie les travaux d'impression, le système d'exploitation et le périphérique d'impression rattaché à l'imprimante.

WWW.DZPEN.COM | قلم الجزائر

Pour partager une imprimante sous réseau nous devons suivre les étapes suivantes :

- **Installation du rôle :**

- Aller dans "Gestionnaire de Serveur" puis dans "Rôles" cliquer sur "Ajouter des Rôles".

- Sélectionner "Services de documents et d'impression" est cliqué sur "Suivant"(voir figure 81).

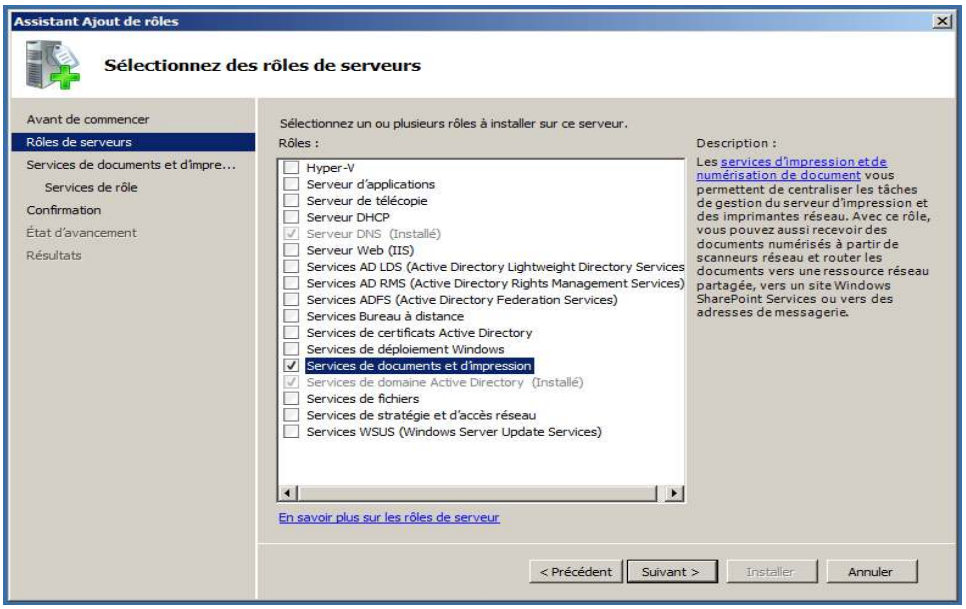


Figure 81

-Sélectionner "**Serveur d'impression**" puis cliquer sur "**Suivant** "(voir figure 82).

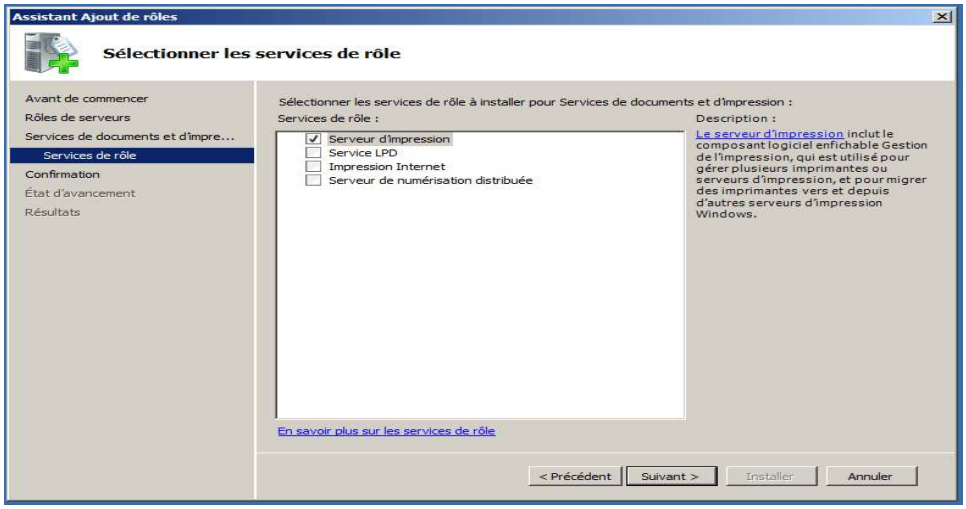


Figure 82

WWW.DZPEN.COM | قلم الجزائر

Voici le résumé de se qui va être installé, cliquer sur "**Installer**"(voir figure 83).

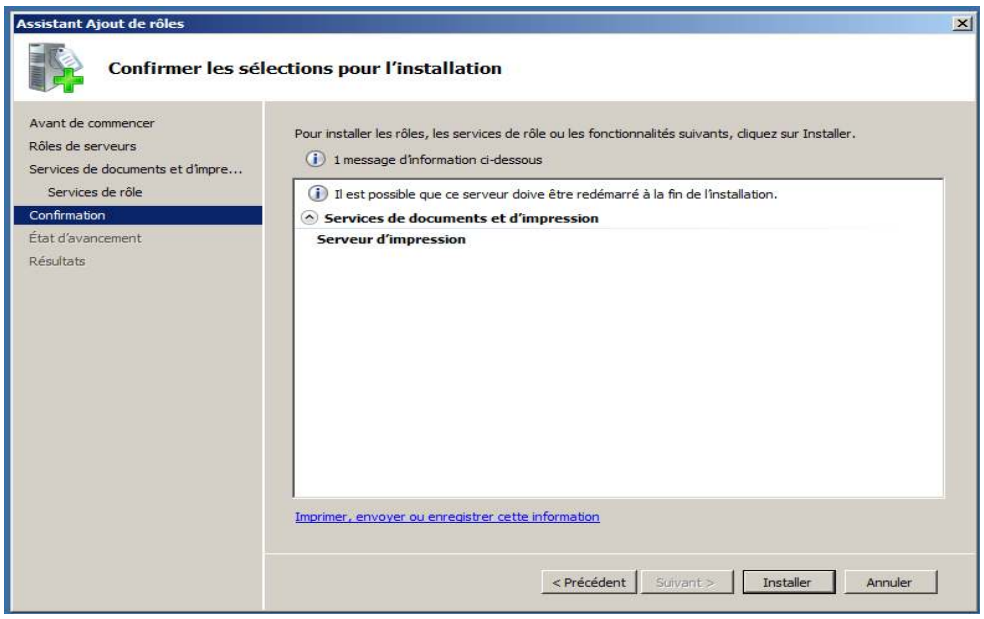


Figure 83

L'installation et la configuration commence, cette étape dure quelques minutes (voir figure 84).

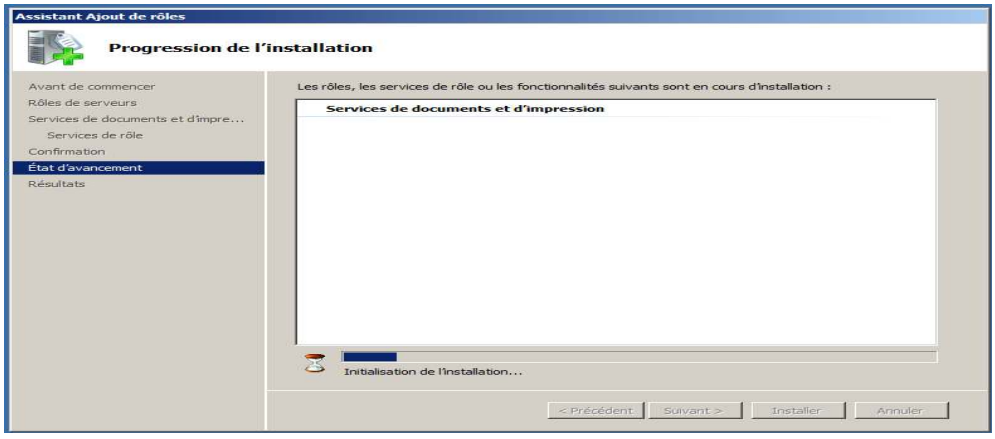


Figure 84

WWW.DZPEN.COM | قلم الجزائر

A la fin de l'installation et si tous c'est bien passer vous aurez se message, cliquer sur "**Fermer**"(voir figure 85).

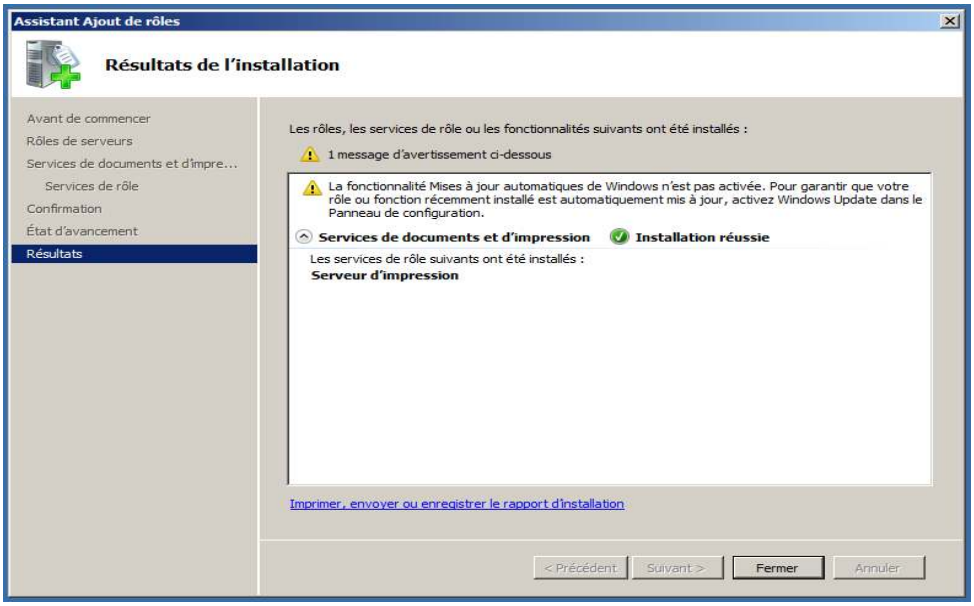


Figure 85

- Installation d'une imprimante réseaux sur le serveur d'impression

L'imprimante doit être configuré au niveau réseau, Aller dans "**Périphériques et imprimantes**" qui se trouve dans le "**Panneau de configuration**", Cliquer sur le bouton "**Ajouter une imprimante**", la fenêtre ci-dessous s'ouvre, cliquer sur "**Ajouter une imprimante locale**"(voir figure 86).

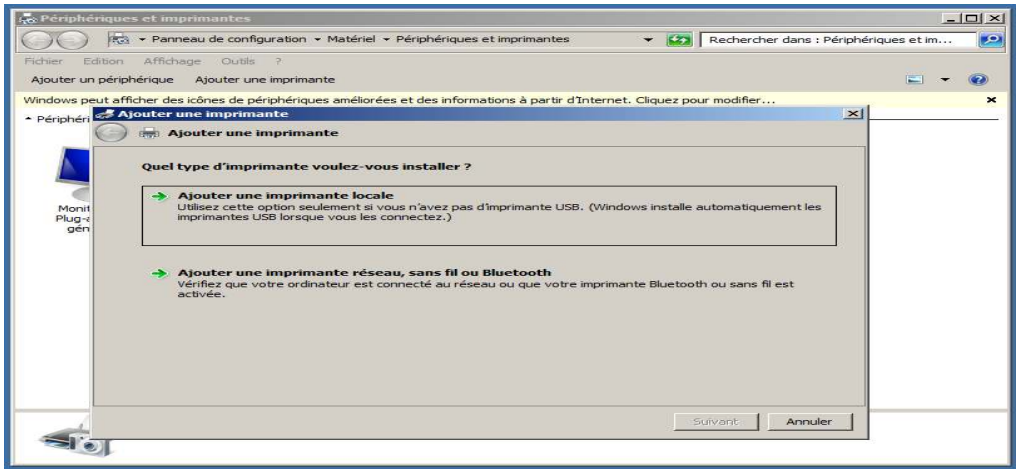


Figure 86

WWW.DZPEN.COM | قلم الجزائر

Sélectionner "**Créer un nouveau port**" puis dans la liste choisissez "**Standard TCP/IP Port**", cliquer sur "**Suivant**" (voir figure 87).

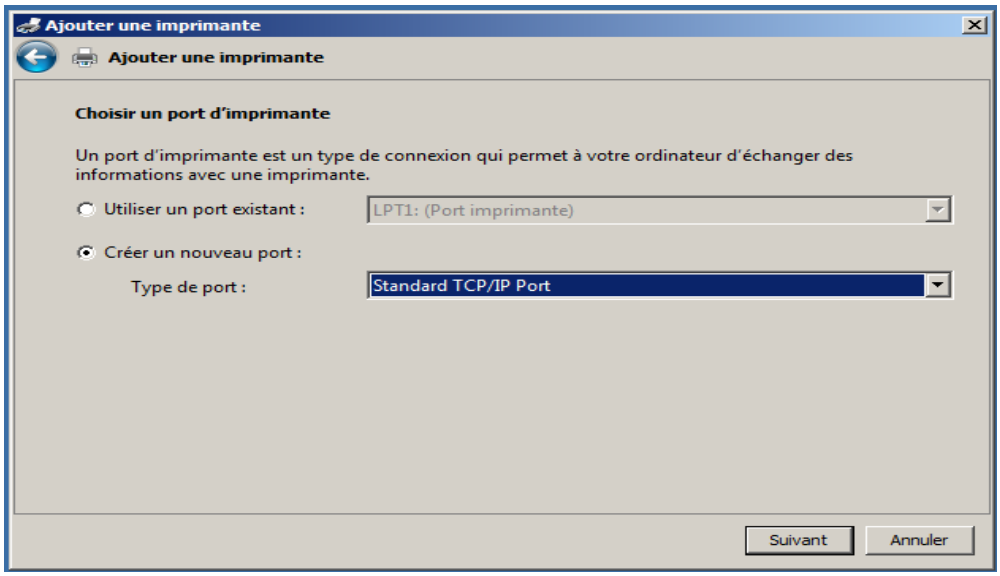


Figure 87

Dans le champ "**Nom d'hôte ou adresse IP**", indiquer **l'adresse IP** de l'imprimante et cliquer sur "**Suivant**"(voir figure 88).

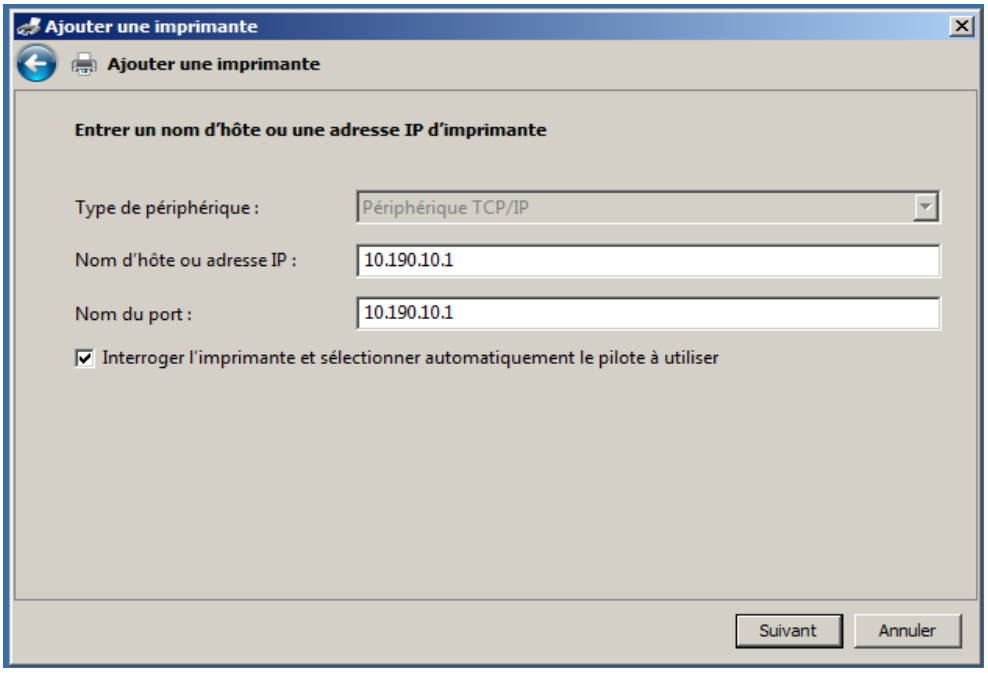


Figure 88

WWW.DZPEN.COM | قلم الجزائر

La détection peut durer plusieures minutes (voir figure 89).

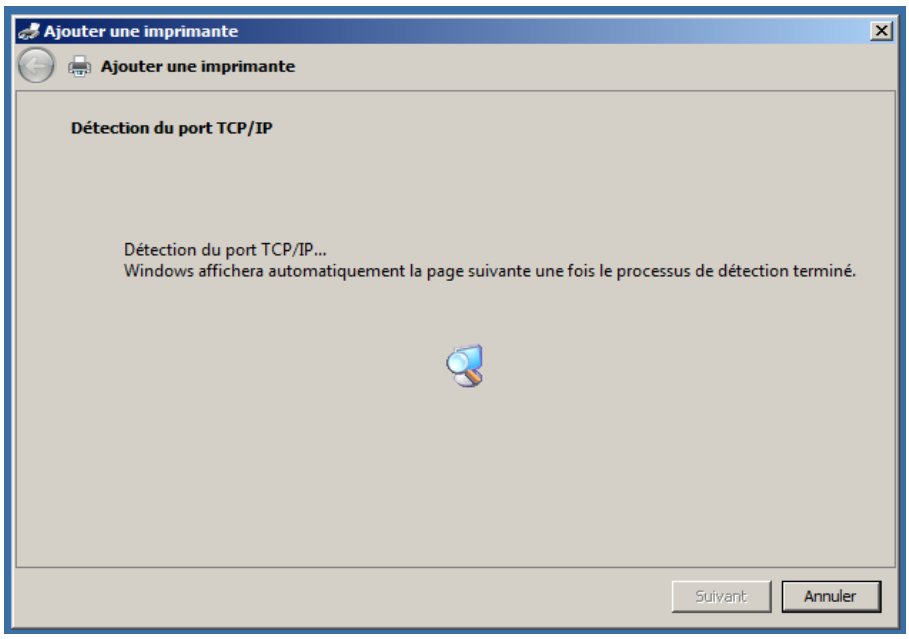


Figure 89

Dans "**Type de périphérique**", sélectionner "**Standard**" et "**Generic Network Card**", puis cliquer sur "**Suivant**" (voir figure 90).

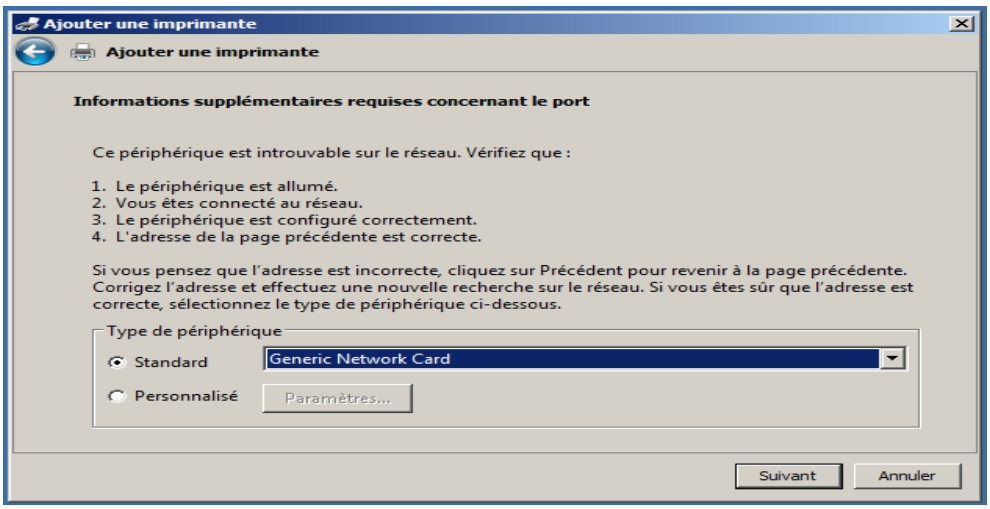


Figure 90

WWW.DZPEN.COM | قلم الجزائر

La détection peut durer plusieurs minutes (voir figure 91).

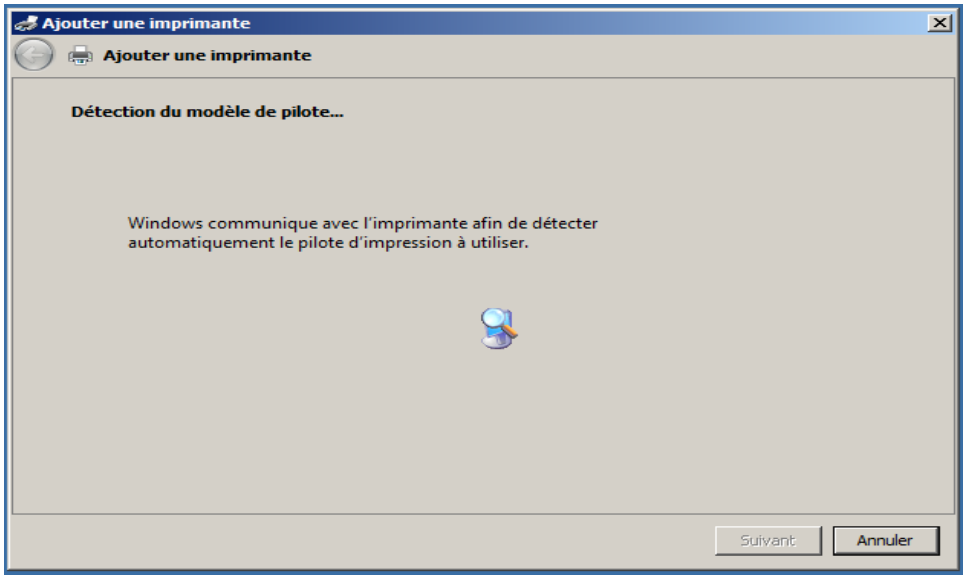


Figure 91

Le serveur affiche la liste de fabriquent d'imprimante cliquer sur "**Disque fourni...**" et le sélectionner les fichiers inf (le pilote x64), puis cliquer sur "**OK**" (voir figure 92).

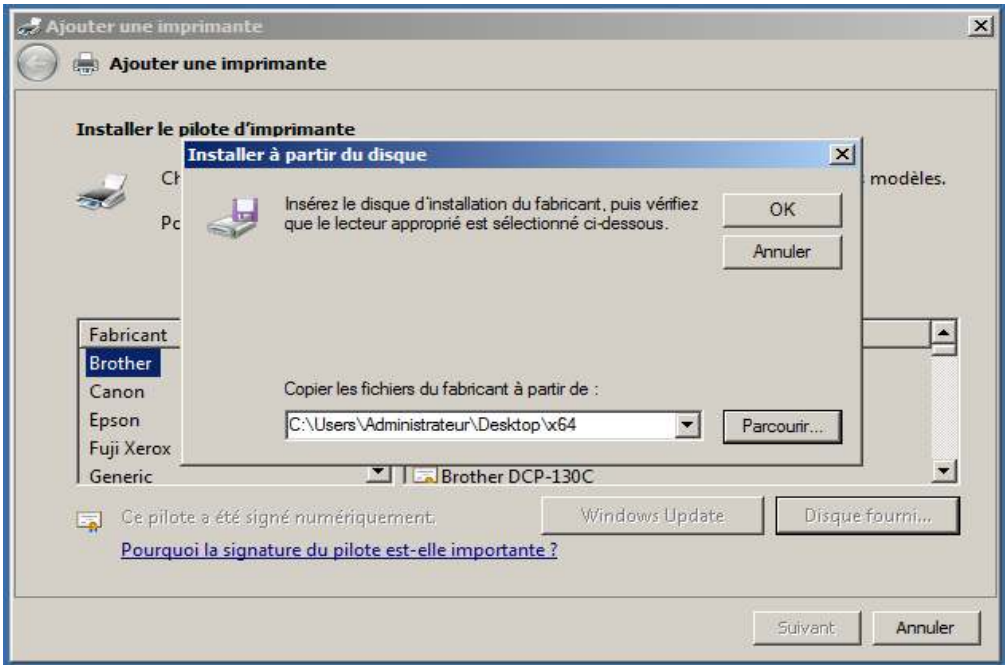


Figure 92

WWW.DZPEN.COM | قلم الجزائر

Sélectionner votre modèle d'imprimante et cliquer sur "**Suivant**" (voir figure 93).

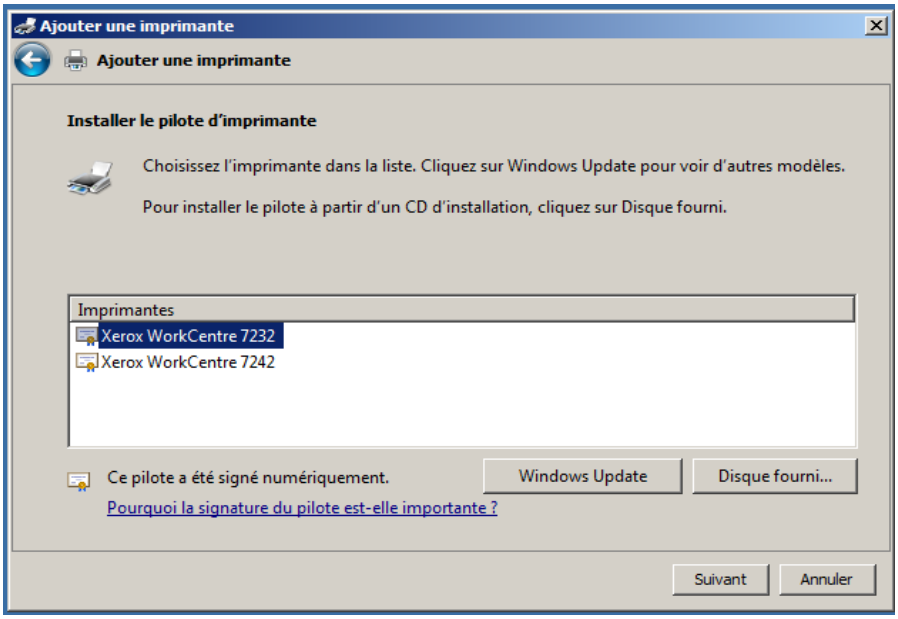


Figure 93

Choisissez un nom pour l'imprimante et cliquer sur "**Suivant**" (voir figure 94).

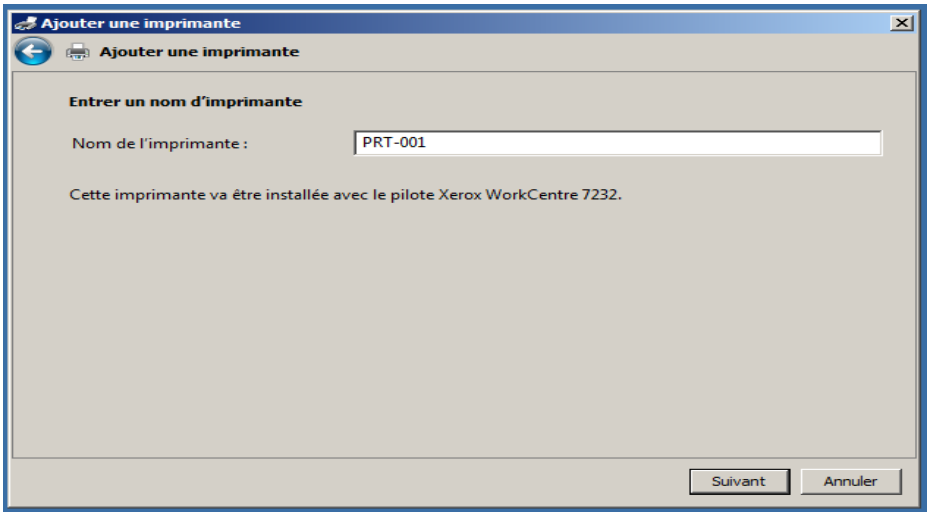


Figure 94

WWW.DZPEN.COM | قلم الجزائر

Le serveur installe le pilote (voir figure 95).

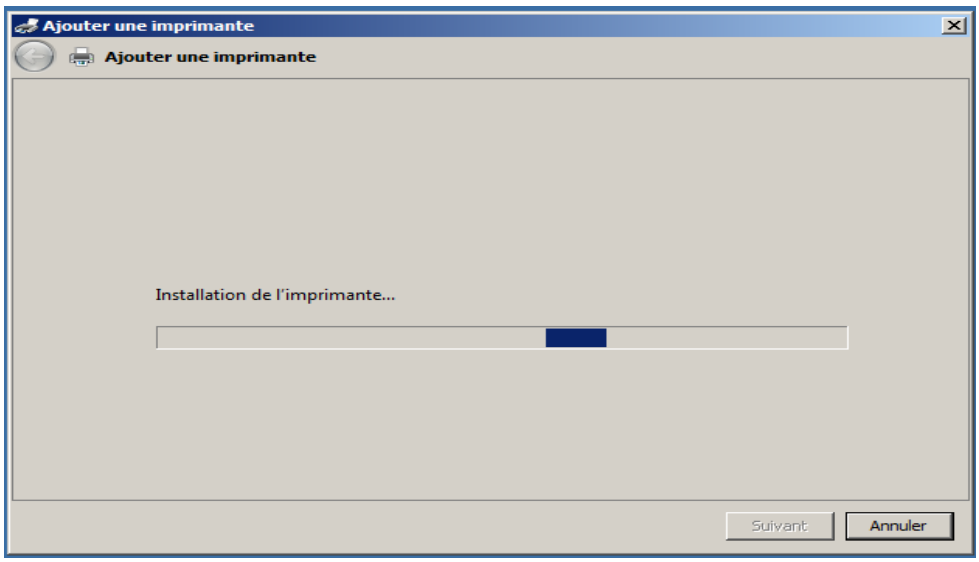


Figure 95

Partage de l'imprimante

– Sélectionner "**Partager cette imprimante afin que d'autres utilisateurs puissent l'utiliser**" puis remplir les trois champs :Nom du partage : nous mettons le même nom de l'imprimante,
Emplacement : l'emplacement physique de l'imprimante, Commentaire : nous mettons l'adresse IP de l'imprimante ainsi que le modèle, Puis cliquer sur "**Suivant**" (voir figure 96).

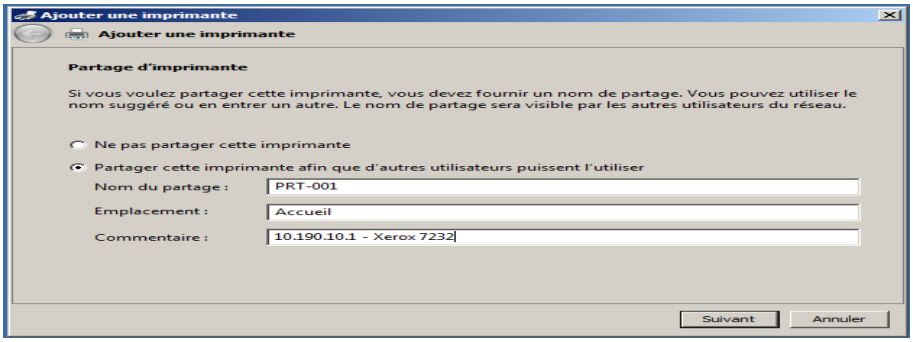


Figure 96

WWW.DZPEN.COM | قلم الجزائر

– Là, cliquer sur "**Imprimer une page de test**", si tous est bien configuré l'imprimante devrait sortie une page de test (voir figure 97)

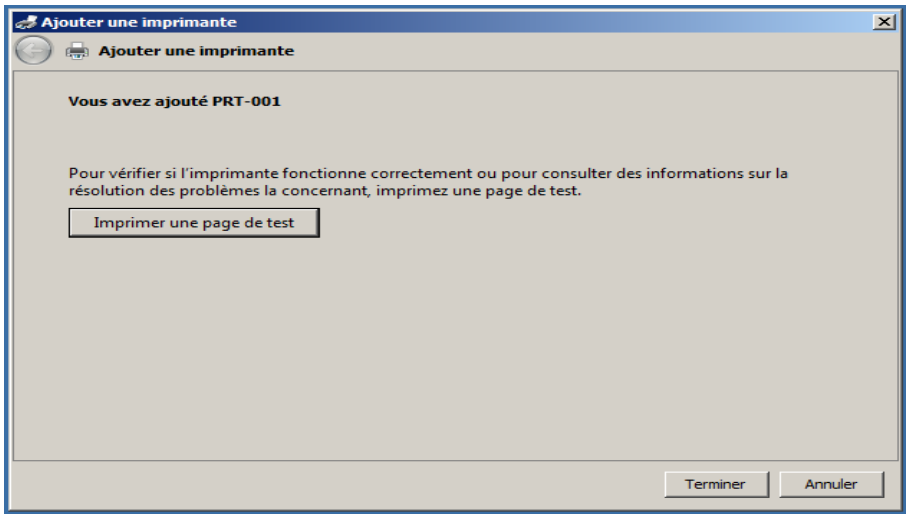


Figure 97

Remarque

Nous allons ajouter le pilote x86 afin que les poste en 32 bits puissent installer l'imprimante facilement, pour cela, aller dans "**Périphériques et imprimantes**" puis sur **l'imprimante** faite un clique droit "**Propriétés de l'imprimante**" (voir figure 98).

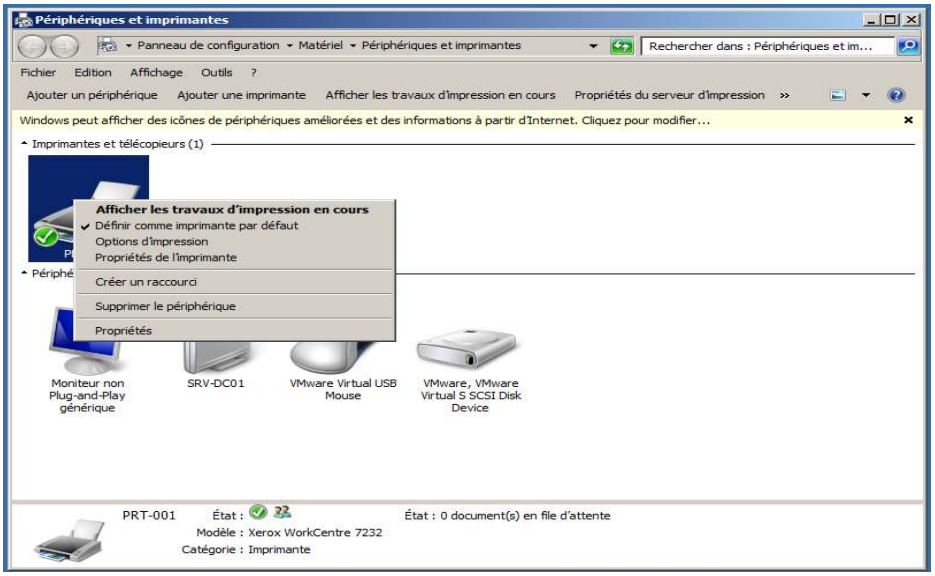


Figure 98

WWW.DZPEN.COM | قلم الجزائر

– Aller dans l'onglet "**Partage**" puis cocher "**lister dans l'annuaire**" puis cliquer sur "**Pilotes supplémentaires...**" (voir figure 99).

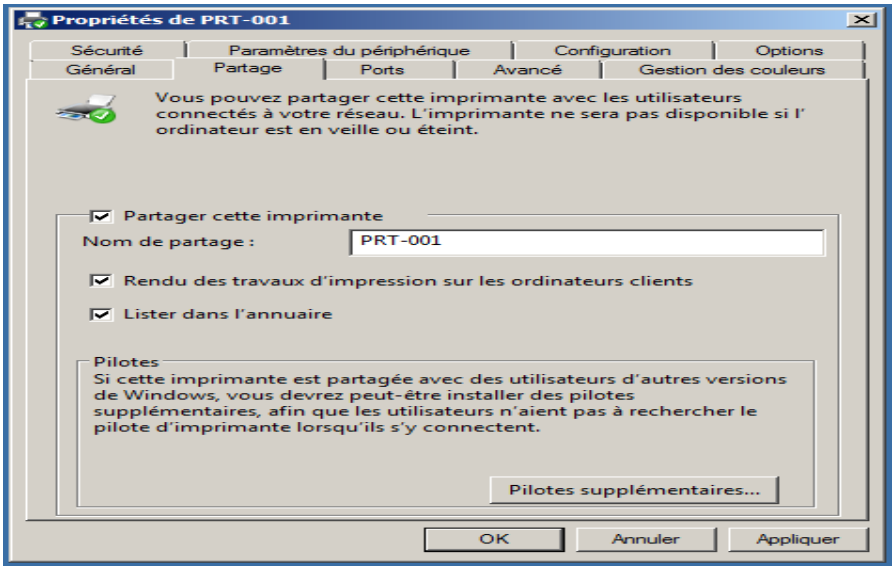


Figure 99

La fenêtre ci-dessous s'ouvre, cocher "**x86**" et cliquer sur "**OK**" (voir figure 100).

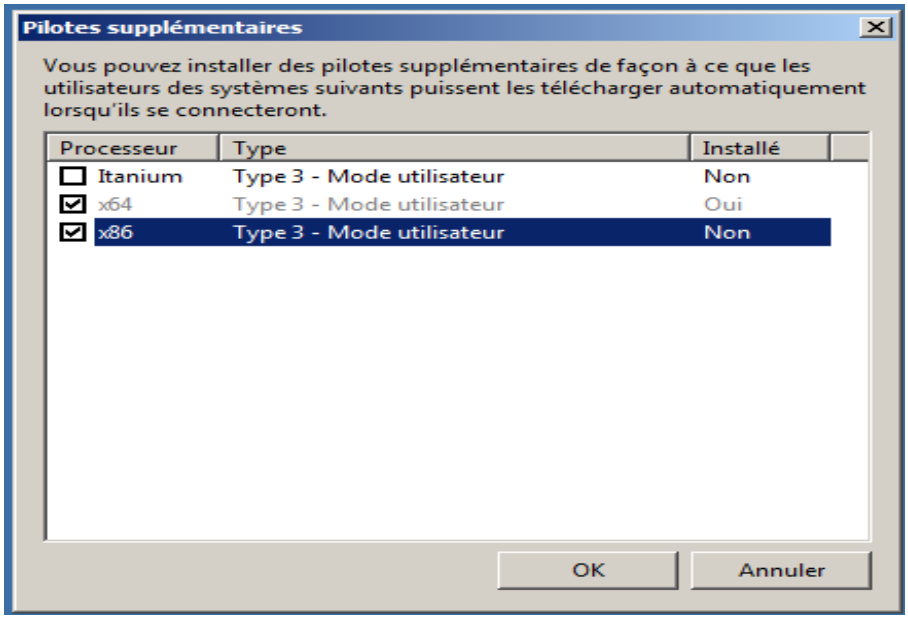


Figure 100

WWW.DZPEN.COM | قلم الجزائر

– Sélectionner les fichiers du pilote x86, puis cliquer sur "**OK**" (voir figure 101).

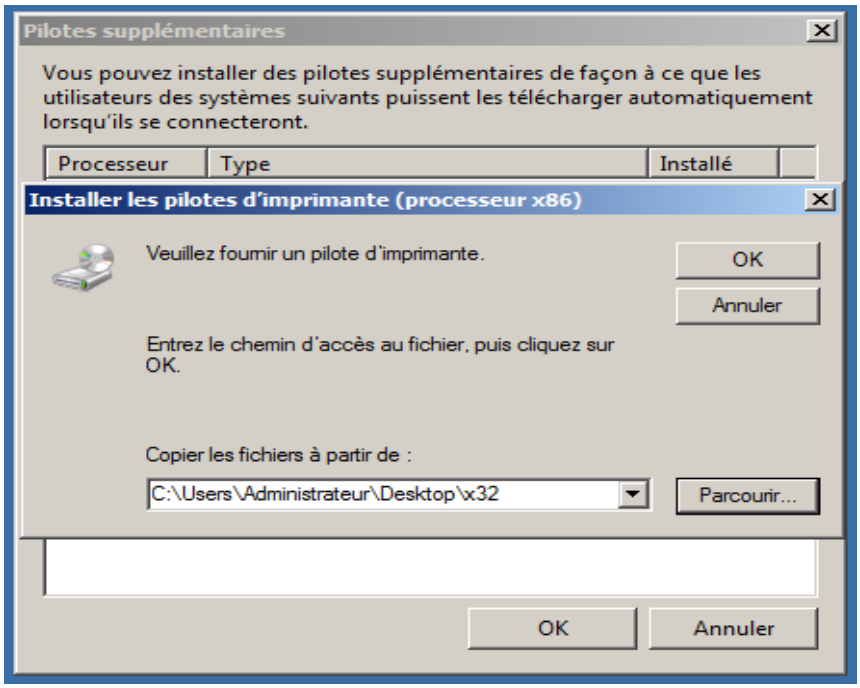


Figure 101

Pour finir cliquer sur "**Appliquer**", cliquer de nouveau sur "**Pilote supplémentaires...**" (**voir** figure 102).

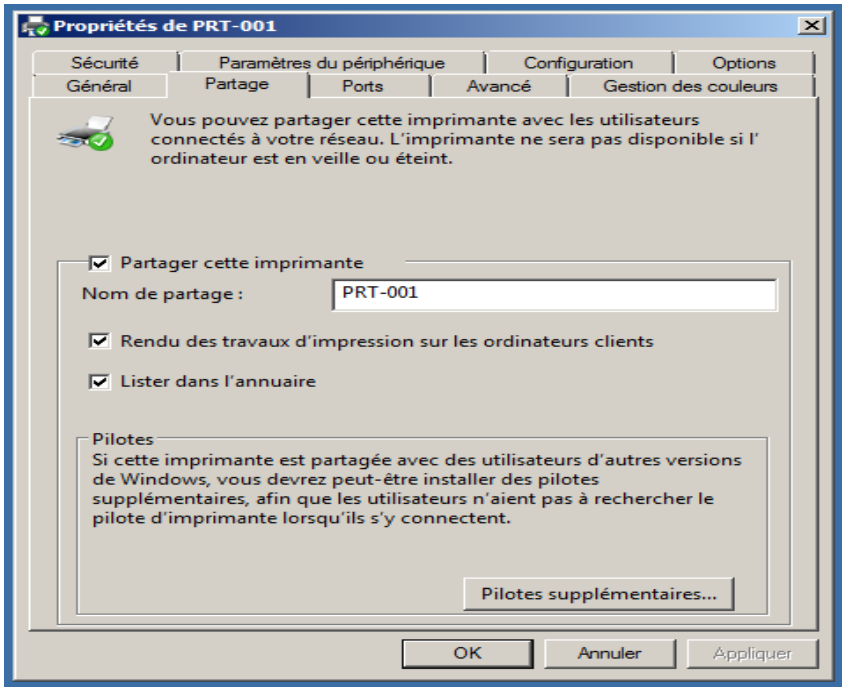


Figure 102

WWW.DZPEN.COM | قلم الجزائر

Les deux lignes "x64" et "x86" doivent être grisé, comme le montre l'image ci-dessous (voir figure 103).

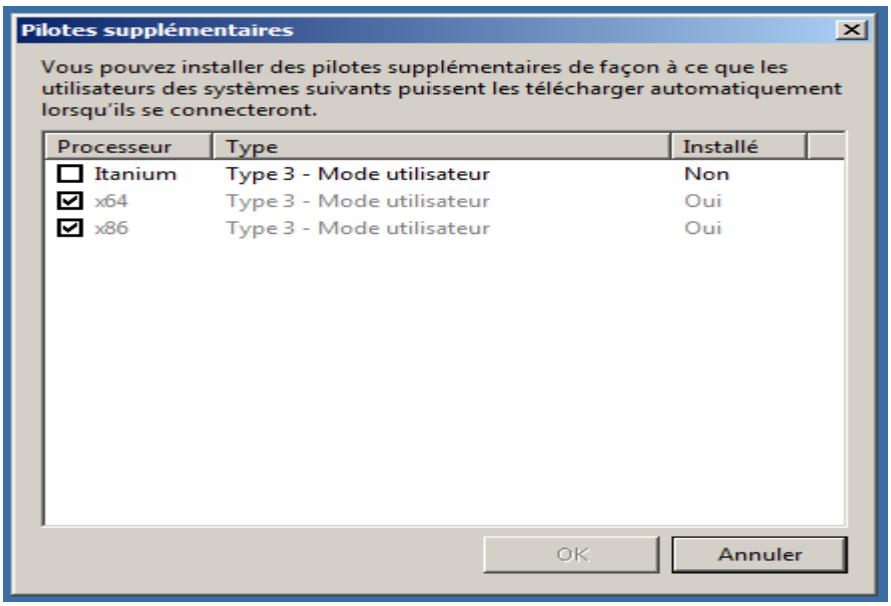


Figure 103

Voilà, l'imprimante est désormais disponible sur le serveur d'impression.

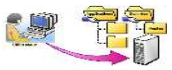
7.3 Système de fichiers :

NTFS est un système de fichier, il permet de stocker efficacement les données sur une partition. Ainsi, on peut accorder des autorisations d'accès sur les dossiers et les fichiers afin de contrôler le niveau d'accès aux ressources dont bénéficient les utilisateurs. Pour une bonne optimisation de l'espace disque, NTFS compresse les données et permet la configuration des quotas de disque.

7.3.1 Structure du Système de fichiers NTFS :

Ce système de fichiers existait déjà sous NT4, mais on le trouve dans sa version 5 sous Windows 2003. Le formatage NTFS est recommandé par Microsoft, car il permet des fonctions supplémentaires par rapport aux systèmes FAT. En ce qui concerne les fonctions de récupération des données de compression dossiers par dossiers en temps réel de limitation de capacité par utilisateur (quotas de disque) d'individualisation des répertoires du disque (sécurité individuelle) de sécurité. Les autorisations NTFS sur les dossiers et les fichiers

WWW.DZPEN.COM | قلم الجزائر



garantissent leur accès aussi bien par rapport aux utilisateurs travaillant sur l'ordinateur qu'à ceux qui y accèdent par le réseau d'encryptage. NTFS permet d'encrypter les données inscrites sur les partitions. Se système est composé de :

- **Structure de volume ou de partition**

NTFS utilise des clusters (ou unités d'allocation) constitués de un ou plusieurs secteurs. La taille des clusters varie en fonction de la taille de la partition NTFS. Par exemple, pour une partition de 512 Mo, il n'y qu'un secteur par cluster et La taille de ce cluster est de 512 octets. Pour une partition (stockage de base) ou un volume (stockage dynamique) de 32Go, il y a 128 secteurs par cluster et la taille des clusters est donc de 64Ko.

- **Secteur d'amorçage**

Le secteur d'amorçage contient le code qui permet de localiser et charger les fichiers de démarrage de Windows 2003-2008 tel que le fichier **Ntdlr.**

- **MFT (Master File Table)**

Cette table contient pour chaque volume les informations concernant chaque fichier: son nom, sa taille, sa date de création et celle de mise à jour, les autorisations, les attributs et autres. Pour chaque répertoire et chaque fichier, il y a un enregistrement dans la table MFT.

- **Conversion d'un volume au format NTFS**

La conversion FAT (16 ou 32) vers NTFS est possible sans perte de données.

Pour cela vous devez exécuter l'utilitaire nommé**Convert.exe**qui se trouve dans le dossier % systemRooot% ,lorsque vous convertissez un volume avec cet outilla structure des fichiers et des répertoires est préservée et aucune donnée ne sera perdue.

✓ **Syntaxe complète de la Commande CONVERT :**

Volume /FS : NTFS [/V] [/X] [/CvtArea :nomfichier] [NoSecurity] :

– **Volume**: spécifie la lettre de lecteur (C:, D: …) ou le nom de volume

/FS:NTS spécifie que le volume va être converti en NTFS.

– /V : indique que CONVERT va s'exécuter en mode« bavard ».

(Commentaires).

WWW.DZPEN.COM | قلم الجزائر

– /X : force le démontage du volume avant la conversion (si nécessaire).

– /CvtArea : nom fichier définit le nom d'un fichier à secteurs contigus dans le répertoire racine qui recevra les fichiers systèmes NTFS.

– /NoSecurity supprime tous les attributs de sécurité et rend les fichiers et les répertoires accessibles au groupe Tout le monde, par contre le passage de NTFS vers FAT n'est pas possible.

– Solution: Sauvegarde complète de vos données, formater une nouvelle partition en FAT, Restaurer vos données sur cette partition.

– **Exécution de Check Disk depuis la ligne de commande :**

Cet utilitaire peut être exécuté à partir de l'invite de commande ou depuis d'autres utilitaires. A partir de l'invite de commande tapez **CHKDSK** pour vérifier le lecteur courant (voir figure 104).

Cette commande possède de nombreuses options :

- **Volume:** indique le volume à manipuler.
- **Nom de fichier** (FAT/FAT 32 uniquement) : indique les fichiers à contrôler du point de vue de la fragmentation.
- **/F :** Répare les erreurs du disque.
- **/V** sur FAT/FAT 32 : affiche le chemin d'accès complet et le nom de chaque fichier du disque. Sur NTFS : affiche mes éventuels messages de nettoyage.
- **R :** Localise les secteurs défectueux et récupère les informations lisibles (implique l'utilisation du commutateur /F).
- **/L :** taille NTFS seulement : modifie la taille du fichier journal.
- **/X :** Entraîne le démontage préalable du disque si nécessaire (implique l'utilisation du commutateur /F).
- **/I NTFS seulement :** effectue une vérification minimale des entrées d'index.
- **/C NTFS seulement :** saute la vérification des cycles au sein de la structure de dossiers.

WWW.DZPEN.COM | قلم الجزائر

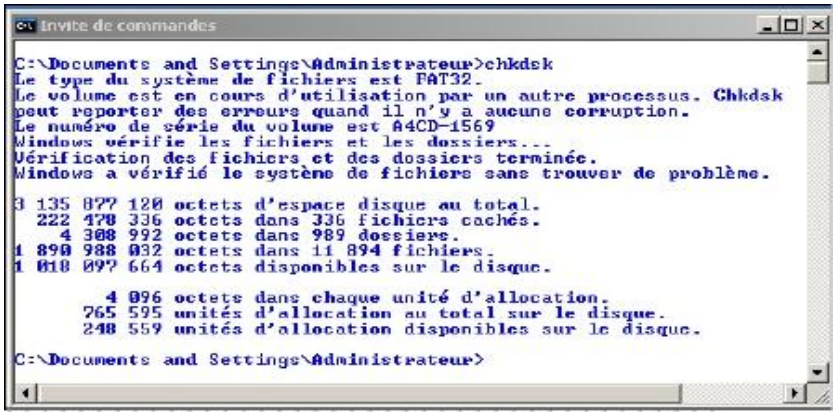


Figure 104

- **Exécution de Check Disk de manière interactive :**

  Vous pouvez exécuter Check Disk de manière interactive à l'aide de l'explorateur de Windows ou de l'outil Gestion des disques. A partir du lecteur à tester, cliquez droit dessus puis sélectionnez Propriétés, puis cliquez sur **Vérifier maintenant**. Dans la fenêtre inter active Check Disk vous pouvez cocher : Rechercher et tenter une réparation des secteurs défectueux **Réparer automatiquement les erreurs du système de fichiers** (voir figure 105).

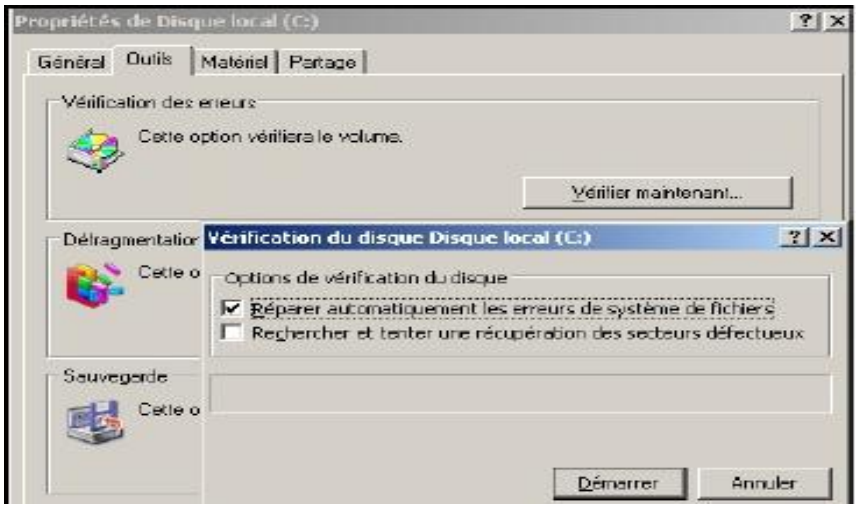


Figure 105

WWW.DZPEN.COM | قلم الجزائر

7.3.2 Système de fichier CDFS :

Windows 2003,2008 permet la lecture des CD-ROM conformes aux normes ISO9660 et ISO 9660 niveau 2 avec noms de fichiers longs. Les noms des fichiers et répertoires doivent être en majuscules.

7.3.3 Système de fichier UDF :

Le format **UDF** (Universal Disk Format) permet la lecture de certains CD-ROM, mais surtout des DVD. Il permet aussi l'écriture sur des supports réinscriptibles CD-RW ou à écriture unique CD-R ou WORM.

Le système Windows 2003 ,2008 seuls, permet la lecture directe de ce type de support.

Pour l'écriture, il faut lui adjoindre une application spécifique (type NERO).La prise en charge des DVD en lecture seule permet de disposer de supports à grande capacité. Ainsi le support technique Microsoft TechNetest fourni sur ce support.

7.4 Sécurité des systèmes de fichiers :

Les permissions vues précédemment s'appliquent aux utilisateurs accédant aux ressources via le réseau. Par contre aucune limite de partage n'est mise en œuvre pour les utilisateurs accédant localement à l'ordinateur. Nous allons voir comment sécurisé les données contre un accès non autorisé et cela localement.

Cela n'est possible qu'avec le système de fichier NTFS car il permet la mise en œuvre des attributs de sécurité et d'audit NTFS permet de maintenir à jour par fichier ou dossier une liste de contrôles d'accès ou ACL contenant au niveau système de fichiers les numéros d'utilisateurs (SID) ainsi que leurs permissions sur la ressource.

Les systèmes de fichiers utilisés sur Windows 2003 permettent le partage des dossiers et de leur contenu. Ceci permet aux utilisateurs en réseau de travailler sur les fichiers du serveur Windows 2003.L'accès aux répertoires partagés ou non, d'un serveur Windows 2003 est régit par des **autorisations**. On distingue les deux types d'autorisations :

Autorisations simples qui sont utilisées pour les partitions **FAT**

Autorisations de sécurité utilisables uniquement avec les partitions **NTFS.**

WWW.DZPEN.COM | قلم الجزائر

7.4.1 Autorisations simples de partages :

Les autorisations de partages sont **contrôle total**, **modifier**, **lecture**. (Voir figure 106)

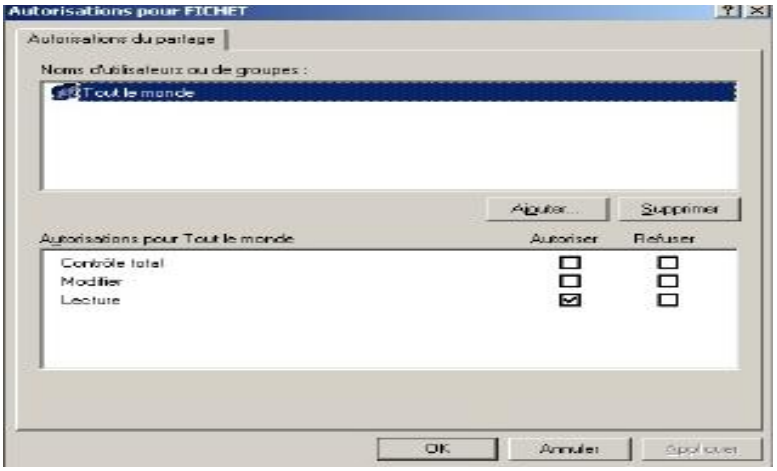


Figure 106

7.4.2 Autorisations simples et autorisations de Sécurité :

Les autorisations simples s'appliquent aux dossiers, en aucun cas aux fichiers.

Les autorisations simples s'appliquent aux utilisateurs utilisant le partage à partir du réseau mais pas aux utilisateurs ayant ouvert une connexion sur la station du serveur.

L'autorisation appliquée par défaut est "**Contrôle total**" et elle est donnée au groupe "**Tout le monde**".

Les icônes d'un dossier partagé sous windows2003, 2008 sont les suivantes , dans l'explorateur Windows, un dossier peut être partagé avec des autorisations et des noms différents pour des utilisateurs ou des groupes distincts .

Il est possible de limiter l'accès à un partage à un nombre donné d'utilisateurs (bouton "nombre d'utilisateurs" du panneau partage) (voir figure 107).

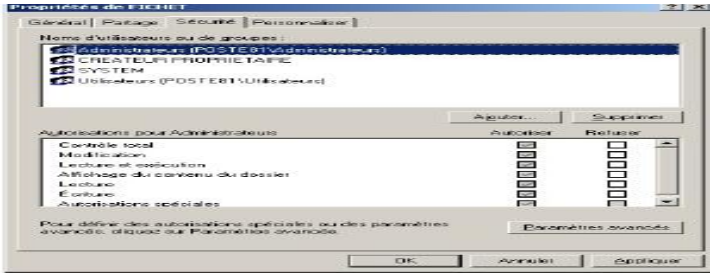


Figure 107

WWW.DZPEN.COM | قلم الجزائر

Il existe 3 types d'autorisations simples (voir tableau108) :

Lecture	Les utilisateurs peuvent afficher les noms des dossiers et des fichiers, lire ou exécuter les fichiers
Modifier	Donne l'autorisation de lecture, plus la possibilité de modifier le nom des dossiers et des fichiers, ainsi que leur contenu.
Contrôle total	Donne l'autorisation de modifier, plus l'autorisation de modifier les autorisations sur le partage.

Tableau108

Ces autorisations peuvent être accordées soit à des groupes, soit à des utilisateurs particuliers (voir figure 109).

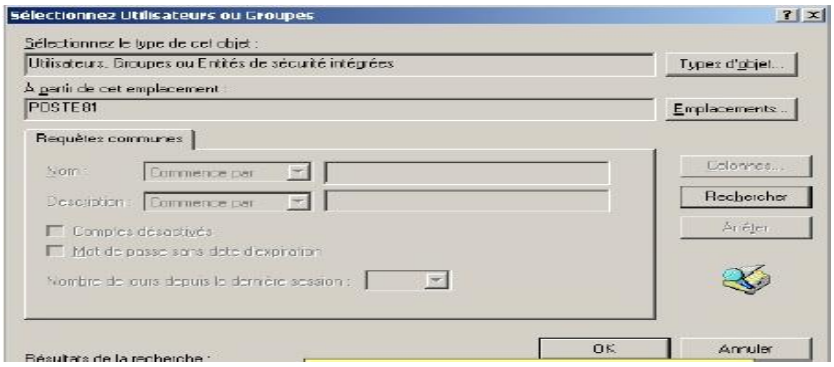


Figure 109

7.5 Exercice théorique :

1. Qu'est- ce- que NTFS ?

2. Quelle est la différence entre FAT et NTFS ?

3. Quelle est la différence entre le système de fichiers CDFS et UDF ?

4. Quel est la différence entre les autorisations de partage et les autorisations de sécurité ?

7.6 Exercice pratique:

1. Créer un dossier sous le nom test et créer dedans un fichier texte.

2. Partager le dossier test et déterminer les autorisations de partage par défaut.

3. Supprimer les autorisations par défaut et ajouter le groupe administrateurs.

4. Attribuer l'autorisation contrôle total au groupe administrateurs.

5. Ajouter le groupe Gpersonnel et attribuez- lui l'autorisation modifier.

6. Ajouter le groupe Gchefservice et attribuez-lui l'autorisation lecture.

WWW.DZPEN.COM | قلم الجزائر

7.7 Résumé :

Windows Server 2003-2008 met à votre disposition tous les outils nécessaires au partage sécurisé de dossiers à travers le réseau. Les autorisations de partage s'appliquent de manière précise et efficace au niveau des comptes d'utilisateurs et de groupes. Ce mode d'autorisation d'accès aux dossiers, garantissent un degré de sécurité maximal.

7.8 Exercice de synthèse :

1. Ouvrer une session administrateur.

2. Créer un dossier DOSMSI et créer dedans un fichier texte.

3. Partager le dossier DOSMSI.

4. Déterminer les autorisations par défaut sur le dossier partagé DOSMSI ?

5. Supprimer les autorisations par défaut et ajoutez le groupe administrateurs.

6. Attribuer au groupe administrateurs l'autorisation contrôle totale.

7. Créer un lecteur réseau vers le dossier partagé.

8. Connecter un lecteur réseau au dossier partagé.

9. Déconnecter le lecteur réseau, et connecté au dossier partagé DOSMSI.

10. Tester l'accès au dossier partagé par un l'utilisateur non autorisé.

11. Connectez-vous au dossier partagé DOSMSI en tant qu'administrateur.

12. Supprimer le partage du dossier DOSMSI.

WWW.DZPEN.COM | قلم الجزائر

Résumé général

L'administrateur système consiste à gérer les comptes d'utilisateurs et les groupes. Ces comptes sont des objets Active Directory permettent aux utilisateurs de l'entreprise d'accéder aux diverses ressources réseau dont ils ont besoin. Les comptes d'utilisateurs permettent aux utilisateurs d'ouvrir des sessions et d'accéder aux ressources locales ou de domaine.

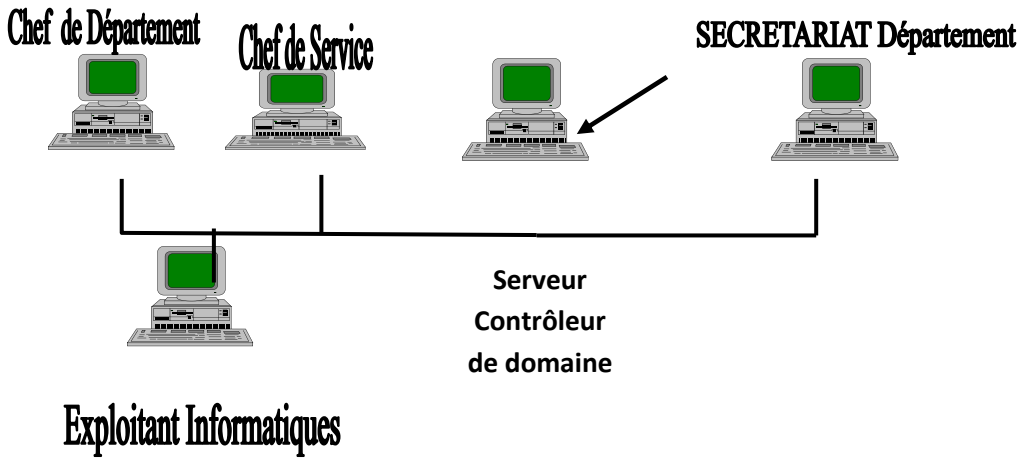
Dans ce module vous allez acquérir les connaissances et les compétences nécessaires à la modification des comptes d'utilisateurs et des comptes d'ordinateurs sur les ordinateurs qui exécutent Microsoft Windows Server 2003-2008 dans un environnement réseau.

A la fin un administrateur réseau doit pouvoir gérer les clients en ce qui concerne les comptes, les groupes et le profil et aussi l'administration des permissions entre autre le partage des ressources et l'attribution des autorisations de partage et autorisation de sécurité et NTFS.

WWW.DZPEN.COM | قلم الجزائر

Exercice de synthèse générale

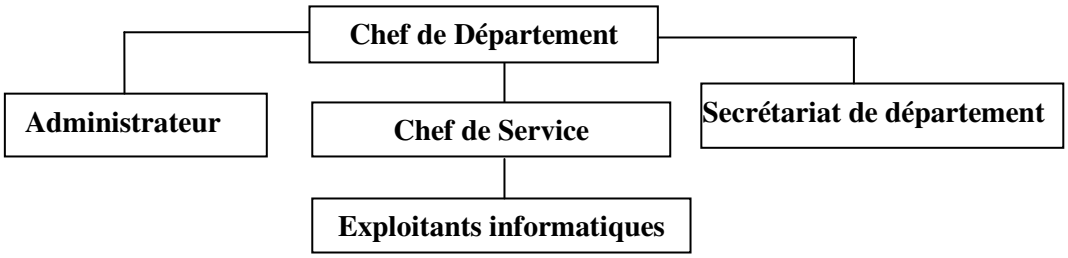
Pour son département Informatique, une entreprise veut mettre en place un réseau administré à base de Windows 2008 Serveur R2, dont le schéma du réseau est :



Le département informatique est structuré comme suit :

- Chef de Département
- Chef de Service
-Agents (Exploitant Informatiques).

L'organigramme de ce département administratif est décrit ci-dessous



Ce département sera divisé en 3 groupes :

Responsable comprenant : **Chef de Département et Chef de service**.

Secrétaire comprenant : **Secrétariat Département**

Agents comprenant : **Exploitants (3)**

En tant qu'administrateur réseau de l'entreprise avec :

(Nom utilisateur « **Administrateur** » mot de passe « **Sysvol03** ») vous devez effectués les tâches suivantes :

WWW.DZPEN.COM | قلم الجزائر

Tâche 01 :

Installer le système d'exploitation 2008 Server R2sur le poste serveur.

Installer le système d'exploitation windows7 sur les postes clients.

Attribuer des adresses IP pour le serveur et les clients.

Tâche 02 :

Configurer un contrôleur de domaine sur le serveur contrôleur de domaine, avec les paramètres suivants :

- Contrôleur de domaine pour un nouveau domaine
- Pour une nouvelle arborescence de domaine
- Pour une nouvelle forêt d'arborescences de domaine
- Nom DNS : NOM..net (NOM est votre nom)
- Nom de domaine Net Bios : NOM

Tâche 03:

- Adhérer les postes clients au domaine.

Tâche 04:

Les dossiers exploités au niveau de ce département sont :

-Fiches de maintenance.

-Fiches d'inventaires.

-Les responsables (Chef de département-Chef de service) auront l'autorisation de lecture sur ces dossiers de ce département, les autres auront un contrôle total sur les dossiers.

- Créer les comptes utilisateurs, chaque utilisateur avec son dossier de base et son profil itinérant.
- Créer les groupes d'utilisateurs.
- Intégrez les comptes dans leurs groupes correspondants

Tâche 05 :

- Créez les dossiers
- Partagez et accorder les autorisations nécessaires.

Test :

1. Ouvrir une session sur le poste client avec le compte utilisateur.

2. Vérifier le dossier de base.

3. Vérifier le profil.

4. Accéder à un dossier partagé.

Remarque :

Le test doit se faire pour un seul utilisateur.

WWW.DZPEN.COM | قلم الجزائر

Bibliographie :

Windows Server 2008 Volume 1Installation et mise en réseau

CHARLIE, Russel. SHARON, Crawford.Adapté de l'américain par: Bénédicte Volto et Véronique Warion.

Server 2008 Active Directory Délégation de contrôle.

Etudiant : PELLARIN, Anthony.Professeur :LITZISTORF, Gérald

En collaboration avec : Pictet et Cie.Date du travail : 17.09.2007

Essentiel Windows 2003 Administrer Et Gérer Un Environnement Microsoft Windows Server 2003.

Auteurs : YANN, Alet. BRAHIM, Nedjimi. et LOIC, Thobois.

Version 1.0 – 2004-01-12.Ecole Supérieure d'Informatique de Paris

Windows server 2003 :profil d'utilisateur

Auteur : FREDERIC, Diaz.

Direction Recherche Et Ingénierie De Formation Secteur NTIC.

Office de la Formation Professionnelle et de la Promotion du Travail(OFPPT)

http://www.laboratoire-microsoft.org

www.supinfo.com.

http://perso.mediaserv.net/ganja/softs/support_cours/Support_cours_win2k/2053B%20Delivery%20Guide/X08-7738904.pdf.

http://obm.org/media/documents/documentation/guides/grp_module_groupes.pdf

http://www.courstechinfo.be/OS/ComptesLocaux_XP.pdf

http://medialog.ac-creteil.fr/ARCHIVE49/reseau49.pdf

file:///C:/Users/DELL/Desktop/document%20du%20manuele/12102014/51.html

file:///C:/Users/DELL/Desktop/document%20du%20manuele/12102014/Administration%20syst%C3%A8me.htm

http://salihayacoub.com/420keg/Semaine3/KEGAtelier5.2.pdf

http://doc.esaip.org/~ptregouet/Cours/Windows/Autorisations%20NTFS/autorisations%20NTFS.pdf

http://clerentin.iut-amiens.fr/ASR3_Windows/Partie4.pdf

WWW.DZPEN.COM | قلم الجزائر

ANNEXES

Annexe A : Corrigé Des Exercices

Exercices théoriques du chapitre 1:

Exercice N°1 :

1. Le rôle d'un compte utilisateur local permet d'ouvrir une session uniquement sur l'ordinateur qui contient le compte de l'utilisateur crée.

2. Le rôle d'un compte administrateur permet de gérer l'ensemble de la configuration des ordinateurs et du domaine et en particulier la création, modification et suppressions des comptes d'utilisateurs et de groupes.

3. Le compte invité est réservé aux utilisateurs qui ne possèdent pas de compte sur l'ordinateur. Aucun mot de passe ne lui est associé, ce qui permet aux utilisateurs d'ouvrir rapidement une session pour consulter leurs courriers électroniques ou surfer sur Internet.

4. Un compte utilisateur local peut être crée uniquement par l'administrateur.

Exercice N°2 :

1. Ce sont les comptes crées automatiquement à la création de l'annuaire : Administrateur et Invité.

2. Non il est impossible de supprimer ce compte.

3. Oui d'ailleurs c'est conseillé par Microsoft.

4. Non et cela pour des raisons de sécurité.

5. Non la modification d'un nom de compte ne modifie pas l'identifiant unique de sécurité de compte (SID) qui est utilisé par le système pour entre autres, octroyer des droits et permissions aux utilisateurs.

6. Oui, car il s'agit dans ce cas de la création d'un nouveau compte, donc d'un nouvel SID, même si le compte est identique et le mot de passe aussi.

7. En cochant l'option « utilisateur doit changer le mot de passe à la prochaine ouverture de session.

Exercice pratique du chapitre 1 :

1. Pour ouvrir une session Administrateur sur votre ordinateur local aller sur le nom du compte administrateur puis entrer le mot de passe et cliqué sur suivant.



WWW.DZPEN.COM | قلم الجزائر

2. Pour Créer un Compte d'utilisateur local portant votre nom il faut suivre les étapes suivantes :

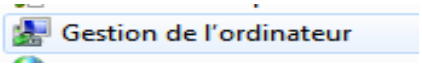
- Menu démarrer – tous les programmes – panneau de configuration



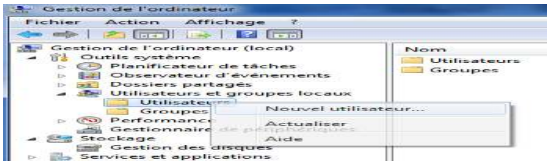
- Outils d'administration



- Gestion de l'ordinateur

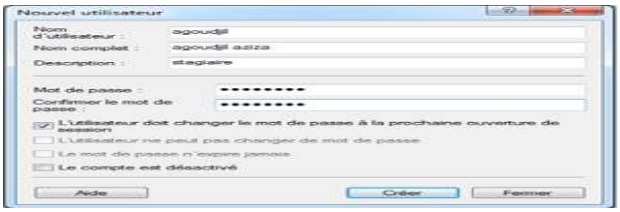


- Utilisateur et groupes locaux bouton droit nouvel utilisateur.





- Saisir les données concernant le compte utilisateur.



3. Ouverture d'une session avec votre nom. :

- Aller au menu démarrer puis arrêter et changer d'utilisateur
- Faire un double clique sur le nom du compte d'utilisateur vous obtenez un bureau.



4. Vous constatez à cette étape qu'une session de travail a été ouverte.

Exercice de synthèse du chapitre 1 :

1. Ouverture d'une session en tant qu'administrateur sur le poste client avec localpw

2. A partir du menu **Outils d'administration** ouvrir la console **Gestion de l'ordinateur**

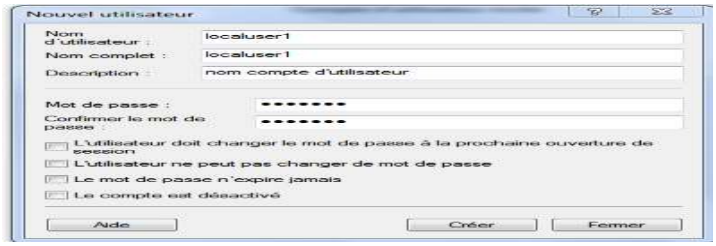
- Dans l'arborescence de la console, sous **Outils système**, développer **Utilisateurs et groupes locaux**, puis cliquer sur **utilisateur**
- Cliquer avec bouton droit sur **utilisateur**, puis cliquer sur **nouvel utilisateur**
- Dans la boite de dialogue nouvel utilisateur, saisir les informations suivantes :

WWW.DZPEN.COM | قلم الجزائر

Utilisateur : localuser1

Description : mon compte d'utilisateur

Mot de passe : Passe01.



➢ Cliquer sur crée pour créer le compte utilisateur puis fermer pour fermer la boite de dialogue nouvel utilisateur.

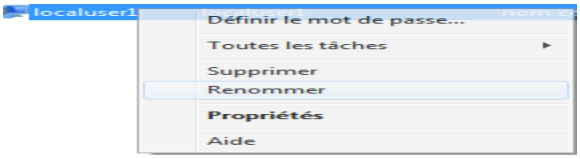
3. Désactivation de la case à cocher l'utilisateur doit changer de mot de passe à la prochaine ouverture de session, puis faire un clique sur Créer.

4. Fermeture de la boite de dialogue nouvel utilisateur

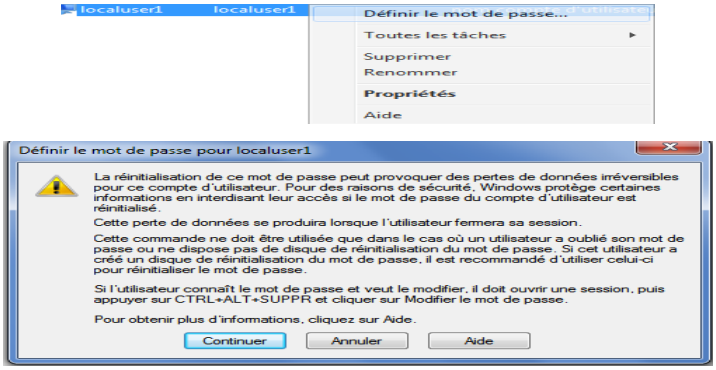
5. Fermeture de la console gestion de l'ordinateur, puis la session.

6. Pour modifier le nom, le mot de passe et l'image du compte utilisateur vous devez suivre les étapes suivantes :

✓ Modification du nom du compte d'utilisateur :



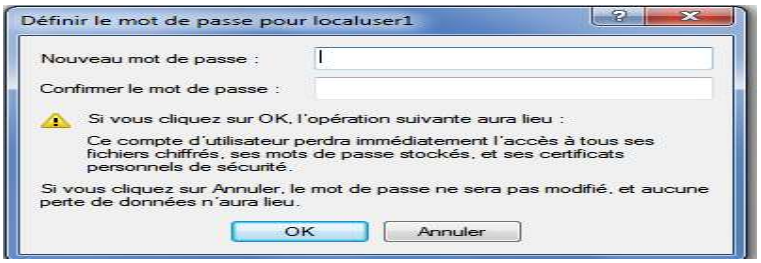
✓ Modification du mot de passe du compte d'utilisateur :



Faire un Clic sur le bouton continuer.

Entrer le nouveau mot de passe puis confirmer le mot de passe.

WWW.DZPEN.COM | قلم الجزائر



✓ Modification de l'image du compte :



Test :

1. Quand nous essayons d'ouvrir une session avec localuser1 et son mot de passe sur serveurx le compte ne s'ouvre pas par ce que le compte est créer localement

2. Nous pouvons ouvrir une session sur poste client avec localuser1.

3. Création d'un autre compte utilisateur localuser2:

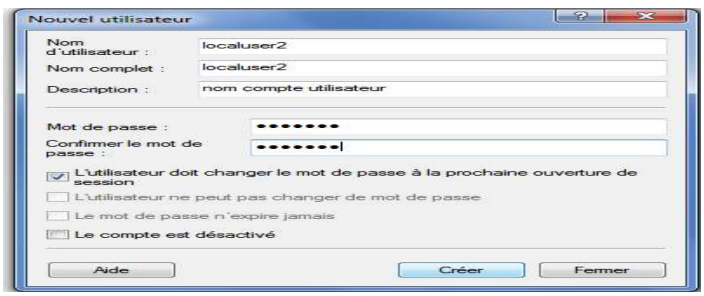
A partir du menu **Outils d'administration** ouvrir la console **Gestion de l'ordinateur**

- Dans l'arborescence de la console, sous **Outils système**, développer **Utilisateurs et groupes locaux**, puis cliquer sur **utilisateur**
- Cliquer avec bouton droit sur **utilisateur**, puis cliquer sur **nouvel utilisateur**
- Dans la boite de dialogue nouvel utilisateur, entrer les informations suivantes :

Utilisateur : localuser2

Description : mon compte d'utilisateur

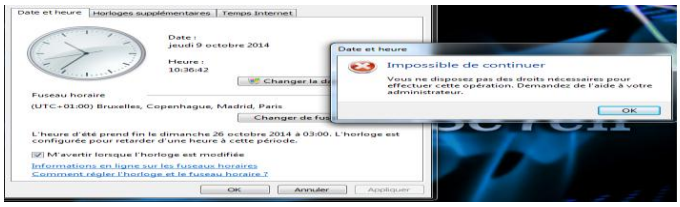
Mot de passe : Passe02.



WWW.DZPEN.COM | قلم الجزائر

➢ Cliquer sur crée pour créer le compte utilisateur puis fermer pour fermer la boite de dialogue nouvel utilisateur.

4. L'heure système ne peut pas être modifiée, par ce que nous ne disposons pas les droits nécessaires.

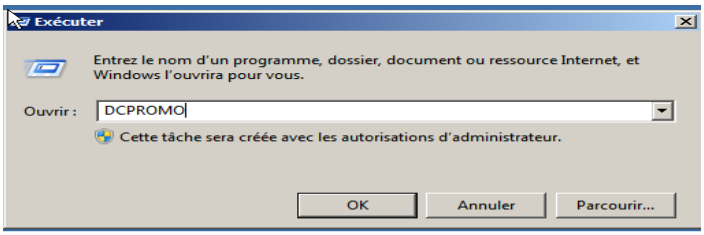


5. Nous ne pouvons pas accédez au serveurx via voisinage réseau.

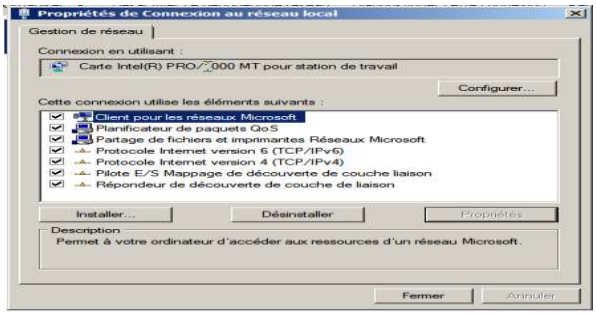
Nous pouvons interpréter ce fait parce que le compte utilisateur a été crée localement.

Exercice d'application du chapitre 2 :

Avant la création d'un compte utilisateur de domaine il faut configurer le serveur comme un serveur contrôleur de domaine, pour cela il faut installer active directory en utilisant la commande DCPROMO puis configurer l'adresse IP du serveur.

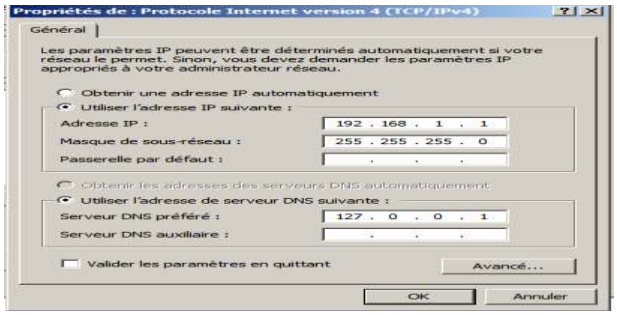


- **Configurer le réseau** » à partir de l'assistant qui ouvre « **Connexions au réseau local** » Un clic droit sur la carte réseau pour accéder à ses propriétés va nous permettre de modifier les paramètres TCP/IP.



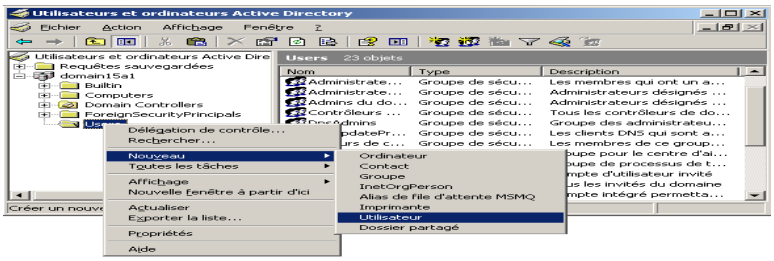
- Cocher utiliser l'adresse IP suivante

WWW.DZPEN.COM | قلم الجزائر



1. Pour Créerun compte utilisateur de domaine section1 nous suivons les étapes suivantes :

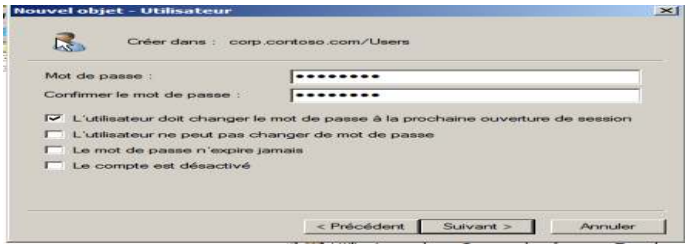
➢ Démarrer –Outil d'administration- utilisateur et ordinateur Active Directory-nom du domaine –Users -bouton droit nouvel utilisateur.



➢ Saisir les informations du nouvel utilisateur.



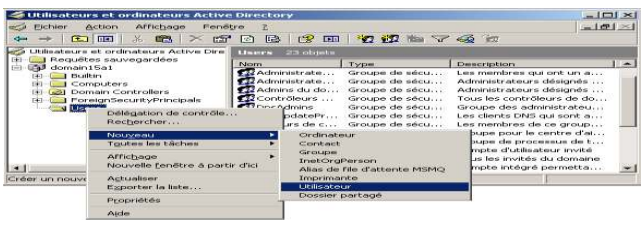
➢ Taper le mot de passe



➢ Cliquer sur suivant puis sur terminer.

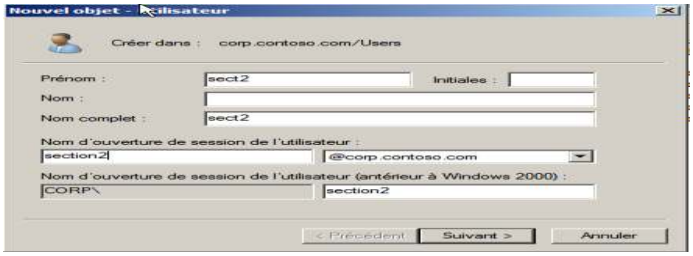
2. Pour Créer un compte utilisateur de domaine section2nous suivons les étapes suivantes :

➢ Menu Démarrer –Outil d'administration- utilisateur et ordinateur Active Directory-non du domaine -Users-bouton droit nouvel utilisateur.

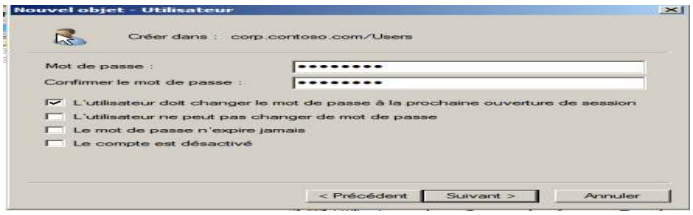


WWW.DZPEN.COM | قلم الجزائر

➢ Saisir les informations du nouvel utilisateur.



➢ Taper le mot de passe

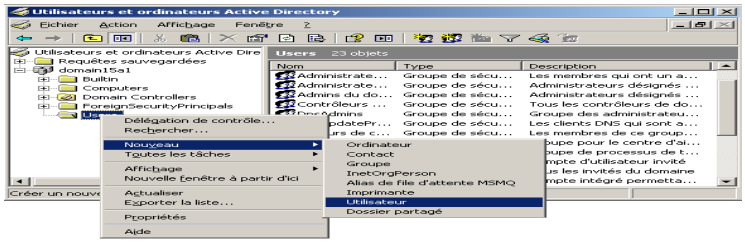


➢ Cliquer sur suivant puis sur terminer.

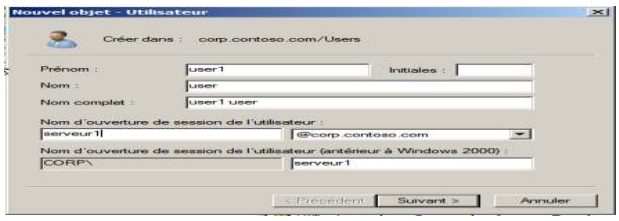
Exercice de synthèse du chapitre 2 :

1. Pour Créer un compte utilisateur de domaine serveur1 nous suivons les étapes suivantes :

➢ Démarrer –Outil d'administration- utilisateur et ordinateur Active Directory- cliquer avec le bouton droit sur Users -nouveau utilisateur puis saisir les données de chaque utilisateur.



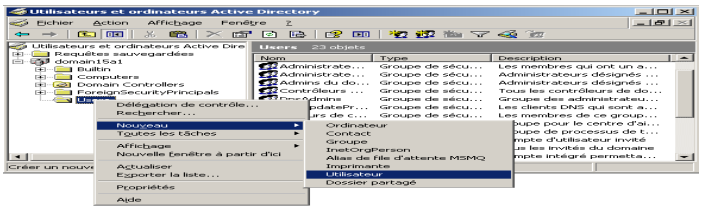
➢ Saisir les informations du nouvel utilisateur.



➢ Pour Créer un compte utilisateur de domaine serveur2nous suivons les étapes suivantes :

- Menu Démarrer –Outil d'administration- utilisateur et ordinateur Active Directory-nom du domaine -Users-bouton droit nouvel utilisateur.

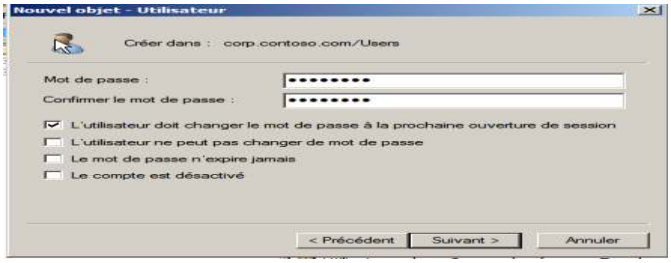
WWW.DZPEN.COM | قلم الجزائر



- Saisir les informations du nouvel utilisateur.



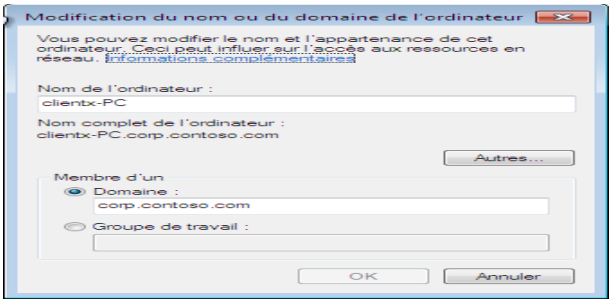
- Taper le mot de passe.



- Cliquer sur suivant.

2. Adhérer le poste clientx au domaine serveurx.

Aller au menu démarrer –ordinateur –propriétés –modifier les paramètres –modifier –membre d'un –nom du domaine.



Cliquer sur OK.

Pour tester l'adhésion du poste clients au domaine serveurx aller au :

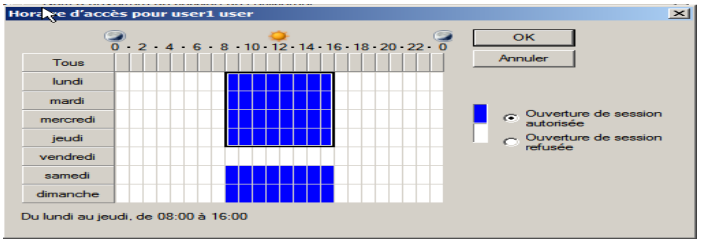
Menu démarrer – outils d'administration – utilisateurs et ordinateurs active directory – computers.



WWW.DZPEN.COM | قلم الجزائر

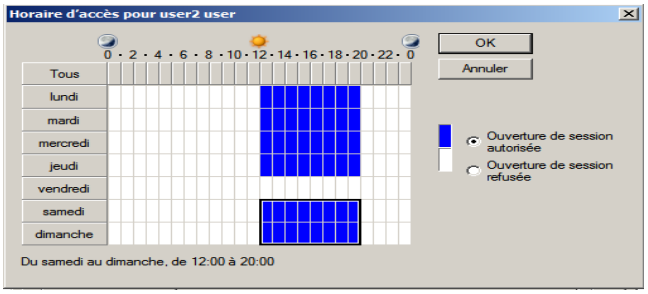
3. Définition des propriétés du compte serveur1avec les horaires d'accès du samedi à Jeudi de 8:00 à 16:00

- Dans la console **utilisateurs et ordinateurs active directory**, faire un double clic dans le volet détails sur serveuruser1
- Dans la boite de dialogue Propriétés de serveuruser1, dans l'onglet **Compte**, cliquer sur **horaires d'accès.**



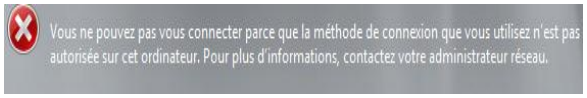
- Dans le coin supérieur gauche de la boite de dialogue horaire d'accès pour serveuruser1, cliquer sur **Tous**, puis sur **connexion refusée.**
- Faire glisser le curseur sur les heures d'ouverture de session pour que la description sous le calendrier indique Samedi à Jeudi de 8:00 à 16:00, cliquer sur connexion autorisée puis sur ok.

4. Pour **serveuruser2** définir les horaires d'accès entre **12:00 et 20:00**, le reste des propriétés est le même que serveuruser1.



5. Test :

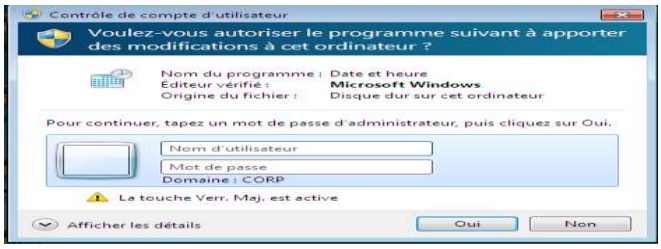
6. Nous avons constaté que ne nous pouvons pas ouvrir une session avec serveur1 à partir de serveur.



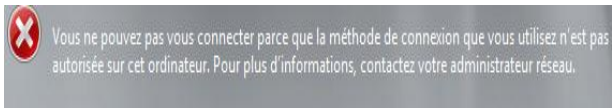
7. Nous pouvons ouvrir une session serveur1 à partir du poste client.

8. Nous ne pouvons pas changer l'heure système à partir du poste client.

WWW.DZPEN.COM | قلم الجزائر



9. Nous avons **constaté** que ne nous pouvons pas ouvrir une session avec serveur2 à partir de serveur parce qu'il n'est pas autorisé.



- Nous pouvons ouvrir une session serveur2 à partir du poste client.

Exercice théorique du chapitre 3 :

1. Le profil d'utilisateur itinérant est crée par l'administrateur système et stocké sur un serveur. Ce profil est disponible à chaque fois qu'un utilisateur ouvre une session sur un ordinateur sur le réseau.

2. la différence entre le profil itinérant et le profil obligatoire, est que le profil obligatoires est un profil itinérant créé par l'administrateur réseau et réside sur le serveur, et ne peut pas être modifié lors des modifications.

3. Le rôle d'un dossier de base est de rassembler dans un même emplacement tous les dossiers de bases des utilisateurs.

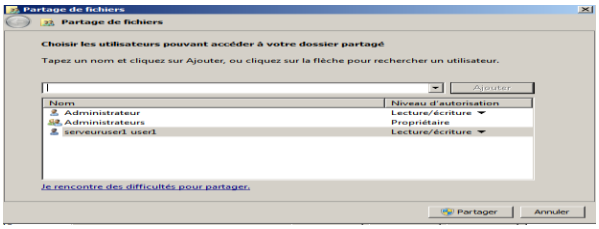
4. Un script d'ouverture de session est un fichier de commandes exécuté à l'ouverture de session.

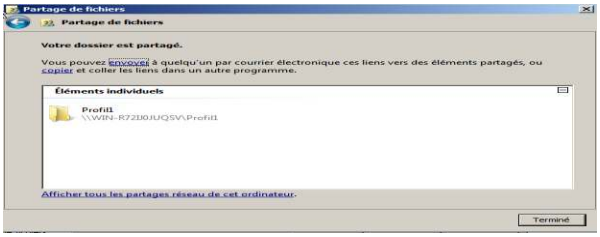
Exercice pratique du chapitre 3 :

1. Pour Créer un dossier sur le serveur appelé Profils et le partagé avec un nom Profil nous suivons les étapes suivantes :

- Dans le lecteur C:/ bouton droit nouveau – dossier (profil).
- cliquer avec le bouton droit de la souris sur le dossier (profil) – propriétés – partage.

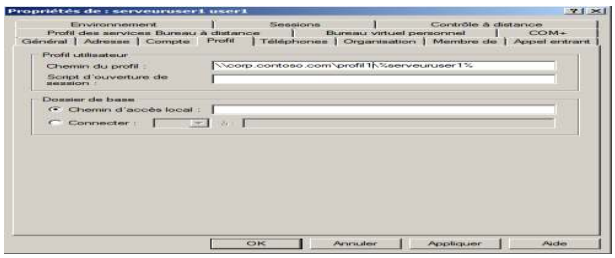
WWW.DZPEN.COM | قلم الجزائر





➢ Cliquer sur terminer.

2.Création d'un profil itinérant pour l'utilisateur serveur1Dans les propriétés du compte serveur1 /Onglet Profil/Dans chemin du profil taper : \\NomServeur\Profil\%username%.



3.Pour créer un profil itinérant obligatoire pour serveur2, nous devons créer un dossier profil2 et le partagé, Dans le lecteur C:/ faire un clic avec le bouton droit de la souris sur nouveau – dossier (profil).

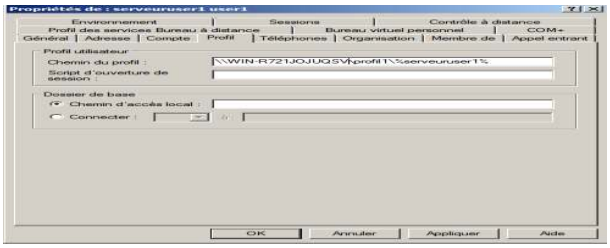
➢ cliquer avec le bouton droit sur le dossier (profil) – propriétés – partage.



➢ Cliquer sur terminer

➢ Pour créer un profil itinérant obligatoire pour l'utilisateur serveur2 Dans les propriétés du compte serveur2 /Onglet Profil/Dans chemin du profil taper : \\NomServeur\Profil2\%serveuruser2%. et Renommer le fichier Ntuser.dat avec le fichier Ntuser.man.

WWW.DZPEN.COM | قلم الجزائر



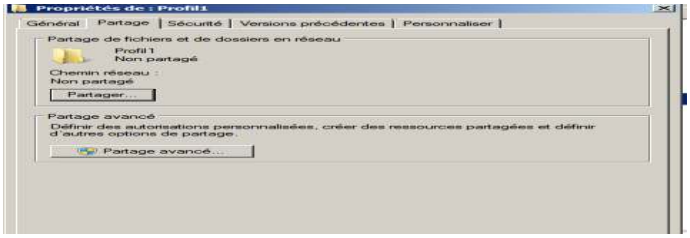
4. Une session avec le compte serveur2 a été ouvert le bureau a été personnalisé avec la création des raccourcis (un raccourci vers le C par exemple) et un fichier texte.

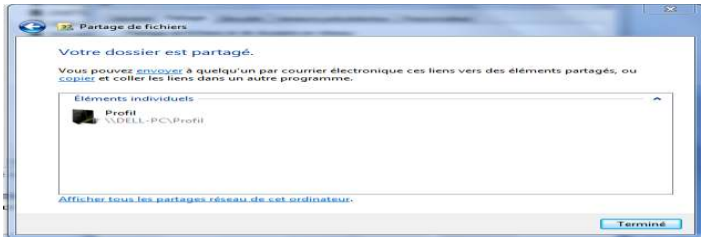
Exercice de synthèse du chapitre 3:

1. Pour Créer un dossier sur le serveur dans le lecteur **C:** appelé Profils et le partager avec un nom Profil nous suivant les étapes suivantes :

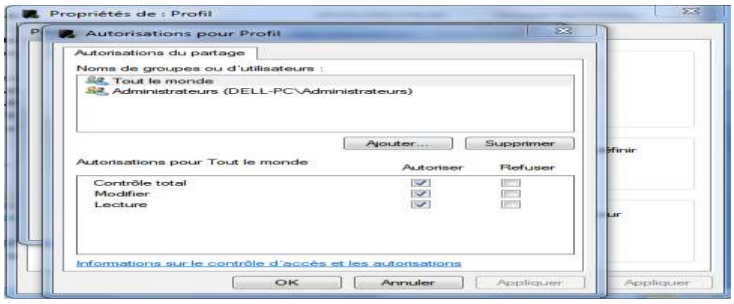
Dans le lecteur C:/ bouton droit nouveau – dossier (profil).

2. Pour partager ce dossier avec le nom de partage par défaut «Profils» cliquer avec le bouton droit sur le dossier (profil) – propriétés – partage – partager –sélectionner tout le monde.





3. Cochez la case Contrôle total autoriser.



4. Pour créer un compte utilisateur qui servira à créer des modèles de profils nous utilisons les informations suivantes :

Prénom Profil.

Nom Compte.

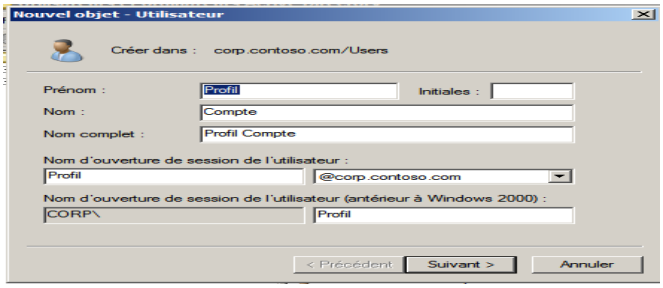
Nom d'ouverture de session de l'utilisateur Profil

WWW.DZPEN.COM | قلم الجزائر

Nom d'ouverture de session de l'utilisateur (antérieur à 2000) Profil.

Mot de passe password001.

Aller au menu démarrer – outils d'administration – utilisateur et ordinateur active directory - utilisateur - clic avec le bouton droit nouveau utilisateur.

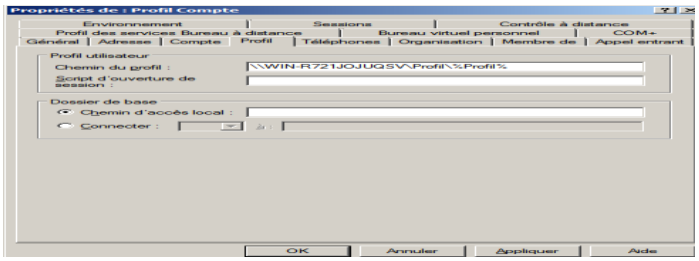


5. Déconnectez-vous de votre serveur.

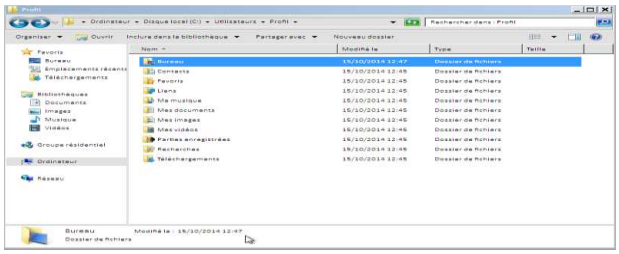
6. Ouverture d'une session avec le compte Profil : sur le poste client –démarrer –changer d'utilisateur – saisir le nom et le mot de passe du compte.

7. Nous avons personnalisé notre bureau grâce à l'application affichage du panneau de configuration. Ajout sur le bureau les icônes : Mes Documents, Poste de travail, Favoris Réseaux, document texte.

8. Création d'un profil itinérant pour l'utilisateur Profil Dans les propriétés du compte Profil /Onglet Profil/Dans chemin du profil taper : \\WIN-R721JOJUQSV\Profil\%Profil%.



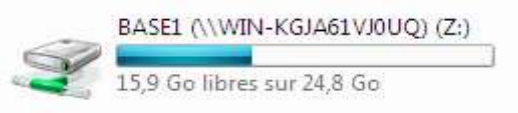
9. Pour testez le bon fonctionnement du profil se connecter avec le compte sur le poste client Windows 7.



10. Pour créer un dossier de base nommée BASE, suivre les étapes suivantes :

- Création d'un nouveau dossier sur une partition sous le nom BASE.
- Partage du dossier BASE avec clic droit de la souris propriété- partage- partagé.
- Aller au compte d'utilisateur avec le bouton droit de la souris propriétés puis profil et sélectionner l'option connecter Z : à chemin d'accès (\\WIN6KGJA61VJOUQ\BASE1).

WWW.DZPEN.COM | قلم الجزائر



Exercice théorique du chapitre 4 :

1. Un groupe de distribution est utilisé par exemple pour envoyer des messages électroniques à l'ensemble des utilisateurs de ces groupes. Ces groupes ne sont pas utilisables pour la sécurité.

2. Un groupe de sécurité est un groupe utilisé pour gérer la sécurité des ressources du ou des domaines.

3. Groupe de distribution et groupe de sécurité possèdent une étendue qui spécifie les personnes qui peuvent en faire partie (compte utilisateur, ordinateur ou groupe) ainsi que l'endroit à partir duquel ils sont utilisables. Ces types d'étendues sont au nombre de trois :

- Domaine local : pour appliquer des permissions
- Globale : pour organiser les comptes d'utilisateurs
- Universelle : pour regrouper des utilisateurs de n'importe quel domaine et leur assigner des permissions dans n'importe quel domaine.

Le contenu de ces groupes varie selon le mode de configuration du domaine : mode mixte ou mode natif. Le mode mixte (par défaut à l'installation d'Active Directory) est un mode permettant la cohabitation de contrôleur de domaine fonctionnant avec Windows NT, Windows 2000 et Windows 2003 dans une même forêt. Le mode natif est la cohabitation de contrôleur de domaine Windows 2000 et Windows 2003 dans une même forêt.

❖ En mode mixte :

➢ un groupe domaine local peut contenir des comptes utilisateurs et des groupes globaux de n'importe quel domaine.

➢ Un groupe global contient des utilisateurs de même domaine que le sien.

➢ Les groupes universels, n'existent pas en mode mixte.

➢ En mode natif Windows 2000 ou 2003 :

➢ Un groupe domaine local peut contenir des comptes d'utilisateurs, des groupes globaux, des groupes universels d'un domaine quelconque de la forêt ainsi que des groupes locaux de domaine de son propre domaine.

➢ Un groupe global : peut contenir des comptes d'utilisateurs et des groupes globaux du même domaine.

➢ Un groupe universel peut contenir des comptes d'utilisateurs, des groupes globaux et des groupes universels d'un domaine quelconque de la forêt.

WWW.DZPEN.COM | قلم الجزائر

Les groupes locaux de domaine peuvent obtenir des permissions du domaine dans lequel ils existent.

Les groupes globaux et universels bénéficient d'autorisations dans tous les domaines de la forêt.

Exercice pratique du chapitre 4 :

1. Pour créer le groupes GRETA, ouvrez ADUC, cliquez droit sur le conteneur **Users,** choisissez **New** et cliquez sur **Group**.

2. Soit sur les propriétés du compte Serviceon utilise l'onglet « Membre de » et on ajoute le groupe, soit sur les propriétés du groupe on utilise l'onglet « Membres » pour ajouter l'utilisateur.

3. Propriétés de CHAMPLAIN, onglet « membres », ajouter le groupe GRETA.

4.Dans utilisateurs et Ordinateurs Active Directory/clic droit sur le Groupe GRETA/Propriétés/onglet Membres/bouton ajouter/ choisir un ordinateur (client).

Exercice de synthèse du chapitre 4 :

5. Pour créer les deux groupes d'utilisateurs globaux Gchefservice, Gpersonnel sur le serveur aller dans le menu Outils d'administration, cliquer sur Utilisateurs et ordinateurs Active Directory cliquer avec le bouton droit sur Users – Nouveau groupe puis saisir les données de chaque groupe.

6. l'étendue des deux groupes est globale, le type des deux groupes est sécurité

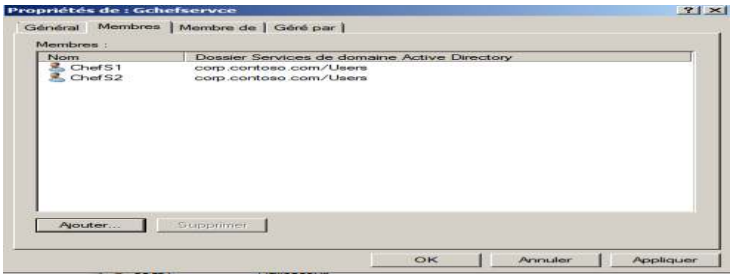
7. Pour la Création des utilisateurs suivants : ChefS1, ChefS2, Employer1, Employer2 nous suivant les étapes suivantes :

- Démarrer –Outils d'administration- utilisateur et ordinateur Active Directory- cliquer avec le bouton droit sur Users -nouveau utilisateur
- saisir les données de chaque utilisateur.
- Saisir le mot de passe de chaque utilisateur

8. Pour Ajouter les utilisateurs ChefS1, ChefS2 au groupe global Gchefservice suivre le chemin suivant :

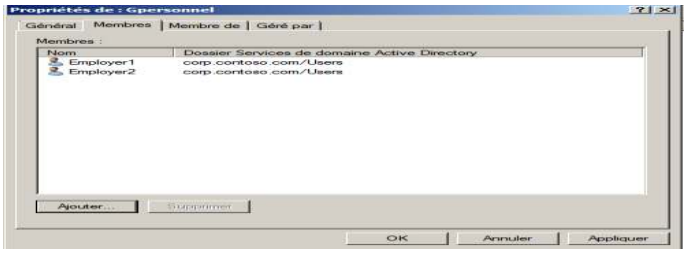
- Double cliquer sur le groupe Gchefservice, dans sa boite de dialogue et dans l'onglet membre cliquer sur ajouter. Dans la boite de dialogue cliquer sur avancé puis rechercher, sous nom cliqué sur ChefS1, puis sur ajouter et ChefS2 puis sur ajouter.
- Valider et cliquer sur appliquer puis OK.

WWW.DZPEN.COM | قلم الجزائر



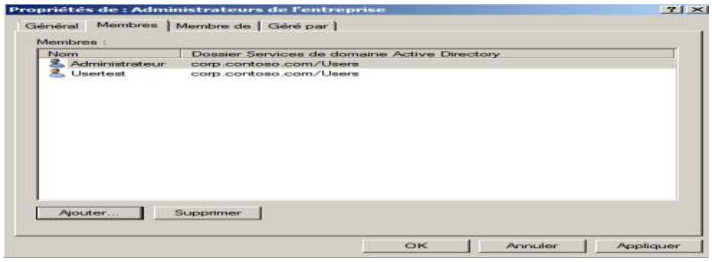
5. Pour ajouter les utilisateurs Employer1 et Employer2 dans le groupe Gpersonnel suivre le chemin suivant:

Double cliquer sur le groupe Gpersonnel, dans sa boite de dialogue et dans l'onglet membre cliquer sur ajouter. Dans la boite de dialogue cliquer sur avancé puis rechercher, sous nom cliqué sur Employer1 puis sur ajouter et Employer2, puis sur ajouter. Valider et cliquer sur appliquer puis OK.



6. Pour Créer un nouvel utilisateur Usert est suivre le cheminDémarrer –Outils d'administration- utilisateur et ordinateur Active Directory- cliquer avec le bouton droit sur Users -nouveau utilisateur puis saisir les données de l'utilisateur usertest.

7. Pour ajouter l'utilisateur usertest dans le groupe prédéfini Administrateurs nous cliquons sur le groupe administrateur à partir de la console Active directory, puis double clique sur le groupe, cliquer sur membre puis ajouté - avancé – rechercher puis sélectionner le nom usertest.



7. Nous pouvons ouvrir une session avec Usertest sur le contrôleur de domaine.

8. Nous pouvons ouvrir une session avec Usertest sur le contrôleur de domaine.

Exercice théorique du chapitre 5 :

1. L'accès aux ressources se configure en trois étapes : le partage, la publication, les permissions.

2. Pour créer un partage invisible nous ajoutons le signe $ à la fin du nom de partage

WWW.DZPEN.COM | قلم الجزائر

3. Le rôle des ACL vérifient les permissions des ressources.

4. le rôle du contrôle d'accès est le processus autorisant des utilisateurs, des groupes et des ordinateurs à accéder à des objets sur le réseau au moyen d'autorisations, de droits d'utilisateur et d'audit d'objets.

5. les composants du contrôle d'accès sont :les entités de sécurité, le SID, DACL

6. L'utilité des fichiers mis hors connexion est de permettre de continuer à travailler avec des fichiers ou des programmes réseau, même lorsque vous êtes déconnectés.

Exercice pratique du chapitre 5 :

1. Pour Créer un Compte d'utilisateur local test2 et test3 il faut suivre les étapes suivantes :

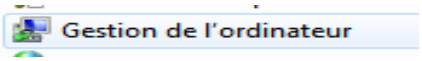
- Menu démarrer – tous les programmes – panneau de configuration



- Outils d'administration

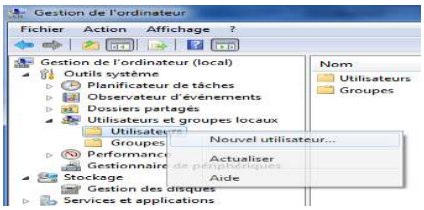


- Gestion de l'ordinateur

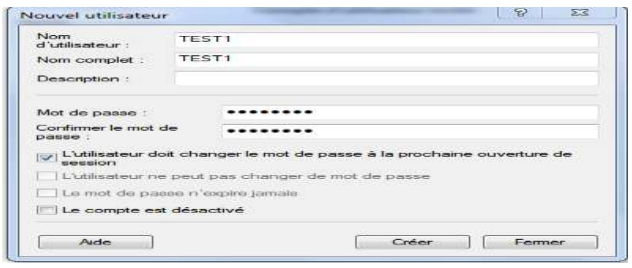


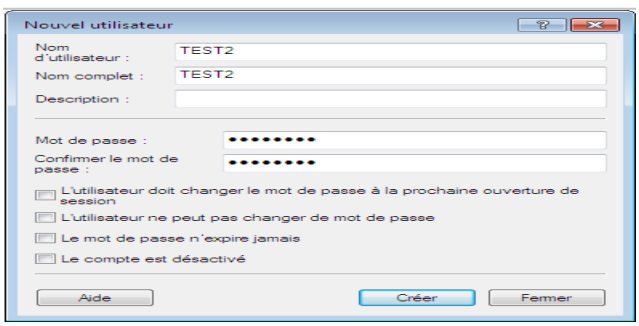
- Utilisateur et groupes locaux bouton droit nouvel utilisateur.





- Saisir les données concernant les comptes utilisateurs TEST1 et TEST2.

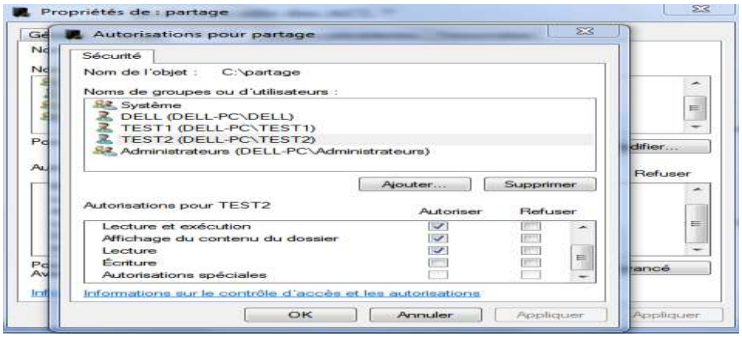




WWW.DZPEN.COM | قلم الجزائر

2. Pour créer un dossier partage dans le lecteur C:\ nous suivons les étapes suivantes :

- Aller au lecteur C:\ clic droit de la souris nouveau dossier puis faire un clic avec le bouton droit de la souris sur propriétés - partage – partager.
- Sélectionner les utilisateurs concernés.



- Attribution des permissions :

TEST1accès en lecture/écriture.

Administrateur accès en contrôle total.

TEST2accès en lecture.

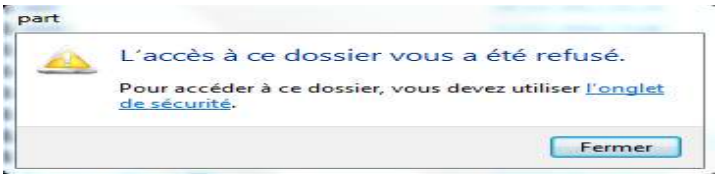
3. Ouverture d'une session en tant que TEST2 un message d'erreur s'affiche :

Vous ne disposez pas des autorisations requises pour accéder à ce dossier.



Puis cliquer sur continuer un message s'affiche cliquer sur fermer.

4. L'accès au dossier partagé est refusé.

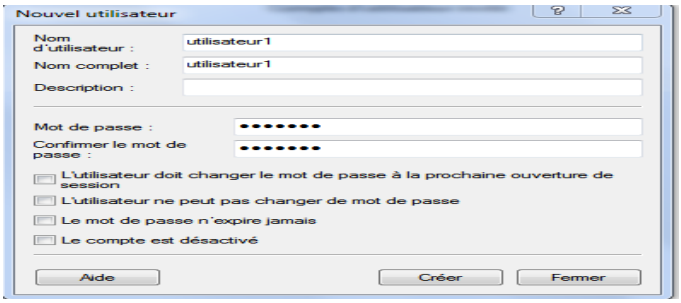


Exercice de synthèse du chapitre 5 :

1. Quatre utilisateurs ont été crées sur chaque poste de travail de la manière suivant :

Menu démarrer – tous les programmes – panneau de configuration-outils d'administrateur-gestion de l'ordinateur – utilisateur et groupes locaux –utilisateurs –nouvel utilisateur –saisir les informations concernons chaque utilisateur, l'utilisateur ne doit pas changer son mot de passe à la première ouverture de session.

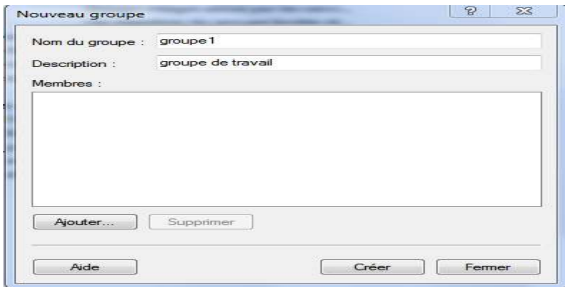
WWW.DZPEN.COM | قلم الجزائر



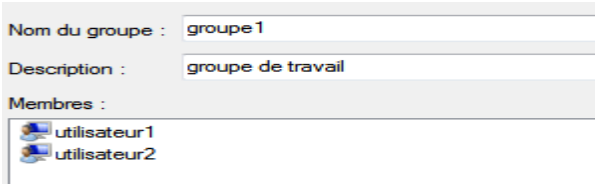
Le même principe pour les trois autres utilisateurs.

2. Deux groupes, nommés Groupe1 et Groupe2 ont été crées de la manière suivante :

Menu démarrer – tous les programmes – panneau de configuration –outil d'administrateur – gestion de l'ordinateur – utilisateur et groupes locaux –groupes – nouveau groupe.



3. Insertion des deux premiers utilisateurs (utilisateur1, utilisateur2) dans le groupe Groupe1.

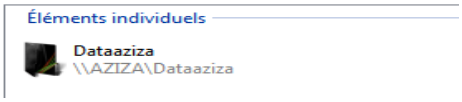


les deux autres (utilisateur3, utilisateur4) dans le groupe Groupe2

4. Création d'un dossier (sur le lecteur D:) ayant le nom Dataaziza.

Création d'un dossier nommé Alireaziza dans le dossier Dataaziza, un fichier texte à été placé dedans. Dans ce dossier Dataaziza , nous avons crée un fichier texte avec notepad appelé MonTexte.txt contenant votre nom.

5. Partage du dossier Dataaziza en conservant le nom du dossier.



6. Dans voisinage réseau l'autre ordinateur du groupe de travail apparait.



7. Création d'un lecteur réseau nommé T, vers le dossier partagé de votre binôme.

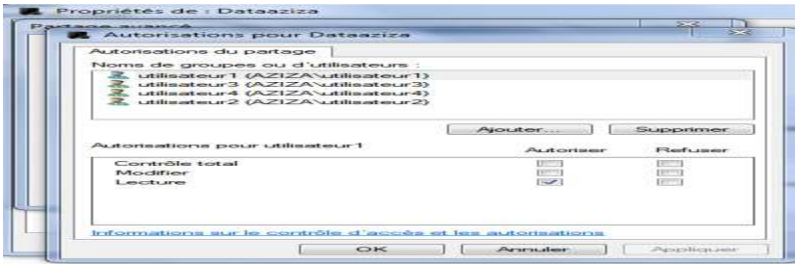
Aller au favoris réseau – connecter un lecteur réseau –lecteur – parcourir – sélectionner le dossier Dataaziza .

WWW.DZPEN.COM | قلم الجزائر



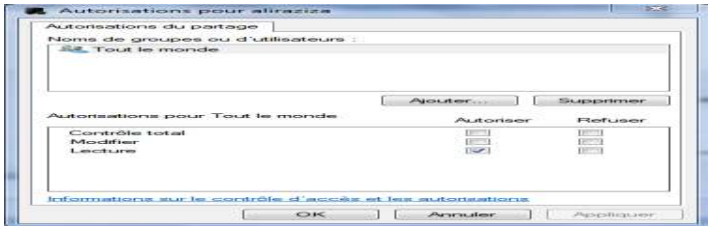
Le test de la connexion sur ce lecteur réseau se fait avec un double clic sur ce lecteur.

8. Affichage des autorisations d'accès sur le partage du dossier Dataaziza avec un clic droit – Partager - partage avancé - bouton Autorisations.

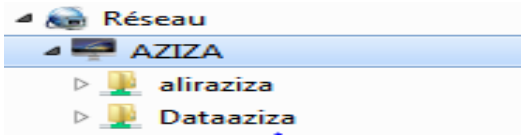


9. les autorisations d'accès sur le partage possibles sont contrôle totale –modifier – lecture.

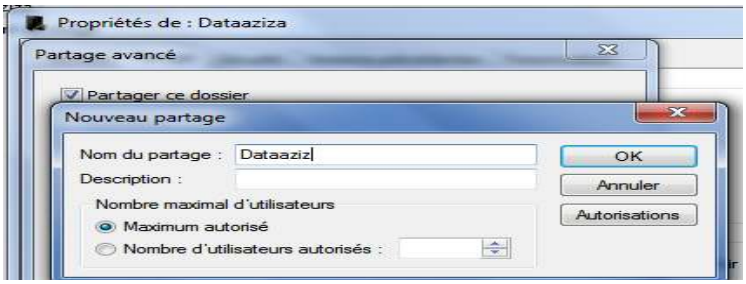
Partage du dossier 'Alire' en n'autorisant que la lecture pour tous.



10. le dossier Alire apparaît par rapport au dossier Dataaziza dans Favoris réseau (sur mon poste et sur le poste de mon binôme) comme suit :



11. Ajout d'un nouveau nom de partage sur le dossier Dataaziza, sans supprimer l'ancien, Clic droit sur le dossier Dataaziza – propriétés – partage - Partage avancé - Bouton Nouveau partage –saisie le nouveau nom du partage Dataaziza1.



12. On peut définir des autorisations différentes sur le nouveau partage.

13. l'accès sur le nouveau partage dans Favoris réseau à été effectué.



WWW.DZPEN.COM | قلم الجزائر

14. A partir d'une session ouverte avec un compte utilisateur sur mon poste je n'ai pu que lire le fichier par contre sur le poste de mon binôme toute les modifications ont pu être effectuées (ajouter et supprimer des fichiers dans le dossier 'Alire').

Explication :

Sur mon poste l'autorisation donnée est uniquement lecture.

Sur l'autre poste les autorisations données sont : modification, lecture, écriture.

Exercice théorique du chapitre 6 :

1. les permissions d'un fichier F créé dans D par un commercial sont :

Commercial Modifier.

Fabrication Lecture.

2. Oui le chefs1 peut supprimer D1, car le droit final est Modifier (Lecture+Modifier=Modifier).

3. Non ChefS1 ne peut pas voir le contenu de D2, car le refus est prioritaire.

4. Oui ChefS1 peut supprimer le fichier F, car Modifier est prioritaire par rapport à Lecture.

5. Les droits du fichier F devient Modifier.

Exercice pratique du chapitre 6 :

1. L'attribution des autorisations suivantes sur le dossier travaux aux utilisateurs sur le contrôleur de domaine.

Utilisateurs	Partage	NTFS
Serveur1	contrôle total	lecture
Serveur1	lecture	contrôle total
Serveur1	contrôle total	contrôle total

- L'attribution d'autorisation de partage contrôle total pour l'utilisateur Serveur1 : cliquer avec le bouton droit de la souris sur le dossier travaux –propriétés – partage – partage avancé – autorisations sélectionner Serveur1 puis activer la case à cocher contrôle total autoriser puis cliquer sur l'onglet sécurité puis modifier - autorisation de lecture.
- L'attribution d'autorisation de partage lecture pour l'utilisateur Serveur1 : cliquer avec le bouton droit de la souris sur le dossier travaux –propriétés – partage – partage avancé – autorisations sélectionner Serveur1 puis activer la case à cocher lecture autoriser puis cliquer sur l'onglet sécurité puis modifier - autorisation contrôle total.

WWW.DZPEN.COM | قلم الجزائر

- L'attribution d'autorisation de partage contrôle total pour l'utilisateur Serveur1 : cliquer avec le bouton droit de la souris sur le dossier travaux –propriétés – partage – partage avancé – autorisations sélectionner Serveur1 puis activer la case à cocher contrôle total autoriser puis cliquer sur l'onglet sécurité puis modifier – autorisation contrôle total.

Exercice de synthèse du chapitre 6 :

Les utilisateurs chefs1, chefs2, employer1, employer2 ainsi que les groupes Gchefservice et Gpersonnel ont été déjà crées dans le chapitre 4 comme suit :

Pour les utilisateurs :

Démarrer –Outils d'administration- utilisateur et ordinateur Active Directory- cliquer avec le bouton droit sur Users -nouveau utilisateur puis saisir les données de chaque utilisateur. Pour les groupes : Démarrer –Outils d'administration- utilisateur et ordinateur Active Directory- cliquer avec le bouton droit sur Users -nouveau groupe puis saisir les données de chaque groupe.

1. Ouverture d'une session avec le compte administrateur sur le contrôleur de domaine.

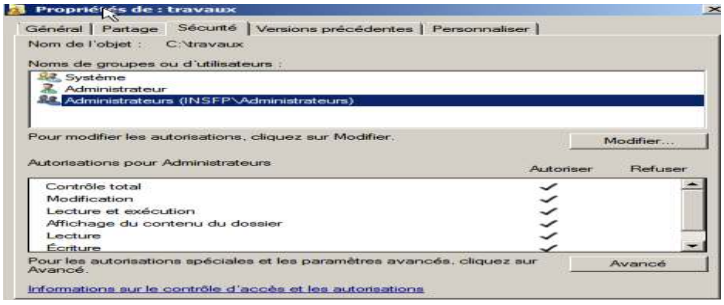
2. Création d'un dossier appelé travaux dans la partition C:\,et création d'un fichier texte dans le dossier travaux.

3. Pour partager le dossier travaux cliquer avec le bouton droit de la souris –propriétés – partage – partager – sélectionner tout le monde – partager.



4. Affectation de l'autorisation de partage control total au groupe administrateur et le groupe tout le monde : cliquer avec le bouton droit de la souris sur le dossier travaux –propriétés – partage – partage avancé – autorisations sélectionner le groupe tout le monde et le groupe administrateur on sélectionne l'autorisation control total.

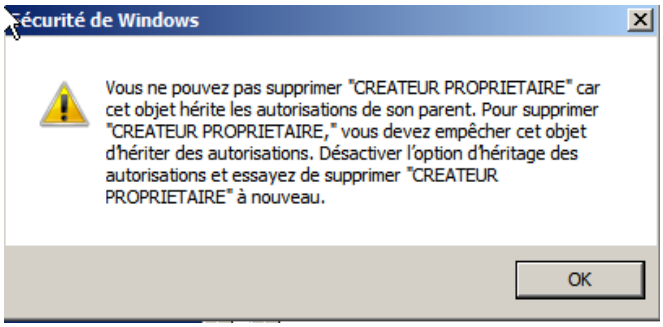
5. Affichage des autorisations NTFS par défaut sur le dossier travaux cliqué avec le bouton droit de la souris –propriétés – sécurité.



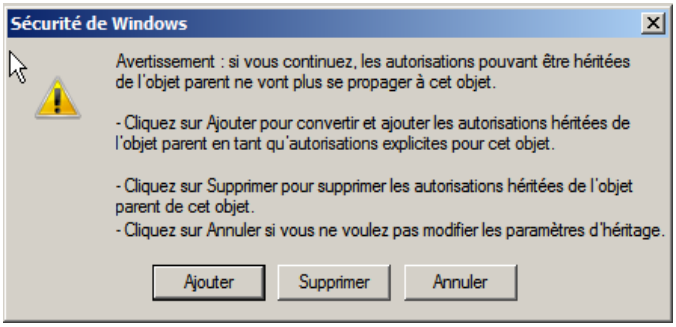
WWW.DZPEN.COM | قلم الجزائر

6. les autorisations actuellement accordées sur le dossier sont : Le groupe Tout le monde dispose de l'autorisation Contrôle total, elles sont grisées car elles sont héritées du dossier parent.

7. Pour supprimer le groupe tout le monde sélectionné Sous nom Tout le monde, cliquer sur Supprimer, un message vous indique que vous ne pouvez pas supprimer le groupe Tout le monde, car l'objet hérite d'autorisations de son parent et, Cliquez sur OK pour fermer le message.



8. Pour bloquer l'héritage des autorisations et supprimer toutes les autorisations accordées sur le dossier travaux propriétés – sécurité – avancé - modifier les autorisations - désactivez la case à cocher inclure les autorisations pouvant être héritées du parent de cet objet .Un message vous invite à copier les autorisations actuellement héritées dans le dossier ou à supprimer toutes les autorisations accordées sur le dossier cliquez sur Supprimer.

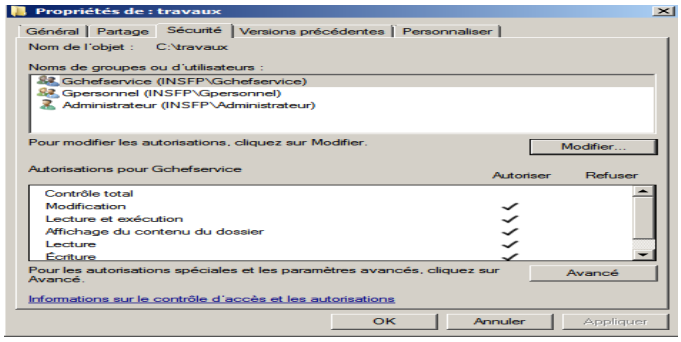


9. Accord des autorisations sur le dossier travaux comme suit:

Dans la boîte de dialogue Propriétés de dossier travaux, cliquez sur Ajouter- Dans la boîte de dialogue Sélectionnez Utilisateurs, Ordinateurs ou Groupes, dans la zone – avancé – Rechercher, sélectionner avec un double clic sur le nom du l'un des utilisateurs ou des groupes.

- L'autorisation control total au compte administrateur.
- L'autorisation modifier au groupe Gchefservive.
- L'autorisation lecture au groupe Gpersonnel.

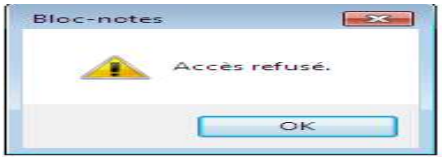
WWW.DZPEN.COM | قلم الجزائر



10. Le Test :

1. En se connectant en tant qu'utilisateur chefs1, nous avons pu faire des modifications sur le fichier texte dans le dossier travaux. parce que nous avons attribué une autorisation de modification.

2. En se connectant en tant qu'utilisateur employer1, nous n'avons pas pu faire des modifications sur le fichier texte dans le dossier travaux, parce que nous avons attribué une autorisation de lecture.



Exercice théorique du chapitre 7 :

1. NTFS est un système de fichier, il permet de stocker efficacement les données sur une partition.

2. la différence entre FAT et NTFS est que NTFS permet des fonctions supplémentaires par rapport aux systèmes FAT en ce qui concerne les fonctions :de récupération des données , de compression dossiers par dossiers en temps réel , de limitation de capacité par utilisateur (quotas de disque)d'individualisation des répertoires du disque (sécurité individuelle) de sécurité.

3. la différence entre le système de fichiers CDFS et UDF est que CDFS permet la lecture des CD-ROM conformes aux normes ISO 9660 et ISO 9660 niveau 2 avec noms de fichiers longs , par contre le systèmes de fichier UDF permet la lecture de certains CD-ROM, mais surtout des DVD. Il permet aussi l'écriture sur des supports réinscriptibles CD-RW ou à écriture unique CD-R ou WORM.

4. la différence entre les autorisations de partage et les autorisations de sécurité est que les autorisations de partages sont control total, modifier, lecture par contre les autorisations de sécurité sont les autorisations NTFS.

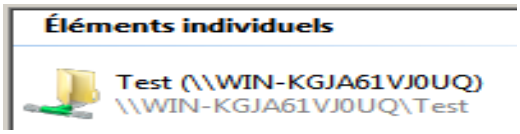
WWW.DZPEN.COM | قلم الجزائر

Exercice pratique du chapitre 7 :

1. Création d'un dossier sous le nom test et création d'un fichier texte dan le dossier Test : C:\Test\fichier texte.

2. Partage du dossier Test et la détermination des autorisations de partage par défaut :

Pour partager le dossier Test cliquer avec le bouton droit de la souris –propriétés – partage – partager – sélectionner tout le monde – partager.



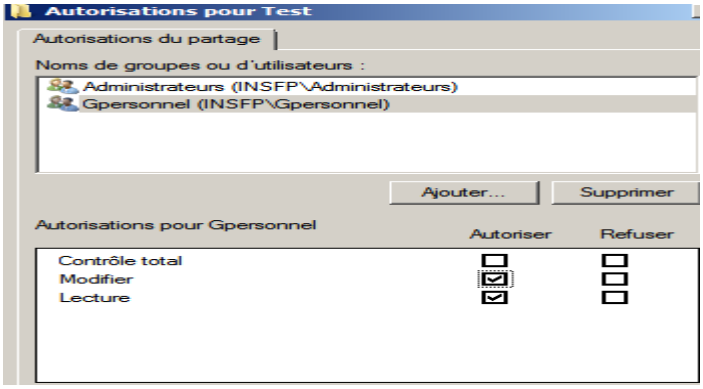
Les autorisations de partage par défaut sont le groupe tout le monde qui à les autorisations : contrôle total, modifier , lecture.

3. Pour Supprimer les autorisations par défaut et pour ajouter le groupe administrateurs :

Propriétés du dossier Test – partage –partage avancé – autorisation – cliquer sur le groupe tout le monde – supprimer puis cliquer sur ajouter pour ajouter le groupe administrateur.

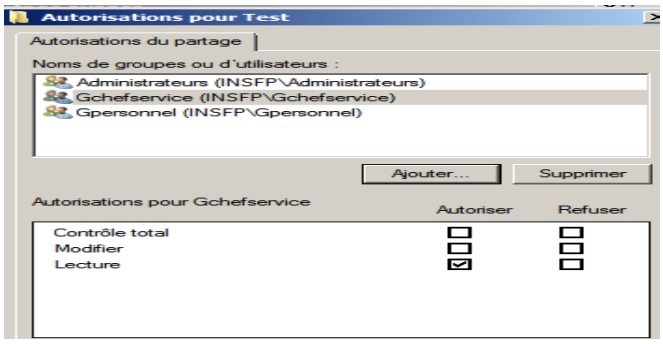
4. Pour attribuer l'autorisation control total au groupe administrateurs activer la case à cocher contrôle total Autoriser.

5. Pour ajouter le groupe Gpersonnel et lui attribué l'autorisation modifier : cliquer sur ajouter pour ajouter le groupe Gpersonnel , et activer la case à cocher modifier Autoriser.



6. Pour ajouter le groupe Gchefservice et lui accordé l'autorisation lecture : cliquer sur ajouter pour ajouter le groupe Gchefservice, et activer la case à cocher lecture Autoriser.

WWW.DZPEN.COM | قلم الجزائر



Exercice de synthèse du chapitre 7 :

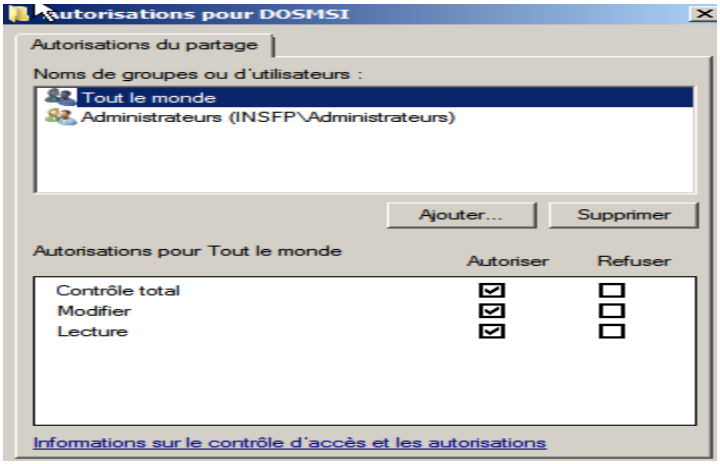
1. Ouverture d'une session en tant que administrateur.

2. Création d'un dossier sous le nom DOSMSI et création d'un fichier texte dans le dossier DOSMSI:C:\DOSMSI \fichier texte.

3. Pour partager le dossier DOSMSI cliquer avec le bouton droit de la souris –propriétés – partage – partager – sélectionner tout le monde – partager.



4. les autorisations par défaut sur le dossier partagé DOSMSI sont :contrôle total, modifier, lecture.



5. Pour Supprimer les autorisations par défaut et pour ajouter le groupe administrateurs : Propriétés du dossier DOSMSI– partage –partage avancé – autorisation – cliquer sur le groupe tout le monde – supprimer puis cliquer sur ajouter pour ajouter le groupe administrateur.

6. Pour attribuer l'autorisation contrôle total au groupe administrateurs activer la case à cocher contrôle total Autoriser.

WWW.DZPEN.COM | قلم الجزائر

7. Pour créer un lecteur réseau vers le dossier partagé DOSMSI :

Cliquer sur ordinateur avec le bouton droit – connecter un lecteur réseau – choisissez un lecteur – parcourir – sélectionner un dossier réseau partager.



8. Pour connectez un lecteur réseau au dossier partagé :

Aller vers l'explorateur puis double clic sur le nom du lecteur.

9. Pour déconnectez le lecteur réseau cliquer avec le bouton droit sur le lecteur réseau du dossier partagé puis sur Déconnecter.

Pour se connecté au dossier partagé DOSMSI à l'aide du poste de travail : ordinateur – C:\ DOSMSI.

10. L'utilisateur non autorisé ne peut pas accéder au dossier partagé.

11. L'administrateur peut accéder au dossier partagé.

12. Pour Supprimer le partage du dossier DOSMSI : à partir d'outils **système -** Gestion de l'ordinateur -Dossiers partagés, Partage – cliquer avec le bouton droit sur le dossier - sélectionner arrêter le partage.

Remarque :

Le corrigé type de l'exercice de synthèse général à été fait sous forme d'une vidéo.

WWW.DZPEN.COM | قلم الجزائر

Annexe B : Table des Figures

N° de la figure	Titre de la figure	N° de page
01	Les caractères du mot de passe	**16**
02	Création d'un compte d'utilisateur sur un ordinateur local	**17**
03	Création d'un nouvel utilisateur	**17**
04	Les informations du compte utilisateur	**18**
05	L'emplacement du compte local	**18**
06	Modification du compte utilisateur local.	**19**
07	Propriétés du compte utilisateur	**19**
08	Installation d'active directory	**23**
09	La nomination du domaine	**23**
10	Spécification de l'emplacement d'Active Directory	**24**
11	L'installation d'Active Directory est en cours	**24**
12	La fin de l'assistant d'installation des services de domaine Active Directory	**25**
13	Le service de domaine d'Active Directory	**25**
14	Création d'un compte utilisateur de domaine	**26**
15	La boite de dialogue Nouvel objet – utilisateur	**27**
16	Définition des options du mot de passe	**27**
17	Propriétés de connexion au réseau local	**28**
18	Protocole Internet (TCP/IP)	**29**
19	L'adresse IP et le masque de sous-réseau	**29**
20	Modifier les paramètres système	**30**
21	Propriétés système	**31**
22	Modification du nom de l'ordinateur et nom du domaine	**31**
23	Teste de la connexion de poste client au domaine	**32**
24	Propriétés d'un compte utilisateur de domaine	**32**
25	Modification des propriétés d'un compte utilisateur de domaine	**33**
26	Rechercher des personnes ou ordinateurs ou objets dans Active Directory	**34**
27	sélection d'une personne ou ordinateur ou objet dans Active Directory	**35**
28	Heure de disponibilité ou restrictions d'horaires	**35**
29	Ordinateurs autorisés	**36**
30	Expiration de compte	**36**
31	Copie d'un compte utilisateur	**37**
32	Profil d'utilisateur local	**39**
33	Les dossiers et les fichiers d'un profil	**40**

WWW.DZPEN.COM | قلم الجزائر

34	Création d'un profil à la première ouverture de session	**40**
35	Configuration d'un profil d'utilisateur itinérant	**41**
36	Création d'un profil itinérant personnalisé	**42**
37	Création de Dossier de base	**43**
38	script d'ouverture de session	**45**
39	Qu'est-ce qu'un groupe	**48**
40	Groupes prédéfinis sur un ordinateur local	**49**
41	Création d'un groupe local	**51**
42	La Description de la boîte de dialogue Nouveau groupe	**52**
43	Stratégie d'utilisation de groupes locaux dans un groupe de travail	**53**
44	Groupe d'utilisateur dans un domaine	**54**
45	Affectation des ressources ou groupe	**54**
46	Les groupes simplifient l'affectation d'autorisations à des ressources	**54**
47	Les utilisateurs peuvent être membres de plusieurs groupes	**55**
48	Les groupes peuvent être imbriqués dans d'autres groupes	**55**
49	L'attribution des autorisations d'une même ressource à plusieurs	**55**
50	Imbrication de groupes	**57**
51	Possibilité d'Imbrication des groupes	**58**
52	La stratégie A G DLP	**60**
53	Le conteneur Builtin	**63**
54	Les groupes prédéfinis	**64**
55	Le conteneur Users	**65**
56	Schéma d'imbrication des groupes et comptes utilisateurs dans un domaine	**66**
57	Création de groupes dans un domaine	**70**
58	Le partage	**73**
59	Création de dossiers partagés	**76**
60	Mise en place des fichiers hors connexion	**77**
61	Les permissions et les autorisations NTFS pour les utilisateurs	**80**
62	Autorisation NTFS sur un Dossier	**81**
63	onglet "Sécurité d'un dossier	**82**
64	Autorisations NTFS sur les fichiers	**82**
65	onglet "Sécurité d'un fichier	**83**
66	Les Autorisations NTFS spéciale	**83**
67	Présentation de l'héritage NTFS	**84**
68	partager un dossier	**88**
69	Partage à partir de l'Explorateur	**89**
70	droit de créer plusieurs noms de partage différents	**90**
71	Partage A partir de la console Gestion de l'ordinateur	**90**
72	Assistant création d'un dossier partagé	**91**
73	Nom et description du partage	**91**
74	déterminer les autorisations de partage	**92**

WWW.DZPEN.COM | قلم الجزائر

75	La fin de partage	**92**
76	Supprimer un partage	**93**
77	Se connecté à une ressource partagée	**93**
78	Connectez à un lecteur réseau	**94**
79	Contrôler les partages par le dossier fichier ouvert	**95**
80	La rubrique partage de gestion de l'ordinateur	**95**
81	Installation du rôle	**96**
82	Sélection du serveur d'impression	**96**
83	Résumé de l'installation du serveur d'impression	**97**
84	Installation des services de documents et d'impression	**97**
85	Résultat de l'installation des services de documents et d'impression	**98**
86	Installation d'une imprimante réseaux sur le seveur d'impression	**98**
87	Création d'un nouveau port	**99**
88	Confirmation de l'adresse IP	**99**
89	Détection du port TCP/IP	**100**
90	Informations supplémentaires requises concernant le port	**100**
91	Détection du modèle de pilote	**101**
92	Installation du pilote d'imprimante	**101**
93	Choix du modèle d'imprimante	**102**
94	Sélection du nom de l'imprimante	**102**
95	Le serveur installe le pilote	**103**
96	Partage de l'imprimante	**103**
97	Impression d'une page test	**104**
98	Ajout du pilote X86	**104**
99	Recherche du pilote X86 dans pilotes supplémentaires	**105**
100	Localisation du pilote X86	**105**
101	Sélection du fichier du pilote X86	**106**
102	Application du pilote X86	**106**
103	Fin du partage de l'imprimante	**107**
104	Exécution de Check Disk depuis la ligne de commande	**110**
105	Exécution de Check Disk de manière interactive	**110**
106	Autorisations simples de partages	**112**
107	Autorisations simples et autorisations de Sécurité	**112**
108	Les types d'autorisations simples	**113**
109	Affectation des autorisations NTFS a des utilisateurs, groupe ou objet	**113**

WWW.DZPEN.COM | قلم الجزائر

Annexe C : Fiche Modulaire Modifiée

OBJECTIFS INTERMEDIAIRES	CRITERES PARTICULIERS DE PERFORMANCE	ELEMENTS DE CONTENU
• Créer et modifier un Compte utilisateur local	▪ Définition correcte d'un Compte utilisateur ▪ Création correcte d'un compte ▪ Modification correcte d'un compte	▪ Utilisateurs locaux ▪ Utilisateurs prédéfinis (Administrateur, Invité) ▪ Création d'un compte d'utilisateur sur un ordinateur local ▪ Modifier un compte sur un ordinateur local
▪ Gérer et configurer des comptes utilisateurs dans un domaine	▪ Caractéristique exactes des comptes utilisateurs	▪ Gestion et configuration des comptes utilisateurs dans un domaine : -Définition d'Active Directory -Installation d'active directory -Compte d'utilisateur de Domaine -Création d'un compte utilisateur de domaine -Intégration d'un client dans un domaine -Propriétés d'un compte utilisateur -Rechercher des personnes ou ordinateurs ou objets dans Active Directory - Options de compte - Heure de disponibilité ou restrictions d'horaires - Ordinateurs autorisés - Expiration de compte - Copie d'un compte Utilisateur
▪ Définition d'un profil utilisateur	▪ Définition exacte du profil utilisateur ▪ Création correcte de dossier de base ▪ Création correcte de scripts	▪ Profil par défaut et Profil Utilisateur - Profil d'utilisateur par défaut - Profil d'utilisateur local ▪ Profils d'utilisateurs itinérants - Profils obligatoires - Configuration d'un profil d'utilisateur itinérant -Création d'un profil itinérant personnalisé Profil itinérant personnalisé obligatoire ▪ Création de dossier de base ▪ Création d'un script d'ouverture de session dans Windows Server 2003/2008/2012

WWW.DZPEN.COM | قلم الجزائر

OBJECTIFS INTERMEDIAIRES	CRITERES PARTICULIERS DE PERFORMANCE	ELEMENTS DE CONTENU
▪ Gérer les groupes d'utilisateur	▪ Définition correcte d'un groupe ▪ Gestion correcte des groupes ▪ Enumération exacte des Types de groupes ▪ Définition juste des étendues ▪ Définition correcte de Groupe par défaut	▪ Qu'est-ce qu'un groupe ▪ Groupes prédéfinis sur un ordinateur local ▪ Groupes prédéfinis standards ▪ Groupes prédéfinis spéciaux ou Groupes dits systèmes. ▪ Création d'un groupe. ▪ Stratégie d'utilisation de groupes locaux dans un groupe de travail ▪ Groupes d'utilisateur dans un Domaine ▪ Les types de groupes -Groupes de sécurité -Groupes de distributions ▪ Les étendues de groupes - Groupe global -Groupe de domaine local -Groupes Universels -Imbrication de groupes (en mode natif et En mode mixte) ▪ Méthodologies d'utilisation des groupes ▪ Les groupes par défaut sur les serveurs contrôleurs de domaine - Groupes prédéfinis -Groupes intégrés à étendue de domaine local **- Schéma d'imbrication des groupes et compte utilisateurs dans un domaine** ▪ Les groupes par défaut Sur tous les ordinateurs - Groupes spéciaux ▪ Création de groupes

WWW.DZPEN.COM | قلم الجزائر

BJECTIFS INTERMEDIAIRES	CRITERES PARTICULIERS DE PERFORMANCE	ELEMENTS DE CONTENU
▪ Gérer des permissions (autorisations et droits)	▪ Attribution juste des droits et permissions ▪ Gestion correcte des Permissions	▪ Gestion d'accès aux ressources - le partage -la publication -les permissions - Contrôle d'accès - Administration des accès aux dossiers locaux partagés -Description des dossiers partagés -Partage administratif -Création de dossiers partagés -Autorisation sur les dossiers Partagés -Connexion à un dossier partagé - Mise en place des fichiers hors connexion
▪ Attribuer les permissions et les autorisations NTFS pour les utilisateurs	▪ Attribution adéquate des permissions	▪ Les permissions et les autorisations pour les utilisateurs - Autorisation sur un dossier - Autorisation NTFS sur les fichiers -Présentation de l'héritage NTFS ▪ Règles concernant les autorisations NTFS
▪ Partage des ressources et des dossiers.	▪ Opérabilité du partage ▪ Sécurisation juste des fichiers	▪ Partager un dossier - Partage à partir de l'Explorateur - A partir de la console de gestion de l'ordinateur - Supprimer un partage - Se connecter à une ressource partagée - Contrôler les partages ▪ Partager une imprimante ▪ Système de fichiers Windows/Linux) - Structure du système de fichiers NTFS - Système de fichiers CDFS - Système de fichiers UDF ▪ Sécurité des systèmes de fichiers -Autorisations simples de partage - Autorisations simples et autorisations de sécurité

WWW.DZPEN.COM | قلم الجزائر