ExpertWeb

Systèmes d'information - Ingénierie & Formations

WINDOWS 95 – SECURITE – MIGRATION VERS NT - GESTION DE RESEAU
TABLE DES MATIERES

Tél /fax : 0467.42.68.11 -Mobile : 0621.447.851
E-mail : info@expertweb.fr Site web : http://www.expertweb.fr/dotclear/
Avenue de l'AGAU – Le Vivaldi 35 –34970 Lattes

QUE SE PASSE T'IL AU DEMARRAGE DE WINDOWS 95 ?

Au démarrage, le système cherche sur le disque dur le fichier WINBOOT.SYS qui génère les étapes suivantes :

A- Affiche le logo de win95ou98 (vous pouvez le changer si vous êtes allergique.)

B- Charge :

1. IO.SYS ET MSDOS.SYS

2. DBLSPACE.BIN et DRVSPACE.BIN pilote de compression du disque (s'il y a lieu)

3. SYSTEM.DAT et USER.DAT fichiers de la base de registre de Windows

4. CONFIG$ pilote d'un Plug and Play Configuration Manager

5. CONFIG.SYS si présent

6. HIMEM.SYS gestionnaire de la mémoire vive

7. IFSHELP.SYS

8. SETVER.SYS

9. Les pilotes CON (consol-écran vidéo), AUX (auxiliaire-périphérique), PRN (imprimante)

10. COMMAND.COM

11. Traite AUTOEXEC.BAT s'il le trouve

12. Lance WIN.COM pour lancer windows (KERNEL386 (le programme central de windows95 et 3.1), GDI.EXE et GDI32.EXE (interface graphique), USER.EXE et USER32.EXE (interface utilisateur), VMM32, etc.) les anciens (Win 3.1) fichiers SYSTEM.INI et WIN.INI sont chargés s'ils existent.

Pour les application DOS, Win95 (plus précisément VMM32.VXD) crée lors de chaque lancement d'une application DOS un ordinateur virtuel (machine virtuelle) qui pense être la seule machine à travailler en DOS sur cet ordinateur. Le bon vieux DOS existe à temps partiel, au besoin

AJOUTER DES ELEMENTS AU MENU DEMARRER

Utiliser le menu Démarrer/Paramètres/Barre des tâches/Programmes du menu Démarrer/Ajouter/Parcourir pour indiquer le nouveau programme que vous désirez ajouter dans la liste des programmes du menu Démarrer. ATTENTION: Ne pas choisir le bouton Avancé lorsqu'on est débutant.

C- Ouvrir par le bouton de droite le menu Démarrer/Programmes/Cliquer le groupe de programme ou vous désirez ajouter un autre programme. Ouvrir le menu Fichier en haut et sélectionner Nouveau/Raccourci/Parcourir pour indiquer le nouveau programme que vous désirez ajouter dans la liste des programmes du menu Démarrer..

SUPPRIMER DES ELEMENTS DU MENU DEMARRER

Sélectionner l'élément avec le bouton de gauche. Avec le bouton de droite, cliquer une fois pour afficher le menu contextuel. Choisir Supprimer.
B- Utiliser le menu Démarrer/Paramètres/Barre des tâches/Programmes du menu Démarrer/ sélectionner le programme par un clic gaucher/ cliquer Supprimer pour indiquer le nouveau programme que vous désirez ajouter dans la liste des programmes du menu Démarrer. ATTENTION: Ne pas choisir le bouton Avancé lorsqu'on est débutant.

DEPLACER DES ELEMENTS AU MENU DEMARRER

Ouvrir par le bouton de droite le menu Démarrer et Choisir Programmes
Sélectionner le groupe de programmes ou le programme par le bouton gauche;

Vous pouvez maintenant Copier, Couper, Coller ou Supprimer la sélection.

Vous pouvez avec le bouton de gauche maintenu enfoncé, Glissez et laissez tomber l'icône sélectionner dans un autre dossier.

SUPPRIMER DES FICHIERS TEMPORAIRES

Voyons en premier lieu les fichiers avec l'extension TEMP. Avant tout effacement nous allons prendre la précaution de vider la corbeille.
Ce qui permettra de tout restaurer en cas de problèmes.
Il faudra ensuite s'assurer qu'aucune application n'est ouverte, car Windows crée des fichiers " TMP " pour le fonctionnement de ses programmes.
Examiner le contenu du dossier \TEMP. Il suffit d'aller, à l'aide de l'explorateur, dans \Windows\TEMP : il contient une majorité de fichiers ayant l'extension TMP , mais aussi certains autres avec des extensions diverses.
Sélectionnez les .TMP en les mettant en surbrillance et appuyez sur la touche "Suppr" ou "Delete ".
N'effacez les autres fichiers de ce dossier que si vous êtes sûrs qu'il sont inutiles. Après ce premier nettoyage, redémarrez la machine et vérifiez si tout va bien.
Dans ce cas vous ouvrez la corbeille et vous la videz . ATTENTION : n'effacez jamais le dossier \TEMP (c'est le répertoire qui contient les fichiers TMP)

De la même façon vous pouvez effacer les fichiers ayant l'extension GID , ainsi que les fichiers .FTS. Pour les fichiers ayant l'extension Bak , c'est un peu plus délicat , car certains ne sont pas effaçables sans risque.
Enfin dans le dossier WINDOWS\SYSBCKUP : vous pouvez sélectionner ces fichiers et les supprimer , (mais windows en conservera deux). Attention si vous voyez des fichiers .DLL, .SYS, .VXD, c'est que vous avez coché l'option "Afficher tous les fichiers" dans le tableau "Fichiers cachés" de la commande "Affichage/Options" de l'Explorateur. Réfléchissez avant de les supprimer, même si ce sont des archives !

Quand vous aurez fini de nettoyer , redémarrez la machine , essayez puis videz la corbeille .

SAUVEGARDER LA BASE DE REGISTRE

Pour faire une sauvegarde rapide de la base de registre (par exemple, avant d'installer un programme dont on n'est pas sûr ...), une méthode rapide est de recopier, sous DOS, les fichiers system.dat et user.dat après avoir enlevé les attributs cachés, système et lecture seule, puis remettre ensuite ces attributs.
C'est fastidieux : il est plus facile d'automatiser cette tâche en mettant ces commandes dans un petit fichier "Batch".

Pour vous aider à aller plus vite, voici le contenu de 3 fichiers "Batch" qui automatisent la chose :

Regback.bat (Sauvegarde des fichiers user.dat et system.dat en user.dak et system.dak)

```
@echo off
attrib -h -s system.dat
attrib -h -s user.dat
if exist system.dak attrib -h -r -s system.dak
if exist user.dak attrib -h -r -s user.dak
copy system.dat system.dak /v /y > null
copy user.dat user.dak /v /y > null
attrib +h +s system.dat
attrib +h +s user.dat
attrib +h +r system.dak
attrib +h +r user.dak
```

Regman.bat (Restauration des fichiers user.dak et system.dak en user.dat et system.dat)

```
@echo off
attrib -h -r -s system.dat
attrib -h -r -s user.dat
if exist system.dak attrib -h -r -s system.dak
if exist user.dak attrib -h -r -s user.dak
if exist system.dak copy system.dak system.dat /v /y > null
if exist user.dak copy user.dak user.dat /v /y > null
attrib +h +s +r system.dat
attrib +h +s +r user.dat
if exist system.dak attrib +h +s +r system.dak
if exist user.dak attrib +h +s +r user.dak
```

Regrecov.bat (Restauration des fichiers user.da0 et system.da0 en user.dat et system.dat)
Utiliser ce fichier batch si Windows 95 démarre en Mode sans échec pour remplacer les fichiers system.dat et user.dat par la bonne version précédente de ces fichiers.

```
@echo off
attrib -h -r -s system.da0
attrib -h -r -s user.da0
attrib -h -r -s system.dat
attrib -h -r -s user.dat
copy system.da0 system.dat /v /y > null
copy user.da0 user.dat /v /y > null
attrib +h +s +r system.dat
attrib +h +s +r user.dat
attrib +h +s +r system.da0
attrib +h +s +r user.da0
```

Vous les copiez dans le répertoire WINDOWS, et vous faites 3 raccourcis sur votre Bureau ou dans votre Menu "Démarrer", avec un nom bien évocateur pour ne pas les confondre et une belle icône.
Et puis de temps en temps, un petit clic sur une icône pour faire une sauvegarde ou une restauration automatique, ça prend une seconde !

MASQUEZ UN LECTEUR DANS POSTE DE TRAVAIL POUR WINDOWS 95/98

Masquer le lecteur a :
Résumé :
Démarrez Regedit
Cherchez HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Faites un click-droit sur la page de droite
Sélectionnez Nouveau, Valeur Dword
Nommez-la NoDrives
Affectez lui la valeur 1.

Explications détaillées
Base de registre : masquer un lecteur (Win95/98)
Pour masquer un lecteur, il faut aller dans la clé suivante de la **BdR** :
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion \Policies\Explorer]

Pour ouvrir la Base de Registres, plusieurs moyens :

> Lancer l'Explorateur Windows. Chercher le fichier **REGEDIT.EXE** dans le répertoire C:\WINDOWS, double-cliquer dessus pour le lancer.
> Autre solution plus rapide : cliquer sur le Menu Démarrer, puis Exécuter... Taper regedit, OK, et hop, voilà.
> Encore plus rapide : faire un raccourci qui pointe vers le fichier REGEDIT.EXE (dans le Menu Démarrer ou sur le Bureau).

Ouvrir la clé **HKEY_CURRENT_USER**, puis **Software**, puis **Microsoft**, **Windows**, **CurrentVersion**, **Policies**, puis **Explorer**.

Vous voyez dans la fenêtre de droite la valeur **NoDrives** : elle est à **0** (zéro). Ca veut dire qu'**aucun** lecteur n'est **masqué**, (autrement dit, ils sont tous visibles).
Si vous voulez cacher le lecteur A, il faut donner à **DWORD** la valeur **1**.
Pour cela, cliquer sur **NoDrives** avec le bouton droit, puis **Modifier**.

Taper **1** au lieu de **0** dans **Données de la valeur**. Cocher **Décimale**, puis **OK**.

La prochaine fois que vous démarrerez l'ordinateur, le lecteur **A** sera masqué.

Si vous voulez masquer le lecteur **B**, il faut donner à **DWORD** la valeur décimale **2**.
Si vous voulez masquer le lecteur **C**, il faut donner à **DWORD** la valeur décimale **4**.
Si vous voulez masquer le lecteur **D**, il faut donner à **DWORD** la valeur décimale **8**.
Si vous voulez masquer le lecteur **E**, il faut donner à **DWORD** la valeur décimale **16** (=**10** en hexadécimal).
Etc.
Vous avez compris ? A chaque fois, il faut **doubler** la valeur précédente.

Voici donc un petit tableau récapitulatif, qui vous donne la valeur de **DWORD**, en **décimal** et en **hexadécimal**, pour cacher n'importe quel lecteur :

Cacher lecteur	Décimal	Hexa	Cacher lecteur	Décimal	Hexa	Cacher lecteur	En décimal	En hexa
A	1	1	**J**	512	200	**S**	262144	40000
B	2	2	**K**	1024	400	**T**	524288	80000
C	4	4	**L**	2048	800	**U**	1048576	100000
D	8	8	**M**	4096	1000	**V**	2097152	200000
E	16	10	**N**	8192	2000	**W**	4194304	400000
F	32	20	**O**	16384	4000	**X**	8388608	800000
G	64	40	**P**	32768	8000	**Y**	16777216	1000000
H	128	80	**Q**	65536	10000	**Z**	33554432	2000000
I	256	100	**R**	131072	20000			

Faites juste attention à une chose : si vous entrez une valeur décimale, pensez bien à cocher la case **Décimale**.
Si vous entrez une valeur hexadécimale, pensez à cocher la case **Hexadécimale**.

Si vous voulez cacher plusieurs lecteurs, il faut ajouter les valeurs.
Ex : si vous voulez cacher les lecteurs **A** et **C**, il faut donner à **DWORD** la valeur **1 + 4 = 5** (en décimal).
Si vous voulez cacher **A**, **C** et **D**, il faudra donner la valeur **1 + 4 + 8 = 13** (en décimal), **D** en hexadécimal.

Si vous voulez cacher **tous** les lecteurs, il faudra donner la valeur **67 108 863** en décimal (**3FFFFFF** en hexa).
(enfin, quelle drôle d'idée...)

Créer un fichier Reg pour simplifier les manipulations

Maintenant, pour simplifier, on pourrait faire des petits fichiers **REG** à fusionner dans la Base de Registres, plutôt que de lancer **REGEDIT** chaque fois qu'on veut cacher un lecteur.
Comment faire ? Facile.

Ex : on veut cacher le lecteur **A**.
Avec **REGEDIT**, il faudrait aller dans la clé
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
Et mettre la valeur **DWORD** à **1**.

On peut faire exactement la même chose avec un fichier **REG** qui contient les informations suivantes :

```
REGEDIT4
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion
\Policies\Explorer]"NoDrives"=dword:00000001
```

Vous voyez que c'est la même chose. Et ça évite d'ouvrir la Base de Registres pour ceux que ça effraie.

MASQUEZ L'ONGLET PROFILS UTILISATEUR DANS MOT DE PASSE POUR WINDOWS 95/98

Démarrez Regedit
Cherchez HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System
Faites un click-droit sur la page de droite
Sélectionnez Nouveau, Valeur Dword
Nommez-la NoProfilePage
Affectez lui la valeur 1.

WINDOWS : TROUVEZ LA PANNE EN CAS DE PLANTAGE

Windows possède un utilitaire fort sympathique en cas de plantage. Docteur Watson permet d'obtenir tous les détails: les tâches, les drivers chargés, les ressources système afin de trouver l'origine du plantage.
Pour lancer Docteur Watson, cliquez sur le bouton Démarrer, sur Exécuter et tapez drwatson.

SECURISER L'ACCES A VOTRE ORDINATEUR

Pour rendre le mot de passe au démarrage de windows obligatoire, il faut faire une petite manip :

- choisir dans les propriétés réseau "Gestionnaire de sessions individuelles de windows"

- rajouter la clé : hkey_local_machine --> Network --> logon --> nouveau DWORD --> MustBeValidated 1

Ainsi à chaque démarrage s'affiche la liste des différents profils, vous êtes obligé de rentrer le mot de passe correspondant au profil sélectionné. Bien sur, si le profil n'a pas de mot de passe, ca ne sert a rien...

PARTAGE DE RESSOURCE

Sur une machine quelconque du réseau (win3.11, win95/98, win NT, Linux/Samba...)
Menu panneau de configuration, paramètres réseau, active le partage de fichiers
explorateur, crée un répertoire de travail (le nom n'a aucune importance)

- Partage le : clic droit sur le répertoire et choisir "Partager..."
- "Partager en tant que"
- "Nom de partage" : donne lui un nom facile à identifier
- "Accès complet"
- Mot de passe

Exemple : mot de passe vierge :
Ce répertoire partagé deviens visible sur tout le réseau, et tout le monde peut écrire dedans.

PARTAGEZ UN PC EN LIBRE-SERVICE

Lorsque plusieurs utilisateurs travaillent sur un même poste, il est nécessaire de partager les ressources du système. Chacun conserve ainsi son espace de travail.

Dans une entreprise, lorsque les ressources informatiques sont limitées ou que le nombre de PC est inférieur à celui des utilisateurs, mieux vaut établir des règles pour utiliser les machines rationnellement. Même si un PC est utilisé à plusieurs, rien n'empêche chacun des utilisateurs de personnaliser l'interface et d'en régler les paramètres, afin de s'y sentir aussi à l'aise que sur son propre PC. Avec les profils de Windows 95 et Windows NT (3.51 ou 4.0), chaque utilisateur exploite des fichiers de réglage de Windows entièrement différents de ceux des autres. De plus, pour éviter que les différents utilisateurs manient les mêmes fichiers - ce qui présente des risques (suppression, espionnage ...) mieux vaut organiser l'espace disque intelligemment à l'aide d'une arborescence adéquate.

CREEZ DES PROFILS

Introduction
Avec Windows 95 comme avec Windows NT. il est possible de créer et d'utiliser un profil différent par utilisateur. Cela permet de personnaliser l'apparence et l'organisation de son bureau. Avec Windows NT, les profils sont automatiquement créés à la première ouverture de session. Toutes les modifications que vous apporterez à l'interface seront sauvegardées dans votre fichier Profil.

Contrairement à NT, les profils ne sont pas utilisés par défaut par windows 95
, Windows 95 propose cette gestion des utilisateurs en option.
Pour travailler avec les profils, il faut d'abord activer les mots de passe, si ce n'est pas déjà fait. Dans le Panneau de configuration, sélectionnez Mots de passe et indiquez votre " sésame ". Il vous servira à démarrer votre connexion à Windows avec vos paramètres personnalisés. Attention : " connexion " est à prendre ici dans un sens purement logiciel; la procédure n'a strictement rien à voir avec la connexion physique à un réseau local.

Les profils sont donc à mettre en oeuvre. Ceci fait, ils sont "locaux" c'est à dire mémorisés sur le poste Windows 95.
Pour une sécurité accrue, il faudra poser les profils sur le serveur et donc indiquer à windows 95 qu'à la connexion il devra les prendre sur le serveur NT.

Mise en oeuvre des profils locaux
(pas sur le serveur)
sur le client Windows95
Panneau de configuration/Mots de passe/...
Dans l' onglet "Profils utilisateurs"
Cochez : "Les utilisateurs peuvent personnaliser..."
Cochez : les options "Inclure le Menu Démarrer ..."
Redémarrez la machine
Connectez-vous en tant que "X", Windows 95 vous demande confirmation que vous voulez bien mémoriser ce nouveau profil : répondez Oui
A l'aide de l'explorateur allez vérifier la présence d'un nouveau répertoire "X" dans le répertoire C:\WIN95\Profiles ; dans ce répertoire vous trouverez "votre" profil sous la forme d'un fichier "User.dat"
Limites des profils locaux :
Ces profils sont locaux. Ils sont utiles pour diversifier les environnements des utilisateurs du client. Ils n'offrent aucune garantie de sécurité (pas de contrôle des accès -type NTFS- sur Windows 95).
La connexion (et l'authentification) de l'utilisateur sur NT est un mieux.
Pour mieux contrôler les actions des utilisateurs il faut mettre en oeuvre les "stratégies système", dans lesquelles est incluse la mise en oeuvre des profils gérés par NT (Cf. chapitre ci-dessous)

A la première connexion, le système vous informe que vous n'étiez pas connecté à cet ordinateur auparavant et vous demande si vous souhaitez qu'il retienne tous les paramètres individuels. Répondez Oui. Dorénavant, toutes les modifications que vous effectuerez sur le Bureau de Windows (menu Démarrer, couleurs de Windows et polices) seront sauvegardées dans votre profil.

Bougez, votre profil suit
Si, en raison d'un changement d'organisation dans le service par exemple, vous devez changer de poste, vous pouvez emporter vos réglages et retrouver, sur votre nouveau PC, un environnement de travail identique à celui que vous venez de quitter. Avec Windows NT 4.0 et Windows 95, les profils se trouvent dans le dossier C:\Windows\Profiles.

Chaque dossier correspond à un utilisateur et contient tous les réglages personnalisés. Copiez simplement le dossier correspondant à votre compte (sur une disque exemple) et placez dossier Profil du nouveau poste de travail.

Utilisez une stratégie de groupe
Avec l'Éditeur de stratégies système, vous pouvez paramétrer finement les réglages des utilisateurs sur l'utilisation de Windows.
Commencez par l'installer à partir du CD-ROM de Windows 95. Il se trouve dans le dossier Admin\Apptools\Poledit.
Ensuite, exécutez Poledit.exe, et faites Fichier/Ouvrir la base de registres. Vous vous trouvez face à deux icônes: Utilisateur local et Ordinateur local. Comme vous pouvez le deviner, la première icône définit les réglages concernant les utilisateurs du poste et la deuxième tous les réglages du PC. Vous pouvez ainsi régler et appliquer toute une série de restrictions visant les utilisateurs, afin de sécuriser le système et de limiter les erreurs de manipulation. Vous avez ainsi le moyen d'interdire aux utilisateurs, par exemple, de modifier les réglages de la

mémoire virtuelle. En outre, vous pouvez créer un fichier personnel de stratégie visant à régler les droits de chaque utilisateur référencé. N'hésitez pas à fouiller dans tous les paramètres pour optimiser la personnalisation de votre profil.

Gérez les permissions
Il est possible, avec Windows NT 4.0, de verrouiller un dossier. Pour cela, faites un clic droit sur le nom du dossier et choisissez Propriétés/Sécurité/Permissions.

Désignez ensuite la liste des utilisateurs qui disposeront d'un accès à votre dossier, tant en lecture qu'en écriture. Windows 95 n'offre pas une telle possibilité. Il permet seulement de partager des dossiers et de les rendre accessibles sur un réseau par un mot de passe commun à tous les utilisateurs

MIGRER VERS NT

Notions de base : petit glossaire réseau

Domaine
Bien que la notion de "Groupe de travail" (au sens WfW du terme) soit maintenue c'est désormais la notion de domaine qui s'impose dans NT4. Il s'agit de l'ensemble des machines, des services et des utilisateurs travaillant autour d'un (ou plusieurs) **serveurs** NT. Ce domaine est nommé (chez ExpertWeb c'est EW4) et il est requis à la connexion.

Serveur
Au sens traditionnel du terme, c'est une machine qui offre des services aux utilisateurs (clients). NT distingue 3 types de serveurs :

- **serveur primaire de domaine** : il est obligatoire et unique dans un domaine. C'est lui qui maintient la base des comptes utilisateurs (SAM)
- **serveur secondaire de domaine** : il peut y en avoir plusieurs. Il vient en secours d'un serveur primaire (en cas de besoin). Il maintient une copie de la base des comptes utilisateurs (SAM).
- **serveur autonome** : serveur banalisé ; serveur d'application, serveur d'impression, serveur d'accès distant, serveur DNS,...

NTFS
C'est la sécurité au sens NT du terme. C'est un type de formatage du disque (ou de certaines partitions) requis pour pouvoir mettre en oeuvre cette sécurité.

Utilisateur
Une personne connue dans le domaine. Elle a accès aux ressources du domaine en fonction des permissions qui lui sont accordées. Il est recommandé de les rassembler en **groupes**

Groupe
Un ensemble d'**utilisateurs** d'un même domaine ayant des points communs. Le but du groupe est de simplifier l'administration. On distingue :

- les groupes locaux (définis localement dans un domaine)
- les groupes globaux (qui peuvent s'exporter vers d'autres domaines)
- les groupes spéciaux : prédéfinis dans NT, ex. : le groupe "tout le monde"

Profil
C'est l'environnement de l'**utilisateur**. Généralement, ce profil est maintenu sur le "client" (le profil est dit local). Il peut être mémorisé sur un **serveur** du domaine. Il est alors baptisé **errant** car il peut-être téléchargé par l'utilisateur se connectant sur un client ou un autre...
Il peut, éventuellement, être défini, restreint et figé par l'administrateur (il est alors dit **obligatoire**).

Partage
Point d'accès dans une arborescence. Se caractérise par un nom de partage (ex. : APPS pour le répertoire des applications sur le serveur NT4S) et des **permissions de partage** accordées aux utilisateurs sur cette arborescence (ne pas confondre avec les **permissions NTFS**).

Permissions

- permissions de sécurité **NTFS** : les droits posés sur des fichiers et des répertoires pour définir (limiter) les accès aux utilisateurs.
- permissions de **partage** : notion identique à la précédente mais qui ne s'applique que dans le cadre d'un accès au travers d'un "partage" : classiquement un accès via le réseau (depuis un client) à une ressource et décrite sous la forme \\serveur\partage\ressource

UNC - nommage des ressources

- Abréviation de "Universal Naming Ressource".
  Convention de nommage des ressources.
  syntaxe : \\serveur\ressource\répertoire\fichier
  Ex. : \\NT4S\APPS\Office\excel.exe

PREALABLES POUR PERMETTRE LES CONNEXIONS, LE CONTROLE D'UN POSTE NT WORKSTATION ET DE SES UTILISATEURS VIA LE RESEAU

Pour qu'un utilisateur d'un poste NT4WS puisse se connecter sur un serveur NT (être authentifié par le serveur, son mot de passe est validé par NT), à fortiori pour que son environnement soit contrôlé et des limitations à ses actions soient posées, un certain nombre de préalables sont à réaliser :

Sur chaque poste NT4 Workstation
Il faut indiquer à NT4WS qu'il devra se connecter au domaine NT au démarrage :
Panneau de config/Réseau/onglet Identification
Si le poste est configuré dans un "workgroup", cliquez le bouton "Modifier...", puis sélectionnez l'option "domaine" pour remplir le champs avec par exemple « EWNT4 »
Cf., aussi, "Note sur l'authentification" ci-dessous.

Sur le serveur NT4

- Enregistrer le ou les utilisateurs. Cf. "Note sur l'authentification" ci-dessous.
- En règle générale, les utilisateurs se connectant depuis une station du réseau n'ont pas accès aux ressources du serveur. Si l'utilisateur est arrêté par le message : "Accès réseau refusé : l'utilisateur ne

bénéficie pas du type d'accès demandé sur cet ordinateur", vous devez lui octroyer un droit : cf. permettre une connexion réseau

- Les stations de travail ou les serveurs NT doivent être ajoutés manuellement au domaine. cf. Intégration de machines NT au domaine

Note sur l'authentification

Lorsque votre machine NT4WS est configurée (Panneau de config/Réseau/Identification) comme appartenant à un groupe de travail, elle vous propose, à l'ouverture d'une session, une grille d'authentification à 2 requêtes (à l'instar de Windows 95) : "Nom" et "Mot de passe".
Lorsque votre machine NT4WS est configurée (Panneau de config/Réseau/Identification) comme appartenant à un domaine NT, elle vous propose, à l'ouverture d'une session, une grille d'authentification à 3 requêtes : "Nom", "Mot de passe" et "Domaine".
Il est donc facile de "repérer" de quel type connexion/authentification il s'agit : "groupe de travail", gérée par NT4WS ou "domaine NT", gérée par un serveur NT controleur du domaine.
Il est aussi facile de comprendre que si vous avez des couples "Nom d'utilisateur"/"Mot de passe" différents sur les deux machines (client et serveur) vous serez obligé jongler avec.
Conseil : harmonisez vos "Mot de passe"

PREALABLES POUR PERMETTRE LES CONNEXIONS ET LE CONTROLE D'UN CLIENT WINDOWS 95 VIA LE RESEAU

Pour qu'un poste Windows 95 puisse se connecter sur un serveur NT (être authentifié par le serveur, son mot de passe est validé par NT), à fortiori pour que son environnement soit contrôlé et des limitations à ses actions soient posées, un certain nombre de préalables sont à réaliser :

Sur chaque poste Windows 95

- **Installation de l'éditeur de stratégie (Poledit)**

  L'éditeur de stratégies (Poledit) n'est pas installé de base dans Windows 95. Il faut donc l'installer :

  - Démarrer/Paramètres/Panneau de configuration/...
    Ajout-Suppression de programmes/...
    Onglet Installation de Windows/...
    Disquette fournie/Parcourir...
    Lecteurs: sélectionner le lecteur du CDROM
    puis descendez dans le répertoire \Admin\AppTools\PolEdit
    Nom de fichier : "poledit.inf"
    OK
    Cochez "Editeur de stratégie système"
    Cochez "Stratégie de groupe"/...
    Installer...
  - L'éditeur de stratégie s'installe et un raccourci est apparu dans les "outils système" de votre "menu démarrer".

- **Modification de la configuration réseau**

  Cette configuration peut se faire par le "Panneau de Configuration/Réseau/..." ou par "Poledit" . Cette deuxième solution est proposée ici car elle offre plus de possibilités.

  - Démarrer/Programmes/Outils d'administration/...
    Editeur de stratégie système
    Fichier/**Ouvrir la base de registres**/...
    Sélectionner "**Ordinateur Local**"
    - **Réseau**
      - **Contrôle d'accès/...**
        De base, un poste Windows 95 est une simple ressource du réseau. L'accès à ce poste se gère par des mots de passe posés sur les ressources (répertoires, fichiers, imprimantes) de ce poste. L'utilisateur du poste est anonyme.
        Il est possible d'opter pour une utilisation par utilisateur. Les ressources du poste sont alors protégées des mots de passe associés à ces utilisateurs. Ne pourront accéder à ces ressources (localement, ou via le réseau) que les utilisateurs **authentifiés**. Pour mettre en oeuvre profils et stratégies cette deuxième option est requise.
        cochez "au niveau utilisateur"
        - nom d'authentificateur : nom du domaine
        - type d'authentificateur : "domaine NT"
      - **Ouverture de session/...**
        cochez "Nécessite une validation par réseau..." si vous souhaitez désactiver le bouton "annuler" de la bannière de connexion : Windows 95 ne démarrera pas sans un mot de passe valide !
      - **Client Microsoft/...**
        - cochez "Ouverture de session sur NT" si vous souhaitez authentifier les utilisateurs via un serveur NT4 et précisez alors le nom du domaine (Ex. : EXPERTWEBNT4)
        - cochez "Groupe de travail" et précisez son nom (Ex. : EXPERTWEBWG)
      - **Mettre à jour/...**
        Cochez "Mettre à jour à distance" pour indiquer où sera conservé le fichier des stratégies :
        - Mode de mise à jour : "Automatique..."
          il sera conservé dans : \\nt4s\netlogon\config.pol
        - ou (peu recommandé)
          Mode de mise à jour : "Manuel" et précisez alors le chemin : il sera conservé, par ex., dans : \\nt4s\ailleurs\config.pol
    - **Système**
      - cochez "Activer les profils utilisateurs" si vous souhaitez mettre en oeuvre les profils. Cette option est requise pour la mise oeuvre des stratégies système.

  Note : les modifications ainsi apportées à "la base des registres" nécessitent un redémarrage de la machine pour être prises en compte :
  Démarrer/Arrêter/Redémarrer l'ordinateur
  et non pas :
  Démarrer/Arrêter/Fermer toutes les applications etc. ...

SUR LE SERVEUR NT4

En règle générale, les utilisateurs se connectant depuis une station du réseau n'ont pas accès aux ressources du serveur.
Si l'utilisateur est arrêté par le message :
"Accès réseau refusé : l'utilisateur ne bénéficie pas du type d'accès demandé sur cet ordinateur", vous devez lui octroyer un droit : cf. permettre une connexion réseau

Note sur l'authentification NT4 et Windows 95
Lorsque vous relancez votre machine, Windows 95 vous propose une grille d'authentification avec 2 requêtes : "Nom" et "Mot de passe".
Lorsque vous ouvrez une session sur Windows NT, celui-ci vous propose une grille d'authentification avec 3 requêtes : "Nom", "Mot de passe" et "Domaine".
Il est donc facile de "repérer" de quelle authentification il s'agit.
Il est aussi facile de comprendre que si vous avez des couples "Nom d'utilisateur"/"Mot de passe" différents sur les deux machines, vous serez obligé de remplir 2 grilles ; par contre si ces deux authentifications sont identiques seule la grille NT4 sera proposée.
Conseil : pour harmoniser vos "Mot de passe" vous pouvez effacer votre fichier ".pwl" dans le répertoire "Windows 95". A la prochaine relance de votre machine, il vous demandera de saisir votre nouveau "Mot de passe".

"CLIENTS RESEAU MICROSOFT"

"Clients réseau Microsoft" est la formulation choisie par Microsoft pour un poste Windows 95 intégré dans un réseau Microsoft. Au delà de ce cas particulier, dès lors que l'on installe une carte réseau et un système d'exploitation "Microsoft" dans un PC, on confère à celui-ci la qualité de "Clients réseau Microsoft" et un (assez) grand nombre de mécanismes peuvent être mis en oeuvre de façon plus ou moins consciente (et maîtrisée) selon les options choisies :

- Contexte réseau : "poste à poste" ("groupe de travail" Workgroup,...), "client-serveur" ("domaine" NT,...), mixte, "accès réseau à distance", le franchissement d'un routeur,...
- Protocole réseau : Microsoft (NetBEUI), TCP/IP, PPP, ...et combinaisons,...
- Les "ressources réseau", les serveurs, les services utilisés : aucun, DNS, Wins, domaine NT, ...

On peut donc être confronté à des situations nombreuses et parfois déroutantes ; l'objectif de cette page est d'apporter quelques éclaircissements sur certains points et particulièrement quelle vision du réseau ("Voisinage réseau") a-t-on (impossible, partielle, incorrecte) voir ci après .

et peut-on accéder aux ressources réseau (visibles ou pas) ?

Vision et accès aux ressources des réseaux Microsoft

Influence de l'utilisation (dans un contexte de réseau local type "Workgroup") du "Protocole/Microsoft/NetBEUI

Contexte ("mon poste" et réseau)	**Configuration** **" réseau "** de "mon poste" (Panneau de configuration/Réseau)	**La vision** des "réseaux Microsoft" (Icône "Voisinage réseau")	**L'accès** aux "réseaux Microsoft" (Explorateur/Outils/Connecter un lecteur réseau)
"mon poste" est un client Windows 95 (en général, mais aussi bien NT) dans un contexte de "Réseau local" Le seul protocole utilisé est NetBEUI	• Client réseau MS (Préciser obligatoirement le WG (*) dans l'onglet " Identification ") Carte réseau **Protocole NETBEUI** Service "Partage"	"Mon poste" voit (#) les "réseaux Microsoft" (&) configurés avec NetBEUI "Mon poste" est visible dans le "Voisinage réseau" des "réseaux Microsoft" (&) configurés avec NetBEUI	Les membres de mon WG (*) peuvent accéder aux ressources que j'ai mises à leur disposition. Je peux accéder à un domaine NT si j'y ai un compte et si le PDC est configuré avec NETBEUI

(*) WG / Workgroup / "groupe de travail"
(#) une machine hors tension peut être momentanément visible sur le réseau (problème de MAJ)
(&) des membres du ou des "groupes de travail" et/ou domaines NT4

Vision et accès aux ressources des réseaux Microsoft

- Client Windows 95
  - Influence de l'absence ou de la présence (Panneau de configuration/réseau) de "Client/réseau Microsoft" et/ou "Service/Microsoft/Fichier et imprimante partagés..."

Contexte ("mon poste" et réseau)	**Configuration** **" réseau "** de "mon poste" (Panneau de configuration/Réseau)	**La vision** des "réseaux Microsoft" (Icône "Voisinage réseau")	**L'accès** aux "réseaux Microsoft" (Explorateur/Outils/Connecter un lecteur réseau)

"mon poste" est un client Windows 95. Quel est l'effet induit par la présence du client " Client réseau Microsoft " et/ou service " Fichiers et imprimantes partagés " ? Ceci quelque soit le ou les protocoles utilisés.	Pas de Client réseau MS Carte réseau Protocole X Pas de service "Partage"	Pas d'icône Voisinage réseau Aucune vision des WG (*)	Aucun accès aux WG (*)
	Client réseau MS (Préciser obligatoirement le WG (*) dans l'onglet " Identification ") Carte réseau Protocole X Pas de service "Partage"	"Mon poste" voit (#) des "réseaux Microsoft" (&) "Mon poste" n'est pas visible dans le "Voisinage réseau" des "réseaux Microsoft" (&)	Je peux accéder aux ressources visibles (#) dans "Voisinage réseau" (si leur propriétaire me le permet)
	Client réseau MS Carte réseau Protocole X **Service "Partage"**	Je peux offrir des ressources aux membres des "réseaux Microsoft" (&) "Mon poste" est visible dans le "Voisinage réseau" des postes des "réseaux Microsoft" (&)	Les membres des "réseaux Microsoft" (&) peuvent accéder aux ressources que j'ai mises à leur disposition.

(*) WG / Workgroup / "groupe de travail"

(#) une machine hors tension peut être momentanément visible sur le réseau (problème de MAJ)

(&) des membres du ou des "groupes de travail" et/ou domaines NT4

Vision et accès aux ressources des réseaux Microsoft

- Client Windows 95

Dans un contexte "Internet-TCP/IP", influence de l'absence ou de la présence (Panneau de configuration/réseau) de "TCP-IP/Configuration Wins..." et/ou "Configuration DNS..." ; utilité du "fichier LMHOSTS

Contexte ("mon poste" et réseau)	**Configuration** **" réseau "** de "mon poste" (Panneau de configuration/Réseau)	**La vision** des "réseaux Microsoft" (Icône "Voisinage réseau")	**L'accès** aux "réseaux Microsoft" (Explorateur/Outils/Connecter un lecteur réseau)
"mon poste" est un client Windows 95 dans un contexte "Réseau Internet" TCP/IP : Sans DNS Sans Wins	Client réseau MS (Préciser obligatoirement le WG (*) dans l'onglet " Identification ") Carte réseau Protocole TCP/IP (@) **Sans DNS** **Sans WINS** Service "Partage"	"Mon poste" voit (#) les "réseaux Microsoft" (&) du réseau local et configurés avec TCP/IP Aucune visibilité au delà du routeur	Les "réseaux Microsoft" (&) du réseau local et configurés avec TCP/IP peuvent échanger des ressources visibles Les "réseaux Microsoft" situés au delà d'un routeur (et donc non visibles dans le "Voisinage réseau") sont accessibles via le **fichier LMHOSTS**
"mon poste" est un client Windows 95 dans un contexte "Réseau Internet" TCP/IP : Avec DNS Sans Wins	Client réseau MS (Préciser obligatoirement le WG (*) dans l'onglet " Identification ") Carte réseau Protocole TCP/IP (@) **Avec DNS** **Sans WINS** Service "Partage"	"Mon poste" voit (#) les "réseaux Microsoft" (&) du réseau local et configurés avec TCP/IP Aucune visibilité au delà du routeur	Les "réseaux Microsoft" (&) du réseau local et configurés avec TCP/IP peuvent échanger des ressources visibles Les "réseaux Microsoft" situés au delà d'un routeur (et donc non visibles dans le "Voisinage réseau") **mais connus du DNS** peuvent accéder aux ressources que j'ai mises à leur disposition.
"mon poste" est un client Windows 95 dans un contexte	Client réseau MS (Préciser obligatoirement le WG (*) dans l'onglet " Identification ")	"Mon poste" voit (#) les "réseaux Microsoft" (&) du réseau local et configurés avec TCP/IP **Aucune visibilité au delà**	Les "réseaux Microsoft" (&) du réseau local et configurés avec TCP/IP peuvent échanger des ressources visibles Les "réseaux Microsoft" situés au

"Réseau Internet" TCP/IP : Avec DNS Avec Wins	Carte réseau Protocole TCP/IP (@) **Avec DNS** **Avec WINS** Service "Partage"	**du routeur (contrairement au contexte équivalent de NT4)**	delà d'un routeur (et donc non visibles dans le "Voisinage réseau") **mais connus du DNS ou du WINS** peuvent accéder aux ressources que j'ai mises à leur disposition.

(*) WG / Workgroup / "groupe de travail"

(#) une machine hors tension peut être momentanément visible sur le réseau (problème de MAJ)

(&) des membres du ou des "groupes de travail" et/ou domaines NT4

(@) TCP/IP ou PPP

Vision et accès aux ressources des réseaux Microsoft

Poste NT4 (serveur ou Workstation) : dans un contexte "Internet-TCP/IP", influence de l'absence ou de la présence et donc de l'utilisation ou non d'un service (serveur) WinS et/ou DNS ; utilité du "fichier LMHOSTS"

Contexte ("mon poste" et réseau)	**Configuration** " réseau " de "mon poste" (Panneau de configuration/Réseau)	**La vision** des "réseaux Microsoft" (Icône "Voisinage réseau")	**L'accès** aux "réseaux Microsoft" (Explorateur/Outils/Connecter un lecteur réseau)
"mon poste" est un serveur ou client Windows NT4 dans un contexte "Réseau Internet" TCP/IP : Sans DNS Sans Wins	Carte réseau Protocole TCP/IP (@) **Sans DNS** **Sans WINS**	"Mon poste" voit (#) les "réseaux Microsoft" (&) du réseau local et configurés avec TCP/IP Aucune visibilité au delà du routeur	Les "réseaux Microsoft" (&) du réseau local et configurés avec TCP/IP peuvent échanger des ressources visibles Les "réseaux Microsoft" situés au delà d'un routeur (et donc non visibles dans le "Voisinage réseau") sont accessibles via le **fichier LMHOSTS**
"mon poste" est un serveur ou client	Carte réseau	"Mon poste" voit (#) les "réseaux Microsoft" (&)	Les "réseaux Microsoft" (&) du réseau local et configurés

Windows NT4 dans un contexte "Réseau Internet" TCP/IP : Avec DNS Sans Wins	Protocole TCP/IP (@) **Avec DNS** **Sans WINS**	du réseau local et configurés avec TCP/IP Aucune visibilité au delà du routeur	avec TCP/IP peuvent échanger des ressources visibles Les "réseaux Microsoft" situés au delà d'un routeur (et donc non visibles dans le "Voisinage réseau") **mais connus du DNS** peuvent accéder aux ressources que j'ai mises à leur disposition.
"mon poste" est un serveur ou client Windows NT4 dans un contexte "Réseau Internet" TCP/IP : Avec DNS Avec Wins	Carte réseau Protocole TCP/IP (@) **Avec DNS** **Avec WINS**	"Mon poste" voit (#) les "réseaux Microsoft" (&) du réseau local et configurés avec TCP/IP Contrairement au contexte équivalent de Windows 95, " Mon poste " peut voir des ressources au delà du routeur.	Les "réseaux Microsoft" (&) peuvent échanger des ressources visibles Les membres des "réseaux Microsoft" situés au delà d'un routeur, non visibles dans le "Voisinage réseau" (non connues du WINS), **mais utilisant un DNS ou leur fichier LMHOSTS** peuvent accéder aux ressources que j'ai mises à leur disposition.

(*) WG / Workgroup / "groupe de travail"

(#) une machine hors tension peut être momentanément visible sur le réseau (problème de MAJ)

(&) des membres du ou des "groupes de travail" et/ou domaines NT4

(@) TCP/IP ou PPP

PRINCIPE D'UTILISATION DE POLEDIT (CLIENT WINDOWS 95)

Après avoir donné à chaque poste Windows95 la possibilité d'être géré par le serveur NT4, il reste à choisir un des postes pour définir le cadre d'utilisation de l'ensemble des postes et à le mémoriser en "lieu sûr" sur le serveur.

- **Connecté sur un client en tant qu'administrateur du domaine :**
  Démarrer/Programmes/Outils d'administration/...
  Editeur de stratégie système
  Fichier/Nouveau/Edition/Ajouter/...
  Ajouter un utilisateur/parcourir/indiquer l'utilisateur
  ou mieux,
  Ajouter un groupe/parcourir/indiquer le groupe,
  Sélectionner le nouvel icône, et limiter l'environnement de l'utilisateur ou du groupe (Cf. paragraphe ci-dessous)
- Une fois votre "environnement limité" défini, enregistrez-le :
  Fichier/**Enregistrer...**
  1. **Cas d'un domaine géré par un seul "contrôleur de domaine" :**
     - ...sous le nom **config.pol**,
       dans le répertoire partagé sous le nom NETLOGON :
       le_CPD\NETLOGON\ qui est en principe : WinNT\System32\Repl**Import**\Script
  2. **Cas d'un domaine géré par plusieurs "contrôleurs de domaines" :**
     - ...sous le nom **config.pol**,
       dans le sous-répertoire "Script" du répertoire partagé sous le nom REPL$:
       le_CPD\Repl$\Scripts qui est en principe : WinNT\System32\Repl**Export**\Script
     - Mise en oeuvre de la duplication
       de façon à ce que ce fichier config.pol soit automatiquement recopié dans les répertoires NETLOGON des contrôleurs du domaine, y compris le CPD.

...puis, pour gérer l'environnement de l'utilisateur :

Vous devez choisir entre deux options :

- Celle visant à **fortement sécuriser** le poste Windows 95, le serveur, le réseau, mais qui aura l'inconvénient de n'offrir que peu de fonctionnalités à l'utilisateur. Cette option consiste à utiliser au maximun les restrictions offertes par "poledit". Cf. limiter l'environnement et en particulier l'option "N'exécuter que les applications windows autorisées"
- Celle visant à offrir un environnement stable et convivial à des utilisateurs sans pour autant par trop limiter leurs actions. Il s'agira là d'éventuellement poser quelques restrictions mais surtout de Mettre en oeuvre les profils

LIMITATION DE L'ENVIRONNEMENT DE L'UTILISATEUR CLIENT WINDOWS 95

Localement :

Ces pages n'ont pas pour objet de développer cet aspect : cette parenthèse s'adresse donc à ceux qui souhaiteraient tenter de limiter localement (sans l'aide d'un serveur NT) les actions des utilisateurs de la machine Windows 95. Ces limites étant mémorisées dans la base des registres du poste Windows 95, aucune sécurité NTFS ne peut y être posée et elles peuvent donc être facilement transgressées par un utilisateur moyennement averti !

- Démarrer/Programmes/Outils d'administration/Editeur de stratégie système
  Fichier/**Ouvrir la base de registres**/...
- Modifier la stratégie à appliquer à "**Ordinateur Local**" et/ou "**Utilisateur Local**"
  - **Utilisateur local** : permet de réduire les possibilités d'un utilisateur se connectant "en tant que utilisateur" sur ce poste.
    Faites le tour des différentes rubriques :
    - Panneau de configuration
    - Bureau
    - Réseau
    - Environnement
    - Système
  - **Ordinateur local** : permet de réduire les possibilités d'un utilisateur quelconque se connectant sur ce poste.
    Faites le tour des différentes rubriques :
    - Réseau
    - Système

Via le serveur NT :

 Connecté sur un client 95 en tant qu'administrateur du domaine :
Démarrer/Programmes/Outils d'administration/Editeur de stratégie système
Fichier/**Ouvrir la base de registres**/...
Faites le tour des restrictions de "**utilisateur local**" pour supprimer toute restriction qui serait éventuellement définie : elles se feront ailleurs (Cf. ci-dessous).
Par contre vérifiez que "**Ordinateur local**" est bien configuré comme indiqué dans installation de Poledit,
 Fichier/**sélectionnez le fichier de stratégie** "config.pol" (en bas de la liste)

- Faites le tour des restrictions de "**utilisateur par défaut**" et/ou "**ordinateur par défaut**" pour supprimer toute définition ou restriction qui serait éventuellement définie : la gestion se fera ailleurs (Cf. ci-dessous).
- **Groupe et/ou Utilisateur défini dans le paragraphe précédent** : permet de réduire les possibilités de CE groupe et/ou utilisateur lorsqu'il se connecte via le réseau.
  Faites le tour des différentes rubriques "restrictions" :
  - Panneau de configuration
  - Bureau
  - Réseau
  - Environnement
  - Système

PREPARATION DU SERVEUR NT4 ET DEBUT DE L'INSTALLATION SOUS DOS

Notes préliminaires

Un serveur NT peut-être monté (en principe pour une période de test) sur une machine "à côté" d'un système DOS (ou windows 95) permettant ainsi un "double ou triple boot" (DOS, Windows 95 ou NT). La machine peut (et c'est le cas le plus normal pour un serveur) être dédiée à NT.

Nous disposons actuellement de machines (Cf. bios de la carte mère) capables de booter sur un CD-ROM. L'installation de NT est facilité dans sa partie initiale (vous pouvez sauter l'étape suivante et passer à "L'installation proprement dite").

Début de l'installation sous DOS

- Démarrez la machine sous DOS (une DK système incluant le driver du CDROM fait l'affaire) et utilisez FDISK (ou un produit plus convivial type Partition Magic) pour créer une partition principale (qui recevra NT) et une partition étendue.
  Pour assurer la **sécurité** (cf. paragraphe spécial ci-dessous) et faciliter l'administration, il est souhaitable de découper la partition étendue en autant de volumes que nécessaire, par exemple :
  - un pour les applications partagées (utilisable en lecture par les clients)
  - un pour les comptes utilisateurs (pour leur répertoire personnel, utilisables en lecture/écriture)
  - etc...
  - Exemples de partition :
    - pour 1 disque de 1GO, 300 MO pour le système, 400 MO pour les appli, 300 MO pour les utilisateurs.
    - pour 1 disque de 2.5 GO, 500 MO pour le système, 1 GO pour les appli, 1 GO pour les utilisateurs.
- A l'aide du logiciel (diagnostics/tests/setup) livré avec elle, **testez votre carte réseau** et relevez ses paramètres de configuration (IO address, IRQ) : vous en aurez peut-être **besoin** plus tard !
- Créez **le jeu de DK de boot** (3 DK) en vous plaçant dans le répertoire "I386" du CDROM et en lançant la commande : "winnt /ox". Puis donnez et étiquetez les 3 DK comme demandé.
- Redémarrez sur la DK N°1

Installation proprement dite

- Redémarrez sur la DK N°1 du jeu de DK de boot (ou sur le CDROM, si possible).
- Vous devez choisir entre "reconnaissance automatique du matériel" (entrée)
  ou "non reconnaissance automatique" (I)
  Tentez entrée : WinNT doit reconnaître vos disques, CDROM, carte SCSI ; sinon, consultez la page : Microsoft à http://www.microsoft.com/hwtest/ et recommencez la manip, éventuellement en choisissant une l'autre option qui, elle, vous permettra de spécifier manuellement le type de votre CDROM par exemple.
- Il vous proposé un descriptif de votre configuration : acceptez
- Choisissez la partition sur laquelle va être installé le système WinNT (en principe C)
  Péférez un formatage NTFS. Vous pourriez le faire plus tard mais le plus tôt est le mieux.
- Acceptez le nom du répertoire d'installation (WINNT)
  Acceptez l'examen du disque (~scandisk)
  La copie des fichiers sur le disque dur démarre. Elle s'achève par une proposition de redémarrage.

Configuration

- Redémarrage sous Windows NT
- indiquez vos Nom/Société
  Choisissez le mode de licence clients (par serveur=nombre maximum de connexions simultanées sur le serveur ; par siège=nombre de postes connectés)
- affectez un nom au serveur ex. : NT4S
  indiquez le type de serveur (principal/secondaire/autonome) ; si c'est le seul dans le domaine, probablement : principal
- choisissez le mot de passe de l'administrateur
- selectionnez les composants à installer (comme dans Windows 95)
- Si vous êtes connecté au réseau, indiquez :
  - si vous voulez installer IIS (le serveur Web de NT)
  - le modèle de votre carte réseau et l'emplacement du driver (CDROM pour une carte "classique" ou disquette pour un driver "récupéré" par ailleurs)
  - les protocoles, ex. : TCP/IP, ne pas garder IPX/SPX si vous n'avez pas de NetWare dans votre environnement

- et les services, ex. : tous
- en principe vous n'avez pas de DHCP (service NT d'affectation dynamique d'adresse IP)
- **configurez TCP/IP**
  - Adresse IP : N° IP, masque de réseau, passerelle
  - DNS : Cf. votre administrateur réseau, ex. : domaine = expertweb.fr, DNS = 195.220.59.2
  - Wins, DHCP, Routage : points développés ultérieurement
  - liaisons : ne modifiez celles proposées qu'en connaissance de cause
  - une connexion au réseau s'établit
    ATTENTION :
    vous devez indiquer dans quel domaine vous travaillez (le nom sous lequel seront rassemblées les machines travaillant autour du serveur), ex. : EXPERTWEBNT4
    si vous négligez cette étape importante, vous pourrez ultérieurement modifier le nom du domaine dans Panneau de Config/réseau/Identification/modifier...
- éventuellement, sélectionnez les options d'installation de IIS

- choisissez votre fuseau horaire (Paris) et choisissez la résolution de l'affichage (800x600)
- Puis, l'installation se termine. Un dernier redémarrage et vous êtes sous Windows NT 4 serveur.

Sécurité...

Si vous n'avez pas encore protégé votre serveur par un mot de passe au boot (dans le setup de la machine), **faites-le dès maintenant...**
Vous êtes sous NT4, prêt à enregistrer vos utilisateurs et à installer les applications et autres ressources.
Dans les deux étapes précédentes (installation et configuration) vous avez partitionné votre disque et formaté la partition WinNT en NTFS.
Il est probable que les autres partitions ne sont pas encore formatées NTFS.
Dans un contexte TCP/IP et de réseau ouvert vers l'Internet, vous devez assurer un maximum de sécurité. Cela passe **obligatoirement** par l'utilisation de la sécurité NTFS.
N'attendez pas, réalisez les étapes suivantes :

Formatage NTFS des partitions

- Démarrer/Programmes/Outils d'administration/...
  Administrateur de disque/...
- sélectionnez une partition/Outils/Formatter/...
- Système de fichier : NTFS
  Taille d'unité d'allocation : 512
  nom du volume : à vous de dire
- Démarrer

LES "PERMISSIONS" NT

Au sens "Microsoft NT" de ce terme, sont rattachés les outils permettant de donner (ou ne pas donner) l'accès à une ressource à tel ou tel utilisateur. Les deux notions importantes sont :

- Les **permissions de sécurité** : ce sont des droits (lire, écrire, effacer,...) que l'on pose sur les ressources (fichiers, répertoires, ...)
- Les **permissions de partage** : notion identique à la précédente mais qui ne s'applique que dans le cadre d'un accès au travers d'un "partage" : classiquement un accès via le réseau (depuis un client) à une ressource et décrite sous la forme \\serveur\partage\ressource

Notion d'héritage des permissions

Lorsque vous créerez des sous-répertoires, les permissions de ceux-ci seront héritées du répertoire parent. Il est donc recommandé de bien poser d'emblée les permissions des répertoires racine que vous venez de créer. Attention : ne touchez aux permissions de la partition WinNT qu'en connaissance de cause !

Modifier les permissions

- Explorateur/sélectionnez un répertoire
- Fichier/Propriété/Sécurité/Permissions pour modifier les permissions de sécurité
  ou
  Fichier/Propriété/Partage/Permissions pour modifier les permissions de partage

Quelles permissions poser

- **Répertoires des applications et Répertoires utilisateurs** : (Voir permissions ci après)Gestion des utilisateurs, rubrique "Déclaration / enregistrement des groupes d'utilisateurs" et des utilisateurs
- **Répertoires Système** : en principe, il ne faut pas y toucher ! Les permissions de sécurité par défaut sont bonnes et le plus souvent:

  Administrateurs : Contrôle Total
  Créateur Propriétaire : Contrôle Total
  Opérateurs de Serveur : Modifier
  Système : Contrôle Total
  Tout le monde : Lire RX

Notes

- Il n'est pas gênant d'avoir une permission de partage "Tout le monde : Contrôle Total" si, en dessous, les permissions de sécurité sont suffisamment restrictives
- De même, il n'est pas forcément gênant d'avoir une permission de sécurité "Tout le monde : Contrôle Total" si, en dessus, aucun partage n'est défini.
- Lors des opérations courantes d'administration, il est fréquent que les problèmes soient liés à des accès insuffisants : il est conseillé de porter une attention toute particulière à cet aspect.

Les permissions NT4

Généralités

Pour pouvoir accéder à des répertoires (et plus généralement à des ressources) sur le serveur, l'utilisateur et l'administrateur devront répondre à certaines obligations :

- L'utilisateur devra se présenter au serveur avec une identité (nom d'utilisateur / mot de passe) valide (reconnue du serveur).
- Le répertoire aura été "partagé" par l'administrateur avec des accès (de partage et NTFS) adéquats.
- Le compte de l'utilisateur doit être activé.
- La connexion via le réseau doit être autorisée.
- Si l'utilisateur accède au serveur via un client NT, son poste doit être rajouté au domaine par l'administrateur du domaine
- Pour plus de détails sur ces points, voir pages spécifiques (incluant aussi les pré-requis pour le contrôle de l'environnement des clients voir chapitres sur les préalables)

Les répertoires "applications" sur le serveur

- **Les répertoires**
  Il s'agit là des répertoires offrant des ressources de type "application". On parle d'"applications partagées" ou d'"applications réseau"
- **Permissions sur les répertoires "application"**
  En règle générale, ces répertoires sont accessibles au travers d'un "partage" dont les permissions (partage et NTFS) sont "lecture" pour les "utilisateurs".
  Les exceptions à cette règle sont rares et spécifiques des applications qui les exigent. D'où l'intérêt de réserver un volume (ou un disque) à cet effet et sur lequel on aura d'emblée posé ces permissions à la racine.

Un "espace utilisateur" sur le serveur

- **Le répertoire utilisateur**
  Dans le volume des utilisateurs [ex. : Users (F:)], créez le répertoire personnel du nouvel utilisateur (ex. : F:\Dupont)
- **Permissions sur répertoire "utilisateur"**
  Explorateur / sélectionnez le répertoire de l'utilisateur Dupont/Fichier/Propriété/...
  - **Attributs** éventuellement, modifiez les attributs
  - **Partage**
    Partage/Partagé en tant que/Dupont
    Permissions
    - supprimer les accès à "tout le monde"
    - donner l'accès "Contrôle total" à Dupont
  - Il est judicieux de modifier le "profil" de l'utilisateur "Dupont" en déclarant ce répertoire comme "Répertoire de base".

Un "espace public" sur le serveur

- **Le répertoire public :**
  Typiquement, un répertoire dans lequel on met à disposition de "Tout le monde" certaines ressources.
- **Permissions sur répertoire "utilisateur"**
  Explorateur / sélectionnez le répertoire "public"/ Fichier/Propriété/...
  - **Attributs** éventuellement, modifiez les attributs
  - **Partage**
    Partage/Partagé en tant que/...
    Permissions
    - donner l'accès "Lire" à "Tout le monde"
    - **donner l'accès à l'administrateur**

PERMETTRE LES CONNEXIONS D'UTILISATEURS (SERVEUR NT4)

Au delà de la permission de se connecter, c'est l'ensemble des **droits de l'utilisateur** qui pourront être définis par ce processus.

1. Connexions locales

Vous êtes sur votre serveur et vous voulez vous connecter en tant que "utilisateur autre qu'administrateur".
Vous êtes arrêté par le message "Votre stratégie locale ne vous permet pas de connexion locale sur ce serveur"
En effet, par défaut seul l'administrateur peut se connecter sur la console du serveur. Pour permettre à d'autres utilisateurs de se connecter localement, vous devez faire :

- Connectez-vous sur le serveur (contrôleur de domaine) en tant qu'administrateur.
- Démarrer/Programmes/Outil d'adm./Gestionnaire des utilisateurs/...
  - Stratégies/Droits de l'utilisateur...
    - Droits : **Ouvrir une session localement**/...
      ajouter/indiquer les groupes ou utilisateurs autorisés
      (ou supprimer)

Remarque importante : pour des raisons de sécurité, il est très conseillé de n'accorder ces autorisations de connexion locale qu'avec parcimonie.

2. Connexions réseau

Vous êtes connecté, depuis une station du réseau, sur votre serveur et vous êtes arrêté par le message : "Accès réseau refusé : l'utilisateur ne bénéficie pas du type d'accès demandé sur cet ordinateur"
En effet, par défaut, tous les utilisateurs ne peuvent pas accéder au serveur depuis le réseau, vous devez faire :

- Connectez-vous sur le serveur (contrôleur de domaine) en tant qu'administrateur.
- Démarrer/Programmes/Outil d'adm./Gestionnaire des utilisateurs/...
  - Stratégies/Droits de l'utilisateur...
    - Droits : **Accéder à cet ordinateur depuis le réseau**/...
      ajouter/indiquer les groupes ou utilisateurs autorisés
      (ou supprimer)

Les clients Windows 95 ou Windows 3.11 peuvent entrer dans le domaine sans manipulation particulière.
Les stations de travail ou les serveurs NT doivent être ajoutés manuellement au domaine.

Intégration de machines NT au domaine

- Connectez-vous sur le serveur (contrôleur de domaine) en tant qu'administrateur.

- Démarrer/Programmes/Outil d'administration./Gestionnaire de serveur/...
- Ordinateur/Ajouter au domaine...
- Indiquez la nature du poste
  (station/serveur/contrôleur secondaire de domaine)
  et son nom.

MISE EN OEUVRE DES PROFILS POUR CLIENT NT4

La "stratégie" décrite ici consiste à :

- utiliser un groupe global rassemblant les utilisateurs
- déclarer un utilisateur générique pour définir l'environnement des utilisateurs du groupe
- dupliquer puis verrouiller ce profil ainsi généré
- affecter ce profil au groupe

En pratique :

connecté sur le serveur en tant qu'administrateur :

1. créer un groupe (G) pour les utilisateurs, sans membres (pour l'instant)
2. créer un utilisateur générique (UG), destiné à moduler l'environnement des utilisateurs, et le mettre dans le groupe G.
3. donner à ce groupe (G) le droit de se connecter localement

connecté sur le serveur en tant que "UG" :

4. créer l'environnement souhaité.

connecté sur le serveur en tant qu'administrateur :

5. rechercher le répertoire des profils (en principe, WinNT\Profiles),3
   et y créer un sous-répertoire du nom du groupe (ici, WinNT\Profiles\G), destiné à recevoir le profil des utilisateurs et vérifiez les accès.
6. vérifier que le profil de UG a bien été mémorisé dans le répertoire des profils (ici, WinNT\Profiles\UG)
7. dupliquer le profil :
   - Panneau de configuration/Système/Profils utilisateurs
     Sélectionnez le profil préalablement défini (UG)
     Copier vers...
     - parcourir...
       et indiquer le répertoire des profils
       (ici : D:\WinNT\Profiles\G)
     - modifier...
       et indiquer le groupe ou l'utilisateur pour lequel le nouveau profil est ainsi défini (ici, 9le groupe G)
8. "verrouiller" le profil :
   dans le répertoire du profil du groupe G (D:\WinNT\Profiles\G) ainsi créé,
   renommer le fichier ntuser.dat en **ntuser.man**
   qui deviendra ainsi obligatoire
   Note : ce nouveau profil n'apparaîtra dans l'onglet "Profils utilisateurs" qu'après une première connexion l'utilisant
9. affectation de ce profil à un utilisateur :
   utiliser le "Gestionnaire des utilisateurs pour les domaines"
   pour créer ou modifier un utilisateur :

- **Chemin du profil**
  Indiquez le répertoire créé dans l'étape précédente
  sous la forme obligatoire :
  \\nom_de_serveur\nom_de_partage\nom_de_répertoire
  (ici : \\nt4S\Profiles\G)
- **Nom du script d'ouverture**
  A la connexion, il est possible d'exécuter automatiquement un certain nombre de tâches. Ces tâches peuvent être décrites dans un script. Ce script peut-être un ".bat", un ".exe" ou un ".cmd". Indiquez ici le nom du script éventuellement défini pour l'utilisateur (ou le groupe)
- **Répertoire de base**
  Si vous en donnez un, c'est le répertoire dans lequel l'utilisateur viendra poser (par défaut) ses données. L'utilisation de cette option a pour but de centraliser et donc faciliter les sauvegardes des "données utilisateur"

10. autorisez l'utilisateur à ouvrir une session sur le réseau (voir permettre les connexions utilisateurs)

IMPRIMANTES DEFINITIONS

Il faut distinguer deux types d'imprimantes :

- Celles qui sont directement rattachées à une machine, en général par le port "parallèle", et qui sont dites **locales**, même si elles peuvent ensuite être mise à disposition d'autres machines par tel ou tel moyen.
- Celles qui sont connectées à un réseau, en général ethernet et intégrant donc un adaptateur ethernet, et qui sont dites **réseau** ; elles ne sont plus rattachées à un poste mais partagées par une communauté via un serveur d'impression qui se charge de piloter le service impression.

Les imprimantes en Réseau :

Dès lors qu'elle est connectée à un réseau, en général ethernet et intégrant donc un adaptateur ethernet, une imprimante **doit** être gérée par un serveur d'impression qui se chargera de réceptionner les **requêtes d'impression** émises par les utilisateurs et de les gérer (les faire imprimer par l'imprimante).

Imprimante3

objet logique installé sur un serveur d'impression.

Périphérique d'impression

l'imprimante elle même ; réseau ou non.

Serveur d'impression

La machine (NT4 serveur) sur laquelle on installe l'imprimante.

Clients Microsoft

Pour les machines Windows 95 ou NT connectées au serveur d'impression, il suffit d'ajouter une nouvelle imprimante (Cf. Démarrer/Paramètres/Imprimantes) et de la connecter au port "imprimante". Le driver est alors hérité du serveur.

Client NetWare

Une machine utilisant une imprimante gérée par un serveur d'impression Netware. L'administrateur devra installer et activer le service réseau "nwsvc"

Client Unix

Un utilisateur Unix désirant accéder à un périphérique géré par un serveur NT4. L'administrateur devra installer et activer le service réseau "lpdsvc"

IMPRIMANTES INSTALLATIO N

- L'impression peut s'appuyer sur les trois protocoles NetBeui, TCP/IP, IPX/SPX.
  Ici, nous privilégions la solution TCP/IP
- Il s'agit d'activer le service NT4 qui assurera les communications entre le serveur NT4, les clients et les imprimantes réseau

1/Installation du service impression TCP/IP

- Connectez-vous sur le serveur en tant qu'administrateur.
- Cliquez l'icône Voisinage réseau avec le bouton droit de la souris/Propriétés
- Services/Ajouter/Impression MS TCP/IP
- Les fichiers nécessaires sont copiés depuis le CDROM sur le disque et vous devez redémarrer
- Vérifiez dans Panneau de configuration /Services que ce service a bien démarré.
  Sinon :
  - sélectionnez le service ("Serveur d'impression...")
  - Démarrage/Automatique/OK
  - Démarrer

2/Ajout d'une imprimante sur le réseau

Prise en compte par le serveur NT

- Connectez-vous sur le serveur devant gérer l'imprimante en tant qu'administrateur.

- Panneau de configuration/Imprimantes/Ajout
- Indiquer que l'imprimante est gérée par "cet ordinateur"
- Selon la nature de votre imprimante :
    - Imprimante connectée au port série du serveur
        - sélectionner le port LPT1
    - Imprimante réseau (dotée d'un port ethernet)
        - Ajouter un port/port lpr
        - serveur lpd : N°IP ou nom DNS de votre imprimante
        - nom de l'imprimante : donner un nom à la file d'impression qui sera utilisé par les utilisateurs (ex. : HP_laser_Jet)
- Sélectionnez le modèle d'imprimante (éventuellement via "disquette fournie")
- Les copies des drivers sont alors effectuées puis, les fichiers (NT) nécessaires sont copiés depuis le CDROM sur le disque

Mise à jour de la configuration
ajout de "pilotes supplémentaires"

L'installation faite, vous pouvez revenir sur les paramètres de configuration de l'imprimante :

- Connectez-vous sur le serveur gérant l'imprimante en tant qu'administrateur.
- Panneau de configuration/Imprimantes
- Sélectionnez l'icône de l'imprimante/Fichier/Propriétés
  Vous pouvez alors intervenir au niveau des onglets spécifiques de votre imprimante, parmis lesquels :
    - **Ports** : pour éventuellement modifier les paramètres du port spécifiés à l'installation du driver (Cf. ci-dessus)
    - **Partage** : pour donner l'accès aux clients (imprimante partagée en tant que ...)
    - **Pilotes supplémentaires** : pour installer sur le serveur NT les pilotes qui serviront aux clients (Windows 95, par exemple). Vous devrez alors fournir une DK (ou un chemin réseau) contenant ces pilotes (Cf. DK livrées avec le matériel).
      A titre d'exemple, Cf. paragraphe ci-dessous pour l'installation/configuration côté serveur et l'utilisation côté client.

Utilisation d'une imprimante gérée par un serveur NT4 (Coté client)

Un serveur NT peut gérer des imprimantes réseau. Il abrite alors **les pilotes des imprimantes**
Ainsi, une fois installés sur le serveur ceux-ci seront **automatiquement téléchargés sur le client à la connexion** (au démarrage du client).

Installation sur un client
Windows 9x, NT4

- Connectez-vous sur le client
- Poste de travail/Imprimantes/Ajout d'une imprimante
- Sélectionnez "Imprimante réseau"
- Indiquez le chemin réseau de l'imprimante : "Parcourir" ou \\nom_du_serveur\nom_de_partage_de_l_imprimante
- Cochez "Imprimante par défaut"

GESTION DES IMPRIMANTES

"Pcounter for NT" est un logiciel de comptabilité de l'utilisation des imprimantes du réseau. Nous vous conseillons l'essai (gratuit pendant 45 jours) de ce logiciel facile à installer et configurer et qui répondra à beaucoup de vos attentes :

- Comptage des sorties imprimantes (toutes les imprimantes du domaine et du réseau)
- Production de statistiques par imprimante, par utilisateur, par groupes d'utilisateurs,...
- Positionnement de "crédit" d'impression par utilisateur avec possibilité de bloquer les sorties en cas de dépassement
- Fixation du prix de la page imprimée (par format de papier) et autres éléments permettant une facturation.
- L'installation sur le serveur NT (connecté en tant qu'administrateur) consiste à lancer un nouveau service

Mise en oeuvre

- Récupérez l'archive chez pccounter.com
- Laissez vous guider par le programme d'installation.
- Démarrer/Programmes/Pcounter/Pcounter configuration
  vous permet d'installer et lancer ce nouveau service, puis d'indiquer les sorties de quelles imprimantes vous souhaitez comptabiliser et comment (fixation des éléments de facturation).
- Démarrer/Programmes/Pcounter/Waccount
  vous permet de visualiser la "balance" des "crédits" et des "charges" (de les modifier éventuellement) et de produire des états de dépenses.

LA MEMOIRE VIRTUELLE SUR SERVEUR NT4

La mémoire virtuelle se matérialise par le **fichier d'échange pagefile.sys** qui se trouve, en général, à la racine de la partition système.
Pour un bon fonctionnement de NT, la mémoire virtuelle doit être bien configurée et surveillée de temps à autre.

A savoir

- Rappelons tout d'abord que "plus il y a de RAM, mieux c'est"
- La mémoire virtuelle doit être suffisante
- Elle peut être dispersée sur plusieurs volumes
- Elle peut être sur un disque différent de celui du système (c'est même recommandé pour améliorer les performances)

- Il est très recommandé de la définir sur un disque dont l'occupation est stable et pas trop plein (un résidu de la partition DOS ou une partition réservée au système)

Surveillance/modification
de la mémoire virtuelle

- Connectez-vous sur le serveur en tant qu'administrateur.
- Panneau de Config./Système/Performances/...
- Mémoire virtuelle/Modifier...(avec modération)...

REPARATION D'URGENCE (SERVEUR NT4)

Lorsqu'il démarre, NT mémorise automatiquement la configuration dès lors qu'il n'a pas eu de problème pour démarrer. C'est **la dernière bonne config connue** ou "last known good (ou LKG)". En cas de fausse manip d'administration, par exemple, il est possible de récupérer cette LKG au redémarrage de la machine. Le problème est qu'il faut se rendre compte de cette fausse manip rapidement, en tous cas avant d'avoir redémarré ...sinon, on mémorise une mauvaise configuration.
Il est donc prudent de ne pas trop compter sur cette LKG et de descendre cette configuration sur une **DK de réparation d'urgence** qui permettra de revenir sur cette config en cas de gros problème.

I/ Restauration de la dernière bonne config connue

- pour avoir le temps de répondre calmement aux questions lors du prochain redémarrage :
  Panneau de configuration/Système/Profils matériels/
  Attendre indéfiniment le choix de l'utilisateur
- redémarrer la machine et **appuyez sans attendre sur la barre d'espace dès que le message "os loader" apparaît**
- un premier menu vous permet de sélectionner l'option "B" pour basculer sur la dernière bonne configuration connue
- un second menu vous permet de sélectionner l'option "Entrée"
- le système se charge alors en utilisant la LKG.
  Un message en fin de boot vous en averti.

II/ La DK de réparation d'urgence

- **Création de la DK de réparation d'urgence**
  - avec l'explorateur, chercher l'utilitaire **rdisk** dans le répertoire WinNT\System32
  - l'exécuter et sélectionner l'option "créer une DK..."

- **Mise à jour de la DK de réparation d'urgence**

Il est évident que la mise à jour de cette DK devra être faite aussi souvent que touchez à la configuration de WINNT. Sinon, lorsque vous "réparerez d'urgence" vous aurez perdu toutes les modifications depuis la création de la DK...

- avec l'explorateur, chercher l'utilitaire **rdisk** dans le répertoire WinNT\System32
- l'exécuter et sélectionner l'option "Mettre à jour..."

- **Réparation d'urgence**
  - insérez le CDROM NT dans le lecteur
  - booter NT4 avec la 1ère DK de boot
  - à la demande mettre la deuxième et **répondre R (réparer une installation...) au menu proposé**
  - 4 taches de réparation sont alors proposées. Sélectionnez celles qui vous semblent appropriées ou gardez les 4 si vous êtes dans l'expectative.
  - à moins que vous n'ayez des périphériques "spéciaux", acceptez la reconnaissance automatique de ceux-ci (tapez "entrée")
  - insérez, à la demande, la 3ème DK de boot
  - insérez, à la demande, la DK de réparation d'urgence.
  - sélectionnez les fichiers qui vous semblent devoir être restaurés, ou tous, si vous êtes dans l'expectative.
  - croisez les doigts et rebootez

SECURITE PHYSIQUE DU POSTE

Pour un poste de travail dont l'accès n'est pas complètement contrôlé (c'est pratiquement toujours le cas) et en particulier les postes type "libre-service"

- Fixez le poste et les périphériques. Des dispositifs dissuasifs sont commercialisés.
- Si besoin, verrouillez lecteur de CD et de DK.
- Paramétrez le bios :
  - Exigez un mot de passe pour rentrer dans le setup du bios.
  - Séquence de boot commençant par C:\ à l'exclusion de la DK ou du CDROM
  - Relevez les principaux paramètres du bios en particulier ceux du disque dur (cylindres, têtes, secteurs,...) et consignez les.
- Maintenir le disque dur par des "scandisk" et des "defrag" réguliers

Pour un serveur

- Trouvez-lui un local sûr
- Paramétrez le bios :
  - Exigez un mot de passe au boot
  - Séquence de boot commençant par C:\ à l'exclusion de la DK ou du CDROM
- Maintenir le disque dur par des "scandisk" et des "defrag" réguliers

- Protégez-le par un onduleur

SECURITE PAR UN MOT DE PASSE

On a encore rien inventé de plus simple et efficace pour protéger (un peu) ses données. Encore faut-il qu'il soit digne de ce nom.

- Mot de passe du bios de la machine : il pourra être simple surtout s'il n'est utilisé que pour protéger le setup (il faudra s'en souvenir quand on en aura besoin, peut-être dans plusieurs mois)
- Les mots de passe "utilisateurs" devront suivre quelques règles simples
    - Un mot de passe doit être facilement mémorisable
    - Il doit être assez long (8 caractères) et contenir au moins un caractère "spécial"
    - Exclure les mots d'un dictionnaire, et en particulier les noms propres, prénoms, ...
    - Le plus simple est d'utiliser les initiales des mots d'une phrase, une maxime, un proverbe, ...
    - Il est difficile de maintenir avec certitude la confidentialité absolue d'un mot de passe. Changez-en de temps en temps !
    - Si vous devez gérer de nombreux mots de passe, et pour éviter le gros "trou de mémoire", consignez-les sous enveloppe cachetée

SECURITE DU SYSTEME ET DES DONNEES

Client Windows 9x, NT, W2K utilisé par UN utilisateur

Son propriétaire, en général. Il s'agit de le protéger d'une panne matérielle ou logicielle, d'une maladresse de sa part, d'une intrusion.

- Le seul "mot de passe" susceptible de protéger le poste est celui posé dans le **bios** de la machine. Eventuellement celui de la bannière d'**authentification NT** à condition que cette authentification soit "obligatoire".
- Saine gestion
  - Virus / Anti-virus
  - Installations : installez les applications dans des /s répertoires spécifiques, gestion des licences,...
  - Ne pas installer de logiciels inutiles ("juste pour voir"), même après désinstallation, il en reste toujours des traces. Utilisez pour cela une machine "de test".
  - Désinstallations : utilisez les programmes de désinstallation, utilisez Panneau de config/Ajout-suppression de pg,...
  - Pour un poste client d'un serveur NT, sensibiliser l'utilisateur à l'utilisation d'un "vrai mot de passe", à se déloguer à la fin de son travail, ...
- Sauvegardes
  - Des données (Cf. : AutoSav32)
    - Utilisez un répertoire spécifique pour les données
    - Créez des procédures de copie automatique de ce répertoire (DK, autre disque, réseau,...)
    - Placez ce répertoire sur un serveur protégé par des solutions d'archivage.
  - Des fichiers sensibles : utilisez les procédures valables pour les données, pour les fichiers vitaux du système et de quelques applications (les .ini)
  - De l'ensemble du poste : "image disque" (Cf. : Norton Ghost)

SECURITE : VIRUS / ANTIVIRUS

Virus

Il faut savoir qu'un virus est toujours un programme, ou un morceau de programme caché à l'intérieur d'un autre, et qu'il doit s'exécuter pour exercer son action nocive.

Transmission

Un virus peut être véhiculé par des **messages Internet**, mais généralement dans des **documents attachés**. Ce peut être un **programme** que le message vous suggère de lancer pour une raison ou une autre (par exemple HAPPY99), parfois en se camouflant sous l'apparence d'un **simple texte** (cas du virus ILOVEYOU). Certains **programmes de courrier** exécutent tout seuls des scripts lors de la réception de messages textuels, mais les virus sont alors spécifiques du programme de lecture. En novembre 99, est apparu un virus se déclenchant à la simple réception d'un message le contenant, si on utilise une certaine version de Microsoft Outlook Express. Il

est possible, mais non avéré, que des virus se cachent dans des **messages codés en HTML** si ce code contient des scripts (en Javascript ou Jscript). Le **carnet d'adresses**, surtout s'il est bien rempli, surtout celui d'Outlook, est un facteur aggravant.
Le risque est le même que lorsqu'on **consulte des sites WWW**.
Le programme peut aussi être caché dans des **macros Excel ou Word** (cas le plus courant ; et les macros sont bien de petits programmes). Le fait de double-cliquer sur le document Word peut dans certains cas faire exécuter la macro, et donc le virus. Tant qu'on n'exécute pas la macro, il n'y a aucun problème.

Annonces et fausses annonces

Dans le cas des annonces de virus, il faut savoir qu'il existe des **organismes spécialisés** dans les problèmes de sécurité, qui ont des **correspondants** dans chaque grand site. Ce correspondant reçoit des **messages d'alerte sûrs**, qu'il peut retransmettre. Sur ce sujet, il est le seul en qui on puisse avoir confiance. S'il n'y a pas de correspondant de sécurité, demander à l'ingénieur réseau ou système. Les utilisateurs isolés peuvent demander à leur fournisseur de services Internet (provider).
En cas de **fausse alerte** c'est le message lui-même qui est le virus, car il pollue les boîtes aux lettres, les réseaux, et fait perdre du temps à celui qui les traite.

Prophylaxie

Les systèmes antivirus sont relativement inefficaces, car les virus se répandent aujourd'hui tellement vite que ces systèmes sont pris de court.
Le serveur de messagerie du EXPERTWEB est protégé par un logiciel antivirus qui repousse les messages pollués. Cependant on ne peut pas se contenter de cette protection pour se prémunir des virus.
Il est donc impératif de respecter quelques consignes simples.

- Il vaut mieux utiliser un programme de courrier n'exécutant pas de script (Eudora, Netscape Messenger avec Javascript désactivé).
- Il faut réfléchir à deux fois avant de double-cliquer sur un fichier attaché.
- Ne jamais rediffuser de messages émanant de personnes non compétentes sans avoir consulté les services Web consacrés à ce sujet (Ex. : voir à http://www.symantec.com/region/fr/avcenter/index.html Symantec) ou posé une question sur AltaVista ou un autre moteur de recherche, ce qui renseigne parfois en dix secondes. Eventuellement informer ceux qui les ont envoyés de l'erreur qu'ils ont faite.
- Pour les fichiers Word, une prévention simple consiste à les ouvrir avec un autre logiciel compatible, car dans ce cas les macros ne sont pas actives.
  Si on est prévenant à l'égard de ses correspondants, on évitera d'envoyer des fichiers attachés au format Word ; Chaque fois que cela sera possible on préfèrera le format RTF voire du texte coupé/collé dans le corps même du message.
- Evidemment, installer un antivirus et apprendre à faire la mise à jour du fichier de signatures des virus pour se protéger contre les virus récents (LiveUpdate ou signatures (miroir du CCR)).

CLIENT WINDOWS 9X, NT DE TYPE "LIBRE SERVICE"

Un parc de PC livré à des étudiants par exemple. Les risques de panne, de maladresse existent mais les risques de malveillance sont plus graves encore. Les règles données dans le contexte "client Windows 95 propre à un utilisateur" s'imposent encore ; mais pour le reste, deux stratégies (que l'on aura intérêt à utiliser simultanément) sont possibles :

- L'utilisation d'un serveur NT pour limiter et contrôler les connexions et l'utilisation du poste. Cette méthode est lourde à mettre en oeuvre mais nécessite moins de maintenance que la seconde.

- L'utilisation d'un logiciel permettant de créer et restaurer une "image" du disque. Utilisée seule, cette méthode oblige à des restaurations fréquentes. Utilisée en complément de la première méthode, elle constitue une assurance de remise en oeuvre rapide d'un poste "cassé".

Utilisation d'un serveur NT pour mettre en œuvre une "stratégie système"

Il s'agira de poser des "restrictions" aux possibilités offertes par le poste.

- Installez, tant que faire se peut, les applications sur le serveur NT et ce dans un volume en accès "lire" seulement. Cf. pages "Mise à disposition des applicatifs" NT4, W2K
- Utilisez les restrictions permettant de contrôler les connexions et l'utilisation du poste clients (NT4, W2K)
    - Interdire l'utilisation du poste sans authentification.
    - Créer un profil pour chaque type d'utilisateur n'offrant QUE les possibilités requises
    - Supprimer l'explorateur
    - Modifiez la "base des registres" pour positionner "de force" les répertoires de données
- Sauvegarde des données
    - Sensibiliser l'utilisateur à faire ses propres sauvegardes
    - Placez les répertoires de données sur le serveur et protégez-les par des solutions de sauvegarde.

Sauvegarde de l'ensemble du poste : "image disque"

SECURITE DU SYSTEME ET DES DONNEES

Serveur NT4

Si la sécurité physique de l'ordinateur est assurée, les risques majeurs sont la panne, un mauvais contrôle de l'accès au serveur (permissions), en particulier au système, et l'intrusion.
Entre-autres solutions :

- Le risque de panne matérielle (et système) peut-être couvert par le maintient d'un deuxième serveur. C'est lourd ; une alternative moins lourde consiste à maintenir UN serveur, en sauvegarder l'image sur une deuxième machine identique qui pourrait être mise en oeuvre rapidement en cas de panne de la 1ère.
- Contrôle des permissions accordées aux utilisateurs
- Minimiser le risque et repérer l'intrusion

ASSURER LA SECURITE...

du système et des données

Les "bons" accès sur un serveur

Il n'y a pas de bonne solution à ce problème. Cela ne veut pas dire qu'elles sont toutes mauvaises, tout est question d'équilibre entre risques. Trop de restrictions rend la vie impossible aussi bien à l'administrateur qu'aux utilisateurs. Trop peu de permissions laisse le champ libre aux maladroits, aux plaisantins et aux margoulins. Les permissions standard posées par NT sont ni trop restrictives, ni trop permissives : elles sont un (juste) milieu. Selon vos besoins et votre contexte, vous trouverez toutes précisions sur le sujet à la source, chez Microsoft, à http://www.microsoft.com/ntserver/security/exec/overview/Secure_NTInstall.asp paragraphe "Protecting files

and directories"
Au registre des solutions simples à mettre en oeuvre :

- La sécurité **NTFS est l'essentiel** de la protection classique liée aux aléas de l'accès des utilisateurs aux ressources du serveur
- Partitionnez d'emblée votre disque de façon à séparer le système des applications et des répertoires utilisateur. Quand on crée un répertoire fils celui-ci hérite des permissions du répertoire père. D'où l'intérêt de prévoir des branches sans accès, en accès lire, en accès lecture/écriture. Accordez les permissions à des Groupes plutôt qu'à des utilisateurs
- Ne pas toucher aux permissions posées par NT lui même (à l'installation) surtout sous \Winnt et à fortiori de façon automatique dans les /s répertoires
- L'administrateur devra de temps à autre "faire le tour" des permissions pour en vérifier la conformité y compris des fichiers cachés
- Chaque fois que cela est possible, cachez les répertoires partagés
- Ne pas donner d'autre noms de partage aux répertoires partagés par NT lui-même pour des "raisons administives"

SECURITE DU RESEAU

L'intrusion est le risque majeur. Particulièrement si elle s'opère sur un serveur. L'usurpation d'identité est une circonstance aggravante. Les clients windows 95 n'étant que peu protégés, il faudra mettre en oeuvre une protection au niveau "réseau"

Entre autres précautions utiles :

- Maîtrise et contrôle des connexions et permissions (NTFS) accordées et des partages de ressources (NT, Windows 95)
- Utilisation de caches
- Routage, filtres
- Pare-feu. Lire les infos experlan sur http://security.web-france.com/
-

CONTROLER L' ACCES AU WEB GRACE A UN SERVEUR CACHE

Pré-requis
Un certain nombre de points doivent être acquis avant d'envisager comment contrôler l'accès au Web :

- Etant donné que tout le contrôle est assuré par le serveur cache, le poste ne doit pas pouvoir s'adresser directement à un serveur WWW. Pour cela, on peut positionner des filtres au niveau du routeur afin que le trafic HTTP ne soit possible qu'à destination du serveur cache. Il reste ensuite à configurer le navigateur utilisé sur le poste de travail de manière à interroger le serveur cache. Si on positionne des filtres au niveau du routeur, autant en profiter pour déterminer ce qui doit traverser le routeur (quel type de services, vers quelle destination). Cela permettra de réduire les risques d'attaques.
- Le poste doit être suffisamment protégé afin qu'un utilisateur ne puisse pas en modifier la configuration.

Contrôle d'accès

Principe

Un serveur cache est un serveur qui reçoit les demandes de clients WWW (Netscape, Internet Explorer, Mosaic,...) et qui leur donne les documents demandés (s'ils sont dans le cache) ou va les demander au " vrai " serveur. Il joue donc dans ce dernier cas un rôle de mandataire (proxy en anglais) . Il joue ce rôle vis-à-vis de serveurs HTTP, FTP et gopher.
Il est à noter que les clients WWW ont une fonction de cache sur disque et en mémoire, mais ce cache est personnel. Le cache tel que décrit ici est partagé par de nombreux utilisateurs, et c'est justement son intérêt.
Le logiciel utilisé comme serveur cache au EXPERTWEB est squid.

Plusieurs types d'ACLs (Access Control Lists) peuvent être utilisées lorsque l'on utilise squid comme cache HTTP. On détermine ensuite si, pour une requête correspondant à un type ACL, il faut répondre à la requête ou bien la rejeter, offrant ainsi une large gamme de possibilités.
D'un point de vue pratique, le plus commode est de définir des ACLs utilisant des fichiers de configuration (un regroupant les URLs autorisées, un pour les URLs interdites,...). Il suffit ensuite de rajouter ou d'enlever des lignes dans ces fichiers, sans avoir à modifier les ACLs, qui sont elles assez " sensibles " aux modifications. Par contre, la maintenance des fichiers d'URLs est facile à réaliser (transfert vers le poste local, modification, puis recopie sur le serveur cache).

Les ACLs de squid

Voici les différents type d'ACLs :

1. **Contrôle sur les adresses**
   - source (où se trouve le navigateur)
   - destination (quelle page veut-il lire)

   Ce contrôle peut se faire en spécifiant des adresses IP, des plages d'adresses, des noms de machine ou de domaine. Les noms de domaine sont plus ou moins complets (.fr, .expertweb.fr).

2. **Contrôle sur la plage horaire**
   On spécifie ici le(s) jour(s) de la semaine, et pour chaque jour le couple (heure, minute) de début et (heure, minute) de fin.
3. **Contrôle sur l'URL**
   Une URL (Uniform Ressource Locator) est la référence qui permet d'atteindre une page WWW. Une URL est composée principalement du protocole à utiliser pour récupérer la page (http://), du nom du serveur qui en dispose (www.expertweb.fr) et du chemin pour y accéder (index.html). On peut utiliser une expression régulière (une chaîne de caractères à rechercher) qui s'appliquera soit sur l'URL complet (http://www.expertweb.fr/expertweb/index.html) soit sur uniquement la partie "nom complet du fichier" (/expertweb/index.html). Cette dernière possibilité peut permettre de transmettre ou pas des fichiers selon leur nom ou leur extension (par exemple ne pas délivrer des sons :*.wav).
4. **Contrôle sur l'identité du surfeur.**
   Il faut pour cela que la machine à partir de laquelle le surfeur navigue dispose d'un serveur capable de répondre à des requêtes d'un format particulier (RFC1413-identd), qui peuvent se traduire par : " Dis moi qui utilise cette connexion TCP/IP ? ". Dans notre cas c'est squid qui pose la question au poste de travail. Cette fonctionnalité est surtout utile dans le cas de serveurs où plusieurs utilisateurs sont connectés simultanément.
5. **Contrôle sur le port du serveur**
6. **Contrôle sur le protocole utilisé (à choisir dans HTTP,FTP,GOPHER,WAIS)**
7. **Contrôle sur la méthode (GET, POST, PUT, ...)**
8. **Contrôle sur le navigateur utilisé**

Exemples

Voici quelques exemples de contrôle d'accès que l'on peut mettre en place avec le logiciel Squid. La combinaison de plusieurs de ces exemples est possible.

- **Traitement diffèrent selon la source**
  Le cache a un comportement diffèrent selon l'adresse IP du butineur. Si elle se trouve sur le réseau 130.120.74.0 (reseau_extérieur), les adresses autorisées sont celles listées dans le fichier destinations_autorisees.acl auxquelles on enlève www.bidule.fr. Si l'adresse IP se trouve sur le réseau 192.70.79.0 (reseau_intérieur), tous les serveurs sont accessibles sauf www.bidule.fr.
- **Accès limité dans le temps**
  Pour le réseau 130.120.74.0, le service est fermé du lundi au samedi de 8H à 19H et le samedi de 8H à 12H. En dehors de ces plages horaires, les serveurs autorisés sont ceux listés dans le fichier destinations_autorisees.acl.
- **Traitement sur les noms de fichiers**
  Toutes les urls dont la partie chemin d'accès répond à l'expression régulière " se termine par .jpg ou par .exe " ne seront pas transmises au butineur.

Comment faire

1. Sécuriser un poste (sécurisation du poste lui-même + routage)
2. Faire en sorte que la consultation WWW passe obligatoirement par le serveur cache (filtres sur les routeurs)
3. Installer un navigateur WWW s'adressant au cache Web
4. Configurer le cache WWW (définir les ACLs)
5. Faire évoluer la configuration du cache (en modifiant les fichiers de configuration plutôt que les ACLs).

Cette dernière étape sera certainement la plus contraignante, selon la configuration qui sera mise en place. Si le contrôle d'accès sur les adresses autorisées est utilisé, la liste des adresses autorisées devra évoluer rapidement, sous peine d'émeutes ou de tentatives de contournement du système.

CONCEPTS RESEAU ET TCP/IP DANS LE MONDE NT

Tout ordinateur appartenant à un réseau doit être reconnu, identifié. C'est l'objet des notions d'adressage et de nommage. Chaque système de réseau (NetBeui, TCP/IP, NetWare, ...) met en oeuvre ses solutions à ces problèmes. Ici, nous privilégions les solutions orientées TCP/IP transport natif de l'Internet et de loin le plus répandu dans notre environnement.

Adressage / Adresse IP

"Internet Protocol"
Chaque machine d'un réseau doit être identifiée sans ambiguïté. Dans un contexte TCP/IP, c'est l'adresse IP qui remplit cette fonction. Elle se présente sous la forme de 4 valeurs décimales (entre 0 et 255) séparées par un point. En général, les 3 premiers chiffres identifient le réseau et le 4ème identifie une machine dans ce réseau.
Ex. : 193.44.55.234 est l'adresse IP de la machine "234" dans le réseau "193.44.55.0"
Ce paramètre obligatoire de la configuration d'une machine en réseau peut-être donné de façon **statique** (vous rentrez le numéro IP que vous a donné votre administrateur de réseau dans votre machine) ou **dynamique** si vous utilisez le service DHCP d'un serveur NT4.

Nommage

Chaque machine d'un réseau étant identifiée sans ambiguïté par son adresse IP, il est cependant utile de pouvoir utiliser des "noms de machine" pour accéder aux ressources du réseau.
2 types de nommage / serveur de noms :

- **Wins**

  "Windows Name Server"
  Serveur de nom NetBios / Microsoft
  Utilisable malgré-tout par TCP/IP (vs DNS). Minimise les diffusions réseau : pas de broadcast régulier pour obtenir les adresses.

- **DNS**

  "Domain Name Server"
  Serveur de nom TCP/IP Internet

Routage / Routeur

Protocoles de réseau

2 types de protocoles :
Les protocoles Microsoft (NetBios, NBT, ...)
Les protocoles Internet (TCP/IP, SMTP, FTP, ...)

- **TCP/IP**

"Transport Control Protocol/Internet Protocol"
Le protocole de l'Internet.

- **NetBEUI**

  "NetBIOS extended user interface"
  Protocole réseau Microsoft. Protocole de transport au même titre que TCP/IP.

- **NetBios**

  "Network Basic Input Output System"
  Tous les réseaux Microsoft ont été bâtis en utilisant le "protocole" netbios. Il est plus correct de parler d'"interface logicielle".

- **NBT**

  "NetBIOS sur TCP/IP"
  Protocole autorisant les applications écrites avec l'API NetBIOS, à s'exécuter au dessus des couches TCP/IP. Exemple : NET commande

Services réseau

2 types de services :
Les services Microsoft (WINS, partages de ressources, etc...) Les services Internet (DNS, Messagerie, WWW, FTP, etc...).

- **DHCP**

  "Dynamic Host Configuration Protocol"
  Service de configuration dynamique du protocole TCP/IP sur les postes clients d'un serveur DHCP (sous NT4, Unix, ...).

- **DNS**

- **Wins**

TCP/IP

Généralités

Quelque soit la plate-forme et le système utilisés, la mise en oeuvre de TCP/IP peut se résumer à la configuration des 4 éléments suivants :

- **Numéro IP** : c'est le numéro IP (unique) de votre machine qui vous est fourni par votre administrateur de réseau.
- **Masque de sous-réseau** : donnée technique qui dépend de votre réseau et qui vous est fournie par votre administrateur de réseau. En général 255.255.255.0
- **Numéro IP de la passerelle** : c'est le numéro IP (unique) de la porte de sortie de "votre" réseau. Il vous est fourni par votre administrateur de réseau.
- **DNS** (Domain Name Server): C'est un **serveur** qui offre (entre-autres) le **service** indispensable de traduction d'un "numéros IP" en "nom de machine" et vice-versa. Le "domaine" ExpertWeb étant expertweb.fr.

En particulier :

- Windows 95, 98, Millenium
- Windows NT
- TCP/IP dans un contexte PPP (accès Internet via le réseau téléphonique)

ExpertWeb

Systèmes d'information - Ingénierie & Formations

INSTALLATION DE TCP/IP POUR WINDOWS 95, 98, MILLENIUM

1/ Installer la carte réseau

2/ Ajouter la carte à la config Windows 95 :

Panneau de Configuration/Réseau/Ajouter/adaptateur/...

3/ Ajouter TCPIP :

Panneau de Configuration/Réseau/Ajouter/Protocole/...
.../Ajouter/Microsoft/TCPIP/OK/...

4/ Configurer TCP/IP :

Panneau de Configuration/Réseau/TCPIP/Propriétés/...
.../Adresse IP : cf votre administrateur de réseau (Ex. : 130.120.72.201)
.../Adresse de sous-réseau : cf votre administrateur de réseau (Ex. : 255.255.252.0)
.../Configuration WINS/Désactiver la résolution WINS
.../Passerelle : cf votre administrateur de réseau (Ex. : 130.120.72.1)
.../**Configuration DNS :**

- Chaque machine de l'Internet est connue par un numéro IP et un nom de machine uniques. La fonction des "serveur de noms" (DNS : Domain Name Server) est de maintenir la correspondance entre numéros et noms.
- **Votre machine doit-elle être enregistrée dans un DNS ?**
  Oui, car (sécurité oblige) certains serveurs (que vous interrogez) vérifient, avant d'accepter une communication, que votre machine est bien enregistrée dans un DNS.
- **Configuration :**
  - .../Hôte/donner un nom à votre machine (Ex. : pc-dupont)
  - .../domaine/cf votre administrateur de réseau (Ex. : expertweb.fr)
  - .../Ordre de recherche DNS/Numéro IP d'un DNS, cf votre administrateur de réseau

Tél /fax : 0467.42.68.11 -Mobile : 0621.447.851
E-mail : info@expertweb.fr Site web : http://www.expertweb.fr/dotclear/
Avenue de l'AGAU – Le Vivaldi 35 –34970 Lattes

LE PROTOCOLE PPP

- PPP est un protocole d'accès à Internet par lignes asynchrones. Derrière ces lignes asynchrones on peut connecter un modem pour travailler sur le "réseau téléphonique commuté (RTC)" ou une interface RNIS pour travailler à travers Numéris (le service RNIS de FT).
  A ces vitesses (33600, 56600 bits/sec pour un modem, 64000 bits/sec pour une interface RNIS) on peut utiliser le protocole TCP/IP et tous les outils logiciels qui lui sont traditionnellement associés ("navigation", outil de messagerie -Eudora-, les news, ftp, telnet, et même X dans certains cas).

Tél /fax : 0467.42.68.11 -Mobile : 0621.447.851
E-mail : info@expertweb.fr Site web : http://www.expertweb.fr/dotclear/
Avenue de l'AGAU – Le Vivaldi 35 –34970 Lattes