



## SMR Système de formation

Rédaction : Jean-Louis Cech

Version initiale : février 2007

# Manuel d'administration

## Serveur Linux

## PC Windows XP pro

Mises à jour

Date	Objet MàJ
07/08/2007	Suite à rechargement ajout d'une partition pour /var Correction de bugs dans usermanage



## Table des Matières

<b>Introduction.....</b>	<b>4</b>
Objectif du système.....	4
Formation.....	4
Accès en libre service.....	5
<b>Constitution du système.....</b>	<b>6</b>
Poste serveur.....	6
Poste client.....	6
Imprimante.....	6
Accès Internet.....	6
Coût du système.....	7
<b>Conventions typologiques.....</b>	<b>7</b>
<b>SERVEUR.....</b>	<b>8</b>
Composition matérielle.....	8
Système d'exploitation.....	8
Rappel sur SAMBA.....	8
Installation du serveur.....	9
Paramétrage système serveur.....	10
SAMBA.....	10
Script spécifique d'administration.....	10
<b>Poste client ( PC ).....</b>	<b>11</b>
Composition matérielle.....	11
Système d'exploitation réglages de base.....	11
<b>Accès Internet.....</b>	<b>12</b>
Sécurité d'accès depuis l'Internet.....	12
Paramètres initiaux.....	12
Adresse publique (IP fixe).....	13
Accès courriel - Email.....	14
Compte principal.....	14
Compte secondaire.....	14
Paramétrage d'un mailer.....	14
<b>Réseau local.....</b>	<b>14</b>
<b>Administration des PC.....</b>	<b>15</b>
Mode Domaine.....	15
Mode Local.....	15
Mode sans échec.....	15
<b>Administration du serveur Linux.....</b>	<b>16</b>
Rappel sur les principes de la gestion des fichiers.....	16
Exemple de droits.....	16
Exemple 1.....	16
Exemple 2.....	16
Exemple 3.....	17
Changer les droits.....	17
Création des utilisateur / PRINCIPES DE BASE.....	17
Utilisateur Linux - Description.....	17
Utilisateur Linux - Création utilisateur.....	17
Utilisateur Linux - Création Work-Station (PC).....	18
Intégration d'un utilisateur vers SAMBA.....	18
Changement du mot de passe.....	18
Intégration d'un Poste de Travail (Work Station / PC).....	18
Création d'un alias conforme WINDOWS.....	19
Création d'un fichier de configuration SAMBA.....	19
Activation du nouveau fichier smb.conf.....	19
<b>Administration du serveur SMR.....</b>	<b>19</b>
Rappel sur l'arborescence des comptes Windows.....	20
Insertion d'un nouveau PC dans le domaine.....	21
Bug repéré lors d'une réinstallation de SERVEUR.....	21
Validation de l'intégration du PC dans le domaine.....	21
Nom des six PC initiaux du réseau SMRVILLEBON.....	22
Création de compte utilisateur libre service.....	23
Principes de gestion des comptes de formations.....	23
<b>Utilisation du script d'administration.....</b>	<b>24</b>



Lancement du script.....	24
Mise en oeuvre du script.....	25
Ouverture d'un compte « Libre-service ».....	25
Ouverture d'un compte « Modèle ».....	25
Création d'une suite de six comptes « élèves ».....	25
Supprimer un compte.....	25
Lister les comptes actifs.....	26
<b>Sauvegarde des données serveur.....</b>	<b>27</b>
Rappel sur l'organisation des disques durs.....	27
Données à sauvegarder.....	27
Cycles de sauvegarde .....	27
Sauvegardes quotidiennes.....	27
Sauvegardes hebdomadaires.....	28
Récupération des données.....	28
Exemple de séquence de récupération.....	28
<b>ANNEXES.....</b>	<b>29</b>
Annexe 1 Script d'ajout de stations de travail au domaine.....	29
Annexe 2 Fichier de configuration SAMBA.....	30
Annexe 3 Script d'administration utilisateurs.....	31
Annexe 4 Sauvegarde .....	35
Annexe 5 Tâches planifiées.....	36



## **Introduction**

Dans le cadre du service aux habitants de Villebon, afin de participer à la réduction de la fracture numérique, en particulier auprès des retraités, l'exécutif de la Mairie de Villebon a décidé la mise en place d'un outil permettant formation et accès libre à l'informatique et à l'Internet.

Une équipe de formateurs volontaires, des professionnels de l'informatique retraités, des agents volontaires de la commune, assurent les actions de formation et sensibilisation. Au delà de cette vocation primaire, ce système permet d'envisager la formation par objectifs du personnel municipal avec l'assistance d'équipes ad hoc.

A cette fin un studio de la résidence Alphonse Daudet, situé au rez de chaussée a été mis à disposition. Ce local autonome, par sa disposition et ses aménagements, kitchenette, salle de douche avec WC, ouvre la possibilité de recevoir simultanément six « étudiants ». Chacun de ces « étudiants » dispose d'un PC complet connecté en réseau à un serveur de fichiers et à l'Internet.

Un outil d'administration dédié autorise à la fois un accès en libre service banalisé et sécurisé aux données personnelles, une gestion de profils de formation par thème.

A la périphérie du réseau on trouve

- une imprimante laser N/B et couleur. elle permet à chacun de garder une trace papier de ses travaux et courriers,
- un vidéo projecteur pour faciliter l'apprentissage par l'imitation des actions du formateur,
- un bloc sono permet une sonorisation confortable Il est donc possible d'envisager des projections de films.

## **Objectif du système**

Le système mis à disposition, par sa flexibilité, assure plusieurs fonctions :

- Support de formation au moyen d'une gestion spécifique des comptes utilisateurs.
- Accès individuel aux données personnelles quelque soit le poste de travail, c'est la fonction accès libre-service.

Ces fonctions sont détaillées ci-dessous.

## **Formation**

La réalisation d'une formation de qualité repose sur deux points essentiels, à savoir,

- la maîtrise du sujet et de la communication par le formateur,
- un support de cours approprié et uniforme à tous les élèves.

Si le système mis à disposition ne peut que valoriser le premier point, en revanche pour le second une méthode originale a été étudiée et développée spécifiquement pour cette application. Cette méthode, décrite en détail plus bas, est structurée autour du concept suivant.



En amont de la formation, le formateur compose un environnement de travail informatique adapté à l'objectif de cette formation. Cet environnement contient l'ensemble des fichiers sur lesquels les élèves interviendront. Cet environnement est nommé le « modèle ». Lorsque cet environnement est validé et supporté par une documentation associée, par une simple action sur le poste serveur, ce modèle est dupliqué vers six comptes qui sont les environnements individuels des élèves.

Ainsi la formation se déroule sur des environnements maîtrisés à l'origine, les résultats sont individuels, ils sont de ce fait analysables en fin de session.

La formation terminée, le formateur dispose du choix de

- soit ré-initialiser les comptes, dans ce cas les données des comptes élèves sont perdues mais les ressources sont libérées et réallouées,
- soit de créer six nouveaux comptes pour la nouvelle session.

Ce dispositif permet de dérouler simultanément des formations sur de longues périodes sans perdre les acquis en réutilisant les environnements qui auront été ainsi constitués lors des formations antérieures.

En conclusion la fonction formation du système est architecturée dans un environnement MODELE <-> ELEVE. C'est à priori la solution qui offre la meilleure flexibilité.

## Accès en libre service

Le deuxième objectif de ce système est de permettre un accès en libre service au retraités demandeurs d'accès à l'informatique en général et à l'Internet en particulier.

La contrainte principale de ce type d'accès est posé par le poste de travail lui-même : en fonctionnement « standard » le poste de travail contient les données des utilisateurs. Si le poste 1 contient les données de Paul, il faut que ce poste soit libre pour que Paul puisse y accéder, ses données sont inaccessibles sur les autres postes de travail.

Ce n'est pas acceptable, il faut que les données personnelles soient indifféremment accessibles, sans manipulation particulière, sur l'un quelconque des six postes.

C'est pourquoi une architecture de type professionnelle, centrée autour d'un serveur de « Domaine », est mise en place. Vue de l'utilisateur, la mise en oeuvre est simplifiée à l'extrême, elle comporte deux phases, la première est unique, c'est l'ouverture administrative du compte, la seconde en est l'utilisation.

La première phase initialise le compte utilisateur, c'est-à-dire préciser au serveur le nom et le mot de passe du futur utilisateur. Une fois le compte ouvert sur le serveur, il convient de personnaliser l'environnement du nouvel utilisateur sur un poste de travail, par exemple ouvrir un compte de courriel, régler le mode d'accès à l'imprimante réseau... Cette opération est unique, elle est réalisée une seule fois sur le serveur et sur un des six postes de travail.

Ensuite l'utilisateur accède à ses données depuis l'un quelconque des postes de travail, ses données sont hébergées sur le serveur, elles y sont administrées, c'est-à-dire sauvegardées, à intervalle régulier de façon automatique, lors de l'accès suivant, ses données propres restent disponibles indifféremment sur l'un des six postes libre.



## Constitution du système

Le système est composé de quatre postes principaux, ils sont décrits ci-dessous.

### Poste serveur

Le serveur est un ancien poste de travail acquis par la Mairie courant 2000 qui a été extrait du parc opérationnel pour cause d'inadéquation avec les nouveaux environnements imposés par les éditeurs logiciels.

Toutefois, en tant que serveur de fichiers et serveur de Domaine, sous Linux, malgré son âge avancé, son niveau de performance est parfaitement satisfaisant et, sauf panne électronique, il doit assurer encore au moins deux à cinq années de service.

Le serveur assure les fonctions suivantes :

- Serveur de Domaine,
- Serveur de fichiers,
- Administration des données.

Pour ce dernier point un programme spécifique d'assistance à l'administration à été écrit, il est mis à la disposition des formateurs pour le faire évoluer.

### Poste client

Les six postes clients sont des PC tournant sous Windows XP pro. Ils embarquent 1Go de mémoire vive, un disque dur de 80 Go, un lecteur de DVD graveur de CDROM. Au delà des applicatifs standards fournis par MicroSoft dans l'environnement Windows XP pro, ont été ajoutés initialement deux suites bureautiques, MS-Office et Open Office.

Cette dernière est gratuite, fiable, elle embarque toutes les fonctions disponibles dans les suite payantes, elle offre une alternative souple et crédible aux solutions propriétaires, chacun peut la charger gratuitement en toute légalité sur Internet. Cette solution est désormais utilisée par des organismes aussi divers que l'Assemblée Nationale, le Ministère des Finances, PSA... C'est très probablement une solution porteuse d'avenir.

Enfin, aujourd'hui, les contraintes imposées par Vista, en particulier en ce qui concerne la configuration minimale souhaitable, sont hors de propos avec les fonctions à réaliser, les postes resteront pour le moment sous Windows XP..

### Imprimante

Une imprimante laser couleur est mise en réseau. Il est prévu de mettre en place un système de quotas d'impression. Cette gestion sera mise en place ultérieurement.

### Accès Internet

Il est mis en place un accès internet sur l'ensemble du réseau local. Les caractéristiques à l'installation sont les suivantes :

- 8 méga bits par seconde, c'est à dire l'équivalent d'une disquette toutes les deux secondes.



- 640 kilo bits par secondes en sortie, une photo de 1024x768 est émise en 15 secondes.
- La gestion des boîtes à lettres du courriel est faite par le fournisseur d'accès à l'Internet (FAI), Orange.

Au delà des fonctions classiques de navigation et courriel, le dimensionnement du débit choisi permet aussi plusieurs communications audio et vidéo simultanées via des logiciels de téléphonie Internet tels SKYPE.

## Coût du système

Le tableau ci-dessous récapitule les coûts liés au matériel, les aspects d'usage, loyer, amortissement, frais de communication ne sont pas pris en compte.

Poste	Qt	PU TTC	Total	Remarques
PC libre-service	6	600,00	3 600,00	Avec Lecteur DVD et Graveur
Licences logicielles PC	6	150,00	900,00	Windows XP pro
Serveur Linux	1	0,00	0,00	Matériel de récupération
Licences logicielles Serveur	1	0,00	0,00	Licence libre de droits
Imprimante laser couleur	1	420,00	420,00	
Consommables pour une année	1	1 000,00	1 000,00	Estimation pour utilisation intensive
Alimentation secourue	1	320,00	320,00	
Equipement réseau	1	210,00	210,00	Comprend un point d'accès WiFi

<b>Total</b>	<b>6 450,00</b>	<b>Euros</b>
--------------	-----------------	--------------

## Conventions typologiques

Le texte « standard » est imprimé dans la police courante.

Les commandes système tant pour Linux que pour la console de commande MicroSoft sont imprimées comme suit :

```
ls -al /home/répertoire
```

avec en italique les valeurs spécifiques contextuelles, ici le nom ***répertoire*** doit être remplacé par le nom du répertoire à lister.

```
/sbin/service nom_du_service stop|start|restart
```

dans ce cas on choisit **stop** ou **start** ou **restart** pour un service, par exemple **network**.



## SERVEUR

### Composition matérielle

La composition matérielle est fournie par la commande suivante :

```
cat /etc/sysconfig/hwconf
```

Le fichier permet de construire le tableau ci-dessous. L'affectation des partitions est extraite des fichiers `/etc/mtab` et `/ect/fstab`.

Les accès systèmes les plus nombreux, SWAP et `/var` sont effectués dans deux partitions contiguës sur le disque le plus performant.

Désignation	Caractéristique
Memoire vive	64 Mo
Disque dur 1	/dev/hda ( Master sur IDE primaire ) 250 Go
Partitions /dev/hda/	/dev/hda1/ => /boot /dev/hda2/ => SWAP /dev/hda3/ => /var /dev/hda4/ => Réservé pour sauvegardes
Disque dur 2	/dev/hdb ( Slave sur IDE primaire ) 80 Go
Partitions /dev/hdb/	/dev/hdb1/ => /opt /dev/hdb2/ => / /dev/hdb3/ => /home
Lecteur CD	/dev/hdd ( Slave sur IDE secondaire )
Processeur	Celeron 350 Mhz
Carte réseau	3Com 3C905B 10-100 Mbit/s

### Systeme d'exploitation

Le système installé est la FEDORA 1b. Bien que cette distribution date de 2003, celle-ci est stable et ne souffre d'aucun défaut majeur, elle est parfaitement dimensionnée pour les fonctions requises.

### **Rappel sur SAMBA**

Afin de dialoguer ensemble, les machine Windows et Linux utilisent le protocole Server Message Block (SMB) développé par MicroSoft. Ce protocole permet de faire dialoguer en respectant des règles de sécurité d'accès à l'information, lecture, écriture, exécution par utilisateur et par groupe.

Les règles principales sont :

- Tout poste de travail (PC) doit être déclaré avant d'intégrer le domaine.
- Tout utilisateur doit être déclaré avant de pouvoir créer et accéder à ses informations.





- L'intégration dans le domaine Windows<->SAMBA, est nécessairement précédée d'une création de l'utilisateur ou du PC dans l'environnement Linux.

Le respect de ces trois règles et de leur chronologie est centrale. Une fois maîtrisé et compris ce mécanisme simple permet une administration efficace.

## Installation du serveur

L'installation est faite en mode texte plutôt qu'en mode graphique standard, ce choix privilégie la vitesse et la stabilité du programme d'installation. La taille mémoire faible impose dans le cas d'une installation en mode graphique des échanges mémoire disque inutiles et coûteux. Cette opération est unique, son optimisation ne présente que peu d'intérêt au plan opérationnel.

Les informations fournies ci-dessous ne sont pas exhaustives, elles sont indicatives et ne permettent pas l'installation du serveur par un débutant.

Les paquetages impératifs sont :

- X Windows, car certaines fonctions d'administration sont plus conviviales et accessibles dans ce mode.
- KDE et ou GNOME.
- Les serveurs WEB et SAMBA.
- L'impression réseau.

Les paramètres réseau choisis lors de l'installation sont

- adresse IP : 192.168.0.2
- Masque sous réseau : 255.255.255.0

il est recommandé de **ne pas installer le Pare-feu standard** cette machine n'est pas exposée sur l'Internet, dans cette version le Pare-feu n'est pas totalement fiabilisé et peut dans certains cas provoquer une légère instabilité.

Nota :

Lors de la réinstallation du 7 Aout 2007, seul le gestionnaire de fenêtres KDE a été installé.



## Paramétrage système serveur

Le paramétrage du système comporte deux éléments clés :

- la mise en place des paramètres SAMBA,
- la mise en place des scripts d'administration.

Ces deux éléments sont relativement indépendants les uns des autres mais la fonctionnalité du système ne sera réelle qu'à la complétude des ces deux éléments.

### SAMBA

Les fichiers clés de SAMBA sont localisés dans le répertoire

`/etc/samba/`

ils sont décrits dans le tableau ci-dessous

Désignation	Fonction
<code>./smb.conf</code>	Fichier de configuration de l'environnement SAMBA. Le fichier actif est fourni en annexe.
<code>./smbpasswd</code>	Fichier de déclaration des utilisateurs Linux autorisés à accéder au réseau Windows. Il contient les mots de passe échangés avec les postes Windows
<code>./smbusers</code>	Fichier d'alias qui associe aux noms Linux qui interdisent la ponctuation des nom Windows qui l'autorise. Par exemple le compte Linux pierremartin sera associé à pierre.martin qui sera son nom Windows.

Les commandes Linux principales associées à SAMBA sont :

- Arrêt, mise en route ou relance après modification de SAMBA :  
`/sbin/service smb stop|start|restart`
- Ajout d'un utilisateur Linux à SAMBA  
`smbpasswd -a nom_utilisateur`
- Modification du mot de passe d'un utilisateur SAMBA  
`smbpasswd nom_utilisateur`
- Test des modifications apportées à smb.conf  
`testparm`

Le fichier `/etc/samba/smb.conf` est joint en annexe.

### Script spécifique d'administration

Un script spécifique est installé dans le répertoire `/root/admin`. Celui-ci doit être créé en exécutant une seule fois la commande suivante :

```
mkdir /root/admin
```

On copie ensuite le fichier depuis le support fourni.

Ce script se lance par la commande :

```
/root/admin/usermanage
```

Le code ainsi que son mode d'emploi est fourni en annexe.



## Poste client ( PC )

### Composition matérielle

Les PC fournis sont intégrés pour le compte de NEC. Ils embarquent les éléments décrits dans le tableau ci-dessous.

Désignation	Caractéristique
Memoire vive	1024 Mo
Disque dur 1	80 Go
Lecteur/graveur DVD/CD	
Processeur	AMD Sempron 2Ghz
Carte réseau	Realtek RTL 8169/8110 10/100/1000 Mbits/s

### Systeme d'exploitation réglages de base

Ces PC sont intégrés directement dans le Domaine. Les ajustements spécifiques sont précisés dans le tableau suivant :

Désignation	Caractéristique
Compte administrateur	Laisser en mode local et affecter mot de passe
Créer un compte « root » en mode local	Affecter un mot de passe
Créer un utilisateur du domaine « root »	Lui donner les droits d'administration
ICMP - ping	Dans les réglages de sécurité de Pare-feu autoriser la réponse aux pings entrants
Login	Ne pas afficher le nom de l'utilisateur précédant
Réseau local	Laisser le serveur DHCP fournir une adresse. Faire pointer le serveur WINS vers le serveur Linux.
Mises à jour Windows	Les autoriser, valider IE7 et activer le filtre anti phishing.
Nom machine	Déclarer le nom machine dans le serveur Linux puis lui faire rejoindre de Domaine.
Anti-virus	Installer l'anti-virus prévu.
Imprimante	Installer l'imprimante partagée par le serveur Linux en récupérant les driver sur le partage of-fert par le serveur
Installation de MS Office	Lancer la première installation en mode non Domaine en tant qu'administrateur.



## Accès Internet

Un accès à l'Internet est mis à disposition des utilisateurs. Il est composé en tête de réseau d'un modem-routeur, la distribution de l'information est assurée par un switch simple.

## **Sécurité d'accès depuis l'Internet**

Le routeur assure la fonction de Pare-feu, aucune DMZ n'est prévue, les connexions entrantes doivent avoir été initiées depuis l'intérieur.

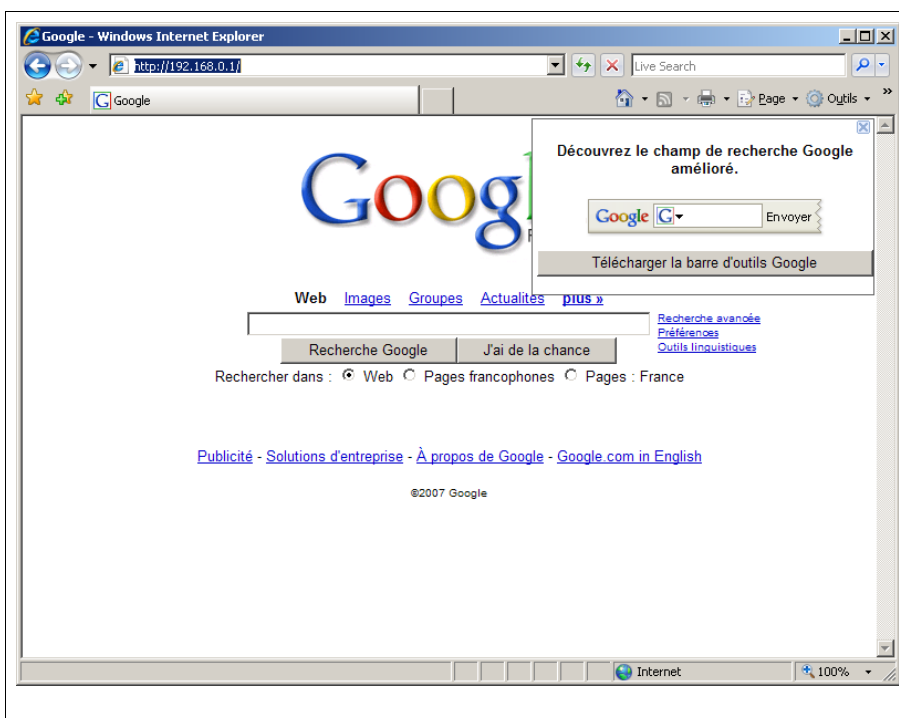
Ce dernier point signifie qu'aucune attaque venant de l'extérieur ne peut spontanément entrer dans le réseau local. A toutes fins utiles un anti-virus est installé sur chaque PC, le serveur est auto protégé.

## **Paramètres initiaux**

La fourniture d'accès est confiée à Orange. Les identifiants et mots de passe sont disponibles auprès du responsable du SMR. Le modem routeur dispose d'une interface WEB pour ses réglages, les principaux écrans sont fournis ci-dessous. On y accède par un navigateur en donnant l'adresse de passerelle.

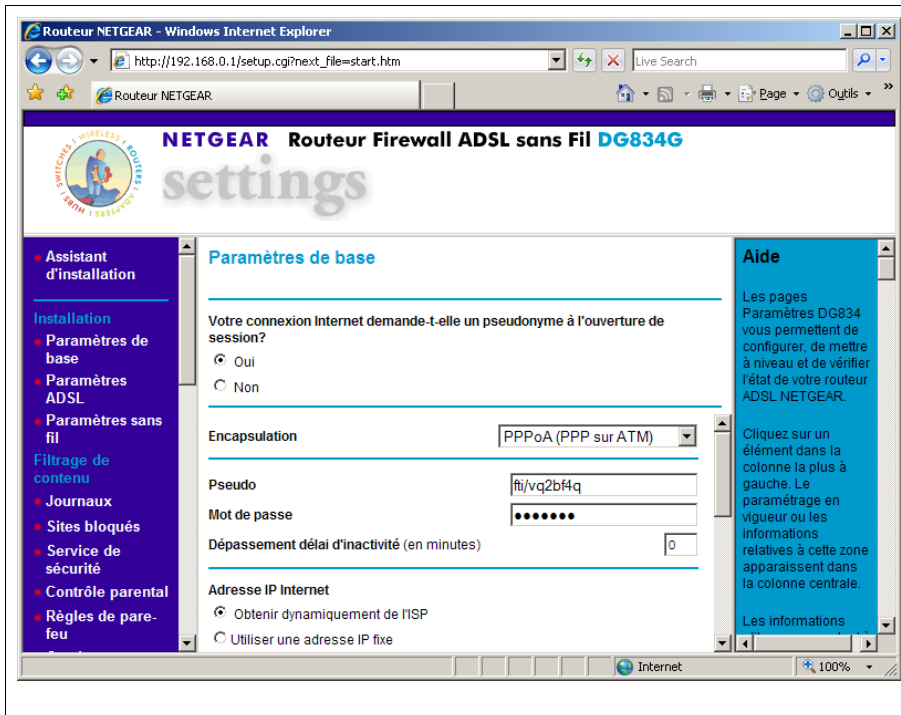
**http://192.168.0.1**

Le réglage effectué lors de l'installation permet une connexion permanente.

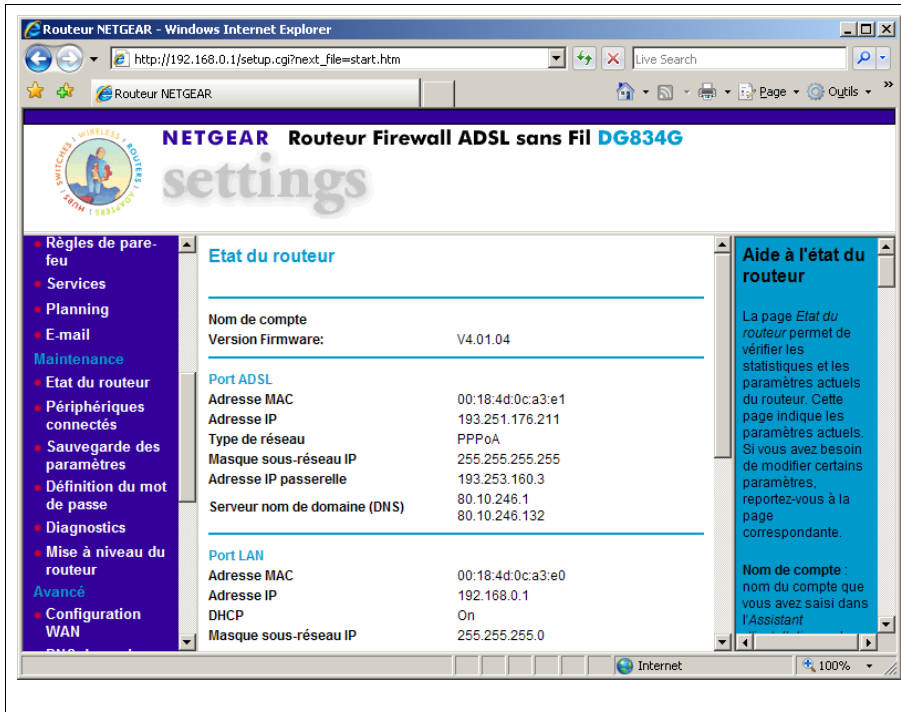


Une fois validée l'adresse de passerelle, le routeur demande un identifiant et un mot de passe, lors de l'installation ceux-ci sont ceux d'usine.

Les écrans de l'interface sont découpés en trois cartouches, le cartouche de droite, en bleu foncé, sélectionne la fonction à paramétrer ou consulter, le cartouche du centre, en blanc, concerne les données, le cartouche de droite, en bleu plus clair, fournit une aide.



Les paramètres de base sont affichés par cet écran.



L'écran « Etat du routeur » fournit l'adresse IP fixe publique du réseau, cette adresse permet, à terme, de gérer l'hébergement d'un site WEB, la réalisation de télémaintenance...

Pour plus d'information se reporter à la notice du produit.

## Adresse publique (IP fixe)

Le type d'abonnement choisi fournit une adresse IP fixe : **193.251.176.211**, celle-ci répond au ping WAN.



## **Accès courriel - Email**

Deux comptes sont disponibles, un compte principal et un compte secondaire, le compte principal est attribué lors de l'ouverture de l'accès Internet par Orange, le second est créé. Disposer d'une paire de comptes permet de valider la fonctionnalité des transmissions.

### **Compte principal**

Adresse messagerie : [rpa.villebon@orange.fr](mailto:rpa.villebon@orange.fr)

Mot de passe : gxhpadt

### **Compte secondaire**

Adresse messagerie : [rpa.compte.test@orange.fr](mailto:rpa.compte.test@orange.fr)

Mot de passe : villebon

## **Paramétrage d'un mailer**

Le paramétrage d'un mailer n'entre pas dans l'objectif de ce document. Toutefois le paramètre spécifique de cet accès est le serveur SMTP qui est :

smtp.orange.fr

## **Réseau local**

Le réseau local est caractérisé dans le tableau ci-dessous :

Désignation	Caractéristique
Masque de sous-réseau	Classe C : 255.255.255.0
Adresse de sous réseau	192.168.0.x
Passerelle	192.168.0.1
Serveur Linux	192.168.0.2
Imprimante réseau	192.168.0.3
PC résidents	Les six PC résidents se voient affecter les adresses suivantes : 192.168.0.21 à 26
Plage DHCP	192.168.0.51 à 69 Cette plage est affectée aux PC nomades. Fonction réalisée par le routeur, les adresses sont attribuées pour 24 heures.
Accès WiFi	Un accès WiFi protégé par clé WEP est disponible, il permet des accès 54 Mbits/s
Paramètres WiFi	SSID diffusée = SMR clé WEP = voir la fonction dédiée du routeur



Les principes d'affectation des adresses IP dans le réseau sont les suivants : les adresses basses 1 à 50 sont réservées aux équipements permanents ou « système », les machines « nomades » récupèrent les paramètres via un serveur DHCP unique dans le réseau.

En ce qui concerne le plan d'adressage, le serveur DHCP autorise 19 clients à se connecter simultanément sur le réseau local (LAN) ce nombre est extensible à la demande en ajustant la plage par la valeur de fin.

## **Administration des PC**

Les PC possèdent trois modes principaux de fonctionnement :

1. En mode Domaine utilisateur ou administrateur,
2. Hors Domaine en mode administrateur
3. En mode sans échec.

### **Mode Domaine**

C'est le mode normal de fonctionnement, l'ensemble des opérations d'utilisations normales sont hébergées par le serveur, les données sont administrées. Ce mode est imposé lors du boot du PC en choisissant dans la ligne

Se connecter à SMRVILLEBON

### **Mode Local**

Ce mode doit être exclusivement réservé aux opérations d'administration locale. C'est en particulier le cas pour l'installation de la suite Office MicroSoft.

### **Mode sans échec**

Ce mode est réservé aux opérations de maintenance lourdes comme par exemple la suppression des données dans le répertoire « Documents and Settings » d'utilisateur ayant disparu.



## Administration du serveur Linux

Le présent document n'a pas pour vocation à fournir une compétence sur Linux, toutefois les grandes règles sont rappelées ci-dessous en préambule.

### Rappel sur les principes de la gestion des fichiers

Un fichier possède 3 classes d'usagers :

- 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 à 7.

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. Sous Linux pour être exécutable sur le serveur, un script, l'équivalent d'un fichier « .bat » doit voir son bit d'exécution à 1.

### Exemple de droits

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

#### 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
:::         > tous les droits pour le propriétaire
:::         > aucun droit pour le groupe
:::         > aucun droit pour le reste du monde
```

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

#### 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





### 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

### 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.

### Création des utilisateur / PRINCIPES DE BASE

#### 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
```

#### Utilisateur Linux – Création utilisateur

Pour disposer du droit de création d'un utilisateur, il FAUT être administrateur. Un utilisateur est créé par la commande décrite ci-dessous :

```
/usr/sbin/useradd -d /home/machin -g users -s /bin/bash -n machin
: : : : : :
: : : : : : Nom Linux
: : : : : : Répertoire du SHELL
: : : : : : Groupe associé à l'utilisateur
: : : : : : Répertoire de travail de l'utilisateur machin
Programme de création de l'utilisateur précédé de son chemin
```

Il convient de noter que chaque paramètre est précédé d'un « flag », par exemple « **-g** » qui spécifie la fonction de la chaîne de caractères qui suit, ici le groupe principal « **users** ».



**REMARQUE IMPORTANTE :** le nom de l'utilisateur, ici « **machin** » ne peut contenir de caractères autres que les lettres de a-z, 0-9 et DOIT débuter par une lettre. Le caractère « . » est interdit, par exemple « jl.cech » est refusé.

## Utilisateur Linux – Création Work-Station (PC)

Pour disposer du droit de création d'un poste de travail, il FAUT être administrateur. Un poste de travail est créé par la commande décrite ci-dessous :

```
/usr/sbin/useradd -s /bin/false -d /dev/null nom_NETBIOS\$
:
:
: --> Nom déclaré par Windows
:
: --> Répertoire data, sans objet pour un PC
:
: --> Répertoire de SHELL, sans objet pour un PC
```

Il convient de noter que chaque paramètre est précédé d'un « flag » qui spécifie la fonction de la chaîne de caractères qui suit.

### REMARQUES IMPORTANTES :

1. le nom de l'utilisateur, ici « nom\_NETBIOS » ne peut contenir de caractères autres que les lettres de a-z, 0-9 et DOIT débuter par une lettre, il est fixé lors de l'initialisation du PC Windows. Toutefois le caractère « \_ » est utilisable en tant que séparateur pour aérer le texte.
2. Le nom NETBIOS fourni dans la commande se termine par « \\$ ». Le caractère \$ placé à la fin du nom signifie qu'il s'agit d'un poste de travail et non d'un utilisateur.

## Intégration d'un utilisateur vers SAMBA

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

Le nom transféré est identique, un utilisateur Linux possède le même nom sous SAMBA. Il est créé comme suit :

```
smbpasswd -a machin
:
:
: Nom utilisateur Linux transféré vers SAMBA
Script de transfert de l'utilisateur.
```

Lors de l'exécution de la procédure un mot de passe est demandé. C'est celui que doit fournir l'utilisateur Windows lors de sa connexion, il peut être vide, l'utilisateur dispose de la 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.

## Changement du mot de passe

En session ouverte, l'appui sur Ctrl-Alt-Sup ouvre la fenêtre suivante, celle-ci permet de modifier le mot de passe qui est défini et conservé dans /etc/samba/smb.conf

## 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.

## 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, en particulier dans cette version du système d'exploitation. Cette restriction saute dans les versions ultérieures mais celles-ci ne peuvent être installées pour cause de mémoire vive trop petite. 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 pcquest smbquest
jlcech = jl.cech
fpuech = f.puech
```

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

## Création d'un fichier de configuration SAMBA

Le fichier `/etc/samba/smb.conf` est critique, il est adapté aux besoins du service de formation, il est calqué sur le fichier déjà utilisé au CTM depuis 2003. 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.

## Activation du nouveau fichier smb.conf

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

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

Le fichier actif `/etc/samba/smb.conf` est fourni en annexe.

Parmi les accès visibles depuis un poste de travail Windows on retrouve :

- Le répertoire de l'utilisateur,
- Le répertoire commun,
- Le répertoire de « bibliothèque » qui contient les logiciels à installer sur les postes de travail,
- L'imprimante gérée par le serveur.

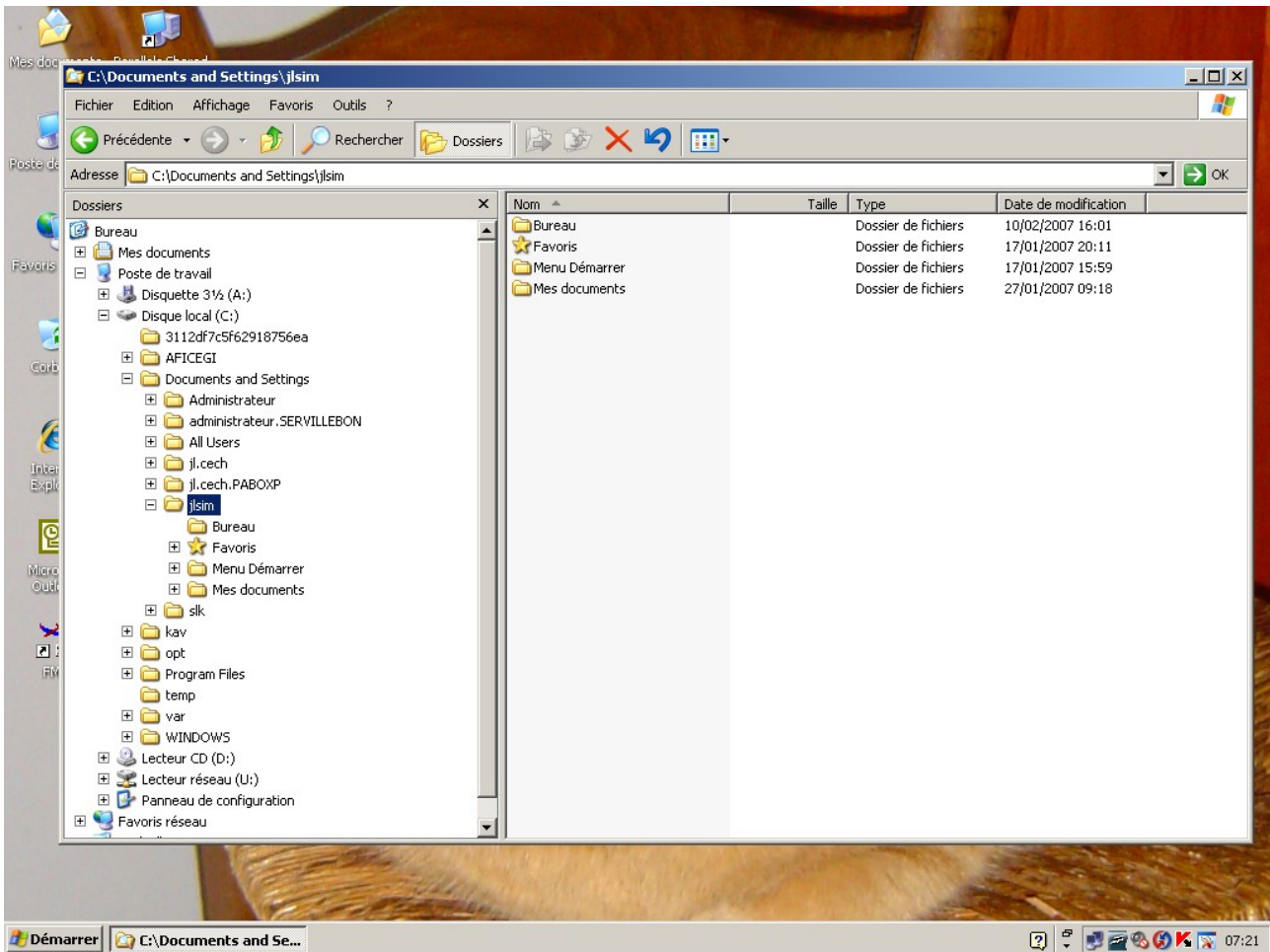
## Administration du serveur SMR

Les tâches courantes d'administration du serveur sont assurées par un script dont la vocation est d'automatiser les tâches courantes repérées. Ce script est ouvert, le responsable du système pourra le modifier à sa guise. Lors de la « remise des clés », il assure les fonctions décrites ci-dessous.



## Rappel sur l'arborescence des comptes Windows

En mode « stand alone » un PC sous Windows stocke toutes les données des utilisateurs ainsi que les environnements sous le répertoire « **Documents and Settings** » qui se présente comme suit :



Dans le cas de l'utilisation dans un domaine Linux, cette arborescence est transférée au serveur Linux qui la gère dans le répertoire « **/home/utilisateur\_courant** ».

Le répertoire Windows « **Mes Documents** » est géré par Windows de façon très spécifique, il est souhaitable d'éviter de le réaffecter dans le monde Linux. Afin de retrouver cette fonction qui est **ABSOLUMENT** vitale, il suffit d'utiliser le « **Bureau** » et y créer les répertoires pour les fichiers personnels.

Pour disposer d'un répertoire « **Mes Documents** » sur le bureau, il « suffit » d'y créer un dossier nommé « **Mes Documents** », celui-ci est administré par le serveur et est pris en charge par les procédures de sauvegarde.



## **Insertion d'un nouveau PC dans le domaine**

Afin d'insérer un PC dans un domaine, la séquence suivante précise les opérations à réaliser sur le PC et le serveur.

1. Insérer le PC dans le réseau local connectant physiquement le PC, câble RJ45 ou WiFi, en activant le client DHCP. A partir de ce moment Internet est accessible.
2. Passer l'ensemble des patches Windows.
3. Installer l'antivirus.
4. Valider la réponse au ping (ICMP) ce point est important car XP par défaut ne répond pas aux pings, ce réglage est désastreux pour les programmes d'administration automatique des adressages réseau.
5. Nommer le PC avec un mot commençant par une lettre ne contenant aucun espace ni caractère de ponctuation. Ce nom ne doit pas pré-exister dans le réseau. Lors de la mise en service de l'ensemble des six PC, il a été décidé d'utiliser des prénoms avec les voyelles sans accent. Cette opération impose un redémarrage du PC.
6. Sur le serveur créer le compte Linux et SAMBA associé au nom de la machine. Voir les sections création Work-Station et Intégration d'un poste de travail.
7. Faire intégrer le PC au domaine SMRVILLEBON par les propriétés du poste de travail puis redémarrer le PC.

Ces opérations ne sont pas détaillées plus avant, l'opérateur DOIT posséder la compétence suffisante pour réaliser ces opérations critiques, elles ne sont à réaliser qu'une seule fois lors de l'intégration du PC dans le domaine.

## **Bug repéré lors d'une réinstallation de SERVEUR**

Lors d'une réinstallation du serveur, les PC doivent être réintégrés dans le domaine SMRVILLEBON. Cette réintégration, en l'état ne fonctionne pas, il faut impérativement suivre le processus suivant :

1. Se loguer en administrateur du poste de travail en mode local.
2. Rejoindre un **groupe de travail dont le nom n'est pas** SMRVILLEBON.
3. Rebooter puis rejoindre le domaine SMRVILLEBON puis rebooter le PC.

Il est possible qu'une erreur Windows apparaisse lors de la finalisation de l'intégration au domaine, celle-ci n'est pas critique, il convient toutefois de vérifier la bonne intégration du PC au domaine, voir le paragraphe suivant.

## **Validation de l'intégration du PC dans le domaine**

Préalablement à cette validation, il faut créer un compte de test avec les paramètres suivants :

Nom Linux et SAMBA :	<b>test</b>
Alias SAMBA :	<b>compte.test</b>
Mot de passe Windows :	<b>tester</b>



Dès la première connexion, sur le premier PC validé, il est utile de créer sur le bureau et dans le dossier « Mes Documents » un jeu de fichiers de test. Ceux-ci permettent de tester que la fonction « Nomade » est correctement activée, ces fichiers doivent apparaître lors de la connexion sur les autres PC intégrés au domaine. Lors de la connexion ne pas oublier de spécifier le domaine SMRVILLEBON, dans le cas contraire, la connexion ne pourra se réaliser.

Il est possible d'utiliser indifféremment les identifiants « test » ou « compte.test », ils désignent le même compte et sont associés au même mot de passe.

NOTA :

Les propriétés du répertoire « Mes Documents » indiquent que celui-ci est localisé sur le disque C: du PC local. Cette information induit à penser que ce dossier est local, il n'est rien. Lors de chaque login et logout les informations utiles sont importées et exportées depuis et vers le serveur. C'est grâce à ce dispositif que la fonction « Nomade » est disponible.

### **Nom des six PC initiaux du réseau SMRVILLEBON**

Les six PC initialement installés sont :

amelie	charles
lucien	marguerite
roberta	rose

Ces noms ont été choisis arbitrairement, totale liberté est laissée pour les renommer et pour les PC à venir. Une restriction doit être prise en compte, ces noms machine sont désormais réservés et doivent plus être utilisés pour nommer des utilisateurs.



## Création de compte utilisateur libre service

Le script assure la création d'un compte Linux et l'intégration de ce compte dans SAMBA dans le serveur.

**Avant la première utilisation** par Windows, le compte utilisateur est quasiment vide, il contient les fichiers système cachés nécessaires au bon fonctionnement de Linux.

**Lors de la première utilisation** d'un compte utilisateur sur un PC, celui-ci crée une structure propre, cette structure est écrite sur le serveur et sera utilisée ensuite. On retrouve toutes les données créées par Windows dans :

/home/utilisateur/profile

**Une fois l'environnement utilisateur créé sur le serveur, tout accès à ce compte, sur une quelconque machine du domaine, permet à l'utilisateur de retrouver tout son environnement de fichiers et aussi de paramétrage.**

## Principes de gestion des comptes de formations

~~La qualité de la réception d'une formation est particulièrement liée à la cohérence de l'action réalisée par l'élève avec la consigne dictée par le formateur. Cela signifie que le formateur et les élèves agissent sur des environnements semblables et maîtrisés. Il convient donc d'offrir à chacun des élèves, du moins au départ, des environnements identiques.~~

~~La solution choisie est calquée sur la notion de « modèles » tels qu'on les retrouve dans les traitements de textes par exemple.~~

~~La procédure est la suivante.~~

- ~~1. Ouverture d'un compte utilisateur, ce compte sera nommé par exemple « tab\_niv\_deb » pour tableur niveau débutant.~~
- ~~2. Le formateur accède à ce compte et y crée les tableaux et documents nécessaires à cette formation. Une fois les données insérées et validées sur le « Bureau », ce compte devient un compte « modèle »~~
- ~~3. Si les six comptes élève n'existent pas, l'accès au script d'administration permet de les créer. Par exemple on crée les comptes dont la racine est « session\_0 », cette racine donne naissance à six comptes nommés « session\_01 » à « session\_06 ». Comme dans le cas de la création de comptes en libre service, il faut les activer avant de pouvoir y transférer les données spécifiques de la formation préparées dans le « modèle ».~~
- ~~4. Les six comptes d'élève pré existent. Lors de la mise en place d'une formation, on copie les données du « modèle » dans les six comptes élève. Les données initiales de formation sont alors disponibles et identiques pour chacun des élèves. Ces comptes suivront alors les élèves pour toute leur formation.~~

~~Dans le cas où une nouvelle session de cette même formation est prévue simultanément, il suffit de lancer la procédure au point « 3 » avec un nouveau nom racine, par exemple « session\_4 », dans ce cas les comptes ainsi créés seront nommés respectivement « session\_41 » à « session\_46 ».~~

Fonction non activée.



## Utilisation du script d'administration

Le script d'administration est fourni en annexe, il permet l'automatisation des fonctions principales, à savoir :

- Création de comptes utilisateurs « normaux ».
- création de comptes « formation ».
- Recopie des données de formation dans les comptes élèves.
- Listage des comptes actifs.
- Suppression de comptes

L'exploitation de ce script se fait à la console du serveur Linux, elle impose la connaissance du mot de passe d'administration courant.

## Lancement du script

Depuis la console du serveur, se loguer en tant qu 'administrateur, puis passer la commande

```
/root/admin/usermanage
```

L'écran d'accueil est auto explicatif.

Il existe deux types de commandes,

- les affichages de paramètres,
- la documentation de ceux-ci.

```
cs Telnet smrserveur
Valeurs courantes
1 Utilisateur Unix = -
2 Groupe           = users
3 Shell            = /bin/bash/
4 Mot Windows     = -
5 Creation de 6 comptes vierges
6
7 Effacer 1 compte Linux et Samba
8

L = lister les comptes actifs
F = Fin et ecriture DATA / X = Fin sans ecriture
Commande = _
```





## **Mise en oeuvre du script**

La structure choisie permet l'ajout simple de fonctions complémentaires ou leur modification. Toutefois, la nature du programme, sa logique interne, sont auto documentées, comme il n'est pas envisagé de généraliser cette application, elle ne sera pas documentée plus avant.

## **Ouverture d'un compte « Libre-service »**

L'ouverture d'un compte « libre-service » demande la documentation impérative de deux paramètres ainsi qu'un paramètre facultatif mais souhaitable, le mot de passe.

1. **Le nom Unix du compte**, celui-ci est arbitraire, le compte de Monsieur Michel Martin peut parfaitement être référencé sous le nom de « truchose » pourvu que ce code soit unique. Toutefois, il est préférable que nom Unix choisi fasse référence au propriétaire, par exemple « mimartin ».
2. **L'alias associé**. Au nom Unix arbitraire, on associe un « alias » qui désigne de façon explicite le propriétaire du compte, par exemple en documentant le nom et le prénom : « michel.martin ».
3. Lors de la création effective du compte le mot de passe SAMBA est demandé. Il est possible de ne pas le créer et le laisser vide, toutefois, pour des raisons évidentes de confidentialité, ceci n'est pas désirable.

Une fois le compte créé, il est possible d'enchaîner sur une nouvelle création ou toute autre fonction proposée par le script.

## **Ouverture d'un compte « Modèle »**

L'ouverture d'un compte « modèle » est identique à l'ouverture d'un compte « libre-service ».

## **Création d'une suite de six comptes « élèves »**

~~La salle de formation comporte six postes de travail, six comptes élèves peuvent être utilisés simultanément. Une procédure permet de créer six comptes Unix et leur pendant SAMBA en une seule opération. Le nom des comptes ainsi créés comporte deux parties, un préfixe qui est identique aux six comptes, un postfixe qui se compose d'un chiffre de 1 à 6.~~

Fonction supprimée du script initial car elle génère des erreurs dans la suppression des comptes. Objet mal maîtrisé et dont l'objet n'est pas vraiment utile.

## **Supprimer un compte**

La suppression d'un compte comporte deux séquences :

1. la désignation du nom Unix du compte à supprimer.
2. Le lancement de la suppression proprement dite.



La désignation se fait par la fonction « 1 » du script, c'est à dire que l'on fournit le nom UNIX du compte à supprimer. Si le nom UNIX à supprimer existe, un avertissement est affiché, il prévient que ce label n'est pas exploitable pour une création, il pré existe. Si le compte Unix n'existe pas, il est désirable de pouvoir lancer cette procédure car même si le compte UNIX n'existe pas, le compte SAMBA résiduel pourrait avoir survécu suite à une fausse manipulation.

Le lancement par la fonction « 7 » supprime les entrées suivantes, si toutefois elles existent :

1. Le compte Unix et les données associées.
2. L'entrée dans /etc/samba/smb.conf
3. L'entrée dans /etc/samba/smbusers

La suppression des comptes élèves est réalisée compte par compte par cette fonction, ainsi pour supprimer six comptes, même consécutifs, la fonction est exécutée à six reprises par l'opérateur.

## Lister les comptes actifs

Le listage des comptes actifs permet de les visualiser et d'associer les alias aux noms systèmes de comptes. En aucun cas les mots de passe ne peuvent être récupérés, en cas de perte, ils sont réinitialisés par l'administrateur.



## Sauvegarde des données serveur

### Rappel sur l'organisation des disques durs

Le serveur est équipé de deux disques durs, un disque portant données actives et le système, un second disque portant la partition de boot, le swap et deux « grosses partitions » non montées en usage normal. C'est sur ces dernières que sont réalisées les opérations de sauvegarde.

Cette organisation est dictée par les inférences suivantes :

- les disques ne tombent pas en panne simultanément.
- La carte mère ou l'un quelconque des composants peut tomber en panne sans remettre en cause l'intégrité des données, ce composant est remplaçable.
- Le serveur ne sera ni volé ni détruit par un incendie.
- En cas de panne l'intégrité du système est rétabli au moyen des éléments restant en activité.

Les sauvegardes quotidiennes et hebdomadaires sont archivées respectivement dans les répertoires /daily et /weekly situés sous le répertoire d'accroche. La suite de ce document explicite les modalités de sauvegarde et celles de la restitution des données.

### Données à sauvegarder

Les données à administrer sont

- les répertoires utilisateur, ils sont résidentes sous le répertoire /home
- les scripts du répertoire /root/admin
- certains fichiers système du répertoire /etc qui contiennent les fichiers de paramétrage et d'environnement du serveur.

### Cycles de sauvegarde

Les sauvegardes sont organisées autour de deux cycles, l'un quotidien, l'autre hebdomadaire. Chacun de ces cycles est placé dans sa partition respective, les sauvegardes sont cadencées automatiquement par un scheduler intégré à Linux.

### Sauvegardes quotidiennes

Les sauvegardes quotidiennes sont au nombre de sept, elles sont identifiées par leur préfixe de 0 à 6, correspondant respectivement au Dimanche et au Samedi. Ce préfixe est obtenu au plan du système par la commande

```
date +%w
```

Ce préfixe ainsi obtenu nomme les fichiers du jour comme suit :

```
0.file.log          Liste des fichiers sauvegardés le Dimanche
```

```
0.tar              Concaténation des répertoires de /home du Dimanche
```

Chaque module sauvegardé est donc composé d'un fichier d'index et d'un fichier concaténant toutes les données. En fin de sauvegarde l'ensemble des fichiers est compressé par la commande gzip.



La partition contient au maximum sept fichiers « data » compressés et autant de fichiers listes, ce choix permet de retrouver facilement le ou les fichiers à restaurer.

La sauvegarde est lancée par la commande :

```
tar -cvvf chemin_et_fichier_destination /repertoire_source_a_archiver > fichier_liste
```

une fois l'opération achevée la destination contient la concaténation des fichiers et répertoires contenus dans le **repertoire\_source\_a\_archiver**, le fichier liste contient le nom et le chemin de tous les fichiers ainsi concaténés.

Les fichiers de données et d'index, la liste des fichiers compressés ainsi obtenus sont compressés par gzip. Toutefois, dans le répertoire /tmp placé sous le répertoire d'accroche, la liste reste disponible en clair pour la dernière sauvegarde.

## Sauvegardes hebdomadaires

Les sauvegardes quotidiennes sont écrasées par la nouvelle sauvegarde, le Lundi courant écrase le Lundi précédant... un cycle d'échappement hebdomadaire permet de conserver les données avec un mois de recul si l'on recycle les sauvegardes hebdomadaires sur quatre semaines.

Il est donc défini un cycle hebdomadaire en calculant le modulo du numéro de semaine dans l'année modulo le nombre de semaines d'historique que l'on souhaite conserver. Si on fixe cet historique à 7 (sept), dans ce cas on obtient un nombre de 0 à 6 qui permet de créer un nouveau cycle, semblable à la sauvegarde quotidienne mais sur la base de la semaine.

## Récupération des données

La récupération des données se passe en quatre étapes :

1. copie du fichier obtenu par gzip dans un répertoire intermédiaire.
2. Décompression de ce fichier
3. extraction locale du fichier tar
4. restitution du ou des fichiers à leur propriétaire.

Ces étapes terminées, on purge les données du répertoire intermédiaire.

## Exemple de séquence de récupération

- On souhaite récupérer un fichier archivé dans la dernière sauvegarde du Mardi, Rappel le Mardi vaut 2.
- La partition affectée à la sauvegarde est /dev/hda4

On passe les commandes suivantes après s'être logué en tant que « root » :

```
mount /dev/hda4 /mnt/bu
rm -f /mnt/bu/tmp/*
cp /mnt/bu/daily/2.* /mnt/bu/tmp/
gunzip /mnt/bu/tmp/2.*
cd /mnt/bu/tmp
tar -xvzf 2.tar
```

La décompression est réalisée dans le répertoire courant, ici /mnt/bu/tmp

Les fichiers sont disponibles dans ce répertoire, les droits initiaux sont restitués, ils peuvent être récopiés pour remise à disposition.



## ANNEXES

### Annexe 1 Script d'ajout de stations de travail au domaine

```
#####  
# Ajout de Client de Domaine SAMBA  
#  
# appel : /root/admin/deviceadd NOM_NETBIOS  
#  
#####  
  
pc=$1  
  
/usr/sbin/useradd -s /bin/false -d /dev/null $pc\  
if [ $? -eq 0 ] ; then  
    echo "Creation UNIX device = OK pour "$pc  
else  
    echo "Erreur creation UNIX de "$pc" corriger probleme"  
    echo "reprendre a la console !!!"  
    echo ""  
    exit  
fi  
  
smbpasswd -a -m $pc  
if [ $? -eq 0 ] ; then  
    echo "Creation SAMBA device = OK pour "$pc  
else  
    echo "Erreur creation SAMBA de "$pc" corriger probleme"  
    echo "reprendre a la console !!!"  
    echo ""  
fi
```



## Annexe 2 Fichier de configuration SAMBA

```
[global]
workgroup = SMRVILLEBON
Netbios name = smrserveur
server string = MAIRIE SMR Linux Server 2
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

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

#===== Share Definitions =====

# Répertoire utilisateur, le proprio est en RW
# le reste du monde est interdit d'accès
[homes]
comment = Home Directories
path = /home/%U
create mask = 600
directory mask = 700
browseable = no
writeable = yes

# Un-comment the following and create the netlogon directory for Domain Logons
[netlogon]
comment = Network Logon Service
path = /opt/netlogon
guest ok = yes
writable = no
share modes = no

# Gestion de l'itinerance
[Profiles]
path = /home/profile
browseable = no
guest ok =yes

# Repertoire partagé avec tous les utilisateurs
# groupe users en RW
# Les reste du monde en Lecture seule
[public]
comment = Repertoire commun
path = /home/commun
public = yes
read only = no
create mask = 664
directory mask = 775

[bibliotheque]
comment = Repertoire des logiciels et applications
path = /opt/biblio
public = yes
read only = no
create mask = 660
directory mask = 770

[printers]
comment = Les imprimantes disponibles
path = /var/spool/samba
browseable = yes
public = yes
guest ok = yes
printable = yes
```



### Annexe 3 Script d'administration utilisateurs

```

#/bin/sh
#####
#
# Creation d'un utilisateur UNIX + SAMBA
# Modifie le 7 Aout 2007
# suppression de la creation de comptes consecutifs
# correction BUG dans la suppression de comptes
#
#####
VERSION="V 1.0 du 07/08/2007"

xUSER="-"
echo "" > /tmp/x_nom_linux

xGROUP="users"

xSHELL='/bin/bash'

xSMB_WINDOWS_ALIAS="-"
echo "" > /tmp/x_alias_samba

xPW=/etc/passwd
xSMBPW=/etc/samba/smbpasswd
xSMB_ALIAS_FILE=/etc/samba/smbusers

touch /tmp/x1
echo $(date) " Journal de la gestion des comptes" >> /tmp/x1

while [ TRUE ] ; do

    SORTIE="0"

    clear
    until [ $SORTIE != "0" ]
    do

        echo "      Valeurs courantes      "$VERSION
        echo "1 Utilisateur Unix = " $xUSER
        echo "2 Groupe                = " $xGROUP
        echo "3 Shell                    = " $xSHELL
        echo "4 Nom Windows              = " $xSMB_WINDOWS_ALIAS
        echo "5 "
        echo "6 Test sur le nom Linux en cours"
        echo "7 Effacer 1 compte Linux et Samba "
        echo "8 "
        echo ""
        echo ""
        echo "L = lister les comptes actifs"
        echo "- "
        echo "F = Fin et ecriture DATA / X = Fin sans ecriture"

        echo -n " Commande = " ; read CDE

        clear

        case $CDE in
        "1")
            echo -n "Utilisateur = " ; read xUSER
            echo "" > /tmp/x_nom_linux
            # Le nom UNIX est-il acceptable ? Test premier caractere est lettre
            echo $xUSER | grep [a-z] >/dev/null
            if [ $? -eq 1 ] ; then
                echo "Nom utilisateur UNIX = "$xUSER
                echo "Err : le premier caractere doit etre une lettre minuscule"
                echo "- "
                xUSER="-"
            fi
            echo $xUSER > /tmp/xu
            cat $xPW | cut -d ":" -f 1 | grep $xUSER >> /tmp/xu
            cat /tmp/xu | awk -f $HOME/admin/user_passwd_find > /tmp/xuu
        esac
    done
done

```



```
if [ $(cat /tmp/xuu) -eq 0 ] ; then
  echo "Le nom UNIX existe déjà ! "
  echo $xUSER > /tmp/x_nom_linux
  xUSER="-"
else
  echo "" > /tmp/x_nom_linux
fi
;;

"2")
echo -n "Groupe = " ; read xGROUP
echo "Fonction non implementee" ; xGROUP="users"
;;

"3")
echo -n "Valeur SHELL fixée dans cette version "
;;

"4")
echo -n "Nom alias Windows = " ; read xSMB_WINDOWS_ALIAS
echo "" > /tmp/x_alias_samba
# Le nom SAMBA est-il acceptable ? Test premier caractere est lettre
echo $xSMB_WINDOWS_ALIAS | grep [a-z] >/dev/null
if [ $? -eq 1 ] ; then
  echo "Nom utilisateur SAMBA-WINDOWS = "$xSMB_WINDOWS_ALIAS
  echo "Err : le premier caractere doit etre une lettre minuscule"
  echo "-"
  xSMB_WINDOWS_ALIAS="-"
fi
echo $xSMB_WINDOWS_ALIAS > /tmp/xu
cat $xSMB_ALIAS_FILE | cut -d "=" -f 2 | grep $xSMB_WINDOWS_ALIAS >> /tmp/xu
cat /tmp/xu | awk -f $HOME/admin/user_smb_find > /tmp/xuu

if [ $(cat /tmp/xuu) -eq 0 ] ; then
  echo "Erreur Le nom ALIAS Windows existe déjà ! "
  echo $xSMB_WINDOWS_ALIAS > /tmp/x_alias_samba
  xSMB_WINDOWS_ALIAS="-"
else
  echo "" > /tmp/x_alias_samba
fi
;;

"5")
;;

"6")
echo "Tester les parametres de "
;;

"7")
echo "Supprimer compte Samba puis Linux"
if [ $(cat /tmp/x_nom_linux | wc -c) -eq 1 ] ; then
  echo "Impossible de supprimer un nom inexistant !!! "
  echo $xUSER > /tmp/x_nom_linux
else

  nsb=$(cat /tmp/x_nom_linux)
  echo "Tentative suppression de "$nsb

  # on supprime en premier lieu l_entree smbpasswd
  touch /tmp/smbpasswd ; rm /tmp/smbpasswd
  cp /etc/samba/smbpasswd /tmp/smbpasswd
  smbpasswd -x $nsb
  if [ $? -eq 0 ] ; then
    echo "Suppression SAMBA de "$nsb" dans smbpasswd OK"
  else
    echo "Erreur Suppression de "$nsb" dans smbpasswd"
  fi
fi

# traitement du fichier des alias
touch /tmp/smb_tmp ; rm /tmp/smb_tmp
cp /etc/samba/smbusers /tmp/smbusers
```





```

xx=$(cat /tmp/smbusers | wc -l)
num_user=1
until [ $num_user -gt $xx ] ; do
    lig=$(cat /tmp/smbusers | head -n $num_user | tail -n 1)
    nom=$(echo $lig | cut -d "=" -f 1)
    #echo $nom ; echo $lig ; exit
    if [ -z $nom ] ; then
        echo $lig >> /tmp/smb_tmp
    else
        # supprimer les espaces entre la fin du mon et le signe =
        echo $nom > /tmp/smb_nom
        if [ $nsb != $(cat /tmp/smb_nom) ] ; then
            echo $lig >> /tmp/smb_tmp
        else
            echo "Suppression ALIAS de "$lig" dans smbusers : OK"
        fi
    fi
    let num_user++
done

echo "Traitement nom Linux"
# si la lg du fichier vaut 1 il est vide
if [ $(cat /tmp/x_nom_linux | wc -c) -eq 1 ] ; then
    echo "Impossible de supprimer un nom inexistant !!! "
    echo $xUSER > /tmp/x_nom_linux
else
    /usr/sbin/userdel -r $(cat /tmp/x_nom_linux)
    if [ $? -eq 0 ] ; then
        echo "Suppression Linux de "$(cat /tmp/x_nom_linux) " dans passwd :
OK"

    else
        echo "Suppression Linux de "$(cat /tmp/x_nom_linux) "Erreur"
        # Attention il faut passer un nom
    fi
fi
cp /tmp/smb_tmp /etc/samba/smbusers

xUSER="-"
xSMB_WINDOWS_ALIAS="-"

;;

"8")
echo "Fonction 8 non implementee"
;;

[Ll])
clear
echo "Liste des utilisateurs actifs mode Windows"
# on extrait de smbpasswd les users avec mot de passe valide
cat /etc/samba/smbusers | sort | more
echo -n "Retour au menu principal : frapper Entrée"
read aa
clear
;;

[Ff])
echo "Test de validité des paramètres"
# xUSER xGROUP xSHELL $xSMB_WINDOWS_ALIAS
SORTIE="1"
if [ $xUSER == "-" ] ; then
    SORTIE="0"
    echo "Erreur nom UNIX"
fi

if [ $xGROUP == "-" ] ; then
    SORTIE="0"
    echo "Erreur GROUP"
fi

if [ $xSHELL == "-" ] ; then
    SORTIE="0"
    echo "Erreur SHELL"

```



```
fi

if [ $xSMB_WINDOWS_ALIAS == "-" ] ; then
    SORTIE="0"
    echo "Erreur nom WINDOWS"
fi

;;

[Xx])
clear
echo "Sortie sans modification"
echo "-"
exit
;;

*)
echo "Commande inattendue = " $CDE
;;

esac

done

# Parametres corrects, on ecrit
# Unix user add
echo "Ajout de "$xUSER "aux utilisateurs UNIX sans mot de passe"
/usr/sbin/useradd -d /home/$xUSER -g users -s $xSHELL -n $xUSER
echo "Ajout de "$xUSER "aux utilisateurs SAMBA avec mot de passe"
smbpasswd -a $xUSER

# samba add + ajout alias windows
echo "Ajout de "$xUSER "avec comme alias "$xSMB_WINDOWS_ALIAS
echo $xUSER" = "$xSMB_WINDOWS_ALIAS >> /etc/samba/smbusers

xUSER="-"
xSMB_WINDOWS_ALIAS="-"

#
echo " "
echo "Fin de creation"
echo " "
```

done



## Annexe 4 Sauvegarde

```

#/bin/sh
#####
# Sauvegarde des repertoires sous /home
#
# prerequis : les repertoires suivants doivent exister
#   /mnt/bu
#   /home/root/syst_files
# dans la partition a monter doivent exister
#   /mnt/bu/daily
#   /mnt/bu/weekly
# ces repertoires sont crees apres montage
#
# La destination est specifiee sans $DEST
#####

SAUV="/mnt/bu/"
DEST="/dev/hda4"
SRCE="/home/"
SYSF=/home/root/syst_files/

# Recup du jour de la semaine 0=Dimanche
DOW=$(date +%w)
# Recup du numero de semaine dans l'annee modulo cycle
CYCLE=5
N WEEK=$(expr $(date +%W) % $CYCLE)

echo $(date) " Depart procedure de sauvegarde"

echo "Montage "$DEST" sur "$SAUV
mount $DEST $SAUV
if [ $? -ne 0 ] ; then
    echo -n "Erreur montage "$DEST
    df | grep ^$DEST > /dev/null
    if [ $? -eq 0 ] ; then
        echo "La partition etait deja montee : tentative demontage et remontage "
        umount $DEST
        if [ $? -eq 0 ] ; then
            echo -n "Demontage OK "
        fi
        mount $DEST $SAUV
        if [ $? -eq 0 ] ; then
            echo "Montage suite a erreur OK"
        else
            echo "Erreur remontage : sortie panique !!!!!"
            exit
        fi
    else
        echo "Erreur montage non recouvrable : sortie panique !!!!!"
        exit
    fi
fi

# Test presence du repertoire temporaire de reception
touch $SAUV/tmp/bidon
if [ $? -eq 1 ] ; then
    echo "Creation du repertoire temporaire pour Backup"
    mkdir $SAUV/tmp
fi

# Preparation sauvegarde de quelques fichiers systeme
rm -R $SYSF ; mkdir $SYSF
cp /etc/samba/* $SYSF
cp /etc/passwd $SYSF

# Lancement de la sauvegarde dans la partition temporaire
cd $SAUV/tmp ; touch bidon ; rm ./ *
echo $(date) " Depart depart archivage des fichiers"
tar -cvvf $DOW.tar /home/ 2>/dev/null > $DOW.file.log

# Copie de puis le repertoire temporaire vers quotidien

```



```
touch $SAUV/daily/$DOW.bidon
rm $SAUV/daily/$DOW*
cp $SAUV/tmp/* $SAUV/daily/
cd $SAUV/daily ; gzip $DOW* ; ls -l
echo $(date)"Fin sauvegarde quotidienne sur "$DEST" "

# Traitement hebdo du Lundi
if [ $DOW -eq 1 ] ; then
    cp $SAUV/daily/$DOW* $SAUV/weekly/
    cp $SAUV/weekly/$DOW.tar.gz $SAUV/weekly/$NWEEK.week.tar.gz
    cp $SAUV/weekly/$DOW.file.log.gz $SAUV/weekly/$NWEEK.week.file.log.gz

    echo "Contenu repertoire sauvegarde hebdomadaire "
    ls -l $SAUV/weekly
    echo "Fin execution sauvegarde hebdomadaire"
fi

echo "Occupation des partitions"
df

echo -n $(date)" Fin des sauvegardes sur "$DEST
cd /root
umount /mnt/bu
if [ $? -eq 0 ] ; then
    echo " ----> Demontage OK"
else
    echo " ----> Erreur demontage <-----"
fi
```

## Annexe 5 Tâches planifiées

```
#####
# crontab pour root
#
#####
#min hour DOM MNTN DOW commande
50 22 ** * cat /root/backup.daily.log >> /root/backup.log
0 23 ** * /root/admin/backup > /root/backup.daily.log
0 8 ** 1,3,5 cat /root/backup.daily.log | lpr

0 3 1* * date >> /root/disk_check.log
30 3 1* * /sbin/e2fsck -f /dev/hda4 >> /root/disk_check.log
```