



Jean-Louis Cech / Resp S.I.  
Mairie de Villebon  
Place Gerard Nevers / 91141  
SDA : 01 69 93 49 09  
GSM : 06 62 24 08 69  
FAX : 01 60 14 30 40  
Horaires Accueil 9-12 / 14-17  
jl.cech@villebon-sur-yvette.fr

NOTE D'INFORMATION

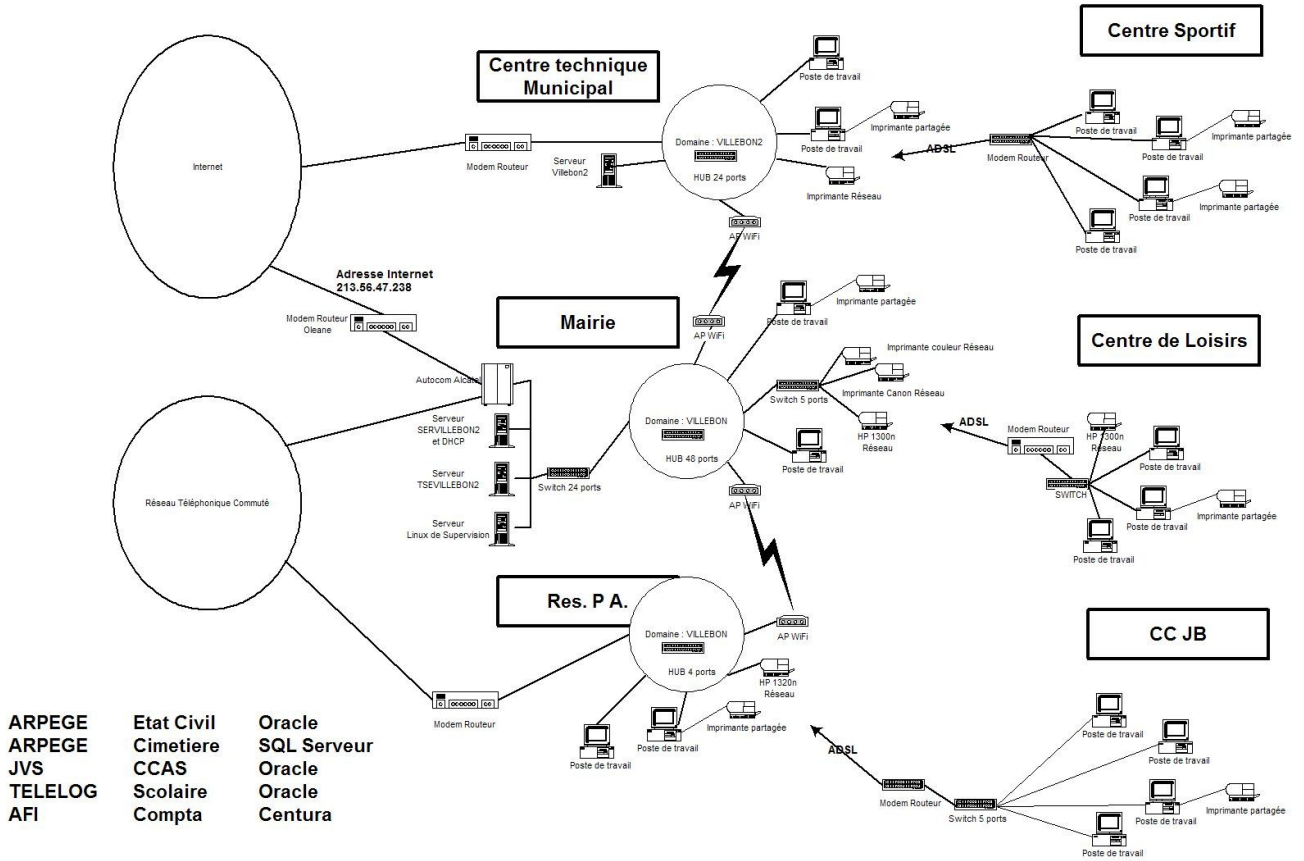
VILLEBON LE : 29/01/07

OBJET :  
ORGANISATION ET ADMINISTRATION  
DU SI / CTM

# Mairie de Villebon

## Architecture globale du Système d'Information

Mairie Système d'Information  
Avril 2006



## TABLE DES MATIÈRES

- 1 - Introduction.....	5
- 2 - Etat des lieux.....	5
- 3 - Machines de remplacement – postes de travail.....	5
- 4 - Machine de remplacement – Serveur.....	5
- 5 - Contraintes liées au poste de travail.....	6
- 6 - Contraintes liées aux logiciels serveur.....	6
- 7 - Coût à ce jour du remplacement.....	6
- 8 - Anti-Virus Version TREND.....	7
- 8.1 - Serveur Anti-Virus Version TREND ( Obsolète ).....	7
- 8.2 - Installation de l'Anti-Virus sur les postes clients Version TREND ( Obsolète).....	7
- 9 - Anti-Virus Version Kaspersky ( Serveur disparu ).....	8
- 9.1 - Serveur Anti-Virus Version Kaspersky ( Sans objet ).....	8
- 9.2 - Installation de l'Anti-Virus sur les postes clients Version Kaspersky.....	8
9.2.1 - Désinstallation de TREND.....	8
9.2.2 - Installation de Kaspersky ( Mode centralisé ).....	8
9.2.3 - Installation de Kaspersky ( Mode local ).....	8
- 10 - Configuration réseau poste client.....	10
- 11 - Installation du serveur.....	10
- 11.1 - Gestion des disques.....	10
11.1.1 - Master IDE 0.....	11
11.1.2 - Disque slave IDE 0.....	11
11.1.3 - Disque master IDE 1.....	11
11.1.4 - Disque slave IDE 1.....	11
- 11.2 - Gestion réseau.....	12
- 12 - Rappel sur les principes de la gestion des fichiers.....	12
- 12.1 - Exemple de droits.....	12
12.1.1 - Exemple 1.....	12
12.1.2 - Exemple 2.....	13
12.1.3 - Exemple 3.....	13
- 12.2 - Changer les droits.....	13
- 13 - Paramétrage du serveur de fichiers Windows.....	13
- 13.1 - Principes mis en Oeuvre.....	13
13.1.1 - Déclaration d'un utilisateur.....	13
13.1.2 - Déclaration d'un machine.....	14
13.1.3 - Fichiers de paramétrage SAMBA.....	14
- 13.2 - Création des utilisateur / PRINCIPES DE BASE.....	14
13.2.1 - Utilisateur Linux - Description.....	14
13.2.2 - Utilisateur Linux – Création utilisateur.....	15
13.2.3 - Utilisateur Linux – Création Work-Station (PC).....	15
13.2.4 - Intégration d'un utilisateur vers SAMBA.....	15
13.2.5 - Intégration d'un Poste de Travail (Work Station / PC).....	16
13.2.6 - Création d'un alias conforme WINDOWS.....	16
- 13.3 - Création d'un fichier de configuration SAMBA.....	16
- 13.4 - Activation du nouveau fichier smb.conf.....	16
13.4.1 - Section [global].....	17
13.4.2 - Section [homes].....	17
13.4.3 - Section [netlogon].....	17
13.4.4 - Section [public].....	17
13.4.5 - Section [warehouses].....	18
13.4.6 - Section [seclurb].....	18
13.4.7 - Section [DOCS].....	18
13.4.8 - Section [Office].....	18
- 14 - Mise en oeuvre.....	19
- 14.1 - Prise de main à distance.....	19
- 14.2 - Création d'un poste dans le domaine.....	21

- 15 - Sauvegarde des données.....	22
- 15.1 - Gestion de la sauvegarde .....	22
15.1.1 - Fichier de configuration.....	23
15.1.2 - Planification des tâches.....	23
15.1.3 - Script de montage des partitions.....	23
15.1.4 - Script de démontage des partitions.....	23
15.1.5 - Script de sauvegarde quotidienne.....	23
15.1.6 - Script de sauvegarde hebdomadaire.....	24
- 16 - Restoration des données.....	24
- 17 - Annexes.....	25
- 17.1 - Chronologie des tâches.....	25
- 17.2 - Montage des partitions .....	26
- 17.3 - Démontage des partitions .....	27
- 17.4 - Sauvegarde quotidienne.....	28
- 17.5 - Sauvegarde hebdomadaire.....	30
- 17.6 - Occupation disque d'un répertoire .....	31

## **- 1 - Introduction**

L'arrêt du serveur NT4 du CTM pour cause de panne ajouté au renouvellement du parc informatique nous a conduit à repenser globalement l'architecture du système d'information de ce service.

L'objectif de cette refonte est triple à savoir

1. gérer une migration qui garantit la pérennité du système d'information,
2. garantir la disponibilité des informations existantes sans modifier les habitudes, us et coutumes du travail collaboratif,
3. maintenir le coût global de cette migration dans un budget minimal.

## **- 2 - Etat des lieux**

Le parc est composé de machines très disparates, Windows 98, NT4, Windows 2000 pro, Windows XP pro.

Avant même le décès du serveur il a été décidé de remplacer tous les CRT (écrans cathodique) ainsi que les PC dont les Systèmes d'exploitation sont obsolètes : Windows 98 et Windows NT4.

Le serveur tournait sous Windows NT4, il est équipé de 2 disques miroirs de 9 Go, non recyclable, il a été mis au rebut.

## **- 3 - Machines de remplacement – postes de travail**

Les PC de remplacement embarquent un disque dur de 80 Go partitionné en 2 partitions de 40 Go. Cette dernière sert de zone de stockage tampon banalisé. Disposant 512 Mo de RAM, en standard, ils ne sont pas équipés de lecteurs de disquette ni de lecteur de CD/DVD, ces périphériques sont disponibles en externe pour des connexions ad hoc, à la demande.

## **- 4 - Machine de remplacement – Serveur**

En prévision du décès du serveur, une machine a été configurée dès le milieu de l'automne avec

- 2 disques durs de 80 Go,
- un OS Linux complet.
- L'environnement SAMBA qui permet l'ensemble des fonctions de partage, protection des fichiers disponible avec un serveur Microsoft.

Les tests ont été menés pendant 4 mois. Connectée au réseau sous un environnement générateur de stress, cette machine n'a présenté aucun glitch de fonctionnement.

L'objectif du présent document est de permettre une administration des fonctions de base par un opérateur moyennement qualifié.

## **- 5 - Contraintes liées au poste de travail**

L'objectif est de permettre à chacun de

- garder un environnement de travail aussi proche que celui qu'il vient de quitter,
- de retrouver toutes les données qui résidaient sur l'ancien serveur,
- si possible récupérer celles qui se trouvent sur le poste de travail, si celui-ci est maintenu en production,
- si possible récupérer celles qui se trouvent sur le poste qui est remplacé.

L'ensemble de ces contraintes ont été respectées, aucun fichier n'a été perdu, seules des altérations de l'arborescence ont été observées.

***Si ces altérations ont provoqué un accès de prurit,  
elles sont sans conséquence repérées  
tant sur le travail passé que celui à venir  
les données étant intégralement restituées.***

## **- 6 - Contraintes liées aux logiciels serveur**

Outre les données personnelles et les données partagées, le serveur héberge les éléments de re configuration de MS Office, cette fonction est requise lors de chaque modification d'un poste de travail. Il héberge ainsi que le logiciel et les bases de données de l'urbanisme, URBAPRO 3.

Parmi les fonctions qui ne sont plus hébergées par le serveur se trouve l'imprimante grand format HP 488CA. Si l'utilité de la connexion de cette imprimante était avérée, cette imprimante sera installée sur un poste utilisateur Windows XP et mise en partage.

## **- 7 - Coût à ce jour du remplacement**

Le coût lié au remplacement du serveur, coût induit par à la fois l'abandon du support de NT4 par MicroSoft et la panne latente du serveur, est NULL.

Ce coût est nul car :

- la machine promue serveur est un poste de travail déclassé, elle était sortie de production,
- l'OS, environnement logiciel système, (Operating System) vient de l'Open Source, il dispense de l'achat de licences, de plus les mises à niveau sont gratuites.

Le coût reste celui lié à la main d'oeuvre, dans tous les cas, MicroSoft ou Linux, il est à engager, le surcoût relève de l'aspect documentation et formation complémentaires.

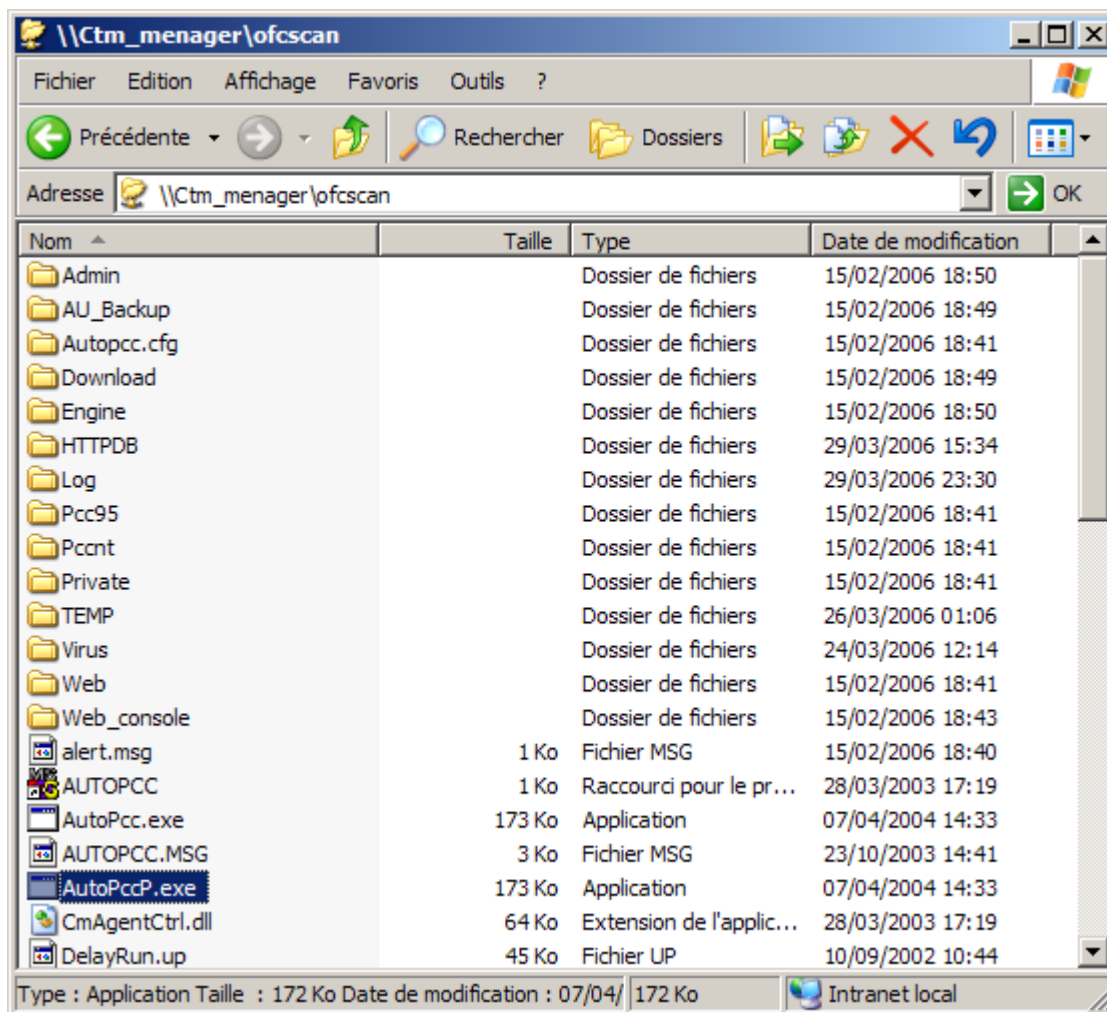
Si le choix serveur classique avait été fait, le coût s'établissait à 1500€ pour le matériel, 1300€ pour les licences.

## - 8 - Anti-Virus Version TREND

L'anti-virus installé est TREND Micro. Celui-ci impose la présence d'un serveur de sécurité sous Windows. Comme le serveur de fichiers Linux ne permet pas de distribuer la sécurité, un poste de travail a été promu serveur de sécurité anti-virus. Il s'agit du poste « **ctm\_manager** ». Celui-ci DOIT rester sous tension en permanence sauf les Samedis et Dimanches.

### - 8.1 - *Serveur Anti-Virus Version TREND ( Obsolète )*

Le répertoire partagé accessible à tous en lecture est :



On le retrouve en ouvrant le « Voisinage Réseau »...

### - 8.2 - *Installation de l'Anti-Virus sur les postes clients Version TREND ( Obsolète )*

Sur le poste Windows il faut créer un raccourci qui pointe vers

**\\Ctm\_manager\ofcscan\AutoPccp.exe**

et le copier dans le répertoire « Démarrage » de « All users ».

Une fois l'installation faite, dans la partie basse à droite de l'écran s'affiche un octogone bleu. Si celui-ci passe en rouge, l'Anti-Virus n'est plus actif ou n'est plus à jour.

## **- 9 - Anti-Virus Version Kaspersky ( Serveur disparu )**

L'anti-virus installé est KASPERSKY. Celui-ci impose la présence d'un serveur de sécurité sous Windows. Comme le serveur de fichiers Linux ne permet pas de distribuer la sécurité, un poste de travail a été promu serveur de sécurité anti-virus. Il s'agit du poste « **ctm\_menager** ». Celui-ci DOIT rester sous tension en permanence sauf les Samedis et Dimanches.

### **- 9.1 - Serveur Anti-Virus Version Kaspersky ( Sans objet )**

Pas encore formalisé.

### **- 9.2 - Installation de l'Anti-Virus sur les postes clients Version Kaspersky**

L'installation de la fonction anti-virus est désormais une fonction « locale » à chaque poste de travail. Chaque poste est responsable de ses propres mises à jour en les récupérant sur Internet.

#### **9.2.1 - Désinstallation de TREND**

- Passer le poste de travail en mode administrateur.
- Créer un compte root local avec comme PW FG73TY
- Désactiver le pare-feu.
- Lancer la désinstallation de TREND. Rebooter le PC à la demande en fin d désinstallation.

#### **9.2.2 - Installation de Kaspersky ( Mode centralisé )**

- Depuis la console serveur repérer le PC client à installer et le sélectionner.
- Dans le cartouche des commandes, lancer l'installation.
- Sélectionner la version WKS (WorkStation)
- Choisir l'identité root et le pw FG73TY
- En fin d'installation lancer Kaspersky Anti-Virus par Programme démarrer, mettre à jour la base de données des virus et lancer un Scan du poste de travail.
- En fin de scan, sur la console serveur, le PC nouvellement installé passera en « VERT » suite à une Synchro.

#### **9.2.3 - Installation de Kaspersky ( Mode local )**

1. Lancer le fichier exécutable xxxwks.exe
2. Accepter le répertoire implicite de décompression.
3. A la demande du programme d'installation fournir la clé d'enregistrement.
4. Rebooter si demandé et exécuter les mises à jour de l'anti-virus.
5. Lancer puis paramétrer la périodicité des mises à jour et



vérification du poste de travail.

## **- 10 - Configuration réseau poste client**

Le poste client, PC, est paramétré comme suit, cette configuration doit prendre en compte la présence du lien WiFi avec la Mairie. Dans ce cas l'affectation de l'adresse fixe doit intégrer l'ensemble des adresses IP utilisées sur l'ensemble du sous-réseau. Un accès spécifique local ADSL est disponible.

<b>Désignation</b>	<b>Valeur</b>
Adresse poste	10.10.10.xx où 1<xx<254 selon le plan d'adressage
Masque sous réseau	255.255.255.0
Passerelle par défaut	10.10.10.9
DNS	10.10.10.9
Serveur Wins	10.10.10.159

A la date de rédaction du présent document la messagerie électronique reste assurée par le serveur de la Mairie, les accès courriel restent dépendants du lien WiFi. Dans le cas de la mise en place d'un réseau privé virtuel, VPN, il conviendra de se reporter aux spécificités du paramétrage.

## **- 11 - Installation du serveur**

L'objectif de ce document n'est pas de permettre à un technicien non familier à Linux de réaliser cette installation, mais de permettre à un « Linuxien » moyennement averti de reprendre la main pour l'administration au jour le jour.

L'OS installé est la FEDORA 1B, elle est installée en mode texte. Les supports, 3 CD, sont disponibles à l'atelier. Les trois CD de la distribution FEDORA 1B sont requis. En cas de remplacement ou ré installation toute distribution validée pour ce type de PC promu serveur fera l'affaire.

Afin de préserver la possibilité de réinstaller le système sans mettre en danger les données utilisateur, un partition est réservée à **/home**.

Le partitionnement est réalisé « à la main » afin de garantir un niveau de performances optimales.

### **- 11.1 - Gestion des disques**

Les quatre tableaux ci-dessous décrivent l'organisation des ports IDE du serveur. Les disques durs sont au nombre de 3 DD

1. Master IDE0 : disque de 4 Go
2. Slave IDE0 : lecteur de CD
3. Master IDE1 : disque de 80 Go
4. Slave IDE1 : disque de 80 Go

L'objectif de cette répartition est, au plan des performances, de limiter les déplacements de têtes des disques durs et au plan de

la sécurité, permettre les sauvegardes de données sur 2 partitions logées sur 2 disques différents.

### 11.1.1 - Master IDE 0

Ce disque héberge le noyau dans **/boot**, il permet le **SWAP**, c'est sa seule activité en production.

Nom unité	Point de montage	Taille
/dev/hda1	Partition Windows	2 Go
/dev/hda2	/boot	256 Mo
/dev/hda3	Zone réservée	1 Go
/dev/hda4	SWAP Linux	256 Mo

### 11.1.2 - Disque slave IDE 0

Nom unité	Point de montage	Taille
/dev/hdb1	CD ROM	N/A

### 11.1.3 - Disque master IDE 1

En production quotidienne, ce disque héberge les données utilisateur dans le répertoire **/home**, s'y ajoutent les logiciels utilisés en mode partagé par les postes de travail Windows, URBAPRO, le CD MSOffice..., dans **/opt**. Les sauvegardes hebdomadaires sont hébergées dans **/dev/hdc3** qui est monté dans l'arborescence à la demande par le script de back-up décrit plus bas.

Nom unité	Point de montage	Taille
/dev/hdc1	/home	16 Go
/dev/hdc2	/opt	8 Go
/dev/hdc3	Zone réservée back up	54 Go

### 11.1.4 - Disque slave IDE 1

En production quotidienne, ce disque héberge les programmes et répertoires système. La séparation physique programmes<->données permet d'envisager la ré-installation du système sans écraser les données utilisateur. Les sauvegardes quotidiennes sont hébergées dans **/dev/hdd2** qui est monté dans l'arborescence à la demande par le script de back-up décrit plus bas.

Nom unité	Point de montage	Taille
/dev/hdd1	/	16 Go
/dev/hdd2	Zone réservée back up	64 Go

## **- 11.2 - Gestion réseau**

la machine emprunte l'adresse et le nom NETBIOS du serveur qu'elle remplace. Les paramètres clés du réseau sont les suivants :

- DHCP : pas activé pour le serveur, si un DHCP s'avère nécessaire, cette fonction sera réalisée par le routeur INTERNET.
- Adresse serveur : 10.10.10.159
- Masque sous réseau : 255.255.255.0
- Passerelle par défaut : 10.10.10.9
- DNS : 10.10.10.9
- Nom NETBIOS : urba\_st
- Chargement et activation du serveur telnet
- Chargement et activation du serveur VNC.
- Chargement et activation du serveur SAMBA.

Accessoirement la machine est promue serveur WINS.

## **- 12 - Rappel sur les principes de la gestion des fichiers**

Un fichier possède 3 classes d'utilisateurs :

- le propriétaire,
- le groupe,
- le reste du monde.

Chaque classe dispose de droits de lecture, écriture, exécution sur un fichier donné. La notion d'exécution s'applique aux scripts et aux répertoires. Dans ce cadre pour une classe donnée les valeurs possibles vont de 0, dans ce cas aucun droit à 7 pour tous les droits.

Les droits d'accès sont définis comme suit.

- Le droit de lecture vaut 4, il est repéré par la lettre R
- l'écriture vaut 2, il est repéré par la lettre W
- l'exécution vaut 1, il est repéré par la lettre X.

Par exemple 4 signifie lecture seule, 6 lecture et écriture. Les droits d'accès à un fichier sont donc décrits par la combinaison de 3 chiffres.

### **- 12.1 - Exemple de droits**

Les exemples ci-dessous explicitent les droits d'accès.

#### **12.1.1 - Exemple 1**

Lecture + Ecriture + Exécution pour jlcech, le propriétaire  
Aucun droit pour le groupe users  
Aucun droit pour le reste du monde.

```

-rwx----- 1 jlcech users    254 jui 29  2005 purge_test
:::~::~:
:::~::~: > Droits des étrangers au groupe    7 = tous les droits
:::~::~: > Droits du groupe                  0 = aucun droit
---      > Droits du propriétaire          0 = aucun droit

```

Le fichier purge.test est un script, donc un exécutable. Les droits d'accès à ce ce fichier est 700, il est accessible à son seul propriétaire.

### 12.1.2 - Exemple 2

```

Lecture + Ecriture pour jlcech, le propriétaire
Lecture seule pour le groupe users
Aucun droit pour le reste du monde

```

```

-rw-r----- 1 jlcech users    139 jui 29  2005 purge.awk

```

Les droits d'accès à ce ce fichier est 640

### 12.1.3 - Exemple 3

```

Lecture + Ecriture pour jlcech, le propriétaire
Lecture + Ecriture pour le groupe users
Lecture seule pour le reste du monde

```

```

-rw-rw-r-- 1 jlcech users    1405 jui 29  2005 updatedb_v1

```

Les droits d'accès à ce ce fichier est 664

## - 12.2 - Changer les droits

L'autorisation de changement de droits relève du droit d'écriture. Si ce droit n'est pas donné à l'utilisateur courant, il relève de l'administrateur.

Par exemple jlcech veut protéger contre la modification le fichier updatedb\_v1 par le groupe et le rendre invisible au reste du monde. Il passe la commande suivante :

```

chmod 640 ./updatedb_v1

```

Une fois cette commande passée, les droits s'affichent comme suit

```

-rw-r----- 1 jlcech users    1405 jui 29  2005 updatedb_v1

```

pour plus d'information sur les commandes Linux il convient de se reporter aux manuels disponibles.

## - 13 - Paramétrage du serveur de fichiers Windows

Linux permet la gestion centralisée des fichiers dans les différents modes d'administration, partage, groupe de travail et domaine. La suite logicielle se nomme SAMBA, elle est disponible dans les distributions du commerce, sa version actuelle est la V3.0. Le choix d'accès au réseau pour le CTM est le « domaine », les éléments ci-dessous décrivent la mise en oeuvre.

### - 13.1 - Principes mis en Oeuvre

#### 13.1.1 - Déclaration d'un utilisateur

La prise en charge d'un utilisateur Windows dans un serveur Linux

repose sur les principes suivants.

1. Déclaration d'un utilisateur Linux (**/etc/passwd**).
2. Transposition de cette déclaration dans le fichier des utilisateurs depuis Windows (**/etc/samba/smb.conf**).
3. Affectation éventuelle d'un alias, pseudonyme, si le nom Windows est incompatible avec les contraintes Linux (**/etc/samba/smbusers**).

### 13.1.2 - Déclaration d'un machine

Une machine, un PC, fait partie du domaine s'il est déclaré dans celui-ci. Dans ce cas les utilisateurs eux-même déclarés pourront se déplacer de PC en PC et garder une configuration semblable de poste en poste. La machine doit faire l'objet de

1. Déclaration d'un « **device** » Linux
2. Transposition de cette déclaration dans le fichier des utilisateurs Windows.

### 13.1.3 - Fichiers de paramétrage SAMBA

Les fichiers requis sont décrits dans le tableau ci-dessous.

<i>Localisation</i>	<i>Nom du fichier</i>	<i>Fonction</i>
/etc	passwd	Fichier Linux qui contient TOUS les utilisateurs de la machine, y compris les utilisateurs système ainsi que la liste des postes de travail dans la cas d'un domaine.
/etc/samba	smb.conf	Fichier de configuration de l'environnement de travail.
/etc/samba	smbpasswd	Fichier contenant la liste des utilisateurs autorisés à se connecter depuis un environnement Windows ainsi que la liste des postes de travail dans la cas d'un domaine.
/etc/samba	smbusers	Fichier de gestion des correspondances de noms Linux<>Windows

## - 13.2 - Création des utilisateur / PRINCIPES DE BASE

### 13.2.1 - Utilisateur Linux - Description

Pour exister un utilisateur doit être déclaré et présent dans le fichier **/etc/passwd**. Tout utilisateur appartient à un groupe, ce groupe peut être composé d'un unique membre. Typiquement la ligne ci-dessous déclare l'utilisateur, le caractère « : » sépare les champs :

```

jlcech:x:501:100:Jean-Louis Cech:/home/jlcech:/bin/bash
:      :      :      :      :      :
:      :      :      :      :      :      Répertoire du SHELL
:      :      :      :      :      :      Répertoire « Mes Documents »
:      :      :      :      :      :      Nom en clair de l'utilisateur
:      :      :      :      :      :      Numéro du groupe principal, typiquement « users »
:      :      :      :      :      :      Numéro de l'utilisateur, UID
:      :      :      :      :      :      Si « x » alors un mot de passe est requis
Nom Linux associé au numéro d'utilisateur

```



possibilité de le changer depuis son poste de travail. Il convient de noter que le chemin d'accès à la procédure n'a pas à être spécifié.

### 13.2.5 - Intégration d'un Poste de Travail (Work Station / PC)

Pour disposer du droit d'intégration d'un utilisateur Linux vers SAMBA il faut être administrateur.

Le nom transféré est identique, un poste de travail Linux possède le même nom sous SAMBA. Il est créé comme suit

```
smbpasswd -a -m nom_NETBIOS
:
:
:      Nom work station Linux transféré vers SAMBA
Script de transfert de l'utilisateur.
```

Lors de l'exécution de la procédure aucun mot de passe n'est demandé. Le caractère « \$ » fourni lors de la création du poste de travail dans `/etc/passwd` ne doit pas être fourni.

### 13.2.6 - Création d'un alias conforme WINDOWS

Dans les noms utilisateur, les caractères tels que le « . » n'ont pas la même signification sous Windows et Linux, s'ils sont permis sous Windows, ils sont interdits sous Linux. Le fichier `/etc/samba/smbusers` permet de contourner cet interdit. Pour disposer du droit de modifier ce fichier, il faut disposer des droits d'administrateur.

Le fichier est structuré comme suit :

```
# Linux_name = SMB_name1 SMB_name2 ...
root = administrator admin administrateur root
nobody = guest pcguest smbguest
jlcech = jl.cech
fpuech = f.puech
```

Une fois le fichier enregistré, l'utilisateur « fpuech » pourra s'identifier en tant que « f.puech ».

## - 13.3 - Création d'un fichier de configuration SAMBA

Le fichier `/etc/samba/smb.conf` est critique, il est adapté aux besoins du CTM. Les sections débutent par « [nom\_section] ». Il est listé et commenté ci-dessous.

Une commande suivante permet le test des modifications :

```
testparm
```

Il FAUT l'exécuter à chaque modification du fichier de configuration.

## - 13.4 - Activation du nouveau fichier smb.conf

Dans l'environnement Fedora 1B le lancement du nouveau se fait comme suit :

```
/sbin/service smb restart
```



### 13.4.1 - Section [global]

La section **[global]** définit les paramètres d'environnement du serveur de fichier. C'est dans cette section que le rôle du serveur est fixé, PDC, SDC... Ici il s'agit d'une configuration PDC.

```
[global]
    workgroup = VILLEBON2
    Netbios name = urba_st
    server string = CTM Linux Server
    encrypt passwords = yes
# les descriptions suivantes forcent le mode PDC
    security = user
    os level = 255
    preferred master = yes
    domain master = yes
    domain logons = yes
    local master = yes

;    logon path = \\%L\Profiles\%U

    wins support = yes
    username map = /etc/samba/smbusers
```

### 13.4.2 - Section [homes]

Dans cette section sont définis les paramètres d'accès aux dossiers personnels des utilisateurs déclarés. Les lignes de définition des « mask » sont centrales dans la politique de partage des données. Dans le cas ci-dessous, les données et répertoires personnels sont lisibles par les membres du groupe.

```
[homes]
    comment = Home Directories
    create mask = 640
    directory mask = 750
    browseable = yes
    writeable = yes
```

### 13.4.3 - Section [netlogon]

Cette section définit les modalités d'hébergement des scripts de connexion.

```
[netlogon]
    comment = Network Logon Service
    path = /home/netlogon
    guest ok = yes
    writable = no
    share modes = no
```

### 13.4.4 - Section [public]

Dans cette section est défini le répertoire partagé, accessible au groupe en lecture et écriture. Typiquement il s'agit du répertoire partagé « COMMUN DU ST ».

```
[public]
```

```
comment = Repertoire commun
path = /home/commun
public = yes
read only = no
create mask = 664
directory mask = 775
```

### 13.4.5 - Section [warehouses]

Voir le commentaire.

```
[Warehouses]
comment = Je sais pas a quoi ca sert
path = /home/commun/Warehouses
read only = no
browsable = yes
create mask = 664
```

### 13.4.6 - Section [serclurb]

Ce partage contient le logiciel de gestion de l'urbanisme.

```
[serclurb]
Comment = Gestion permis de construire
path = /home/commun/Sercl
read only = no
browsable = yes
create mask = 664
```

### 13.4.7 - Section [DOCS]

Ce partage contenait les répertoires de données utilisateur et communs issus de la récupération initiale du serveur défunt. La copie vers les répertoires définitifs de données depuis un poste de travail Windows, permet d'affecter aux informations les bons droits d'accès.

Ces fichiers et répertoires sont à détruire une fois l'ensemble des données transférées.

```
[DOCS]
comment = Acces general aux datas
path = /home/commun/data
public = yes
read only = no
browsable = yes
create mask = 664
directory mask = 775
```

### 13.4.8 - Section [Office]

Dans ce partage sont rangés sur le disque les données fixes telles que CD et logiciels d'installation. Ces fichiers sont invariants, ils peuvent être régénérés à la demande, s'ils sont archivables, ils n'ont pas à être sauvegardés au quotidien.

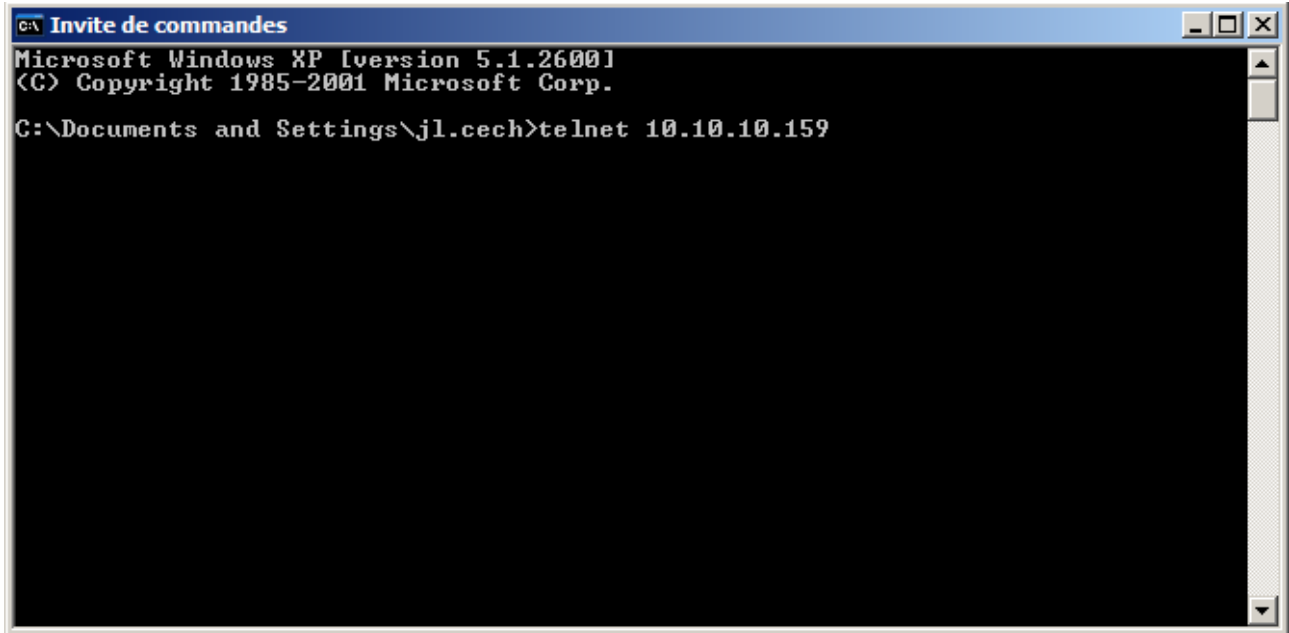
```
[Office]
comment = CD de MS Office et autres
path = /opt/Office
read only = yes
public = yes
```

## - 14 - Mise en oeuvre

### - 14.1 - *Prise de main à distance*

La prise en main à distance se fait via un client TELNET. Depuis l'invite de commande Windows, à l'invite taper :

telnet suivi de l'adresse IP du serveur Linux, ici 10.10.10.159

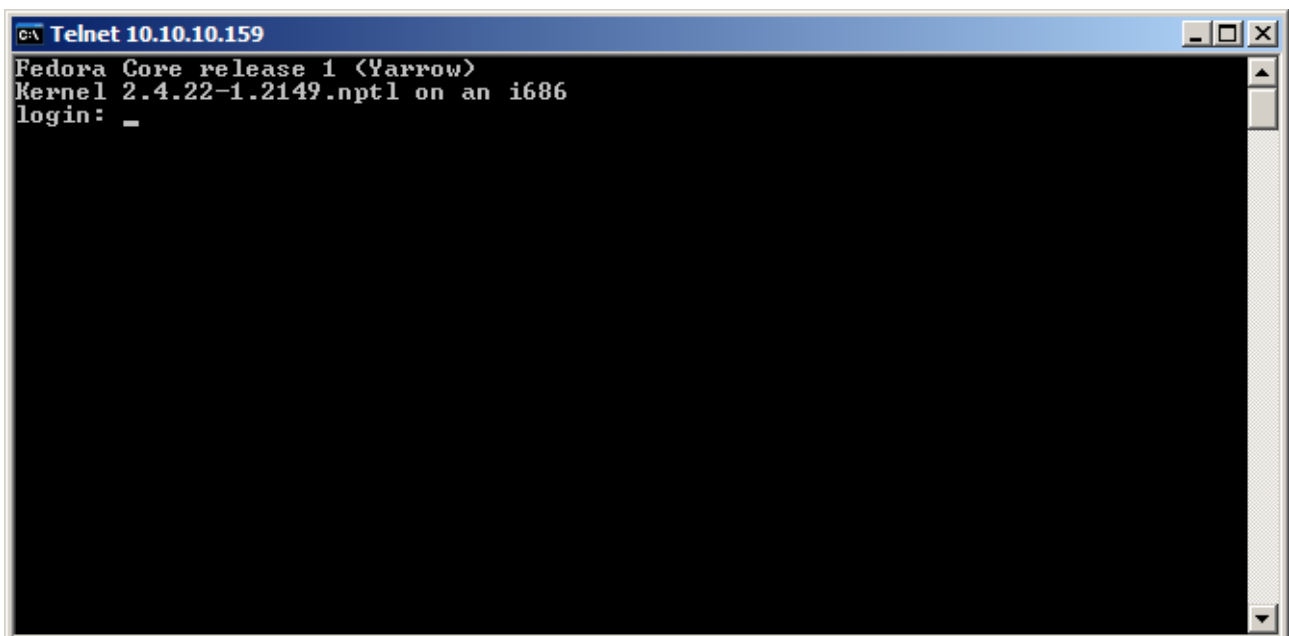


```
C:\ Invite de commandes
Microsoft Windows XP [version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\jl.cech>telnet 10.10.10.159
```

Dès l'établissement de la connexion l'écran suivant apparaît.

Les identifiants sont demandés,

- login **ctm**
- Password **villebon**

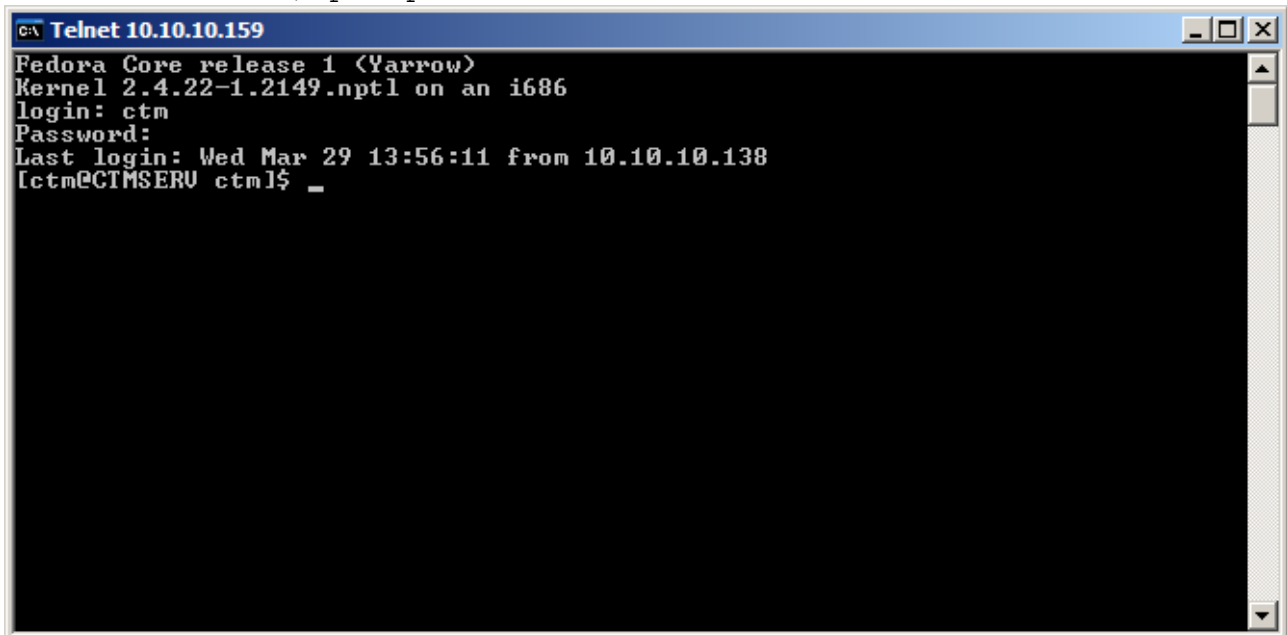


```
C:\ Telnet 10.10.10.159
Fedora Core release 1 (Yarrow)
Kernel 2.4.22-1.2149.nptl on an i686
login: _
```

Dès que la connexion est établie sur le serveur, l'écran se présente comme suit. Sur les deux dernières lignes de l'écran on

retrouve :

1. Informations concernant le dernier login, date et IP.
2. La seconde ligne est l'équivalent de l'invite de commande. Les commandes sont introduites à la suite du « \$ », prompt utilisateur.

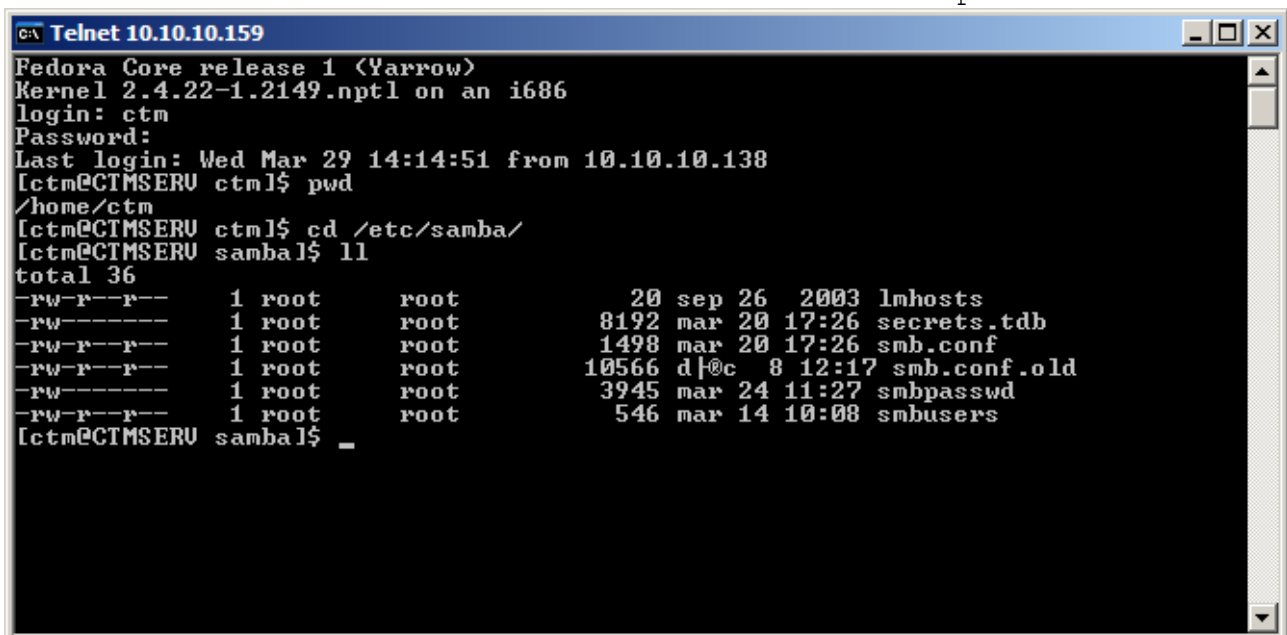


```
C:\ Telnet 10.10.10.159
Fedora Core release 1 (Yarrow)
Kernel 2.4.22-1.2149.nptl on an i686
login: ctm
Password:
Last login: Wed Mar 29 13:56:11 from 10.10.10.138
[ctm@CTMSERU ctm]$_
```

Dans ce mode l'utilisateur « ctm » dispose des droits standard, il ne lui est pas permis de créer, modifier, supprimer des utilisateurs, changer des droits d'accès à des fichiers qui ne sont pas les siens.

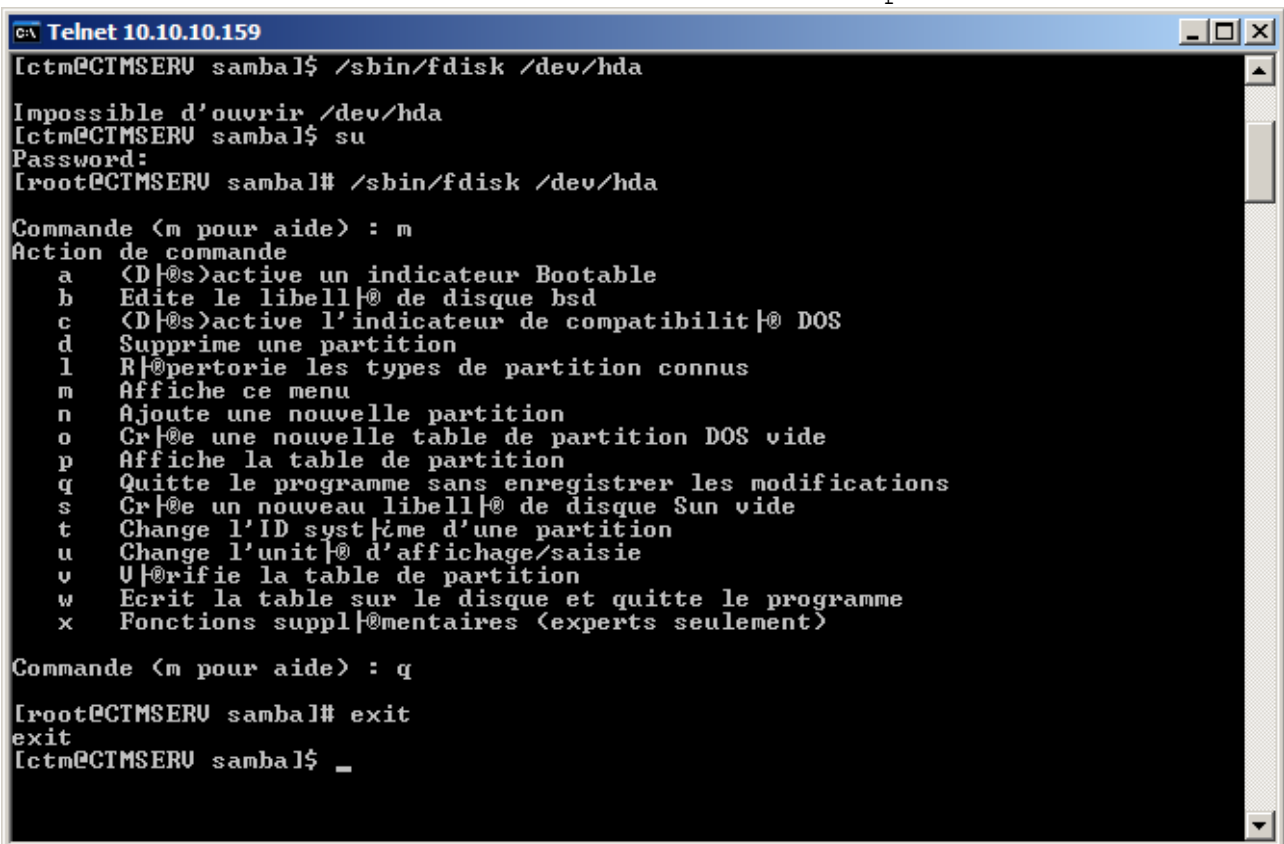
L'écran ci-dessous chaîne les trois commandes suivantes :

1. **pwd** Afficher le répertoire courant
2. **cd /etc/samba** Aller au répertoire
3. **ll** Lister les fichiers du répertoire courant



```
C:\ Telnet 10.10.10.159
Fedora Core release 1 (Yarrow)
Kernel 2.4.22-1.2149.nptl on an i686
login: ctm
Password:
Last login: Wed Mar 29 14:14:51 from 10.10.10.138
[ctm@CTMSERU ctm]$_ pwd
/home/ctm
[ctm@CTMSERU ctm]$_ cd /etc/samba/
[ctm@CTMSERU samba]$_ ll
total 36
-rw-r--r--  1 root    root      20 sep 26  2003 lmhosts
-rw-----  1 root    root     8192 mar 20 17:26 secrets.tdb
-rw-r--r--  1 root    root     1498 mar 20 17:26 smb.conf
-rw-r--r--  1 root    root    10566 d|@c  8 12:17 smb.conf.old
-rw-----  1 root    root     3945 mar 24 11:27 smbpasswd
-rw-r--r--  1 root    root      546 mar 14 10:08 smbusers
[ctm@CTMSERU samba]$_
```

Pour passer les commandes système il faut posséder les droits du « Super Utilisateur ». cette promotion se fait par la commande « **su** » suivie du password affecté à l'utilisateur « root ». Cette promotion est effective si le prompt n'est plus « \$ » mais « # ». L'écran ci-dessous montre la différence de comportement.



```
C:\ Telnet 10.10.159
lctm@CTMSERU samba]$ /sbin/fdisk /dev/hda
Impossible d'ouvrir /dev/hda
lctm@CTMSERU samba]$ su
Password:
[root@CTMSERU samba]# /sbin/fdisk /dev/hda

Commande (m pour aide) : m
Action de commande
a (D|s)active un indicateur Bootable
b Edite le libell| de disque bsd
c (D|s)active l'indicateur de compatibilit| DOS
d Supprime une partition
l R|pertorie les types de partition connus
m Affiche ce menu
n Ajoute une nouvelle partition
o Cr|e une nouvelle table de partition DOS vide
p Affiche la table de partition
q Quitte le programme sans enregistrer les modifications
s Cr|e un nouveau libell| de disque Sun vide
t Change l'ID syst|me d'une partition
u Change l'unit| d'affichage/saisie
v V|rifie la table de partition
w Ecrit la table sur le disque et quitte le programme
x Fonctions suppl|mentaires (experts seulement)

Commande (m pour aide) : q
[root@CTMSERU samba]# exit
exit
lctm@CTMSERU samba]$ _
```

Dans cet exemple l'utilisateur « ctm » tente d'accéder à l'utilitaire de partition du disque dur, n'étant pas administrateur, il s'en voit interdire l'utilisation.

La séquence « su » suivie du password administrateur permet d'accéder à la fonction de partition.

Pour revenir en mode utilisateur « normal », on passe la commande « exit ». le prompt redevient un « \$ ».

## - 14.2 - Création d'un poste dans le domaine

Un nouveau PC doit être intégré au domaine. Sa structure Linux doit avoir été préalablement mise en place. Pour cet exemple le nom NET\_Bios est « ctm\_compta »

L'écran ci-dessus résume les commandes suivantes :

```
C:\ Telnet 10.10.10.159
[ctm@CTMSERU samba]$ su
Password:
[root@CTMSERU samba]# /usr/sbin/useradd -s /bin/false -d /dev/null ctm_compta$
[root@CTMSERU samba]# smbpasswd -a -m ctm_compta
Added user ctm_compta$.
[root@CTMSERU samba]# cat /etc/passwd | grep ctm_com
ctm_compta$:x:539:539::/dev/null:/bin/false
[root@CTMSERU samba]# cat /etc/samba/smbpasswd | grep ctm_com
ctm_compta$:539:E388D001715F233526BAC9EC8CA25A10:47A36CE120287B6F57DCF8CA472435A
B:[W          ]:LCT-442A7FC3:
[root@CTMSERU samba]# exit
exit
[ctm@CTMSERU samba]$
```

1. **su** passage en mode administrateur
2. **useradd** ajout de la machine en mode work station
3. **smbpasswd** ajout de la machine au domaine
4. **cat passwd** montre la ligne d'identification Linux
5. **cat smbpasswd** montre la ligne d'identification SAMBA
6. **exit** retour en mode « normal ».

## **- 15 - Sauvegarde des données**

L'automatisation des tâches de sauvegarde est un pré-requis de la pérennité des données. Cette automatisation est rendue possible par Linux en s'appuyant sur les moyens suivants :

1. la mise en place de tâches automatisées,
2. l'exécution de scripts.

### **- 15.1 - Gestion de la sauvegarde**

Le script de sauvegarde est lancé soit par le démon « **crontab** », voir plus loin, soit par l'opérateur. Il fait référence à un fichier de paramétrage qui définit la destination de la sauvegarde.

La sauvegarde est gérée par des scripts qui assurent :

- la chronologie des lancements : root.cron,
- le montage des partitions et la vérification de la structure des répertoires: montage,
- le démontage des partitions de sauvegarde : demontage,
- la sauvegarde quotidienne : daily
- la sauvegarde hebdomadaire : weekly

Ces différents fichiers sont insérés en annexe.

La méthodologie employée est la suivante.

Une partition est réservée au sauvegardes quotidiennes, la seconde

aux sauvegardes hebdomadaires. Elles ne sont utilisées qu'à cette fin unique. Le serveur du CTM dispose de trois disques, afin de limiter les risques liés à la fiabilité des composants, ces partitions sont placées sur des unités de disques physiquement différentes.

Toutefois en cas de destruction totale ou vol du serveur, ce procédé ne garantit pas la pérennité des données, une sauvegarde sur un support externe reste à prévoir et à mettre en oeuvre.

### **15.1.1 - Fichier de configuration**

Sans Objet dans cette version.

### **15.1.2 - Planification des tâches**

Les tâches sont planifiées au moyen de « **crontab** », ce démon se paramètre au moyen d'un fichier qui spécifie les modalités de lancement d'un script. Le nombre des sauvegardes quotidiennes réalisées dans une semaine est contraint par l'espace disque disponible dans la partition de sauvegarde.

L'ensemble des scripts commente ses actions sur la sortie standard, celles-ci sont récupérées par le planificateur de tâches qui génère et gère les fichiers de log.

Chaque sauvegarde imprime une feuille de récapitulation, ce fichier est ensuite ajouté au fichier de log général.

### **15.1.3 - Script de montage des partitions**

Le script de montage des partitions réalise deux tâches.

1. Montage de la partitions de sauvegarde quotidienne et de la partition de sauvegarde hebdomadaire, respectivement /dev/hdc3 et /dev/hdd2
2. Vérification de l'existence de la structure d'accueil, cette fonction est particulièrement utile dans le cas de l'utilisation d'un nouveau disque qui n'aurait pas été organisé de façon adéquate.

### **15.1.4 - Script de démontage des partitions**

Ce script ne soulève aucune remarque particulière, sinon qu'à l'évidence il ne doit s'exécuter qu'une fois toutes les opérations de sauvegardes terminées.

### **15.1.5 - Script de sauvegarde quotidienne**

La sauvegarde quotidienne est gérée par la procédure « daily ».

Suite au montage la sauvegarde est réalisée dans le répertoire « Zstorage » placé à la racine de la partition /dev/hdc3

Un seul répertoire est utilisé, les sauvegardes du jour sont repérées par le numéro du jour de la semaine qui donne l'argument principal du nom des fichiers associés au jour de l'action. Ici 0

signifie Dimanche, 1 Lundi....

Les fichiers générés sont

x.file.log qui contient la liste des fichiers sauvegardés,  
x.tar.gz qui contient les fichiers proprement dits.

Dans ce cas la sauvegarde du Mardi donnera « 2.tar.log ».

La sauvegarde comporte trois phases principales :

1. Libération de l'espace du jour.
2. Sauvegarde proprement dite par « tar » qui génère deux fichiers, respectivement la liste et le fichier archive.
3. Compactage du fichier « x.tar » en « x.tar.gz ». Ce compactage est particulièrement efficace sur les fichiers textes, il aura un effet nul ou négatif sur les fichiers déjà compactés tels que les fichiers JPEG ou ZIP.

Une fois la sauvegarde réalisée le script analyse l'occupation disque de chacun des utilisateurs.

#### **15.1.6 - Script de sauvegarde hebdomadaire**

La sauvegarde hebdomadaire est gérée par la procédure « weekly »

### **- 16 - Restauration des données**

La restauration des données passe par les opérations suivantes :

1. Montage des partitions de sauvegarde.
2. Copier dans un répertoire ne faisant pas partie des partitions de sauvegarde le fichier contenant les données à récupérer, par exemple  
cp /mnt/disk\_1/Zstorage/3.tar.gz /opt/restore/  
on considère que le répertoire /opt/restore/ existe.
3. Décompresser le fichier par la commande  
gunzip /opt/restore/3.tar.gz  
cette commande décompresse le fichier .gz sur place, il faut donc disposer d'au moins deux fois l'espace du fichier tar. En sortie on récupère le fichier  
3.tar
4. Extraire la sauvegarde sur place en passant la commande  
tar -xvzf 3.tar  
les données sont disponibles localement pour leur restitution dans le répertoire d'origine.

Une fois la restauration terminée, il faut effacer le répertoire de restauration, ici, en tant que root, on passe la commande

```
rm -Rf /opt/restore/*
```

puis on démonte les partitions de sauvegarde.



## - 17 - Annexes

Les annexes présentent les scripts tels que utilisés.  
Se reporter au paragraphe commentant leur usage.

### - 17.1 - **Chronologie des tâches**

```
# Crontab de Supervision
# Fonction des champs
# 1 = min / 2 = h / 3 = dom / 4 = moy / 5 = dow
#
# IMPORTANT : les BU sont lances le soir
#             mais les fins de BU sont traites le lendemain.
#             La sauvegarde hebdo est faite dans la foulee du journalier
#             / 0=Dim, 1=Lun...
#
# Sauvegarde
01 22 * * 0,2,4 /root/admin/daily > /root/admin/dbu.log
01 23 * * 0 /root/admin/weekly >>/root/admin/week_bu.log
01 6 * * 1,3,5 /root/admin/demontage>>/root/admin/dbu.log
31 8 * * 1,3,5 cat /root/admin/dbu.log | lpr
30 8 * * 1,3,5 cat /root/admin/dbu.log >> /root/admin/backup.log
```

## - 17.2 - Montage des partitions

```
# #####
# Montage des 2 partitions Day et Week
# Les points de montage /mnt/disk_1 et /mnt/disk_2
# doivent preexister.
# Version 0.0 2006/08/01
# #####

DAY=hdc3
WEEK=hdd2

cd
msg1=$(mount -t ext3 /dev/$DAY /mnt/disk_1 2>/dev/null)
err1=$?
msg2=$(mount -t ext3 /dev/$WEEK /mnt/disk_2 2>/dev/null)
err2=$?

err=`expr $err1 \+ $err2`

if [ $err != "0" ]
then
    echo $(date) "Valeurs possibles 0=Montage OK / 1=Erreur Montage"
    echo "Montage "$DAY = $err1 $msg1
    echo "Montage "$WEEK = $err2 $msg2
    exit
fi

ls -l /mnt/disk_1 | grep ^d | grep Zstorage 2>/dev/null
if [ $? -eq 1 ]
then
    echo $(date) "Le repertoire Zstorage est absent de /mnt/disk_1 on le cree"
    mkdir /mnt/disk_1/Zstorage
fi

ls -l /mnt/disk_2 | grep ^d | grep Wstorage 2>/dev/null
if [ $? -eq 1 ]
then
    echo $(date) "Le repertoire Wstorage est absent de /mnt/disk_2 on le cree"
    mkdir /mnt/disk_2/Wstorage
fi

if [ $(ls -l /mnt/disk_2/Wstorage | grep Week_ | wc -l) != "10" ]
then
    echo $(date) "Creation des sous repertoires de WEEK"
    mkdir /mnt/disk_2/Wstorage/Week_0
    mkdir /mnt/disk_2/Wstorage/Week_1
    mkdir /mnt/disk_2/Wstorage/Week_2
    mkdir /mnt/disk_2/Wstorage/Week_3
    mkdir /mnt/disk_2/Wstorage/Week_4
    mkdir /mnt/disk_2/Wstorage/Week_5
    mkdir /mnt/disk_2/Wstorage/Week_6
    mkdir /mnt/disk_2/Wstorage/Week_7
    mkdir /mnt/disk_2/Wstorage/Week_8
    mkdir /mnt/disk_2/Wstorage/Week_9
fi
```

### - 17.3 - Démontage des partitions

```
# #####
# Demontage des 2 partitions DAY et WEEK
#
# #####

cd
msg1=$(umount -lf /mnt/disk_1 2>/dev/null)
err1=$?
msg2=$(umount -lf /mnt/disk_2 2>/dev/null)
err2=$?

err=`expr $err1 \+ $err2`

if [ $err != "0" ]
then
    echo $(date) "Valeurs possibles 0=Demontage OK / 1=Erreur demontage"
    echo "Demontage /mnt/disk_1 = "$err1 $msg1
    echo "Demontage /mnt/disk_2 = "$err2 $msg2
else
    echo $(date) "=====  
fi
```

## - 17.4 - Sauvegarde quotidienne

```
#####
# Script de supervision quotidien des stats serveur
# Effectue aussi un backup de /home
# Version mise en production le 27 Juin 2006
#
#####

# Def des constantes
VERS=1.0

BUAREA=/mnt/disk_1/Zstorage
MNTPT=/mnt/disk_

# Forcage des demontages des 2 partitions DAY et WEEK
$HOME/admin/demontage > /dev/null

# Montage des deux partitions
$HOME/admin/montage

# Verification du bon montage
xx=$( df | grep $MNTPT | wc -l )
if [ $xx != "2" ]
then
    echo "===== Debut erreur ====="
    echo $(date) "Erreur DAY et ou WEEK non montes : Backup impossible"
    echo "Action : Verifier le script de montage et le scheduleur !"
    echo "===== Fin erreur ====="
    exit
fi

JOUR=$(date +%w) # recup du jour 0=Dim / 1=Lundi...

# Corps du script
echo
"===== "
echo -n $(date) $VERS " En fonctionnement depuis "
uptime | awk '
BEGIN { }
{ print $3 " " $4 $5 "heures"}
END { } '
echo
"===== "

echo "Debut backup de /home"
cd $BUAREA
if [ $? -eq "1" ]
then
    mkdir $BUAREA
    cd $BUAREA
fi
touch $JOUR.tar
rm $JOUR.tar
tar -cvvf $JOUR.tar /home/ 2>/dev/null > $JOUR.file.log
/home/root/admin/dirsizes $BUAREA
echo "          Fin de backup de "$(cat $JOUR.file.log | wc -l) fichiers
echo "          ====="

df | awk '

```

```

BEGIN { print "Taux occupation des partitions" }
{
if (NR != 1) { print $1 "\t-\t" $5 "\t" $6 }
}
END { } '

echo "
=====
# Utilisation de /home par user
ls -l /home | grep ^d | grep -v root | cut -d ":" -f2 | cut -d " " -f2 > /tmp/x1
echo "Nombre utilisateurs = "$(cat /tmp/x1 | wc -l)
echo "
=====
echo "Usage disque par utilisateur"
cat /tmp/x1 | awk '
BEGIN { }
{ print "/home/"$1 }
END { } ' > /tmp/x2
nusers=$(cat /tmp/x2 | wc -l)
while [ $nusers != "0" ]
do
    $HOME/admin/dirsize $(cat /tmp/x2 | tail -n $nusers | head -n 1)
    let nusers=$nusers\ -1
done
echo "===== fin data =====$(date)

```

## - 17.5 - Sauvegarde hebdomadaire

```
# #####
# Traitement du circulaire hebdomadaire
# Le Vendredi soir on sauve le backup de la veille
#
# On recupere sur /mnt/disk_1/Zstorage le jour 4
# #####

SRC=/mnt/disk_1/Zstorage/
DST=/mnt/disk_2/Wstorage/

# On dispose de WEEK_MAX de sauvegardes
# Elles sont numerotees de 0 a (WEEK_MAX-1)
# dans les repertoires $DST/Wstorage/Week_(numero de semaine)
WEEK_MAX=4

echo $(date) '====Depart Weekly====='
echo "Depart sauvegarde hebdomadaire"

# Extraction du num de semaine dans l'annee modulo WEEK_MAX
WEEK_NBR=`expr $(date +%W) % $WEEK_MAX`

# On considere que les repertoires Week_0 a Week_9 existent
echo -n "Repertoire destination "$DST"Week_"$WEEK_NBR
cd $DST"Week_"$WEEK_NBR/ 2> /dev/null
if [ $? -eq 0 ]
then
    echo " accessible"
else
    echo " non accessible *** ERREUR ***"
    echo $(date) '==== Fin Weekly sur erreur ====='
    exit
fi

# On supprime le contenu du rep semaine en cours
rm -f ./ *
cd ..
rm Last*
touch "Last_Backup_in_Week_"$WEEK_NBR

# Copie du Jeudi dans la semaine courante
cd $SRC
cp 4* $DST"Week_"$WEEK_NBR/

cd $HOME

# Affichage du taux d'occupation des partitions hdax
df | grep "hda" | awk '
BEGIN { print "Taux occupation des partitions hda(x)" }

{ print $1 "\t-\t" $5 "\t" $6 }

END { } '
echo $(date) '====Fin Weekly====='
```

## - 17.6 - Occupation disque d'un répertoire

```
#####
# Obtenir sur stdout la taille de l'arborescence courante
# Elucubre le 17/11/2002
# Modif du 26/02/2006-22/06/2006
#####
echo -e $1 "\c" ; ls -Rl $1 2>/dev/null | grep ^[-d] | awk '
    BEGIN {
        FS = " "
        fichiers = 0
        repertoires = 0
        {
            s=s+$5
            if ( match ( $1, "d" ) == 0 )
                { fichiers ++ }
            else
                { repertoires ++ }
        }
    }
END { printf "\t => Dirs " repertoires "\t Files " fichiers
      MEG=1024*1024
      GIG=MEG*1024
      if ( s>GIG )
          { s=s/GIG
            unit="Go" }
      if ( s>MEG )
          { s=s/MEG
            unit="Mo" }
      if ( s>1000 )
          { s=s/1000
            unit="ko" }
      print " \t Size = "s, unit}'
```