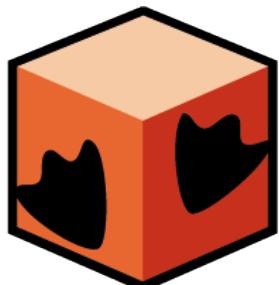


# Formation

---



**Linbox**

**Linux pour exploitants**

Formation

*Nos références FOR/LPE/001/001 du 27/05/2004*

## Fiche de suivi de document

### Identification

Unité	Linbox/Free & ALter Soft
Client	Tous
Intitulé du projet	Linux pour exploitants
Type de document	Formation
Localisation	Machine soda de Linbox/FAS
Document de référence	
Support magnétique	/a/soda/home/doc/any/formation/linux_pour_exploitants/Linux_pour_exploitants.sxw

### Visa

	<i>Responsable</i>	<i>Date</i>	<i>Visa</i>
Rédaction	Nicolas RUEFF	27/05/04	NR
Vérification	Arnaud LAPREVOTE	27/05/04	AL
Validation	Ludovic DROLEZ	27/05/04	LD

### Diffusion

<i>Entreprise</i>	<i>Destinataire</i>	<i>Nb copies</i>	<i>Pour action</i>	<i>Pour info</i>
Publix		1	X	X

### Historique

<i>Version</i>	<i>Nature</i>	<i>Auteur</i>	<i>Date</i>
V1.0	Création	Nicolas RUEFF	27/05/04

## TABLE DES MATIÈRES

1.Objet du document.....	7
2.Le projet.....	8
2.1.Contexte et objectifs.....	8
2.2.Remarques techniques.....	8
2.3.Documents de référence.....	8
3.Terminologie.....	9
3.1.Définitions.....	9
3.2.Conventions.....	9
4.Guide de support niveau I.....	10
4.1.Le support niveau I sous Linux.....	10
4.2.Comprendre le problème.....	10
4.2.1.Détermination.....	10
4.2.2.Délimitation.....	10
4.2.3.Reproduction.....	10
4.3.Est-ce un problème qu'on peut résoudre ?.....	11
4.4.Où trouver des solutions.....	11
4.4.1.Dans la base de solutions.....	11
4.4.2.Chez vos collègues.....	11
4.4.3.Dans les pages de manuel ou d'information.....	11
4.4.4.Dans les Howtos et autre tutoriaux.....	11
4.4.5.Sur Google.....	12
4.4.6.Sur le site du logiciel.....	12
4.4.7.Dans les archives des newsgroups.....	12
4.5.Maintenir une base de solutions.....	13
4.6.questionnaire type de support de niveau I.....	14
4.7.Rapport d'incident.....	15
5.Débuter en Console.....	16
5.1.Se logguer.....	16
5.2.Syntaxe d'une commande Linux .....	17
5.3.Passer d'une console à une autre.....	17
5.4.Trouver de l'aide.....	17
5.5. Répertoires et fichiers .....	18
5.6.Droits d'accès.....	19
5.6.1.Notion de droits.....	19
5.6.2.Droits d'accès.....	20
5.6.3.Catégories d'utilisateurs.....	21
5.6.4.Identification des droits.....	21
5.6.5.Remarques importantes.....	23

5.6.6.Droits étendus.....	23
<b>5.7.Liste des commandes de base à connaître.....</b>	<b>24</b>
5.8.Philosophie de la ligne de commande.....	25
5.9. Les petites commandes pratiques.....	26
5.10.Compression, encodage, archivage .....	27
<b>6.TP1 - Ligne de commande.....</b>	<b>28</b>
<b>7.Top - Monitoring.....</b>	<b>31</b>
7.1.Description de l'application.....	31
7.2.Principaux raccourcis.....	32
<b>8.MC - Midnight Commander.....</b>	<b>34</b>
8.1.Démarrage.....	34
8.2.Commandes standard.....	34
8.3.Raccourcis utiles.....	34
8.4.Configuration de base.....	35
8.5.Système de fichiers virtuel.....	35
8.6.Captures d'écran.....	36
<b>9.TP2 - Outils Avancés.....</b>	<b>37</b>
<b>10.Débuter en réseau.....</b>	<b>39</b>
<b>10.1.L'adressage réseau.....</b>	<b>39</b>
10.1.1.Le protocole IP.....	39
10.1.2.Le protocole ethernet.....	40
10.1.3.Le protocole TCP.....	40
10.1.4.Interaction des protocoles.....	41
<b>10.2.Le routage.....</b>	<b>41</b>
<b>10.3.Le hostname.....</b>	<b>42</b>
<b>10.4.L'adresse IP.....</b>	<b>43</b>
<b>10.5.Se connecter à une machine distante avec ssh.....</b>	<b>44</b>
10.5.1.Connexion avec authentification par mot de passe.....	44
10.5.2.Authentification par clé.....	45
<b>10.6.Se rendre la vie distante plus facile avec Screen.....</b>	<b>45</b>
<b>10.7.Les principaux outils de diagnostic réseau.....</b>	<b>46</b>
10.7.1.arp.....	46
10.7.2.ping.....	47
10.7.3.route.....	48
10.7.4.traceroute.....	49
10.7.5.netstat.....	51
10.7.6.resolv.conf.....	52
10.7.7.Résolution (inverse) de noms.....	53
<b>11.TP3 - Réseau.....</b>	<b>54</b>

12. Service Webmin.....	56
12.1. Architecture générale.....	56
12.2. Administration d'autres serveurs.....	58
13. Service DHCP.....	60
13.1. Architecture.....	60
13.2. Paramètres.....	60
13.3. Fichiers.....	60
13.4. Administration.....	60
13.5. Syntaxe.....	61
13.6. Webmin.....	62
14. Service DNS.....	66
14.1. Architecture.....	66
14.2. Paramètres.....	66
14.3. Fichiers.....	66
14.4. Administration.....	67
14.5. Syntaxe.....	67
14.6. Webmin.....	68
15. Service NFS.....	77
15.1. Architecture.....	77
15.2. Paramètres.....	77
15.3. Fichiers.....	77
15.4. Administration.....	78
16. Service NTP.....	79
16.1. Architecture.....	79
16.2. Paramètres.....	79
16.3. Fichiers.....	79
16.4. Administration.....	79
16.5. Syntaxe.....	80
16.6. Webmin.....	80
17. Service LDAP + SAMBA.....	84
17.1. Écrans de base.....	84
17.2. Gestion des utilisateurs.....	86
17.3. Gestion des groupes.....	91
17.4. Gestion des comptes.....	93
18. Services UML.....	94
18.1. Architecture.....	94
18.2. Paramètres.....	94

<b>18.3.Fichiers.....</b>	<b>95</b>
<b>18.4.Administration.....</b>	<b>95</b>
<b>18.5.Webmin.....</b>	<b>96</b>
<b>19.Maintenance LTSP.....</b>	<b>104</b>
<b>19.1.Démarrage de la machine - câblage.....</b>	<b>104</b>
<b>19.1.1.Problème 1.....</b>	<b>104</b>
<b>19.2.Obtention des paramètres réseau - DHCP.....</b>	<b>104</b>
<b>19.2.1.Problème 1.....</b>	<b>104</b>
<b>19.2.2.Problème 2.....</b>	<b>105</b>
<b>19.2.3.Problème 4.....</b>	<b>106</b>
<b>19.3.Récupération de l'image de boot - TFTP.....</b>	<b>106</b>
<b>19.3.1.Problème 1.....</b>	<b>106</b>
<b>19.3.2.Problème 2.....</b>	<b>107</b>
<b>19.4.Montage du système de fichier - NFS.....</b>	<b>107</b>
<b>19.4.1.Problème 1.....</b>	<b>107</b>
<b>19.5.Lancement de la session graphique - Xfree86.....</b>	<b>107</b>
<b>19.5.1.Problème 1.....</b>	<b>108</b>
<b>19.5.2.Problème 2.....</b>	<b>108</b>
<b>20.Maintenance de serveurs.....</b>	<b>109</b>
<b>20.1.espace disque disponible.....</b>	<b>109</b>
<b>20.2.Mémoire disponible.....</b>	<b>110</b>
<b>20.3.Charge et occupation processeur.....</b>	<b>111</b>
<b>20.4.Fichiers verrous (locks).....</b>	<b>111</b>
<b>20.5.Dépannage d'un serveur au comportement douteux.....</b>	<b>112</b>
<b>21.Annexes.....</b>	<b>113</b>
<b>21.1.Corrrection TP1 - Ligne de commande.....</b>	<b>114</b>
<b>21.2.Corrrection TP2 - Outils Avancés.....</b>	<b>117</b>
<b>21.3.Corrrection TP3 - Réseau.....</b>	<b>119</b>

## 1. OBJET DU DOCUMENT

---

Cette formation vise à permettre à des personnels d'exploitation d'avoir les bases minimum sous Linux pour pouvoir répondre aux demandes simples des utilisateurs sans obligatoirement faire appel à l'ingénieur système. Nous considérons que les personnes formées ne connaissent rien à linux, et que l'essentiel de l'infrastructure informatique de l'entreprise est sous Linux. Certains postes clients sont sous windows, d'autres sont des clients fins fonctionnant sous Linux.

## **2. LE PROJET**

---

### **2.1. CONTEXTE ET OBJECTIFS**

---

### **2.2. REMARQUES TECHNIQUES**

---

### **2.3. DOCUMENTS DE RÉFÉRENCE**

---

Nom du document	Référence

## 3. TERMINOLOGIE

---

### 3.1. DÉFINITIONS

---

Terme	Définition

### 3.2. CONVENTIONS

---

Sans objet.

## 4. GUIDE DE SUPPORT NIVEAU I

---

*La puissance d'un système OpenSource comme Linux est la masse de documentation disponible. Un problème rencontré a de grandes chances d'avoir déjà été traité. Le but de ce document est de vous aider à isoler un problème, puis à savoir où chercher les réponses pour résoudre le problème.*

### 4.1. LE SUPPORT NIVEAU I SOUS LINUX

---

Le support de niveau I vise à résoudre le plus rapidement possible des problèmes techniques de base, et ce sans l'appui d'une quelconque expertise.

Sous Linux, ce soutien est réalisé autour de trois outils:

- questionnaire type de résolution
- base de solutions issues d'expériences antérieures
- bases de connaissance issue du monde du logiciel libre

### 4.2. COMPRENDRE LE PROBLÈME

---

En informatique, 90 % des problèmes sont mal - voire jamais - résolus pour la simple raison qu'ils sont mal compris. Quand un problème est rencontré, il est impératif de répondre aux questions suivantes:

#### 4.2.1. DÉTERMINATION

---

- Quel outil cela touche-t-il ?
- Quels sont les symptômes ?
- Quels sont les messages d'erreurs exacts ?

#### 4.2.2. DÉLIMITATION

---

- À partir de quand le problème a-t-il surgi ?
- Qu'est-ce qui a changé sur la machine ?

#### 4.2.3. REPRODUCTION

---

- Comment le reproduire ?
- Peut-on le reproduire à partir d'un autre compte utilisateur sur la même machine ?

- Peut-on le reproduire à partir du même compte utilisateur sur une autre machine ?

## 4.3. EST-CE UN PROBLÈME QU'ON PEUT RÉSOUTRE ?

---

Il n'est pas forcément nécessaire de se plonger dans la documentation pour corriger des pseudo-problèmes. S'il n'est pas reproductible, il n'y a rien à corriger. La **reproductibilité** d'un problème se définit par une **liste d'actions à effectuer** pour reproduire le problème, et non par le fait que le problème se reproduit de temps à autre.

## 4.4. OÙ TROUVER DES SOLUTIONS

---

Par ordre de rapidité, voici les endroits où vous trouverez probablement des réponses aux problèmes posés.

### 4.4.1. DANS LA BASE DE SOLUTIONS

---

Voir plus bas.

### 4.4.2. CHEZ VOS COLLÈGUES

---

Ils peuvent en savoir plus que vous. À vous de vérifier, sachant que l'aveut de l'ignorance n'a jamais tué.

### 4.4.3. DANS LES PAGES DE MANUEL OU D'INFORMATION

---

- Les problèmes de logiciel se résolvent le plus souvent en lisant la page man associée. En général les problèmes les plus courant y sont décrits et commentés, et une lecture attentive de ses pages permet d'apprendre beaucoup plus qu'on ne le penseraient de prime abord.
- Les logiciels sont le plus souvent livrés avec une excellente documentation. Un petit tour dans `/usr/share/doc/<nom-du-logiciel>` peut avoir son utilité

### 4.4.4. DANS LES HOWTOS ET AUTRE TUTORIAUX

---

- Les Howtos sont des documents qui ont été écrits pour répondre à un problème particulier: mettre en place un serveur NFS, mettre à jour un système, ... Ils sont généralement installés sur le système (par exemple dans `/usr/share/doc/howto`), mais peuvent être trouvés sur internet (par exemple ici: <http://www.tldp.org/HOWTO/HOWTO-INDEX/categories.html>)

- Les FAQ (Frequently Asked Questions) sont des documents rassemblant les problèmes les plus courants ainsi que leur solutions.
- Les guides (comme sur <http://www.tldp.org/guides.html>) sont également une bonne source d'informations.

#### ***4.4.5. SUR GOOGLE***

---

Le problème de Google, c'est l'exhaustivité de ses résultats. Il existe quelques moyens simples pour limiter les résultats renvoyés aux plus utiles:

- Votre problème est spécifique à linux ? essayez avec google.fr/linux !
- Votre problème est spécifique à microsoft ? essayez avec google.fr/microsoft !
- Recherchez en priorité dans votre langue

#### ***4.4.6. SUR LE SITE DU LOGICIEL***

---

Cette remarque s'applique en particulier aux logiciels OpenSource: les sites de référence ([samba.org](http://samba.org) pour samba, [debian.org](http://debian.org) pour debian, ...) possèdent en général des forums dans lesquels il peut être intéressant de fouiller.

#### ***4.4.7. DANS LES ARCHIVES DES NEWSGROUPS***

---

Les newsgroups sont des groupes de discussion autour d'un certain nombre de problématique. Fouiller les archives de ces newsgroups (sur <http://www.google.fr/grphp>) peut être très fastidieux, mais également assez efficace.

Ces groupes sont organisés comme un arbre. La hiérarchie **comp.\***, par exemple, est l'arbre qui regroupe tous les newsgroups gravitant autour de l'informatique.

## 4.5. MAINTENIR UNE BASE DE SOLUTIONS

---

Le plus frustrant quand on a découvert d'où venait un problème, c'est de se rappeler qu'on y a déjà été confronté, sans se souvenir de ce qu'on a fait pour y remédier. Il existe une méthode très simple pour maintenir une base de solutions: la méthode QQOQCP (dérivée du monde de l'industrie):

- Qui est concerné: service, groupe de personnes
- de Quoi s'agit-il: description de la manipulation pour reproduire le problème.
- Où: sur une machine particulière, un groupe de personnes ...
- Quand: circonstances particulières, ...
- Comment le résoudre: dérouler la manipulation pour corriger le problème.
- Combien: estimation des retards et coûts induits par le problème.

## 4.6. QUESTIONNAIRE TYPE DE SUPPORT DE NIVEAU I

---

### 1. Pour l'utilisateur:

1. Sur quelle machine travaille l'utilisateur
2. Quels sont les symptômes
3. Quel est le message d'erreur
4. Quelle est la marche à suivre pour reproduire l'erreur
5. L'erreur est-elle propre à la machine, au compte utilisateur

### 2. Pour vous:

1. Délimiter très finement le périmètre du problème
  - en contactant d'autres services
  - en contactant d'autres sites
2. Établissez-vous une fiche de route
  - comment vérifier l'origine du problème
  - comment le régler, ou le réduire
  - comment revenir en arrière
3. Si le problème dépasse vos connaissances, référez-vous
  - aux fiches d'incident,
  - à vos collègues,
  - à vos sources de connaissance

Si vous n'êtes pas certain de la marche à suivre, qu'un service critique est touché où que vous savez ne pas savoir la compétence: **ne faites rien qui puisse perturber le fonctionnement des autres services.**

## 4.7. RAPPORT D'INCIDENT

---

Rapporté par

le

Machine  
impactée

temps  
d'intervention

---

### ***RÉSUMÉ DE L'INCIDENT***

---

---

### ***MESURES CORRECTIVES***

---

---

### ***SOURCES D'INFORMATION SUPPLÉMENTAIRES***

---

## 5. DÉBUTER EN CONSOLE

Historiquement, Gnu/Linux s'utilise principalement depuis une console en mode texte. Le but de ce guide est de vous apprendre à vous orienter en ligne de commande, ou shell. Le shell est un interpréteur de commandes : il permet à l'utilisateur de dialoguer avec le système. C'est le programme généralement exécuté lorsqu'un utilisateur se connecte. Il affiche un "prompt" et attend les commandes de l'utilisateur. Le shell est aussi un langage de programmation interprété puissant. Il offre à l'utilisateur un environnement composé d'un ensemble de variables et d'alias et un langage de commandes.

### 5.1. SE LOGGUER

Quand vous allumez l'écran de la machine, vous arrivez au prompt de login :

```
Debian GNU/Linux 3.0 lna.emtstvit tty1
lna.emtstvit login:
```

Pour vous logguer, vous avez le choix entre :

- vous logguer en tant que root : tapez **root**, appuyez sur Entrée, ensuite tapez le **mot de passe root** et appuyez sur Entrée. Vous voyez alors apparaître un certain nombre de messages et enfin le prompt du root :

```
lna:~#
```

Quand vous êtes ainsi loggué en tant que root, vous avez tous les droits sur le système.

- vous logguer en tant que simple utilisateur : tapez votre **nom d'utilisateur**, appuyez sur Entrée, ensuite tapez votre **mot de passe** et appuyez sur Entrée. Vous voyez alors apparaître un certain nombre de messages et enfin le prompt de l'utilisateur :

```
user@lna:~$
```

Quand vous êtes ainsi loggué en tant que simple utilisateur, vous n'avez que des droits limités sur le système.

Rappel : l'utilisation du compte root est réservée à la modification de la configuration du système, à l'installation de packages et aux rares tâches qui nécessitent les droits de root ; pour toutes les autres tâches, il faut utiliser un compte utilisateur. En effet, l'utilisation du compte root est dangereuse : une fausse manipulation peut détruire le système... ce qui est impossible en tant que simple utilisateur !

## 5.2. SYNTAXE D'UNE COMMANDE LINUX

---

Lorsque la connexion est établie, un prompt s'affiche à gauche de l'écran : il attend de votre part une commande, un ordre qu'il pourra interpréter et exécuter. Le prompt est spécifique à la machine.

Chaque commande saisie au clavier doit être validée par un "return" (Enter) pour être exécutée. Soit :

Ina:~# commande -options <arguments>

avec:

- commande : ce que l'on veut faire
- options (facultatives) : comment on le fait
- arguments (éventuels) : sur quoi on le fait (fichiers ..)

La commande doit être saisie impérativement en minuscules pour être reconnue.

## 5.3. PASSER D'UNE CONSOLE À UNE AUTRE

---

Vous n'avez peut-être pas encore remarqué, mais vous disposez de plusieurs consoles. Au démarrage, vous arrivez sur la première console, appelée tty1. Vous pouvez passer à la deuxième console (appelée tty2) avec la combinaison de touches Alt-F2. Pour revenir à la première console, utilisez la combinaison de touches Alt-F1. Vous pouvez aussi utiliser Alt-Flèche Gauche et Alt-Flèche Droite pour passer d'une console voisine à l'autre. Par défaut, il y a 6 consoles.

Comme souvent, il existe un cas particulier: le terminal graphique (tty7 en général). Pour basculer d'un terminal graphique à un terminal texte, la combinaison de touches à utiliser est cette fois Ctrl-Alt-Fx.

## 5.4. TROUVER DE L'AIDE

---

La commande **man** (pour manual) fournit des informations (description, options, syntaxe) sur une commande Linux ou une application donnée (Ex: man ls, man emacs, man chmod).

```
Ina:~# man macommande
```

La commande **apropos** indique le nom des commandes et applications indexées par le mot-clé donné.

```
Ina:~# apropos mon-mot-clé
```

## 5.5. RÉPERTOIRES ET FICHIERS

Le système de fichiers (file system) est un arbre (organisation hiérarchique) dont les noeuds sont des répertoires (directories) et les feuilles des fichiers. Le fichier (chemin/nom) peut être désigné :

- soit par un path absolu (chemin absolu), qui commence par le caractère "/" (racine de l'arbre) suivie de la liste des noeuds (sous-répertoires, séparés par le caractère "/"), qu'il faut suivre depuis la racine pour atteindre le fichier

```
lna:~# cd /mon/repertoire
```

- soit par un path relatif : le fichier dans ce cas est désigné depuis le répertoire courant

```
lna:~# cd mon/repertoire
```

Chaque répertoire sous Unix à une fonction particulière :

/	C'est la racine du système (un raccourci facile serait de dire qu'il s'agit du C: de windows), à partir de laquelle tous les répertoires sont repérés, qu'ils soient distants, locaux ou situés sur une autre partition.
/bin	Contient les commandes de bases utilisables à partir du shell (grep, mount, cp ...).
/boot	contient les informations nécessaires au démarrage de la machine.
/dev	contient les fichiers spéciaux correspondant aux périphériques.
/etc	la plupart des fichiers de configuration.
/home	Il contient les répertoires personnels des utilisateurs.
/lib	contient les principales bibliothèques partagées (équivalent aux DLL de Windows)
/lost+found	c'est là que sont entreposés les résultats des scandisk quand ils ont lieu.
/mnt	les répertoires utilisés pour monter temporairement un système de fichiers. /mnt/floppy pour la disquette, /mnt/cdrom pour le cdrom ...
/opt	Permet de reproduire une arborescence /usr complète à partir d'un nouveau répertoire.
/proc	un répertoire factice, dont les fichiers contiennent des infos sur l'état du système et des processus en cours d'exécution.
/root	le répertoire personnel et privé de l'administrateur système : root.
/sbin	Contient les commandes de base nécessaires à l'administration système (fsck, mke2fs ...)
/tmp	Répertoire libre d'utilisation pour des contenus temporaires
/usr	C'est l'équivalent de C:\Programme Files\ Mais en plus ordonné.

/usr/bin	les exécutables (ils n'ont pas l'extension .exe)
/usr/doc	a documentation sur les applications installées.
/usr/lib	les bibliothèques partagées (DLL) non vitales.
/usr/local	une sous-hierarchie qui contient des logiciels compilés sur place à partir des sources. Organisation similaire à /usr.
/usr/man	le manuel en ligne. Les fichiers sont compressés.
/usr/sbin	Des exécutables pour l'administration réseau et système
/usr/share	Des fichiers de données.
/usr/src	Les sources de certains logiciels, principalement le noyau de Linux (/usr/src/linux)
/var	des données fréquemment réécrites, comme les logs
/var/lock	Des fichiers qui servent à marquer l'utilisation de certaines ressources.
/var/log	Les journaux (log) du système.
/var/run	principalement des infos sur les services en fonctionnement.
/var/spool	Les spools: tout ce qui est "de passage" en attendant d'être utilisé par un logiciel. Ca inclut entre autres le mail, les news, les files d'attente des imprimantes...

Le home directory (~) est le répertoire d'accueil dans lequel on se trouve après avoir établi la connexion sur le compte.

Certains caractères ne sont pas autorisés dans le nom du fichier. Notamment, par exemple, le caractère espace, accepté dans les noms de fichiers sous Mac, joue le rôle de séparateur sous UNIX (il sépare commande, options et paramètres les uns des autres). Pour manipuler malgré tout un fichier qui contient ce type de caractère, le nom de ce fichier devra être encadré de guillemets (ex: rm "seq 23.dat"). **En règle générale, il est préférable de se limiter aux caractères alphabétiques, numériques ainsi que "-" et "\_".**

## 5.6. DROITS D'ACCÈS

### 5.6.1. NOTION DE DROITS

Les droits d'accès aux fichiers (appelés encore modes ou permissions) sont un point essentiel du système Unix. Ils permettent de définir des droits différents sur un même fichier selon la catégorie d'utilisateurs.

Ainsi les manipulations de fichiers sont restreintes selon les droits alloués à chaque fichier. A chaque catégorie d'utilisateur correspond des droits spécifiques sur un fichier.

Pour afficher à l'écran les droits alloués à un fichier, il faut utiliser la commande `ls -l` qui permet de lister les fichiers d'un répertoire avec toutes les informations connexes possibles dont les droits du fichier.

```
lna:~# ls -l
-rw-r--r--  1 root    test      98304 nov   6  2003
20055500d00.doc
-rwxr-xr-x  1 root    test      735  fév 19  2003
copiemime.sh
-rwxr-xr-x  1 root    test      694  fév 19  2003
copenotes.sh
-rwxrw-r--  1 root    test      16322 jan 26 11:06
dhcpd.conf
drwxr-xr-x  5 root    test      4096 jan 16 08:43
Documents
drwxrwxr-x  3 root    test      4096 fév 25 12:08 temp
```

En préfixe des droits (et ici en bleu) est affiché le type du fichier (`d` pour les répertoires et `-` pour les fichiers normaux et les exécutables).

On peut voir dans cet exemple que tous les fichiers sont du même propriétaire dont le nom est `root`. Ce propriétaire faisant partie du groupe appelé `test`.

### 5.6.2. DROITS D'ACCÈS

Il existe trois niveaux d'accès à un fichier:

- **Lecture**

- l'accès en lecture autorise la lecture du fichier, c'est-à-dire qu'il est possible d'édition ce fichier avec une application quelconque pour en voir le contenu. Cet accès est désigné par la lettre `r` (`read`).

- Alloué à un répertoire, ce droit permet de lister les fichiers qu'il contient.

- **Écriture**

- l'accès en écriture permet de modifier un fichier et de le supprimer. Il est désigné par la lettre `w` (`write`).
- Alloué à un répertoire, il autorise la modification et la suppression des fichiers qu'il contient quelques soient les droits d'accès des fichiers de ce répertoire (même s'ils ne possèdent pas eux-même le droit en écriture).

- **Exécution:**

- l'accès en exécution permet à un fichier exécutable d'être lancé et à un répertoire d'être ouvert. Il est désigné par la lettre `x` (`execute`). Pour qu'un programme puisse être exécuté, il est indispensable que le droit en exécution sur ce fichier soit autorisé pour l'utilisateur qui souhaite le lancer (Ce droit en exécution est sans effet lorsqu'il est affecté à un fichier qui n'est pas un exécutable).

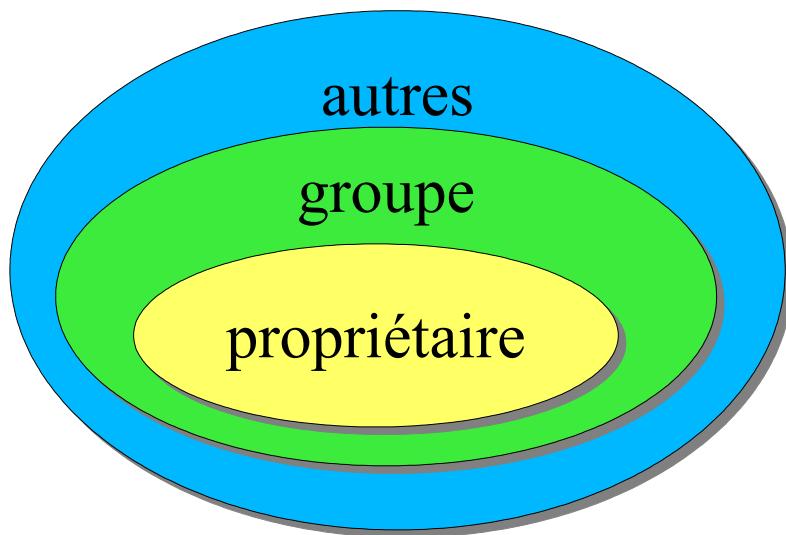
- Quant à un répertoire, il est tout aussi indispensable que son droit en exécution soit autorisé pour qu'on puisse accéder aux fichiers qu'il contient.

### 5.6.3. *CATÉGORIES D'UTILISATEURS*

A un fichier on affecte les droits correspondants à trois catégories d'utilisateurs.

- **Propriétaire:** le propriétaire d'un fichier est la personne qui le crée. Il est désigné par la lettre **u** (**user**).
- **Groupe:** Un groupe d'utilisateur est un ensemble d'utilisateurs privilégiés ayant en général des permissions moindre que le propriétaire d'un fichier mais plus grandes que la catégorie qui suit. Cette catégorie est désignée par la lettre **g** (**group**).
- **Autres:** Cette catégorie regroupe tous les utilisateurs qui ne sont ni le propriétaire d'un fichier ni faisant partie du même groupe que le propriétaire. On les désignent par la lettre **o** (**other**).

Ces droits sont répartis selon un modèle concentrique:



Un ensemble de propriétaires forme un groupe, qu'un ensemble de groupes forme la catégorie "autres". L'accès à un sous ensemble concentrique suppose a priori d'obtenir des droits supplémentaires.

### 5.6.4. *IDENTIFICATION DES DROITS*

#### *IDENTIFICATION GLOBALE*

À chaque catégorie d'utilisateur on associe un triplet de droits : lecture, écriture et exécution. Lorsqu'un droit est alloué, on voit la lettre correspondante (**r**, **w** ou **x**). Si le droit est refusé, on voit un tiret (-):

**rwxrw-r--**

Dans cet exemple, le propriétaire dispose des droits de lecture, d'écriture et d'exécution, le groupe les droits de lecture et d'écriture, les autres ne disposent que du droit de lecture.

#### *COMBINAISONS DES DROITS*

A chacune des 3 catégories d'utilisateur, on associe d'une des 8 combinaisons différentes possibles pour l'allocation des droits que le tableau ci-dessous récapitule.

Triplet	Droits correspondants
---	aucun
--x	exécution
-w-	écriture
-wx	écriture et exécution
r--	lecture
r-x	lecture et exécution
rw-	lecture et écriture
rwx	lecture, écriture et exécution

Les droits globaux d'un fichier sont identifiés par l'association de 3 triplets de droits (un par niveau). Le tableau suivant regroupe quelques unes de ces combinaisons possibles:

Droits globaux	Description
<b>rwxr-xr-x</b>	Le propriétaire a tous les droits, et le groupe ainsi que les autres n'ont pas accès en écriture.
<b>rwxr---r--</b>	Le propriétaire a tous les droits, et le groupe ainsi que les autres n'ont accès qu'en lecture.
<b>rwxr-x---</b>	Le propriétaire a tous les droits, le groupe possède les droits de lecture et d'exécution alors que les autres n'ont aucun droit.
<b>rwx-----</b>	Le propriétaire a tous les droits mais le groupe et les autres aucun.
<b>rw-r--r--</b>	Le propriétaire possède les droits de lecture, écriture mais pas exécution. Et le groupe et les autres ont le droit en lecture.

Droits globaux	Description
<b>rw-rw----</b>	Le propriétaire et le groupe ont le droit en lecture et écriture mais les autres n'ont aucun droit.

Il est offert au propriétaire d'un fichier (et seulement à lui seul) de modifier les droits du fichier. C'est-à-dire qu'il peut supprimer des droits ou bien en rajouter de nouveaux à chacune des trois catégories d'utilisateur (voir la commande **chmod**).

### 5.6.5. *REMARQUES IMPORTANTES*

- **Exécutable:** Un programme ne peut être exécuté que si le fichier exécutable coorespondant possède le droit d'exécution dans la catégorie à laquelle appartient l'utilisateur.
- **Répertoire:** On ne peut accéder à un fichier que si les répertoires successifs constitutifs du chemin absolu de ce fichier possèdent le droit en exécution. Pour pouvoir lister les fichiers d'un répertoire, ce dernier doit être accessible en lecture.
- **Fichier:** Le droit en exécution n'a aucune incidence sur un fichier non exécutable. Par contre, un script (c'est-à-dire un fichier texte contenant des commandes du Shell) doit avoir les droits en lecture et en exécution pour pouvoir être interprété et exécuté par le Shell.

### 5.6.6. *DROITS ÉTENDUS*

#### **SUID**

Lorsqu'un utilisateur lance un programme, ce programme s'approprie les droits de l'utilisateur pour la manipulation des fichiers et non pas ceux du propriétaire du fichier.

Mais il est quelque fois nécessaire de permettre à d'autres utilisateurs l'accès à des données normalement protégées. Ce droit SUID (s) permet de prêter à un utilisateur de façon temporaire, des droits supplémentaires par l'intermédiaire d'un programme (fichier exécutable).

En exécutant un programme possédant un droit SUID, un utilisateur s'approprie les droits du propriétaire du fichier exécutable durant le temps d'exécution du programme. Ces droits supplémentaires ne sont valables que sur les fichiers appelés par le programme et les opérations effectuées par le programme et que durant le temps d'exécution du programme.

Son utilité vient du fait qu'il n'est pas besoin d'accorder durablement des droits étendus à n'importe qui sur des fichiers sensibles. Puisque l'accès à ces fichiers est filtré par un programme qui est seul à prendre des initiatives sur ces fichiers.

#### **SGID**

Le droit SGID (g) fonctionne différemment selon qu'il est affecté à un fichier exécutable ou à un répertoire.

- **Exécutable:** Sur un fichier exécutable, le SGID est similaire au droit SUID vu précédemment sauf qu'il donne à un utilisateur les droits du groupe auquel appartient le propriétaire de l'exécutable et non plus les droits du propriétaire.
- **Répertoire:** Tout fichier créé porte les droits du masque de protection de son propriétaire. De plus, tout fichier porte un UID (identificateur de propriétaire) et un GID (identificateur de groupe). C'est-à-dire qu'un fichier est toujours identifié par le nom de son propriétaire ainsi que par le nom du groupe auquel appartient le propriétaire. Le droit SGID, lorsqu'il est affecté à un répertoire, casse cette logique. Puisque tout nouveau fichier créé dans un répertoire marqué par le SGID sera de groupe non pas celui du propriétaire du fichier mais celui du propriétaire du répertoire. Ainsi, tout fichier créé dans un répertoire portant le SGID, héritera du groupe du propriétaire du répertoire.

#### *STICKY BIT*

---

Le droit Sticky Bit (appelé aussi bit collant) est alloué à la catégorie autres d'un répertoire.

Il permet d'interdire à tout utilisateur (sauf root) de supprimer un fichier dont il n'est pas le propriétaire, quelque soient ses droits.

Si le répertoire en question est accessible en écriture par n'importe quel utilisateur (rwxrwxrwx), n'importe qui peut poser ce bit collant qui protège tous les fichiers d'une suppression ou modification de la part d'un utilisateur autre que son propriétaire.

Ce bit collant permet donc d'aller à l'encontre du droit en écriture d'un répertoire dont héritent les fichiers du répertoire. Il est représenté symboliquement par t.

## 5.7. LISTE DES COMMANDES DE BASE À CONNAÎTRE

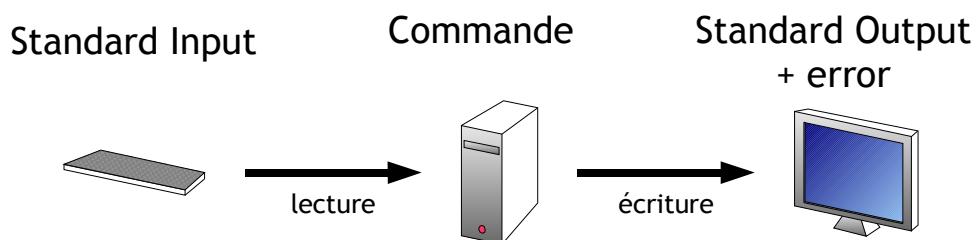
---

cat	Pour <b>afficher</b> le contenu d'un fichier: Ina:~# cat monfichier
cd	Pour <b>changer</b> de répertoire: Ina:~# cd /mon/repertoire (sous Linux, ~ représente le répertoire <b>HOME</b> de l'utilisateur)
chgrp	Pour changer le <b>groupe</b> d'appartenance d'un fichier: Ina:~# chgroup mongroupe monfichier
chmod	Pour changer les <b>droits d'accès</b> d'un fichier: Ina:~# chmod u=rw,g=r,o=r monfichier Les droits possibles sont r (lecture), w (écriture), x (exécution). Les droits sont changés pour l'utilisateur (u), le groupe (g), les autres (o)
chown	Pour changer l' <b>utilisateur</b> d'appartenance d'un fichier Ina:~# chown monutilisateur monfichier
cp	Pour <b>copier</b> un fichier: Ina:~# mv fichier-original fichier-final

du	Pour <b>afficher</b> la taille du répertoire: lna:~# du -h /mon/repertoire
find	Pour <b>trouver</b> un fichier: Pour changer le <b>groupe</b> d'appartenance d'un fichier lna:~# find /dans/ce/repertoire -name monfichier
grep	Pour trouver un <b>mot</b> dans un fichier: lna:~# grep monmot monfichier
less	Pour <b>lister</b> le contenu d'un fichier: lna:~# less monfichier
ln	Pour créer un <b>raccourci</b> vers un fichier: lna:~# ln fichier-original fichier-final
mkdir	Pour <b>créer</b> un <b>répertoire</b> : lna:~# mkdir /mon/repertoire
ls	Pour <b>lister</b> les fichiers d'un répertoire: lna:~# ls /mon/repertoire
mv	Pour <b>déplacer</b> un fichier: lna:~# mv fichier-original fichier-final
rm	Pour <b>supprimer</b> un <b>fichier</b> : lna:~# rm monfichier
rmdir	Pour <b>supprimer</b> un <b>répertoire</b> : lna:~# rmdir /mon/répertoire

## 5.8. PHILOSOPHIE DE LA LIGNE DE COMMANDE

De nombreuses commandes lisent leurs données (entrée = input) à partir de l'entrée standard (stdin), par défaut le clavier, et écrivent leurs résultats (sortie = output) dans la sortie standard (stdout) et les erreurs dans la sortie-erreur standard (stderr), par défaut l'écran, selon le schéma :



Si l'on souhaite rediriger les entrées et sorties, la commande prendra la syntaxe suivante :

```
lina:~# commande [-options] [arguments] < input-file > output  
file
```

avec les métacaractères de redirection suivants :

<	redirige l'entrée standard
>	redirige la sortie standard
>>	redirige et concatène la sortie standard
>&	redirige les sorties standard et erreur
>>&	redirige et concatène les sorties standard et erreur

Dans le même esprit, le caractère "|" (opérateur pipe) redirige la sortie standard (sdtout) d'une commande dans l'entrée standard (stdin) d'une autre commande. Plusieurs commandes peuvent être combinées ainsi:

```
lina:~# commande1 [-options] [arguments] commande2 | ...
```

Quelques exemples:

(pwd; ls -l) > fichier.out	écrit le nom du répertoire et le résultat de la commande ls dans fichier.out (le caractère ; permet d'enchaîner des commandes )
ls -lh > liste.archive	Écrit la liste des fichiers du répertoire courant dans le fichier liste.archive
grep -i dupont fichier > result	Enregistre uniquement les lignes du fichier fichier contenant dupont dans le fichier result.
cat file1 file2 > filen	concatène deux fichiers (contenu de file2 après file1) dans un troisième
cat file2 >> file3	Ajoute le contenu de file2 à la fin de file3
who   sort	tri et édite les utilisateurs connectés
ls -lh   less	édite page par page les noms de fichiers du répertoire

## 5.9. LES PETITES COMMANDES PRATIQUES

bc	une calculatrice en mode texte.
----	---------------------------------

cal	affiche un calendrier du mois courant. cal 2003 affiche un calendrier de l'année 2003.
date	donne l'heure système.
head -n <fichier>	affiche les n 1ères lignes du fichier.
pwd	affiche le nom du répertoire courant.
sort <fichier>	trie un fichier.
tail -n <fichier>	affiche les n dernières lignes du fichier.
tail -n <fichier>	surveille les changements d'un fichier
wc -l -w -c <fichier>	retourne le nombre de lignes, de mots, de caractères dans le fichier indiqué.
who	affiche la liste des utilisateurs connectés.
ctrl-l	permet de rafraîchir l'affichage d'une application en console quand l'affichage est perturbé (par un message d'erreur par exemple).
ctrl-r	permet de rappeler une commande dans l'historique de la ligne de commande

## 5.10. COMPRESSION, ENCODAGE, ARCHIVAGE

La compression d'un fichier vise à réduire la taille d'un fichier. Grossièrement, le taux de compression atteint est de 50-60 pourcent de la taille originelle.

gzip <fichier>	Compression. Génère un fichier.gz.
gunzip <fichier>	Décompression d'un fichier.gz.
tar cf <tarfile> <répertoire_à_tarer>	Archive (tare) un ensemble de fichiers ou les fichiers d'un répertoire en un fichier.tar unique (=tarfile).
tar xf <tarfile>	Désarchive (éclate, restaure) un fichier.tar (tarfile) en n fichiers d'origine.

## 6. TP1 - LIGNE DE COMMANDE

1. Allez dans votre HOME

2. Affichez le nom du répertoire courant

3. Créez un répertoire TP

4. Allez dans le répertoire créé

5. Affichez le contenu du répertoire courant

6. Décompressez l'archive du tp 1 dans le répertoire courant

7. Allez dans le répertoire lsg\_cl/long-noms

8. Afficher le nombre de fichiers du répertoire courant

9. Afficher le nombre de fichiers finissant par "89"

10. Déplacez les fichiers finissant par "977" dans ~/TP/lsg\_cl/long-noms.tmp

11. Listez le contenu de ce dernier répertoire

12. Supprimez ce dernier répertoire

13. Copiez le répertoire ~/TP/lsg\_cl/long-noms vers ~/TP/lsg\_cl/long-noms.tmp

14. Allez dans ce répertoire

15. Affichez la taille de ce répertoire

16. Supprimez tous les fichiers commençant par « **je\_suis\_un\_fichier** »

17. Affichez la taille de ce répertoire

18. Allez dans le répertoire ~/TP/lsg\_cl/invalid

19. Supprimez le fichier « **doit etre supprime** »

20. Supprimez le fichier « **-h** »

21. Allez dans le répertoire ~/TP

22. Trouvez quel fichier du répertoire **recherche** contient le terme « **gagne** »

23.Affichez la date

24.Concaténez la sortie de la commande date vers le fichier « **date-courante** »

25.Ajoutez la sortie de la commande cal vers le fichier « **date-courante** »

26.Affichez le contenu du fichier « **date-courante** »

27.Affichez les premières et dernières lignes du fichier « **date-courante** »

28.Afficher le contenu trié du fichier « **atrier.txt** »

29.Affichez le contenu trié du fichier « **atrier.txt** », uniquement les lignes contenant le mot "LIGNE"

30.Enregistrez le contenu trié du fichier « **atrier.txt** », uniquement les lignes contenant le mot "LIGNE", dans le fichier « **tri.txt** »

31.Affichez avec le pager le contenu du fichier caché du répertoire « **invalides** »

32.Allez dans le répertoire parent

33.Compressez le répertoire **lsg\_cl** dans l'archive « **lsg\_cl.tar.gz** »

## 7. TOP - MONITORING

Top est l'outil de monitoring le plus efficace sous Linux. Il permet d'un simple coup d'œil de juger de l'état d'un serveur et de décider des mesures à prendre.

### 7.1. DESCRIPTION DE L'APPLICATION

L'application top se lance depuis la ligne de commande:

```
lna:~# top
```

System load average: 0.12, 0.03, 0.01									
18 processes: 17 sleeping, 1 running, 0 zombie, 0 stopped									
CPU states: 0.0% user, 0.1% system, 0.0% nice, 99.9% idle									
Mem: 61084K total, 42096K used, 18988K free, 10968K buffers									
Swap: 0K total, 0K used, 0K free, 11324K cached									
PID USER COMMAND									
PRI	NI	SIZE	RSS	SHARE	STAT	%CPU	%MEM	TIME	
1	root	484	484	424	S	0.0	0.7	0:00	init
2	root	0	0	0	SW	0.0	0.0	0:00	keventd
3	root	19	19	0	SWN	0.0	0.0	0:00	ksoftirqd_CPU0
4	root	0	0	0	SW	0.0	0.0	0:00	kswapd
5	root	0	0	0	SW	0.0	0.0	0:00	bdflush
6	root	0	0	0	SW	0.0	0.0	0:00	kupdated
7	root	0	0	0	SW	0.0	0.0	0:02	kjournald
145	root	580	580	464	S	0.0	0.9	0:04	syslogd
148	root	528	528	380	S	0.0	0.8	0:00	klogd

157	root	9	0	508	508	444	S	0.0	0.8	0:00
inetd										
164	root	9	0	1280	1280	1140	S	0.0	2.0	0:00
sshd										
170	root	8	0	676	676	564	S	0.0	1.1	0:00
cron										
173	root	9	0	468	468	408	S	0.0	0.7	0:00
getty										
174	root	9	0	5064	5064	1976	S	0.0	8.2	0:00
miniserv.pl										
947	root	9	0	1872	1872	852	S	0.0	3.0	0:01
named										
955	root	10	0	1840	1840	1564	S	0.0	3.0	0:00
sshd										
959	root	14	0	920	920	744	R	0.0	1.5	0:00
top										

Les 5 premières lignes donnent un résumé de l'état de la machine, les suivantes affichent N processus en fonctionnement sur la machine.

- la première ligne affiche l'heure (10h13m44s), le temps écoulé depuis que la machine a été démarrée (4 jours et 2h33), le nombre d'utilisateurs connectés (1), la charge moyenne sur 1, 5 et 10 minutes.
- la deuxième ligne affiche le nombre de programmes en cours (18 dont 17 en attente, 1 en fonction, aucun zombie, aucun stoppé)
- la troisième ligne affiche le taux d'occupation du processeur par des processus utilisateurs (0%), systèmes (0.1%), de faible priorité (0%) et le complément (99.9%)
- les quatrième et cinquième lignes affichent des statistiques (voir la commande free).

Les lignes suivantes présentent un tableau de statistique des programmes: un programme par ligne.

## 7.2. PRINCIPAUX RACCOURCIS

<b>h ou ?</b>	afficher l'aide(ainsi que la signification des champs)
<b>f</b>	ajouter / enlever des champs
<b>o</b>	déplacer des champs
<b>k</b>	tuer une tâche (suivi du pid)
<b>N</b>	tri par PID
<b>A</b>	tri par âge
<b>P</b>	tri par occupation du processeur
<b>M</b>	tri par mémoire occupée



## 8. MC - MIDNIGHT COMMANDER

*Midnight Commander (MC) est le « couteau suisse » GNU pour la console Linux et autres environnements de terminaux. C'est l'équivalent linuxien des System Commander et PCTools.*

### 8.1. DÉMARRAGE

démarrage de mc	mc
démarrage de mc forcé en couleurs si c'est possible	mc -c

### 8.2. COMMANDES STANDARD

Aide. Naviguer avec les touches flèches à l'intérieur. de mc	F1
Regarde le fichier courant. Colorisation de syntaxe pour les fichiers man. Appel lynx pour les fichiers html. / pour faire une recherche (comme dans vi), G pour aller au bout, g pour revenir au début.	F3
Édition (interne ou externe). L'éditeur interne est assez pratique.	F4
Copie un ou les fichiers courants du panel actif vers l'autre.	F5
Permet de se balader dans les menus de mc par le clavier.	F9
Quitte mc.	F10

### 8.3. RACCOURCIS UTILES

Envoie le nom du fichier courant sur la ligne de commande	Esc Enter
Sélectionne le fichier courant (le passe en jaune).	Ins
Sélectionne des fichiers avec une expression régulière.	+
Sélectionne tous les fichiers du répertoire.	*
Changement des droits sur un fichier.	Control-x c
Envoi le nom du répertoire courant vers la ligne de commande.	Control-x p
Envoi le nom du répertoire du panel opposé vers la ligne de commande	Control-x P
Complétion du nom en train d'être tapé.	Esc-Tab

<i>Envoie le nom du fichier courant sur la ligne de commande</i>	<b>Esc Enter</b>
<i>Commande précédente de l'historique. (On peut aussi cliquer sur [^] au bout de la ligne de commande)</i>	<b>Esc-p</b>
<i>Lancement d'une commande dont le résultat sera montré dans le viewer de mc. Très utile pour les man, car la colorisation rend le man plus lisible.</i>	<b>Esc-!</b>

## 8.4. CONFIGURATION DE BASE

---

<b>Options -&gt; Configuration -&gt; lynx-like motion</b>	utilisation des touches <- -> pour se déplacer dans les répertoires
<b>Options -&gt; Configuration -&gt; Pause after run : Always</b>	après le lancement d'une commande via la ligne de commande, attend un appui sur la barre d'espacement pour revenir à mc
<b>Options -&gt; Configuration -&gt; use internal edit</b>	permet d'utiliser la commande interne lors de l'édition ou un autre éditeur (à choisir en initialisant la variable d'environnement EDITOR)
<b>Options -&gt; Learn keys</b>	permet à mc d'apprendre les touches si il ne les reconnaît pas. Très pratique. Attention cependant, si vous changer souvent de type de terminal, vous écrasez à chaque fois les codes.

## 8.5. SYSTÈME DE FICHIERS VIRTUEL

---

Sous mc, un site ftp ou une archive tar sont des répertoires comme les autres. Pour un fichier tar ou tgz (tar zipé), il suffit d'aller sur le fichier et de taper enter. Vous entrez alors dans l'archive, et vous pouvez sélectionner un ou plusieurs fichiers pour les copier dans le répertoire d'à côté, voir un fichier de l'archive avec F3, .... Toutes les opérations ne sont cependant pas possibles, puisque le système de fichiers est considéré comme étant en lecture seulement.

En ce qui concerne le ftp, vous faites :

```
cd !ftp://nom_de_1_utilisateur@nom_de_1_ordinateur.xx.yy
```

Une fenêtre apparaît alors vous demandant un mot de passe. Vous voyez ensuite les fichiers tout comme si vous étiez dans le répertoire ftp du serveur. Vous pouvez copier (envoyer ou recevoir un fichier du serveur ftp), visualiser un fichier, etc, etc. C'est certainement le moyen le plus simple d'envoyer un arbre de répertoire via ftp. F5 sur le répertoire à copier, et les sous répertoires sont envoyés récursivement, sans que vous vous en préoccupiez.

## 8.6. CAPTURES D'ÉCRAN

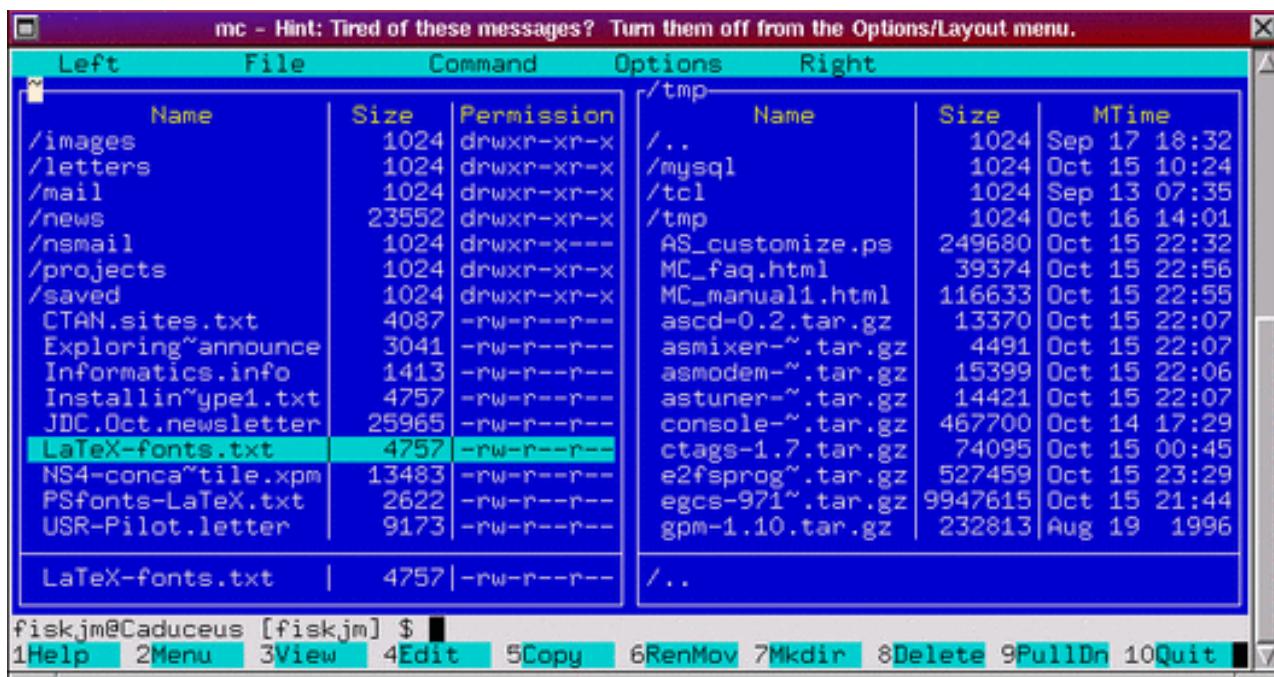


fig 1 - vue générale

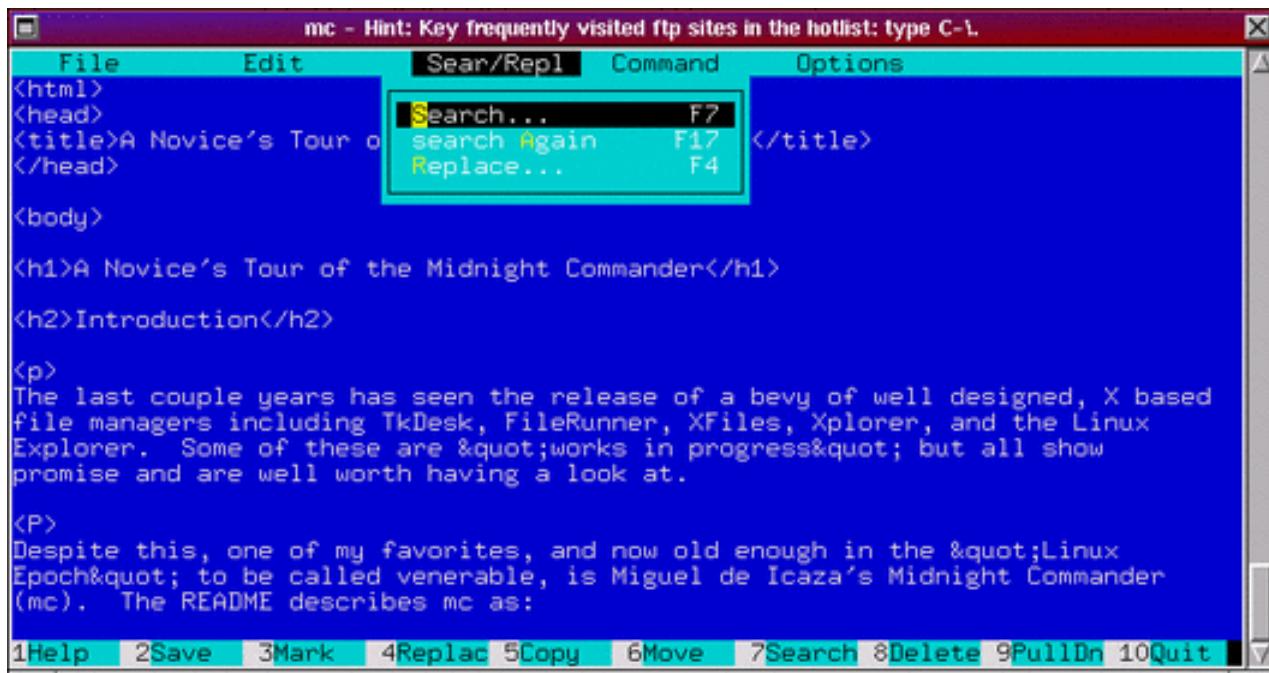


fig 2 - édition d'un fichier

mc - Hint: You may specify the external viewer with the shell variable PAGER.  
File: mc.1 Col 0 8192 bytes [grow] 0%  
mc(1) mc(1)  
  
NAME  
mc - Visual shell for Unix-like systems.  
  
USAGE  
mc [-abcDdfhPstuUVx?] [-l log] [dir1 [dir2]] [-v file]  
  
DESCRIPTION  
The Midnight Commander is a directory browser/file manager for Unix-like operating systems.  
  
OPTIONS  
-a Disables the usage of graphic characters for line drawing.  
-b Forces black and white display.

1Help 2Wrap 3Quit 4Hex 5Line 6RxSrch 7Search 8Raw 9Uniform 10Quit

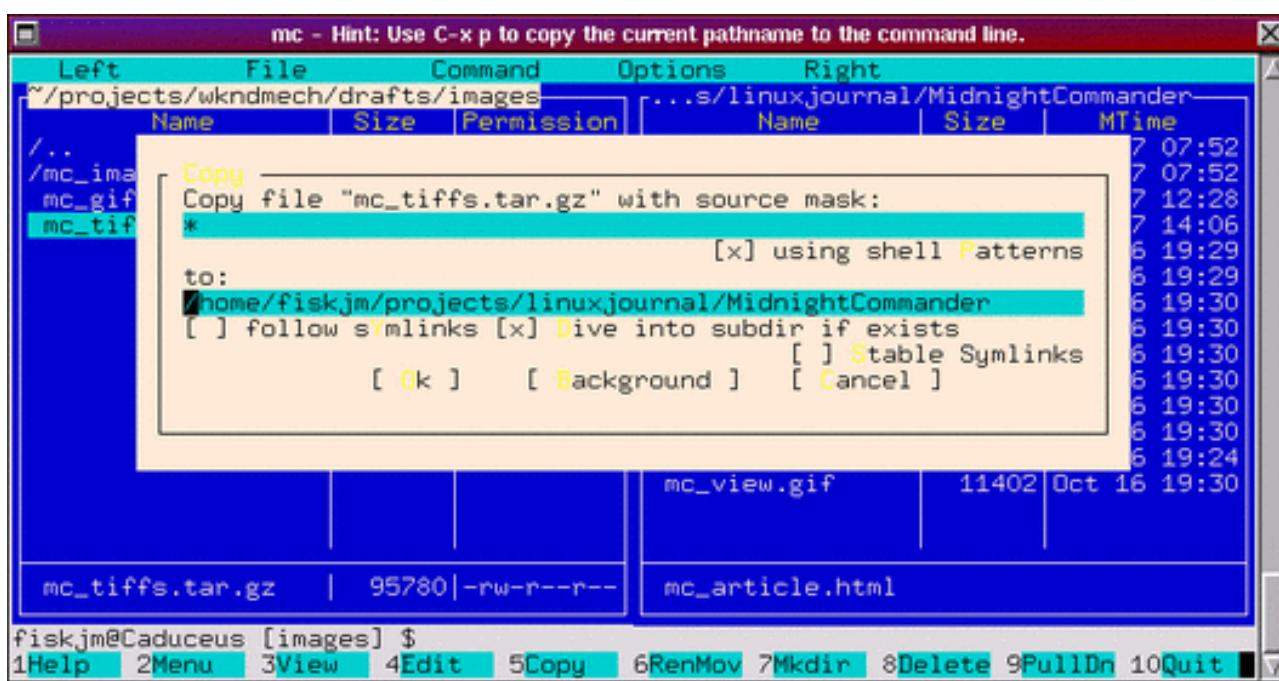


fig 4 - copie de fichier

## 9. TP2 - OUTILS AVANCÉS

### 1. Lancez screen

2. Lancez **top**

3. Triez l'affichage par occupation mémoire

4. Créez une nouvelle console **screen**

5. Lancez **mc**

6. Revenez sur la première console

7. Trier par **age**

8. Créez une nouvelle console **screen**

9. Afficher les tâches en cours avec le **pageur**

10. Depuis **top**, tuer le pageur (signal 9)

11. Exploration de l'arborescence à l'aide de **mc**.

## 10. DÉBUTER EN RÉSEAU

---

Ce document se veut être un document synthétique qui vous permettra de répondre aux questions suivantes :

- Qu'est-ce-que le protocole TCP/IP
- Quelle est ma configuration réseau local et distant ?
- Quels sont les services réseaux configurés sur ma machine ?
- Quels sont les principaux outils de diagnostic réseau sur ma machine ?

Attention : la liste des commandes fournies n'est pas exhaustive et plutôt orientée sur des distributions Debian. Quelques précisions sont toutefois apportées concernant Mandrake et Redhat pour les plus grosses différences.

### 10.1. L'ADRESSAGE RÉSEAU

---

#### 10.1.1. LE PROTOCOLE IP

---

Le protocole TCP/IP est dédié au transport des informations sur un réseau informatique. Il est organisé par réseaux et machines. Chaque machine est identifiée par une adresse IP. Chaque identifiant IP appelé numéro ou **adresse IP** doit être unique sur l'ensemble du réseau. Chaque machine ne dispose que d'une adresse IP par réseau sur lequel elle est connectée. Les machines (routeurs, passerelles) qui sont multi-domiciliées c'est-à-dire qui possèdent plusieurs adresses IP sont des cas spéciaux que nous étudierons plus tard.

Une adresse IP est un nombre codé sur 4 octets. Par habitude, cette adresse est représentée sous la forme décimale pointée w.x.y.z où w,x,y,z sont quatre chiffres décimaux allant de 0 à 255. Cette adresse peut être vue de 2 façons différentes:

- La machine d'adresse w.x.y.z .
- La machine d'adresse z du réseau w.x.y.0 .
- La machine d'adresse y.z du réseau w.x.0.0 .
- La machine d'adresse x.y.z du réseau w.0.0.0 .

Ces différentes façons de lire une adresse IP permettent d'optimiser la façon de calculer les routes vers d'autres réseaux. En résumé, on peut dire qu'un adresse IP se décompose en deux parties: une adresse de réseau plus une adresse de machine sur un réseau.

On peut comparer son fonctionnement des adresses postales: l'adresse du réseau est analogue au code postal, l'adresse de la machine dans le réseau est analogue à la rue dans la ville. chaque carte doit avoir une adresse réseau (i.e. adresse IP) , mais comme pour les grandes villes où il y a beaucoup de maisons, on découpe souvent un réseau en

plusieurs sous-réseaux (le meilleur exemple est Internet lui-même qui est constitué de divers - et nombreux - réseaux plus locaux), pour permettre de les reconnaître facilement, on leur donne un "bout d'adresse" en commun. Puis, comme on classe les maisons par rues et numéros, on classe les réseaux par adresse de réseau (le "bout d'adresse" en commun) et adresse de carte (adresse complète comprenant l'adresse de réseau ainsi qu'une partie spécifique à la carte).

Comment reconnaître le réseau et l'hôte ? On définit ce qu'on appelle un masque de réseau. Par exemple le réseau **192.168.3.0** a un masque de **255.255.255.0**, le réseau **10.0.0.0** un masque de **255.0.0.0**. Par convention, il existe trois réseaux à usage interne:

- Classe A: **10.0.0.0/255.0.0.0**
- Classe B: **172.x.0.0/255.255.0.0**
- Classe C: **192.168.x.0/255.255.255.0**

Certaines adresses de ces réseaux sont réservées: la première (.0) désigne le réseau, la dernière (.255) toutes les machines du réseau (ce qu'on appelle l'adresse de **broadcast**), et en général la seconde (.1) ou l'avant-dernière (.254) est la passerelle pour contacter d'autres réseaux (ce qu'on appelle la **gateway**).

### **10.1.2. LE PROTOCOLE ETHERNET**

Dans un réseau TCP/IP, nous avons dit que chaque machine était identifiée par une adresse IP. Cette adresse est logique, elle ne dépend pas du matériel utilisé pour relier les machines ensemble. Ces adresses IP peuvent être modifiées relativement rapidement par les administrateurs pour diverses raisons.

Cependant il existe des adresses **physiques**, uniques pour chaque machine: les adresses **MAC**. Ces adresses sont de forme aa:bb:cc:dd:ee:ff. Ces adresses dépendent de la carte réseau, et donc de la machine.

Il existe une passerelle entre le monde des adresses IP (réseau logique) et le monde des adresses MAC (réseau physique): c'est le protocole **arp**.

Du point de vue de l'analogie avec le système postal, l'adresse MAC est en quelque sorte le numéro de série de la boîte au lettres.

### **10.1.3. LE PROTOCOLE TCP**

Il est possible d'héberger plusieurs services dans une machine. On a donc besoin de diminuer la granularité des adresses IP. Pour cette raison, le protocole tcp définit le principe de **port**. Ces ports (compris entre 1 et 65535) sont normalisés et propres à chaque service (DNS: 53, HTTP: 80, ...).

Si on reprend l'analogie de la poste, à l'adresse IP correspond un immeuble, et dans ce cas le numéro de port correspond à un numéro d'appartement.

#### 10.1.4. INTERACTION DES PROTOCOLES

Pour comprendre le protocole TCP/IP, il faut comprendre son organisation. Un protocole de communication est classiquement organisé en 7 couches: c'est ce qu'on appelle le modèle OSI:

couche	nom	protocole	adressage	système postal
7	Application	/	/	/
6	Présentation	/	/	/
5	Session	/	/	/
4	Transport	TCP / UDP	port (0 -> 65535)	port = numéro d'appartement
3	Réseau	IP	adresse IP (aaa.bbb.ccc.ddd)	réseau = ville machine = adresse
2	Liaison	ethernet	adresse MAC (aa:bb:cc:dd:ee:ff)	adresse MAC = numéro de série de la boîte
1	Physique	/	/	/

Finalement, pour communiquer avec une machine, il faut connaître son IP et le port sur lequel envoyer la communication.

## 10.2. LE ROUTAGE

Dans le cadre d'un réseau physique (ethernet), chaque carte est connue par une numéro MAC. Mais les réseaux physiques peuvent être incompatibles entre eux (ex: Ethernet / Token Ring), or on a besoin d'acheminer des informations sur des distances variables (petites / moyennes / grandes) sans avoir à se préoccuper du protocole de réseau physique.

Ainsi dans le cadre d'un réseau IP, chaque machine dispose d'un numéro IP unique (4 octets pour IPv4, 16 octets pour IPv6). 2 machines peuvent se parler directement lorsqu'elles sont situées

- dans le même réseau physique
- dans le même réseau logique

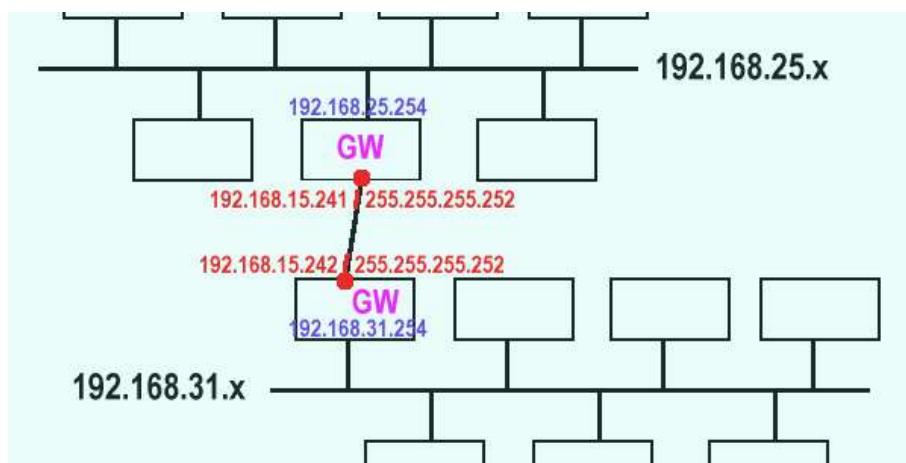
Si les 2 conditions ne sont pas remplies simultanément, alors on met en place des techniques de routage et de passerelles.

2 machines sont dans le même réseau logique lorsqu'elles ont des adresses réseau voisines, s'inscrivant dans un intervalle parfaitement défini (adresse réseau/masque). Par exemple : **192.168.25.0/255.255.255.0** signifie que le réseau logique va de **192.168.25.0 à 192.168.25.255**, dont il faut retrancher la 1re et la dernière adresse:

- la première adresse désigne le réseau en lui-même,

- la dernière désigne la totalité des membres possibles de ce réseau (adresse de broadcast).

Si 2 machines, qui ne sont pas dans le même réseau logique, souhaitent discuter entre elles, alors le routage se met en place. Le routage peut être assimilé à une successions de "sauts de puces" effectués par un paquet IP entre la machine d'émission et la machine de réception. À tout moment, dans une étape du routage il faut respecter la condition: **2 machines situées en vis à vis doivent être dans le même réseau logique.** Pour obtenir ce résultat, les machines routeur se voient attribuer plusieurs adresses IP : 1 pour chaque réalisation d'un vis à vis.



### 10.3. LE HOSTNAME

Le nom de machine, ou hostname en bon français, est extrêmement important et a des conséquences non seulement sur la configuration réseau mais aussi sur le fonctionnement (ou dysfonctionnement) du serveur X et donc de l'interface graphique. Pour afficher le hostname, on utilise la commande `hostname`.

```
lna:~# hostname  
lna.emtstvit
```

Pour modifier le hostname : il suffit de modifier l'un des fichiers suivants: `/etc/sysconfig/network` (sur Redhat et Mandrake), `/etc/HOSTNAME` (sur slackware), `/etc/hostname` (sur Debian), `/etc/conf.d/network` (gentoo), et `/etc/hosts`.

## 10.4. L'ADRESSE IP

Pour connaître l'adressage IP de la machine, quelle que soit la nature du réseau, une commande à connaitre : **ifconfig**. La commande vous retourne quelque chose comme ça :

```
lina:~# ifconfig
eth0  Lien encap:Ethernet  HWaddr 00:10:5A:DA:D3:47
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          inet  adr:192.168.3.2      Bcast:192.168.0.255
              Masque:255.255.255.0
                  RX packets:2006397 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:1863082 errors:0 dropped:0 overruns:0
carrier:0
                  collisions:3679 lg file transmission:100
                  RX bytes:1283974990 (1224.4 Mb)   TX bytes:590947572
(563.5 Mb)
                  Interruption:10 Adresse de base:0xe800
lo    Lien encap:Boucle locale
      inet adr:127.0.0.1  Masque:255.0.0.0
      UP LOOPBACK RUNNING  MTU:16436  Metric:1
      RX packets:442 errors:0 dropped:0 overruns:0 frame:0
      TX packets:442 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 lg file transmission:0
      RX bytes:278720 (272.1 Kb)   TX bytes:278720 (272.1 Kb)

ppp0  Lien encap:Protocole Point-à-Point
      inet  adr:213.41.132.215      P-t-P:62.4.16.248
      Masque:255.255.255.255
      UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1492
      Metric:1
      RX packets:2001693 errors:2006395 dropped:0 overruns:0
frame:0
      TX packets:1858378 errors:0 dropped:0 overruns:0
carrier:0
      collisions:0 lg file transmission:3
      RX bytes:1238624343 (1181.2 Mb)   TX bytes:549766984
(524.2 Mb)
```

Les informations fournies par la commande :

eth0, ppp0, lo...	nom de l'interface réseau
HWaddr	adresse MAC ou matérielle

<b>inet adr</b>	adresse IP liée à l'interface réseau
<b>Bcast</b>	adresse de broadcast
<b>Masque</b>	masque de réseau
<b>UP</b>	état de l'interface réseau - un 1er élément de diagnostic d'une panne réseau (non fonctionnement : DOWN)
<b>MTU</b>	taille maximum des trames physiques
<b>RX / TX packets</b>	nombre de paquets arrivés à destination, perdus ou non reçus à cause de débordements (arrivent de manière trop rapide pour pouvoir être traités par le noyau) - autre élément de diagnostic notamment lorsque les transmissions deviennent très lentes voire inexistantes.
<b>collisions</b>	produit lorsque 2 machines émettent en même temps sur le réseau. Il n'y a pas lieu de s'inquiéter tant que le rapport (nombre de paquets total / nombre de collisions) reste inférieur à 30%.

les principaux fichiers de configuration se situent dans `/etc/network`, ou dans `/etc/sysconfig/network-scripts` pour Redhat et Mandrake. Les fichiers s'appellent respectivement **interfaces** et `ifcfg-ethx` (ou x est le numéro d'instance de la carte réseau).

## 10.5. SE CONNECTER À UNE MACHINE DISTANTE AVEC SSH

Il y a aujourd'hui deux possibilités de travail, en local (local work) ou à distance (remote work). Ce dernier est permis par l'utilisation du réseau, qu'il soit local (LAN) ou réellement éloigné, comme par Internet (WAN). De nombreux outils ont été fournis pour utiliser la capacité du réseau. Échanger, copier, utiliser des shells à distance. Les noms de ces outils sont respectivement FTP, rcp, telnet, etc... Bien que ces outils, utilisés pendant des années et même encore aujourd'hui dans certaines entreprises, soient très pratiques, ils comportent une faiblesse importante. Leurs transactions sont transmises en clair via le réseau.

SH signifie Secure SHell. C'est un protocole qui permet de faire des connexions sécurisées (i.e. cryptées) entre un serveur et un client SSH. Nous allons utiliser le programme OpenSSH, qui est la version libre du client et du serveur SSH.

### 10.5.1. CONNEXION AVEC AUTHENTIFICATION PAR MOT DE PASSE

C'est la méthode la plus simple. Depuis la machine cliente, tapez :

```
lna:~# ssh login@serveur
```

Si c'est la première connexion SSH depuis ce client vers ce serveur, il vous demande si le **fingerprint** de la clé publique présentée par le serveur est bien le bon. Pour être sûr

que vous vous connectez au bon serveur, vous devez connaître de façon certaine le **fingerprint** de sa clé publique et la comparer à celle qu'il vous affiche. Si les deux fingerprints sont identiques, répondez yes, et la clé publique du serveur est alors rajoutée au fichier `~/.ssh/known_hosts`.

Si vous vous êtes déjà connecté depuis ce client vers le serveur, sa clé publique est déjà dans le fichier `~/.ssh/known_hosts` et il ne vous demande donc rien.

Ensuite, entrez votre mot de passe... et vous verrez apparaître le prompt, comme si vous vous étiez loggué en local sur la machine.

### **10.5.2. AUTHENTIFICATION PAR CLÉ**

Au lieu de s'authentifier par mot de passe, les utilisateurs peuvent s'authentifier grâce à la cryptographie asymétrique et son couple de clés privée/publique, comme le fait le serveur SSH auprès du client SSH. Cette méthode requiert deux étapes:

- Générer ses clés: pour générer un couple de clés DSA, tapez :

```
lna:~# ssh-keygen -t dsa
```

Les clés générées ont par défaut une longueur de 1024 bits, ce qui est aujourd'hui considéré comme suffisant pour une bonne protection.

Par défaut (il demande confirmation lors du processus de création), la clé privée est stockée dans le fichier `~/.ssh/id_dsa` avec les permissions 600 et la clé publique est stockée dans le fichier `~/.ssh/id_dsa.pub` avec les permissions 644.

Lors de la création, il vous demande une **pass phrase** qui est un mot de passe pour protéger la clé privée. Cette pass phrase sert à crypter la clé privée. La pass phrase vous sera alors demandée à chaque utilisation de la clé privée, c'est à dire à chaque fois que vous vous logguerez en utilisant cette méthode d'autentification.

Vous pouvez à tout moment **changer la pass phrase** qui protège votre clé privée avec la commande `ssh-keygen -p`.

- Autoriser votre clé publique: pour cela, il suffit de copier votre clé publique dans le fichier `~/.ssh/authorized_keys` de la machine sur laquelle vous voulez vous logguer à distance. La commande suivante permet de réaliser cette opération via SSH:

```
lna:~# ssh-copy-id -i ~/.ssh/id_dsa.pub login@serveur
```

et entrez le mot de passe de votre compte sur le serveur.

- se logguer

La commande est la même que pour une authentification par mot de passe.

## 10.6. SE RENDRE LA VIE DISTANTE PLUS FACILE AVEC SCREEN

L'inconvénient de travailler en distant est qu'on ne dispose plus que d'une seule console. **Screen** est un outil qui permet d'émuler plusieurs consoles.

Il se lance comme un outil classique (après s'être logué sur la machine distante):

```
lna:~# screen
```

À l'affichage de l'écran présentant la version, appuyez simplement sur la barre d'espacement pour poursuivre.

Quelques raccourcis:

<ctrl><a> <?>	affiche l'aide
<ctrl><a> <c>	crée un nouveau terminal
<ctrl><a> <n>	affiche le terminal virtuel suivant
<ctrl><a> <p>	affiche le terminal virtuel précédent
<ctrl><d>	ferme le terminal courant

## 10.7. LES PRINCIPAUX OUTILS DE DIAGNOSTIC RÉSEAU

### 10.7.1. ARP

Permet de visualiser et modifier la table arp stockée en cache. La table arp est une table de correspondance entre adresses IP et adresses matérielles (ou MAC). Elle est générée au fur et à mesure grâce au protocole ARP et stockée en cache.

Cette commande permet de détecter 2 types de problèmes : le **fonctionnement au niveau hardware de la carte** et la **bonne correspondance entre une adresse IP et une carte réseau** au moyen de son adresse MAC (problème de double attribution d'une adresse IP sur un réseau, spoofing, ...).

Exemple : Vous voulez vérifier que la seconde carte réseau appelée eth1 est opérationnelle. Dans un 1er temps, on va pinger la carte, ce qui va permettre d'alimenter la table arp.

```
lna:~# ping 192.168.3.2
```

Une fois la table alimentée, on vérifie son contenu : la présence de l'adresse IP ET de l'adresse MAC

```
lna:~# arp -a
? (192.168.3.14) at 52:54:05:F5:AD:0C [ether] on eth1
? (192.168.3.2) at 00:04:76:8E:B2:90 [ether] on eth1
```

En cas d'erreur dans la table, il est inutile de pousser plus avant le diagnostic... On est face à un problème matériel (certainement le plus pénible à détecter).

### 10.7.2. PING

Véritable outil à tout faire, à connaître absolument ! Il permet de détecter bon nombre de problèmes concernant votre configuration IP : adressage de votre carte réseau (adresse IP, adresse de réseau, routage, configuration de la résolution de nom).

Exemple : Mon réseau ne fonctionne pas. Je vais donc tester l'adresse avec la commande ping

```
lna:~# ping 192.168.3.14
PING 192.168.14 (192.168.3.14) from 192.168.3.2 : 56(84) bytes
of data.
From 192.168.3.2 icmp_seq=1 Destination Host Unreachable
```

Plusieurs causes de non-fonctionnement : je vérifie

- que l'adresse IP existe
- que le masque de sous-réseau est cohérent (ifconfig)
- que ma résolution de nom est opérationnelle (/etc/resolv.conf)
- que le routage est correctement configuré (commande route vue plus loin)

Si la commande ping fonctionne alors ce n'est ni un problème matériel, ni un problème de configuration IP. Toutefois le réseau peut subir des dysfonctionnements tout simplement parce qu'il est chargé. On augmente alors la taille des paquets envoyés:

```
lna:~# ping -s 128 192.168.3.14
PING 192.168.3.14 (192.168.3.14) from 192.168.3.2 : 128(156)
bytes of data.
136 bytes from 192.168.3.14 : icmp_seq=1 ttl=128 time=0.583 ms
136 bytes from 192.168.3.14 : icmp_seq=2 ttl=128 time=0.598 ms
136 bytes from 192.168.3.14 : icmp_seq=3 ttl=128 time=0.640 ms
136 bytes from 192.168.3.14 : icmp_seq=4 ttl=128 time=0.578 ms
--- 192.168.3.14 ping statistics ---
4 packets transmitted, 4 received, 0% loss, time 3008ms
rtt min/avg/max/mdev = 0.578/0.599/0.640/0.038 m
```

Ceci permet d'approfondir le test. On vérifiera :

- les numéros de séquences (icmp\_seq) : ils sont séquentiels et numérotent les paquets envoyés. Une surcharge réseau ou un câblage de mauvaise qualité par exemple entraîne la perte de paquets (voir % loss).
- le temps de transmission (time) : plus il est long, plus le réseau est chargé.

Attention : si vous lancez un ping sur un serveur et que celui-ci ne répond pas, cela ne signifie pas forcément qu'il y ait un problème. En effet, les firewalls peuvent bloquer toute réponse à un ping et faire échouer toute tentative de ping sur eux.

### 10.7.3. ROUTE

Permet d'afficher la **table de routage** en cache. La commande affiche la table de routage et effectue la résolution de nom dès que possible. Les commandes route -n affichent le table de routage sans résolution de nom. À noter que la commande netstat -r affiche les mêmes informations.

```
lna:~# route
```

Table de routage IP du noyau						
Destination	Passerelle	Genmask	Indic	Metric		
Ref	Use	Iface				
dns1.emtstvit	*	255.255.255.255	UH	0	0	0
0	tap8					
dns1.emtstvit	*	255.255.255.255	UH	0	0	0
0	tap0					
Anacam.rain.fr	vpn1.emtstvit	255.255.255.255	UGH	0	0	0
0	eth0					
ldap1.epmtstvit	*	255.255.255.255	UH	0	0	0
0	tap4					
dhcp1.emtstvit	*	255.255.255.255	UH	0	0	0
0	tap7					
dhcp1.emtstvit	*	255.255.255.255	UH	0	0	0
0	tap2					
dhcp2.emtstvit	*	255.255.255.255	UH	0	0	0
0	tap3					
dns2.emtstvit	*	255.255.255.255	UH	0	0	0
0	tap1					
ldap2.epmtstvit	*	255.255.255.255	UH	0	0	0
0	tap5					
ntp.emtstvit	*	255.255.255.255	UH	0	0	0
0	tap6					
192.168.7.0	vpn1.emtstvit	255.255.255.0	UG	0	0	0
0	eth0					
192.168.6.0	vpn0.emtstvit	255.255.255.0	UG	0	0	0
0	eth0					
10.6.69.0	vpn0.emtstvit	255.255.255.0	UG	0	0	0
0	eth0					

192.168.4.0	192.168.3.25	255.255.255.0	UG	0	0
0 eth0					
10.99.100.0	vpn1.emtstvit	255.255.255.0	UG	0	0
0 eth0					
192.168.3.0	*	255.255.255.0	U	0	0
0 eth0					
192.168.2.0	vpn0.emtstvit	255.255.255.0	UG	0	0
0 eth0					
192.168.1.0	vpn0.emtstvit	255.255.255.0	UG	0	0
0 eth0					
193.1.1.0	vpn0.emtstvit	255.255.255.0	UG	0	0
0 eth0					
191.1.0.0	*	255.255.0.0	U	0	0
0 eth1					
10.25.0.0	*	255.255.0.0	U	0	0
0 eth1					
default	vpn1.emtstvit	0.0.0.0	UG	0	0
0 eth0					
default	vpn0.emtstvit	0.0.0.0	UG	0	0
0 eth0					

Pour info: U = routeur installé et opérationnel ; G = passerelle distante ; H = destination est un hôte et non un réseau.

Un examen de la table de routage vous permet de vérifier par exemple que la machine sur laquelle vous travaillez et qui se situe derrière une passerelle a bien une route par défaut qui lui permet d'aller vers l'extérieur (Destination : default).

- Vous ne pouvez pas atteindre l'extérieur car vous n'avez pas cette route, 2 solutions :
  - vous ajoutez la route pour la session en cours :

```
lna:~# route add default gw adresseIP_de_la_passerelle
```

- vous modifiez le fichier de configuration du routage de manière à ce que la table contienne la route pour toutes les sessions : /etc/network/interfaces
- Vous ne pouvez pas atteindre l'extérieur car vous avez une route erronée, 2 solutions :
  - vous modifiez la route pour la session en cours :

```
lna:~# route del default gw adresseIP_de_la_passerelle_erronée
lna:~#           route      add      default      gw
adresseIP_de_la_passerelle_correcte
```

- vous modifiez le fichier de configuration du routage de manière à ce que la table contienne la route correcte pour toutes les sessions : `/etc/network/interfaces`

#### 10.7.4. TRACEROUTE

Vous ne parvenez pas à atteindre une URL ou un poste donné... La commande traceroute, comme son nom l'indique, vous établit la route suivie par les paquets de données vers la destination. La route est constituée de tous les routeurs traversés pour arriver à destination. Par exemple:

```
lna:~# traceroute 192.168.3.14
traceroute to 192.168.3.14 (192.168.3.14), 30 hops max, 38
byte packets
1 appli1 (192.168.3.14) 0.138 ms 0.115 ms 0.103 ms
```

Il s'agit d'une machine locale. Elle est située sur le même réseau, aucun routeur n'est traversé, l'adresse de destination est donc atteinte directement.

```
lna:~# traceroute 192.168.4.1
traceroute to 192.168.4.1 (192.168.4.1), 30 hops max, 38 byte
packets
1 192.168.3.25 (192.168.3.25) 5.204 ms * 1.307 ms
2 trdinov-vrh.arnes.si (193.2.1.11) 7.273 ms * 7.356 ms
3 fichier.emtbes (192.168.4.1) 7.220 ms 7.088 ms 7.001 ms
```

On a ici une adresse située sur le même réseau, dans un autre site. On transite donc par un vpn, et tous les routeurs traversés sont indiqués et numérotés.

```
lna:~# traceroute -n free.fr
traceroute to free.fr (213.228.0.42), 30 hops max, 38 byte
packets
1 192.168.3.22 4.945 ms 9.817 ms 0.142 ms
2 193.252.219.129 41.191 ms 36.178 ms 36.199 ms
3 193.253.2.81 36.221 ms 35.870 ms 37.228 ms
4 193.252.160.114 43.966 ms 42.878 ms 43.615 ms
5 193.252.161.114 48.965 ms 49.621 ms 47.988 ms
6 193.252.161.54 212.797 ms 64.363 ms 88.608 ms
7 193.252.103.85 49.622 ms 48.297 ms 47.615 ms
8 193.251.126.78 61.436 ms 48.271 ms 50.658 ms
9 193.252.103.245 49.991 ms 50.306 ms 50.018 ms
10 213.228.3.1 50.312 ms 49.340 ms 49.292 ms
11 213.228.0.42 49.675 ms 48.973 ms 49.644 ms
```

On a ici une adresse située à l'extérieur, tous les routeurs traversés sont indiqués et numérotés.

Là où traceroute devient un outil de diagnostic :

```
lna:~# traceroute 192.168.3.14
traceroute to 192.168.3.14 (192.168.3.14), 30 hops max, 38
byte packets
 1 192.168.3.14 (192.168.3.14) 2999 ms !H 2994 ms !H 2999
ms !H
```

Cette fois-ci la commande nous donne des informations différentes : il lui est impossible de trouver la route et il affiche directement la destination avec un des codes d'erreur suivant :

**!H** : host unreachable

**!N** : network unreachable

**!P** : protocol unreachable

#### 10.7.5. NETSTAT

On a déjà vu la commande netstat dans le cadre de l'affichage de la table de routage. La commande permet également d'obtenir des informations détaillées sur l'état des interfaces réseau. Par exemple :

```
lna:~# netstat -i
Table d'interfaces noyau
Iface  MTU Met      RX-OK RX-ERR RX-DRP RX-OVR      TX-OK TX-ERR TX-
DRP TX-OVR Flg
eth0    1500 0        01494099532    74     72      01488416789      0
0        0 BMRU
eth1    1500 0        01075647525    0       0      01075729802      0
0        0 BMRU
lo     16436 0        0 2184358      0       0      0 2184358      0
0        0 LRU
tap0    1500 0        65400      0       0      0 65778      0
0        0 BMRU
tap1    1500 0        25696      0       0      0 23148      0
0        0 BMRU
tap2    1500 0        175415     0       0      0 97046      0
0        0 BMRU
tap3    1500 0        55763      0       0      0 28136      0
0        0 BMRU
tap4    1500 0        89947      0       0      0 97810      0
0        0 BMRU
tap5    1500 0        79748      0       0      0 2685       0
0        0 BMRU
```

<b>tap6</b>	1500	0	34075	0	0	0	28165	0
0	0	BMRU						
<b>tap7</b>	1500	0	32076	0	0	0	19522	0
0	0	BMRU						
<b>tap8</b>	1500	0	77757	0	0	0	77172	0
0	0	BMRU						

Avec:

<b>RX</b>	paquets reçus
<b>TX</b>	paquets envoyés (transmis)
<b>OK</b>	paquets reçus/envoyés correctement
<b>ERR</b>	paquets reçus/envoyés avec des erreurs
<b>DRP</b>	paquets reçus/envoyés droprés
<b>OVR</b>	paquets reçus/envoyés retransmis

D'autres options de la commande permettent notamment de visualiser les ports ouverts : **netstat -tu** (tcp et udp). Par exemple :

```
lna:~# netstat -tu
Connexions Internet actives (sans serveurs)
Proto Recv-Q Send-Q Adresse locale                               Adresse distante
Etat      tcp          0          0  lna:ldap                  0  lna:ldap
appli.emtstvit:35619  ESTABLISHED
tcp          0          0  localhost:ldap                  localhost:54786
ESTABLISHED
tcp          0          0  lna:1023                  fichier.emtbes:32771
TIME_WAIT    tcp          0          0  lna:netbios-ssn
192.168.3.210:1036  ESTABLISHED
tcp          0          0  localhost:34427                  localhost:ldap
ESTABLISHED
tcp          0          0  lna:ldap                  appli1.emtstvit:40846
ESTABLISHED
```

### 10.7.6. RESOLV.CONF

Ce fichier permet la configuration d'un client DNS. C'est lui qui permet l'utilisation de serveurs DNS pour la résolution de noms en adresse IP (ce qui vous permet par exemple de taper une URL dans un navigateur et non une adresse IP). Un fichier mal configuré vous empêchera notamment de surfer. La syntaxe est la suivante:

```
lna:~# cat /etc/resolv.conf
search emtstvit
```

```
nameserver 192.168.3.33
nameserver 192.168.3.173
```

La première ligne indique dans quels domaines rechercher le nom en priorité. Par exemple quand on recherche **Ina**, on va implicitement demander l'IP de la machine se nommant **Ina.emtstvit**.

#### 10.7.7. RÉSOLUTION (INVERSE) DE NOMS

Vous avez récupéré des informations sous forme d'IP ou de nom dans vos logs et vous voulez savoir qui se cache derrière cette IP. Voici deux outils qui vous permettront de faire de la résolution de nom ou de la résolution inverse avec des informations complémentaires sur l'identité du serveur.

```
lna:~# host fichier
fichier.emtstvit has address 192.168.3.1
lna:~# host 192.168.3.1
1.3.168.192.in-addr.arpa domain name pointer fichier.emtstvit.
lna:~# host fichiers
Host fichiers not found: 3 (NXDOMAIN)
lna:~# host 192.168.3.23
Host 23.3.168.192.in-addr.arpa not found: 3 (NXDOMAIN)
```

Et avec l'outil **dig**:

```
lna:~# dig 192.168.3.23

; <>> DiG 9.2.1 <>> 192.168.3.23
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 60101
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1,
ADDITIONAL: 0

;; QUESTION SECTION:
;192.168.3.23. IN A

;; AUTHORITY SECTION:
. 10770 IN SOA A.ROOT-SERVERS.NET. NSTLD.VERISIGN-GRS.COM.
2004051500 1800 900 604800 86400

;; Query time: 2 msec
;; SERVER: 192.168.3.33#53(192.168.3.33)
;; WHEN: Mon May 17 11:45:18 2004
```

```
; ; MSG SIZE  rcvd: 105
```

## 11.TP3 - RÉSEAU

1. Loguez-vous sur **192.168.3.2**

2. Déterminez son nom

3. Déterminez à quel réseau appartient la machine

4. Listez les machines sur les réseaux visibles en utilisant l'adresse de broadcast

5. Déterminez les noms des machines sur tous les réseaux visibles

6. Affichez les routes de la machine

7. Listez les passerelles autours de la machine

8. Trouvez par quelle machine aller sur internet

9. Affichez quels services écoutent sur la machine

10.Affichez les machines connectées en ssh sur Ina

## 12. SERVICE WEBMIN

Webmin est un logiciel mettant à la disposition de l'administrateur un moyen simple et graphique pour administrer le plupart des services disponibles sous Linux.

### 12.1. ARCHITECTURE GÉNÉRALE

- La connexion à webmin se fait par l'URL  
[https://<machine sur laquelle fonctionne webmin>:10000](https://127.0.0.1:10000)

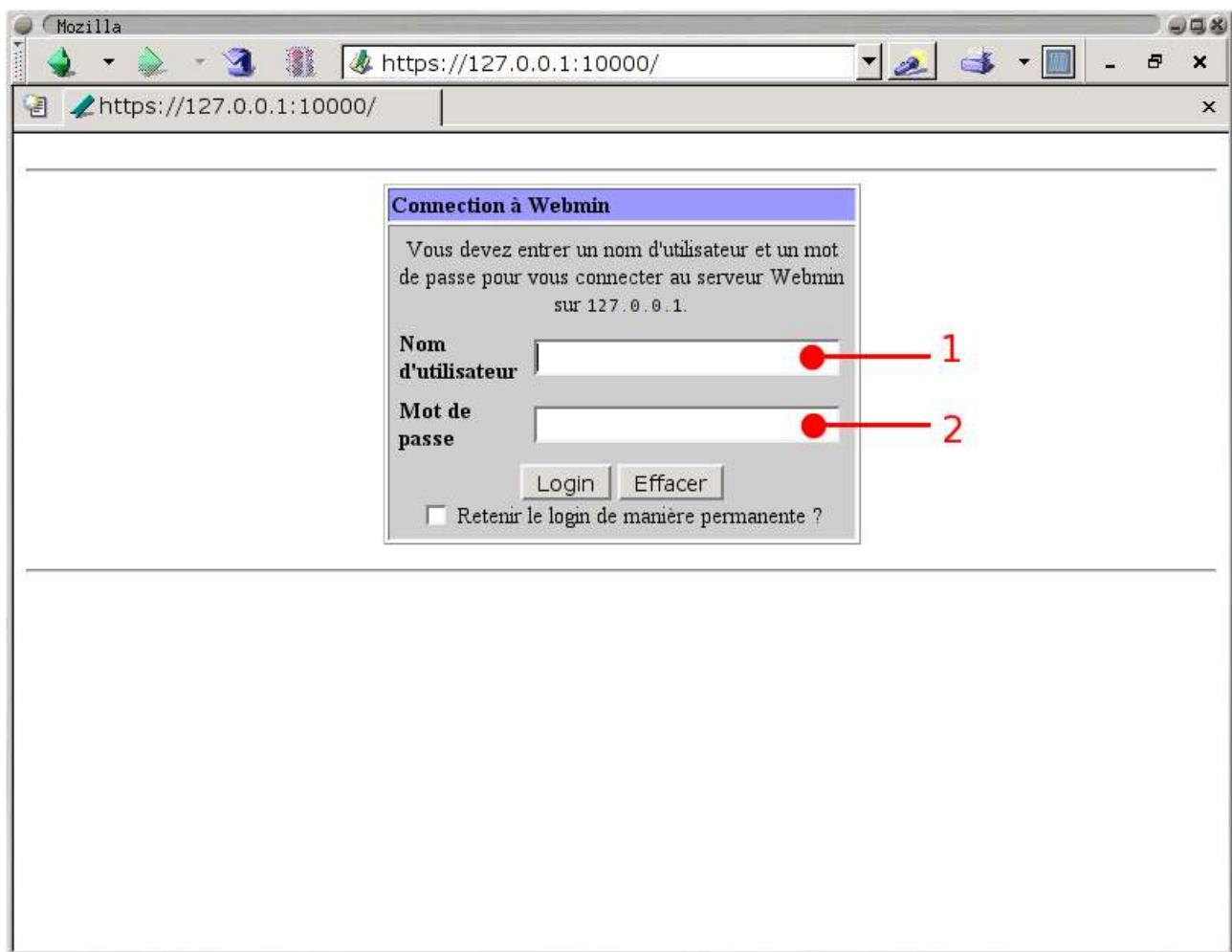


fig 5 - Écran de login à Webmin

1. Nom d'utilisateur: sauf indication contraire, la connexion se fait en tant que super-utilisateur, c'est à dire **root**.
2. mot de passe.

L'interface est par la suite assez claire:

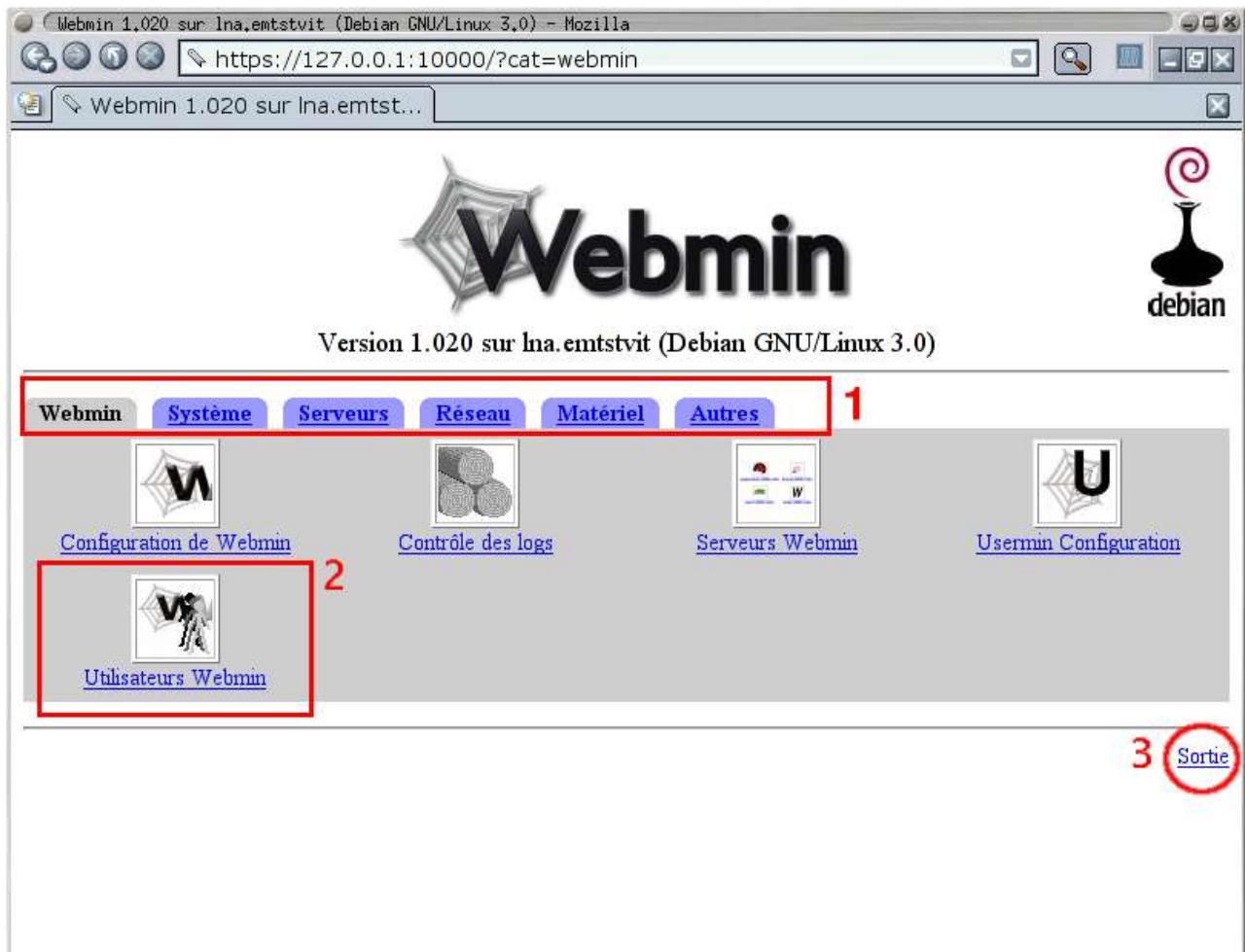


fig 6 - Page d'accueil de webmin

1. Les services administrables sont classés par catégorie accessible via un système d'onglets sur la partie supérieure de l'interface
2. Chaque service est représenté par une icône conduisant à un ensemble de formulaires de renseignement
3. Lien pour se déconnecter

## 12.2. ADMINISTRATION D'AUTRES SERVEURS

Webmin a été conçu pour administrer des services locaux. Il est cependant possible de le configurer pour administrer des services distants, comme c'est le cas pour le Webmin installé sur Ina.

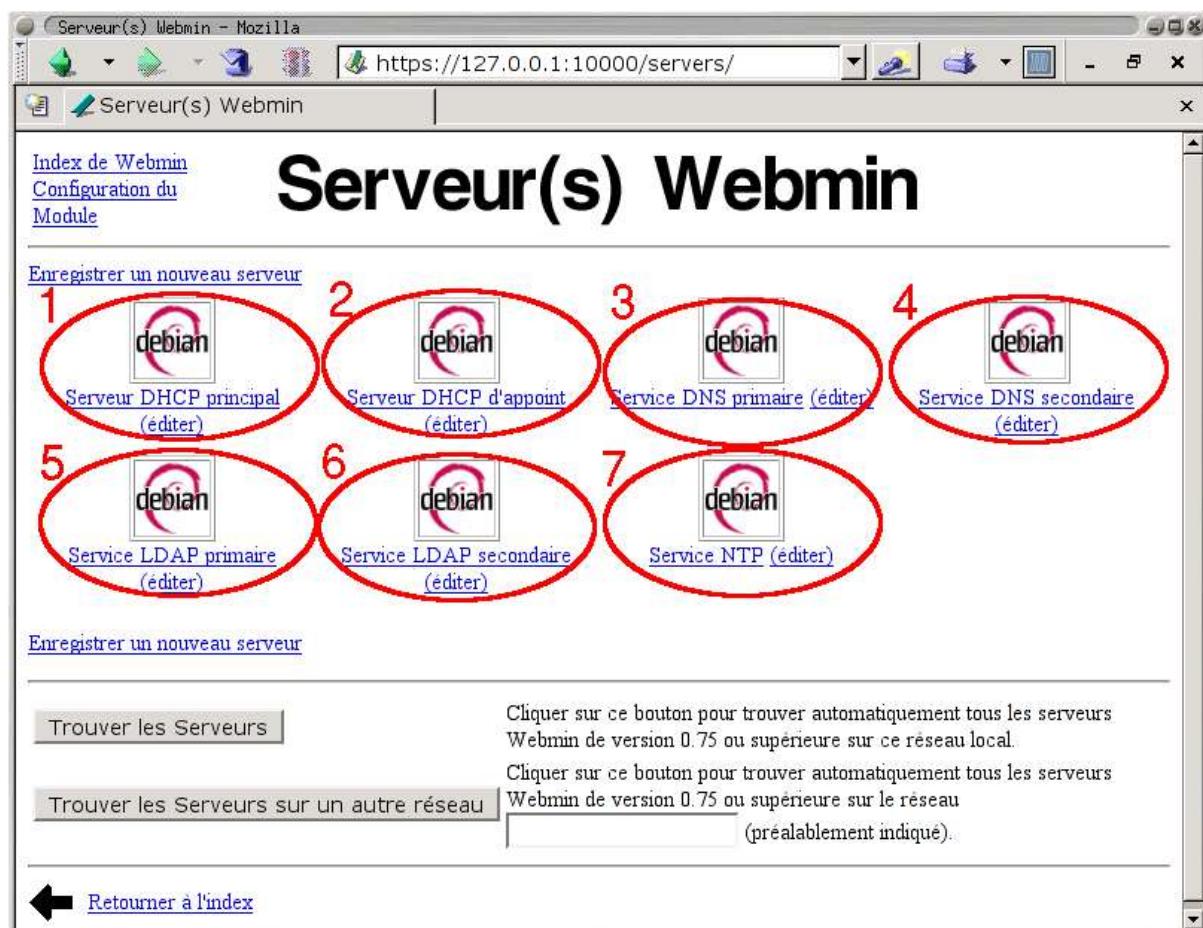


fig 7 - Accès aux interfaces webmin de différents serveurs

1. administration du service dhcp sur l'UML dhcp1
2. administration du service dhcp sur l'UML dhcp2
3. administration du service dns sur l'UML dns1
4. administration du service dns sur l'UML dns2
5. administration du service ldap sur l'UML ldap1
6. administration du service ldap sur l'UML ldap2
7. administration du service ntp sur l'UML ntp

- L'administration d'un serveur distant se fait de manière totalement transparente: le login est automatique.



fig 8 - Interface webmin de dhcp1 depuis l'interface webmin principale

## 13. SERVICE DHCP

---

*DHCP (Dynamic Host Configuration Protocol) est un protocole qui permet de configurer automatiquement les paramètres réseau des postes connectés. Cela évite de mettre les configurations réseau "en dur" sur les postes connectés.*

### 13.1. ARCHITECTURE

---

Deux UMLs sont utilisés comme service DHCP: **dhcp1** et **dhcp2**. Ils fonctionnent symétriquement (pas de relation maître / esclave). Ils utilisent également le même fichier de configuration (le modifier pour un des deux services impacte le fonctionnement de l'autre).

### 13.2. PARAMÈTRES

---

<i>noms</i>	<b>dhcp1</b>
	<b>dhcp2</b>
<i>adresses IP</i>	<b>192.168.3.37</b>
	<b>192.168.3.177</b>

### 13.3. FICHIERS

---

<i>configuration</i>	<b>/etc/dhcp3/dhcpd.conf</b>
	<b>/etc/default/dhcp3-server</b>
<i>logs</i>	<b>/var/log/syslog</b>

### 13.4. ADMINISTRATION

---

<i>arrêter le service</i>	<b>/etc/init.d/dhcp3-server stop</b>
<i>démarrer le service</i>	<b>/etc/init.d/dhcp3-server start</b>
<i>redémarrer le service</i>	<b>/etc/init.d/dhcp3-server restart</b>
<i>lister les logs</i>	<b>grep dhcpcd /var/log/syslog   less</b>

*arrêter le service*                    /etc/init.d/dhcp3-server stop  
*vérifier la présence du ps aux | grep [d]dhcpd3*  
*service*  
*tuer le service*                    killall -9 dhcpcd3

## 13.5. SYNTAXE

- /etc/dhcp3/dhcpcd.conf

```
# sous-réseau
subnet <adresse du réseau> netmask <masque du réseau> {
    allow booting;
allow bootp;
    option broadcast-address <adresse de broadcast>;
option routers <adresse de la passerelle>;
option subnet-mask <masque du réseau>;
option domain-name <noms de domaneis pour la résolution>;
option domain-name-servers <adresse du serveur dns>;
    next-server <adresse du serveur tftp>;
filename "<nom de l'image tftp>";
    # machine
host <nom de la machine> {
hardware ethernet <adresse MAC de la machine>;
option host-name "<nom de la machine>";
fixed-address <adresse IP de la machine>;
}
}
```

## 13.6. WEBMIN

- Localisation:

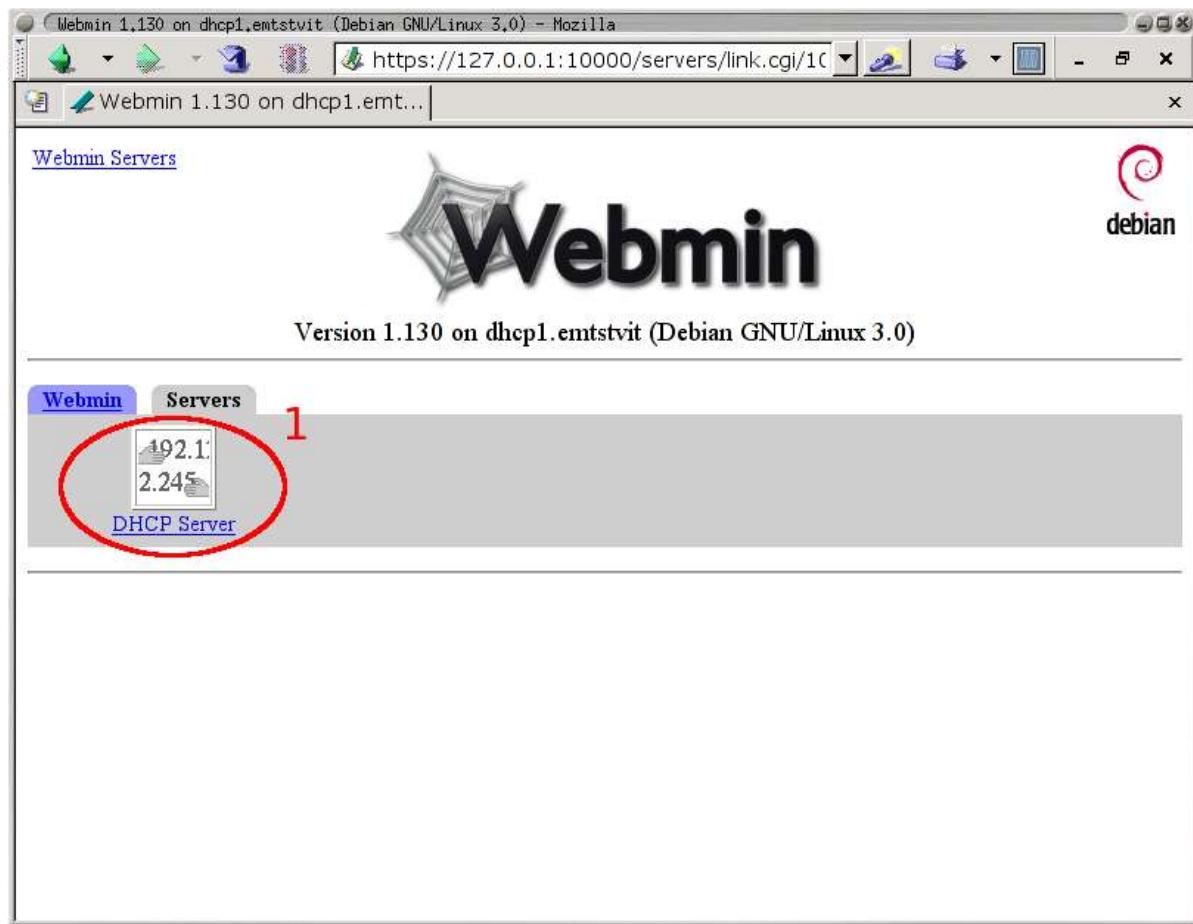


fig 9 - Gestion du service dhcp

1. L'interface d'administration du serveur DHCP se trouve dans la catégorie servers.

- Écran principal:

DHCP Server - Mozilla

https://127.0.0.1:10000/servers/link.cgi/10

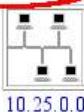
# DHCP Server

ISC DHCPd version 3.0.1

## Subnets and Shared Networks

Display nets and subnets by: Assignment File structure Name/IP address

Add a new subnet Add a new shared network

3  10.25.0.0

1  192.168.3.0

Add a new subnet Add a new shared network

## Hosts and Host Groups

Display hosts and groups by: Assignment File structure Name Hardware address IP address

Add a new host Add a new host group

4  station14

2  station25

station33

Add a new host Add a new host group

Edit Client Options Edit DHCP client options that apply to all subnets, shared networks, hosts and groups

Edit Network Interface Set the network interfaces that the DHCP server listens on when started.

List Active Leases List leases currently issued by this DHCP server for dynamically assigned IP addresses.

5 Apply Changes Click this button to apply the current configuration to the running DHCP server, by stopping and restarting it.

Return to index

fig 10 - détail de l'interface de gestion du dhcp

1. sous-réseau déjà défini
2. machine déjà définie
3. pour ajouter un sous-réseau
4. pour ajouter une nouvelle machine
5. pour enregistrer les changements effectués

- Écran de modification d'un sous-réseau

**Edit Subnet**

**Subnet Details**

Subnet description:  1

Network address: 10.25.0.0 2

Netmask: 255.255.0.0 3

Address ranges:  -   Dynamic BOOTP ?

Shared network: <None>

Default lease time:  Default  [secs] secs

Maximum lease time:  Default  [secs] secs

Boot filename:  None  /tftpboot/pxelinux.bin 4

Boot file server:  This server  10.25.0.1 5

Server name:

Lease length for BOOTP clients:  Forever  [secs] secs

Lease end for BOOTP clients:  Never  [secs] secs

Dynamic DNS enabled?:  Yes  No  Default

Dynamic DNS domain name:

Dynamic DNS reverse domain:  Default

Dynamic DNS hostname:  From client

Allow unknown clients?:  Allow  Deny  Ignore  Default

Server is authoritative:  Yes  Default (No)

Hosts directly in this subnet: ANDROMEDE, BANDIT2X, CATIAV5 6

Groups directly in this subnet:

**Address Pools for Subnet**

No address pools defined

[Add an address pool](#)

[Return to subnet list](#)

fig 11 - gestion des sous-réseaux dhcp

1. nom du sous-réseau (facultatif)
2. adresse su sous-réseau
3. masque du sous-réseau
4. nom de l'image tftp

5. adresse de l'hôte tftp
6. liste des machines appartenant à ce réseau

- Écran de modification d'une machine

The screenshot shows the 'Edit Host' page from the Webmin interface. The URL in the browser is `https://127.0.0.1:10000/servers/link.cgi/1C`. The main title is 'Edit Host' and it specifies 'In subnet 10.25.0.0/255.255.0.0'. The 'Host Details' section contains the following fields:

- Host description:** (Field 1)
- Host name:** `tsp1` (Field 2)
- Hardware Address:** `ethernet 00:0D:56:1B:AC:30` (Field 3)
- Host assigned to:** Subnet dropdown set to `10.25.0.0` (Field 4)
- Fixed IP address:** `10.25.1.1` (Field 5)
- Boot filename:** Radio button selected for 'None'
- Boot file server:** Radio button selected for 'This server'
- Lease length for BOOTP clients:** Radio button selected for 'Forever'
- Dynamic DNS enabled?**: Radio button selected for 'Default'
- Dynamic DNS reverse domain:** Radio button selected for 'Default'
- Allow unknown clients?**: Radio button selected for 'Default'

Below the form are buttons for 'Save', 'Edit Client Options', and 'Delete'. At the bottom left is a link 'Return to host list'.

fig 12 - Ajout manuel d'un hôte dans le dhcp

1. nom de la machine (facultatif)
2. nom d'hôte de la machine
3. adresse MAC de la machine
4. sous-réseau auquel appartient la machine
5. adresse IP de la machine

## 14. SERVICE DNS

---

Un serveur de noms permet d'associer une adresse IP à un nom. Dans un réseau, chaque machine se voit attribuer une adresse IP unique, qui permet de l'identifier. C'est un peu comme une adresse postale, qui permet d'identifier une maison de façon certaine. Mais si une adresse chiffrée est plus facile à manipuler par un ordinateur, elle est difficile à mémoriser par un humain. Ainsi, on se souvient facilement de appli1, mais plus difficilement de 192.168.3.14. Le serveur de noms va permettre de trouver l'adresse IP à partir d'un nom (ou inversement), que l'ordinateur pourra ensuite interroger.

### 14.1. ARCHITECTURE

---

Deux machines sont utilisés comme service DNS: **dns1** et **dns2**. Ils fonctionnent sur un mode maître / esclave. Tous les changements de configuration se font sur le maître (**dns1**), l'esclave (**dns2**) ayant pour seule fonction de répliquer les changements apportés au maître et de le remplacer en cas de défaillance. On peut également les rencontrer sous le terme de **dns primaires et secondaires**.

### 14.2. PARAMÈTRES

---

<i>noms</i>	<b>dns1</b> (maître / primaire)
	<b>dns2</b> (esclave / secondaire)
<i>adresses IP</i>	<b>192.168.3.33</b>
	<b>192.168.3.173</b>

### 14.3. FICHIERS

---

<i>configuration</i>	<b>/etc/bind/named.conf</b>
<i>correspondance ip-&gt;nom</i>	<b>/etc/bind/db.[chiffres]</b>
<i>correspondance nom-&gt;ip</i>	<b>/etc/bind/db.[nom-de-site]</b>
<i>logs</i>	<b>/var/log/syslog</b>

## 14.4. ADMINISTRATION

<i>arrêter le service</i>	/etc/init.d/bind stop
<i>démarrer le service</i>	/etc/init.d/bind start
<i>redémarrer le service</i>	/etc/init.d/bind restart
<i>lister les logs</i>	grep named /var/log/syslog   less
<i>vérifier la présence du service</i>	ps aux   grep [n]amed
<i>tuer le service</i>	killall -9 named
<i>logs</i>	/var/log/syslog

## 14.5. SYNTAXE

- /etc/bind/named.conf

```
options {
    forwarders {
        <première machine à laquelle transmettre des changements>
        <deuxième machine à laquelle transmettre des changements>
        <...>
    };

    allow-transfer {
        <première machine de laquelle recevoir des changements>
        <deuxième machine de laquelle recevoir des changements>
        <...>
    };
};

# zone inverse sur laquelle on est maître
zone "<adresse ip inverse du réseau>.in-addr.arpa" {
    type master;
    file "/etc/bind/<adresse ip inverse du réseau>";
};

# domaine sur lequel on est maître
zone "<nom du domaine>" {
    type master;
    file "/etc/bind/db.<nom du domaine>";
};

# zone inverse sur laquelle on est esclave
zone "<adresse ip inverse du réseau>.in-addr.arpa" {
    type slave;
    file "/etc/bind/db.<adresse ip inverse du réseau>.BAK";
    masters { <adresse IP du serveur maître>; };
};
```

```
};

zone "<nom du domaine>" {
    type slave;
    file "/etc/bind/db.<nom du domaine>.BAK";
    masters { <adresse IP du serveur maître>; };
};

● /etc/bind/db.[chiffres]
$TTL 604800
@           IN SOA lna.emtstvit. root.emtstvit. (
                <numero de version>
                <nb. de secondes avant de contacter les esclaves>
                <nb. secondes avant de recontacter un esclave>
                <nb de secondes de vie d'un adresse en cache>
                <nb de secondes de durée de vie du cache d'adresse>
)
@           IN NS <nom de la machine DNS du domaine>.<nom du domaine>.
<adresse inverse d'une machine dans ce réseau>   IN          PTR
<machine>.<nom du domaine>.
```

- /etc/bind/db.[nom-de-site]

```
$TTL 604800
@           IN SOA lna.emtstvit. root.emtstvit. (
                <numero de version>
                <nb. de secondes avant de contacter les esclaves>
                <nb. secondes avant de recontacter un esclave>
                <nb de secondes de vie d'un adresse en cache>
                <nb de secondes de durée de vie du cache d'adresse>
)
@           IN NS <nom de la machine DNS du domaine>.<nom du domaine>.
<machine>      IN A <adresse IP de la machine>
<alias>        IN CNAME <machine aliasée>
```

## 14.6. WEBMIN

- Localisation:

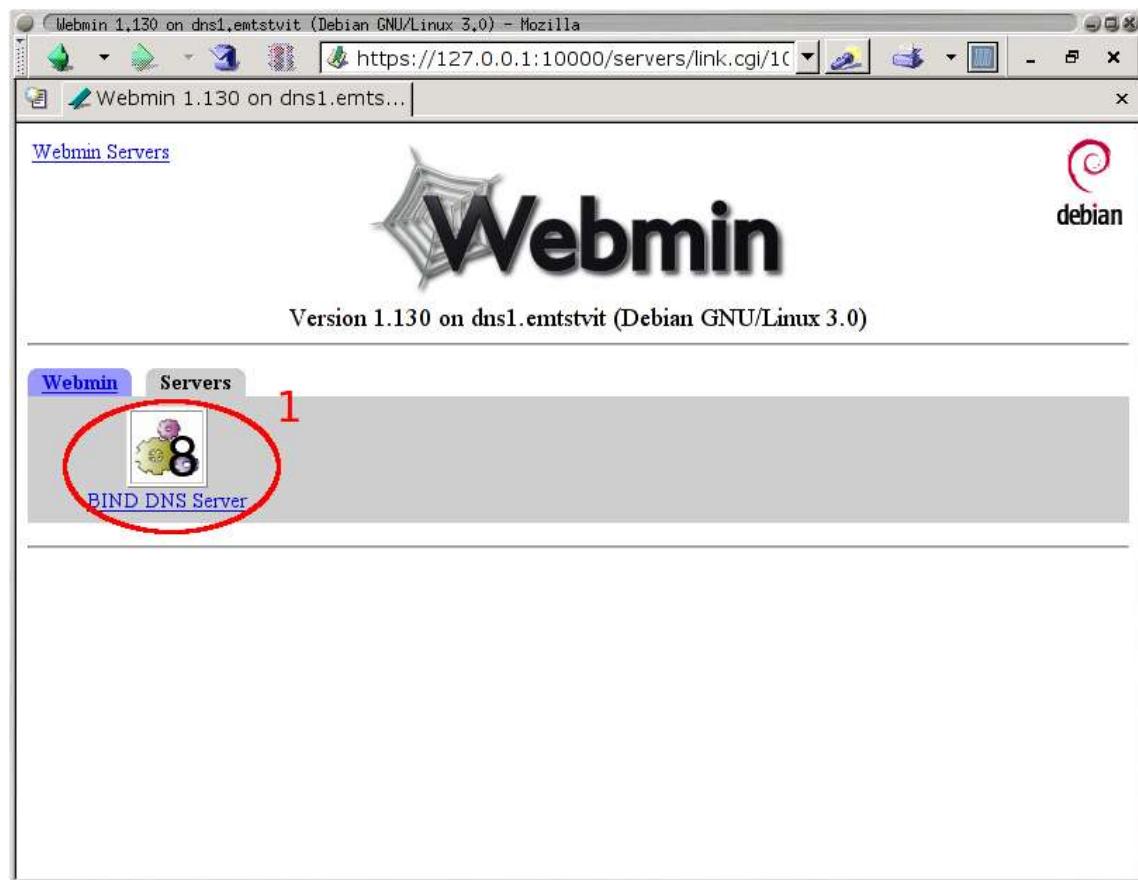


fig 13 - icône d'accès à l'interface de gestion du DNS sous webmin

1. L'interface d'administration du serveur dns se trouve dans la catégorie servers.

- Écran principal:

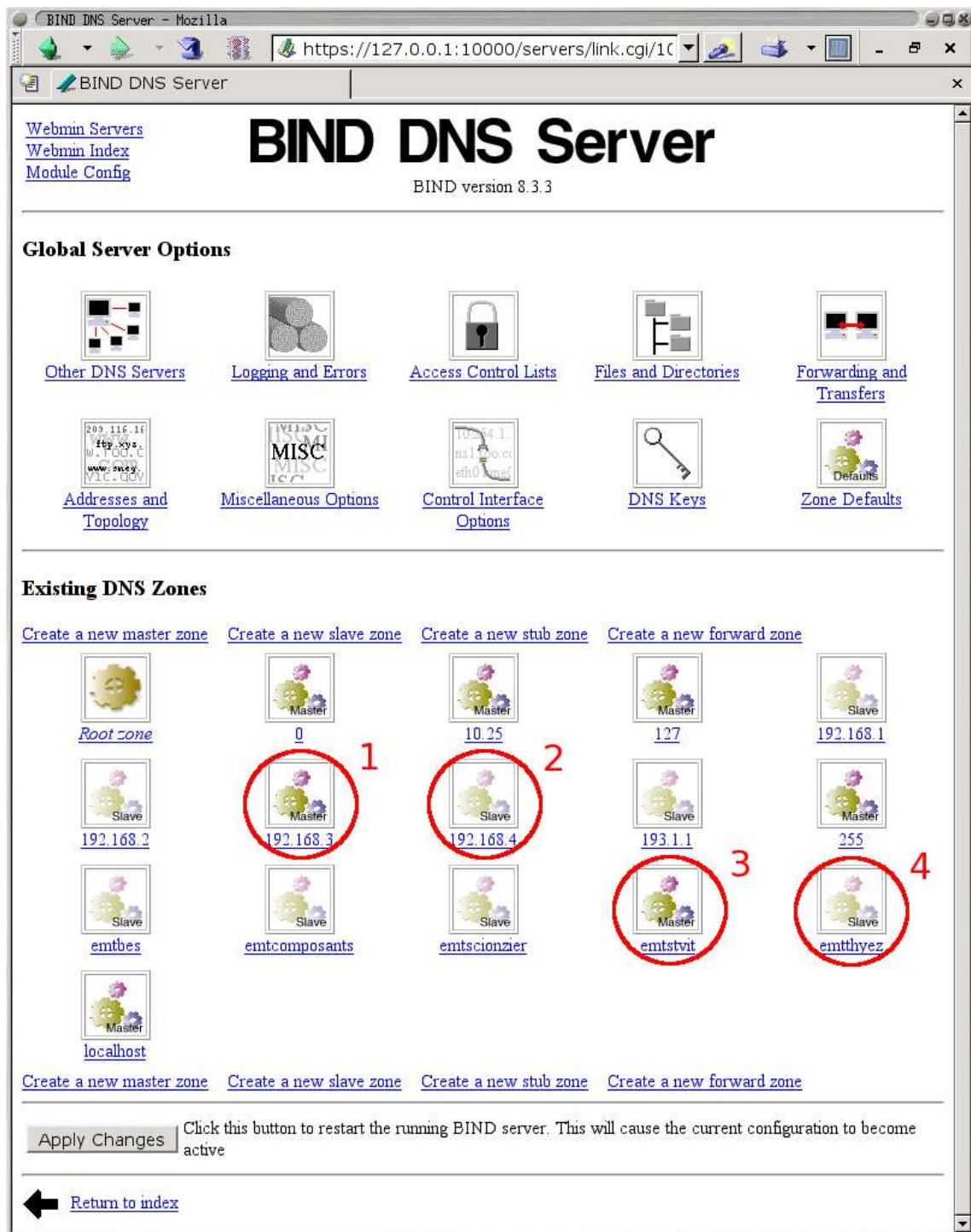


fig 14 - Interface principale de gestion du serveur DNS

1. Zone inverse, serveur maître
2. Zone inverse, serveur esclave
3. Zone directe, serveur maître
4. Zone directe, serveur esclave

- Édition d'une zone inverse

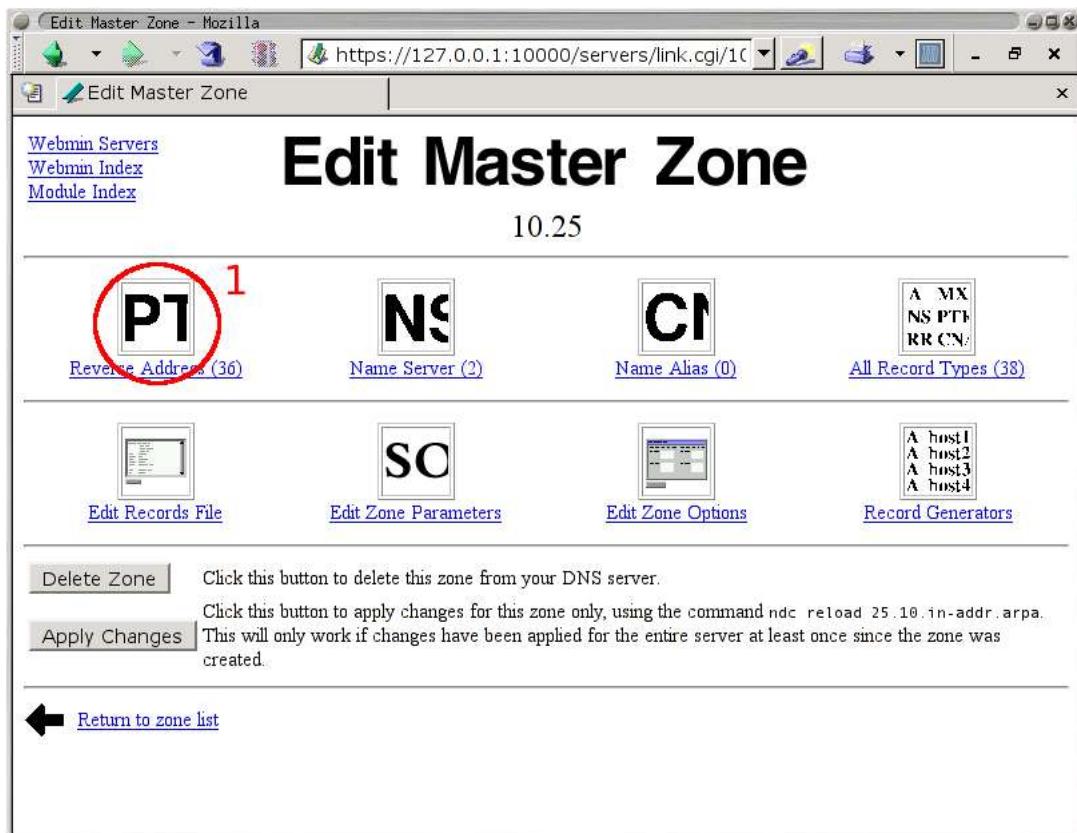


fig 15 - Édition d'une zone inverse

1. Le seul paramètre à modifier est la liste des adresses de la zone

- Liste des enregistrements d'une zone inverse

Name	Type	TTL	Values
25.10.in-addr.arpa.	NS	Default	dns1.emtstvit.
25.10.in-addr.arpa.	NS	Default	dns2.emtstvit.
1.0.25.10.in-addr.arpa.	PTR	Default	lna-ltsp.emtstvit.
2.0.25.10.in-addr.arpa.	PTR	Default	appl1-ltsp.emtstvit.
1.1.25.10.in-addr.arpa.	PTR	Default	ltsp1.emtstvit.
2.1.25.10.in-addr.arpa.	PTR	Default	ltsp2.emtstvit.
3.1.25.10.in-addr.arpa.	PTR	Default	ltsp3.emtstvit.
4.1.25.10.in-addr.arpa.	PTR	Default	ltsp4.emtstvit.
5.1.25.10.in-addr.arpa.	PTR	Default	ltsp5.emtstvit.
6.1.25.10.in-addr.arpa.	PTR	Default	ltsp6.emtstvit.
7.1.25.10.in-addr.arpa.	PTR	Default	ltsp7.emtstvit.
8.1.25.10.in-addr.arpa.	PTR	Default	ltsp8.emtstvit.
9.1.25.10.in-addr.arpa.	PTR	Default	ltsp9.emtstvit.
10.1.25.10.in-addr.arpa.	PTR	Default	ltsp10.emtstvit.
11.1.25.10.in-addr.arpa.	PTR	Default	ltsp11.emtstvit.
12.1.25.10.in-addr.arpa.	PTR	Default	ltsp12.emtstvit.
16.1.25.10.in-addr.arpa.	PTR	Default	ltsp16.emtstvit.
17.1.25.10.in-addr.arpa.	PTR	Default	ltsp17.emtstvit.
18.1.25.10.in-addr.arpa.	PTR	Default	ltsp18.emtstvit.
19.1.25.10.in-addr.arpa.	PTR	Default	ltsp19.emtstvit.
20.1.25.10.in-addr.arpa.	PTR	Default	ltsp20.emtstvit.
21.1.25.10.in-addr.arpa.	PTR	Default	ltsp21.emtstvit.
22.1.25.10.in-addr.arpa.	PTR	Default	ltsp22.emtstvit.
23.1.25.10.in-addr.arpa.	PTR	Default	ltsp23.emtstvit.
24.1.25.10.in-addr.arpa.	PTR	Default	ltsp24.emtstvit.
25.1.25.10.in-addr.arpa.	PTR	Default	ltsp25.emtstvit.
26.1.25.10.in-addr.arpa.	PTR	Default	ltsp26.emtstvit.
27.1.25.10.in-addr.arpa.	PTR	Default	ltsp27.emtstvit.
28.1.25.10.in-addr.arpa.	PTR	Default	ltsp28.emtstvit.
29.1.25.10.in-addr.arpa.	PTR	Default	ltsp29.emtstvit.
30.1.25.10.in-addr.arpa.	PTR	Default	ltsp30.emtstvit.
31.1.25.10.in-addr.arpa.	PTR	Default	ltsp31.emtstvit.

fig 16 - Liste des enregistrements d'une zone inverse

1. Toutes les adresses IP (notation inversée) de la zone sont listées

- Édition d'un enregistrement inverse

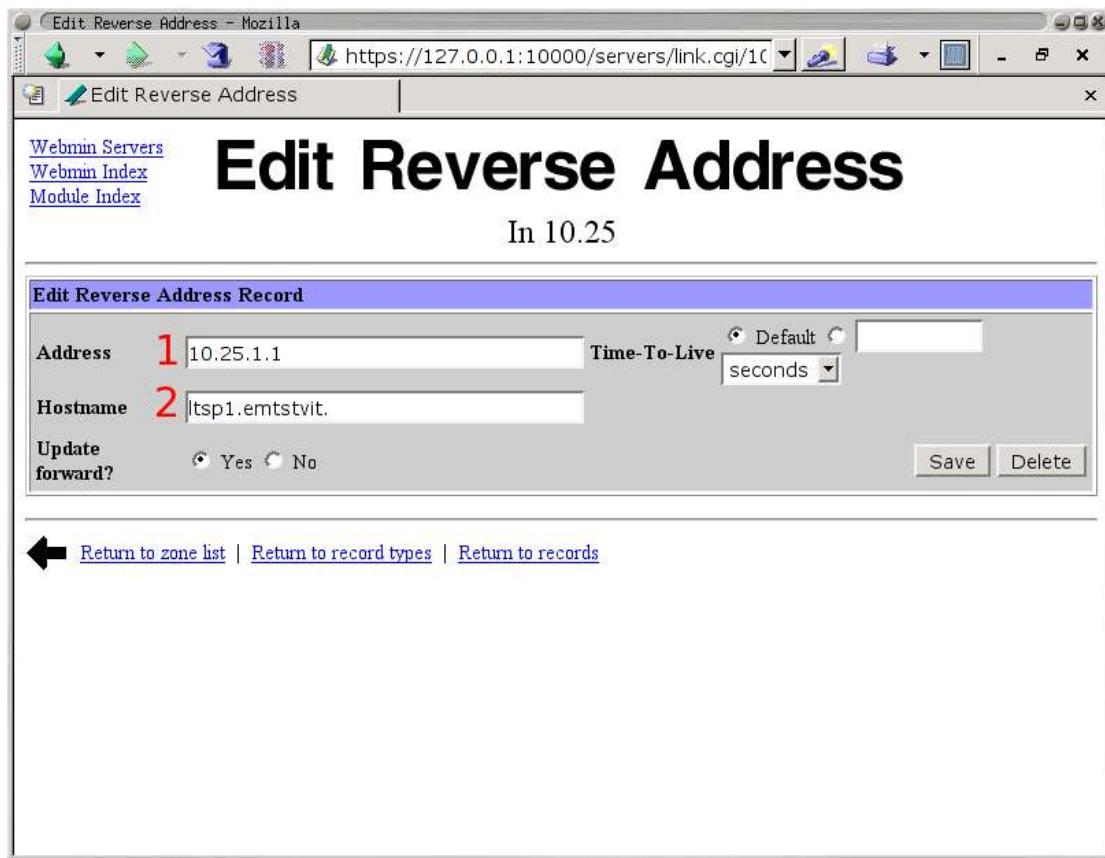


fig 17 - Édition des enregistrements inverses

1. L'adresse IP de la machine éditée
2. le nom de cette machine

- Édition d'une zone directe

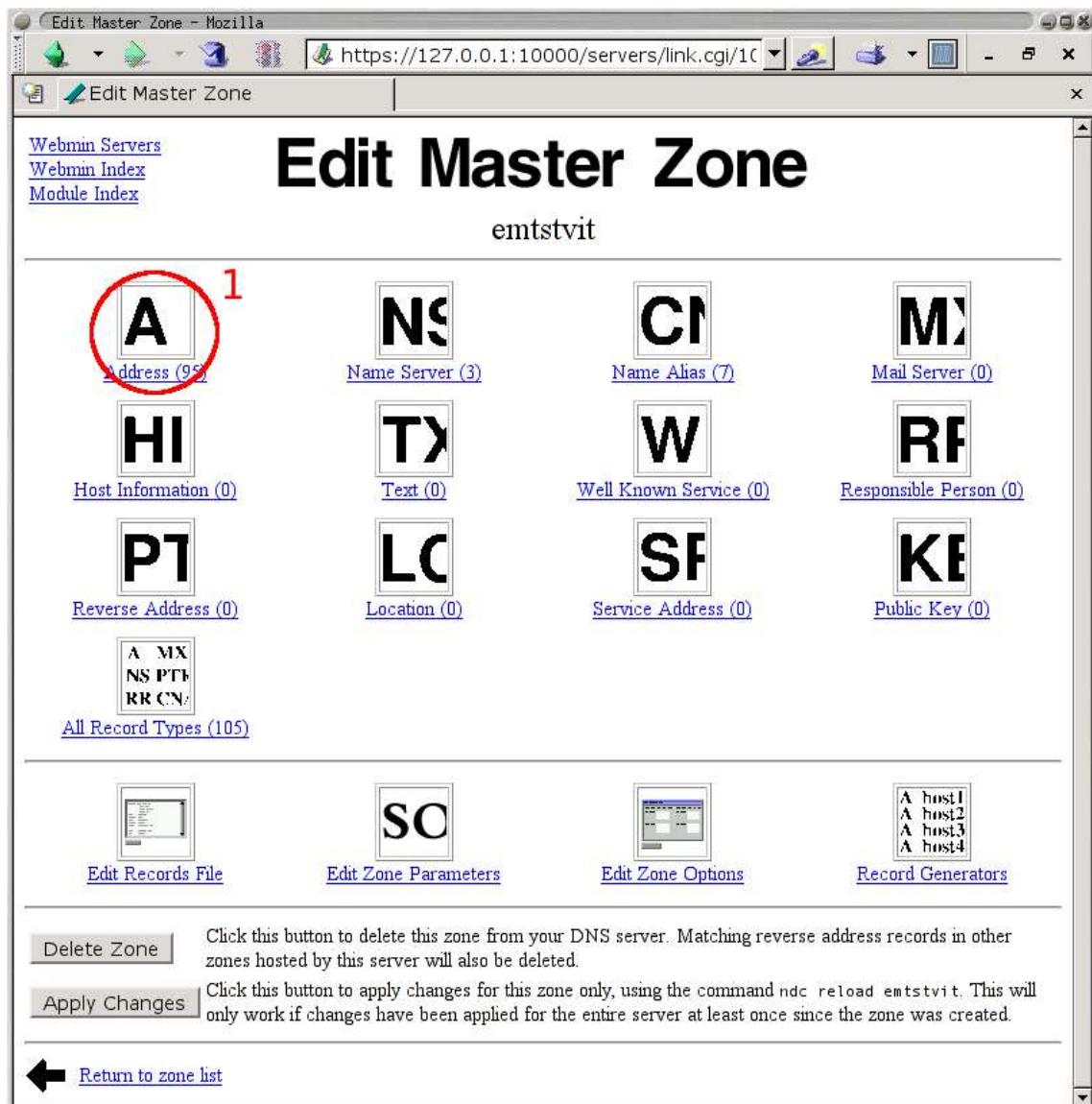


fig 18 - Édition d'une zone directe

1. Le seul paramètre à modifier est la liste des noms du domaine

- Ajout d'un enregistrement à une zone directe

The screenshot shows a Mozilla Firefox browser window with the title "Address Records - Mozilla". The URL bar displays "https://127.0.0.1:10000/servers/link.cgi/1C". The main content area is titled "Address Records" and shows the message "In emtstvit". On the left, there's a sidebar with links: "Webmin Servers", "Webmin Index", and "Module Index". Below the sidebar, a form titled "Add Address Record" is displayed. The "Name" field contains "2" (marked with a red number 1), the "Address" field contains "3" (marked with a red number 2), and the "Time-To-Live" field has "Default" selected. The "Create" button is visible. Below the form is a table listing existing address records, with one row highlighted (marked with a red number 3). The table has two columns: "Name" and "Address".

Name	Address
localhost.emtstvit.	127.0.0.1
fichier.emtstvit.	192.168.3.1
lna.emtstvit.	192.168.3.2
appli.emtstvit.	192.168.3.3
lbs.emtstvit.	192.168.3.4
citrix1sv.emtstvit.	192.168.3.5
citrix2sv.emtstvit.	192.168.3.6
s65ff93a.emtstvit.	192.168.3.8
intranet.emtstvit.	192.168.3.9
station23.emtstvit.	192.168.3.122
station24.emtstvit.	192.168.3.123
station25.emtstvit.	192.168.3.124
station26.emtstvit.	192.168.3.125
station27.emtstvit.	192.168.3.126
station28.emtstvit.	192.168.3.127
station29.emtstvit.	192.168.3.128
station30.emtstvit.	192.168.3.129
station31.emtstvit.	192.168.3.130

fig 19 - Ajout d'un enregistrement en zone directe

1. Nom de la machine à ajouter
2. Adresse IP de la machine à ajouter
3. Tous les noms du domaine sont listés

- Modification d'un enregistrement direct

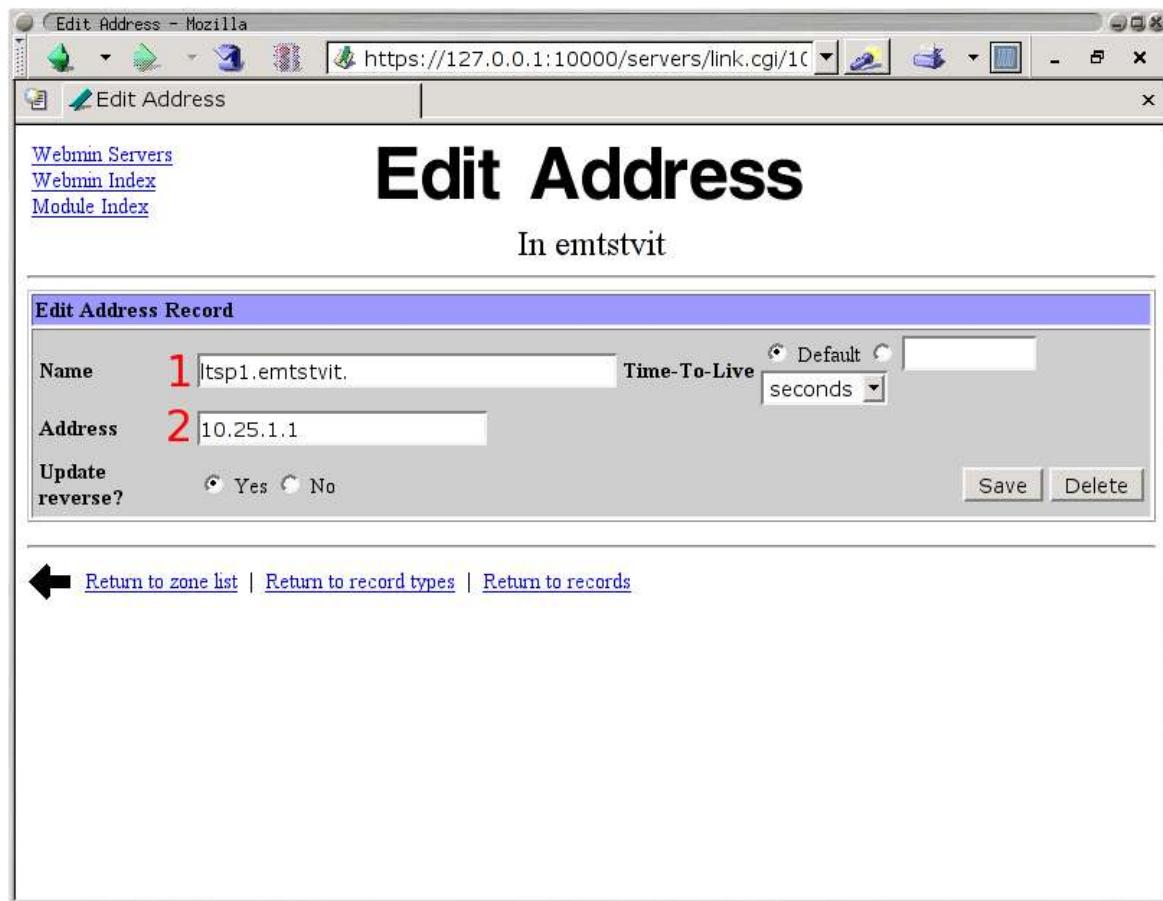


fig 20 - Édition d'une adresse directe

1. Nom de la machine à modifier
2. Adresse IP de la machine à modifier

## 15. SERVICE NFS

---

NFS signifie *Network File System*. C'est, comme son nom l'indique, un système de fichiers en réseau qui permet de partager ses données principalement entre systèmes UNIX. À la différence de SAMBA, NFS gère les permissions sur les fichiers et on peut donc l'utiliser de manière totalement transparente dans son arborescence Linux.

### 15.1. ARCHITECTURE

---

Le service NTP est installé sur la machine **fichier**, d'adresse IP **192.168.3.1**. Pour qu'une machine monte un de ses répertoires partagés, il suffit d'indiquer d'entre la commande suivante:

```
mount      mon.serveur.nfs:/repertoire/sur/le/serveur      /
repertoire/chez/le/client
```

Pour qu'il soit automatiquement monté au démarrage, il suffit de modifier le fichier `/etc/fstab` du client en ajoutant une ligne du type :

```
mon.serveur.nfs:/rep/sur/le/serveur /rep/chez/le/client nfs rw 0 0
```

Le fichier `fstab` contient la liste des partitions qui sont montées au démarrage par le serveur. Ces partitions peuvent être physique et correspondre à un fichier spécial de type device, ou réseau comme dans le cas du nfs.

### 15.2. PARAMÈTRES

---

<i>nom</i>	<b>fichier</b>
<i>adresse IP</i>	<b>192.168.3.1</b>

### 15.3. FICHIERS

---

<i>liste des répertoires exportés</i>	<b>/etc/exports</b>
<i>liste des machines autorisées</i>	<b>/etc/hosts.allow</b>
<i>liste des machines interdites</i>	<b>/etc/hosts.deny</b>
<i>logs</i>	<b>/var/log/syslog</b>

## 15.4. ADMINISTRATION

---

<i>arrêter le service</i>	<b>/etc/init.d/nfs-server stop</b>
<i>démarrer le service</i>	<b>/etc/init.d/nfs-server start</b>
<i>redémarrer le service</i>	<b>/etc/init.d/nfs-server restart</b>
<i>lister les logs</i>	<b>grep nfs /var/log/syslog   less</b>
<i>vérifier la présence du service</i>	<b>rpcinfo -p</b>
<i>tuer le service</i>	<b>killall -9 nfs-server</b>

## 16. SERVICE NTP

---

*NTP signifie Network Time Protocol. C'est un protocole qui permet à un ordinateur de synchroniser son horloge sur un autre ordinateur de précision plus élevée. Dans le cas présent, il permet en particulier de synchroniser les horloges de toutes les machines.*

### 16.1. ARCHITECTURE

---

Le service NTP est installé sur la machine **ntp**, d'adresse IP **192.168.3.31**. Pour qu'une machine l'utilise pour se synchroniser, il suffit de lui indiquer **ntp** comme **serveur de temps**. Ce service n'étant pas critique, il est présent en un seul exemplaire.

### 16.2. PARAMÈTRES

---

<i>nom</i>	<b>ntp</b>
<i>adresse IP</i>	<b>192.168.3.31</b>

### 16.3. FICHIERS

---

<i>configuration</i>	<b>/etc/ntp.conf</b>
<i>logs</i>	<b>/var/log/syslog</b>

### 16.4. ADMINISTRATION

---

<i>arrêter le service</i>	<b>/etc/init.d/ntp stop</b>
<i>démarrer le service</i>	<b>/etc/init.d/ntp start</b>
<i>redémarrer le service</i>	<b>/etc/init.d/ntp restart</b>
<i>lister les logs</i>	<b>grep ntp /var/log/syslog</b>
<i>vérifier la présence du service</i>	<b>ps aux   grep [n]tpd</b>
<i>tuer le service</i>	<b>killall -9 ntpd</b>

## 16.5. SYNTAXE

- /etc/ntp.conf  
**server <nom du premier serveur sur lequel se synchroniser>**  
**server <nom du second serveur sur lequel se synchroniser>**

## 16.6. WEBMIN

- Localisation:

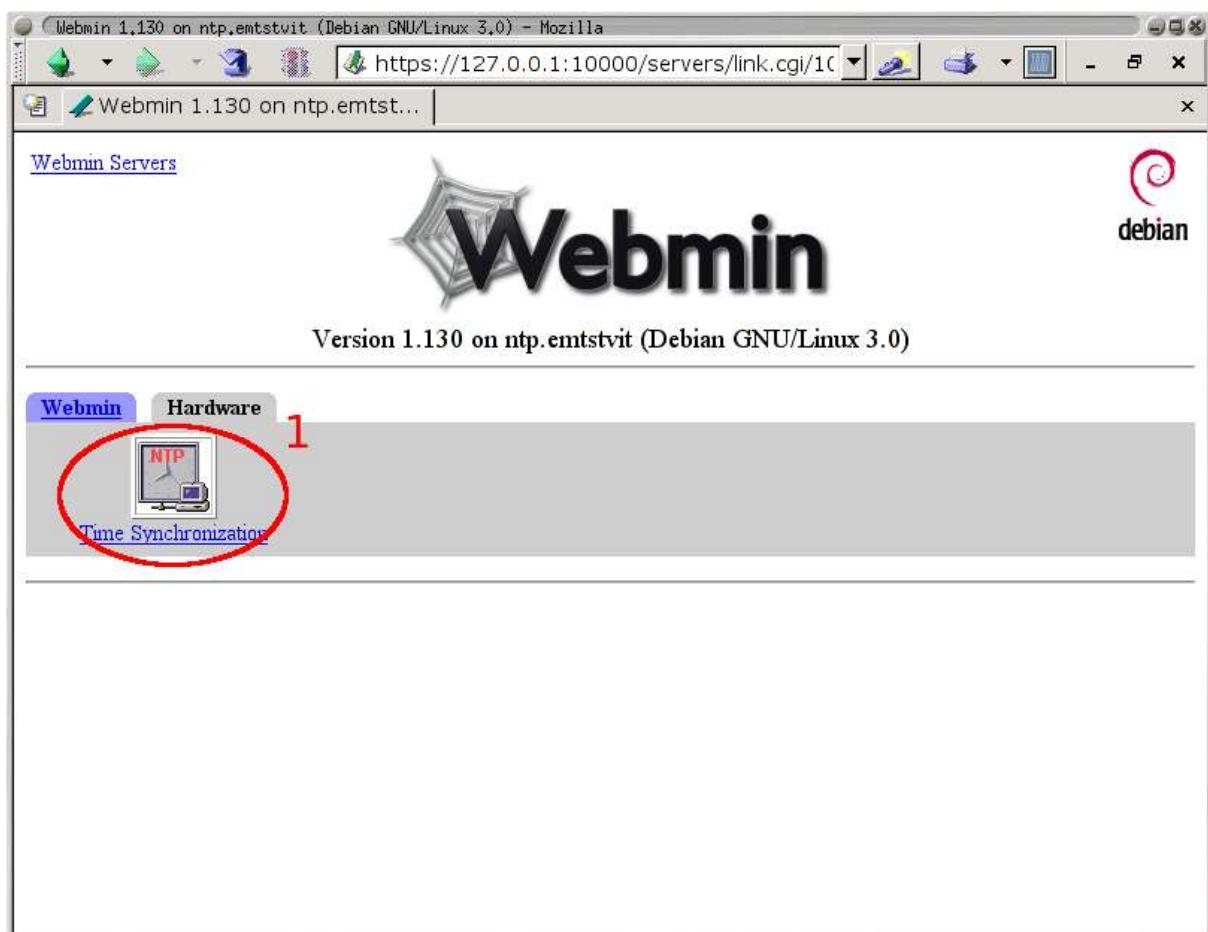


fig 21 - Interface d'administration du service ntp sous webmin

1. L'interface d'administration du serveur NTP se trouve dans la catégorie hardware.

- Écran principal:

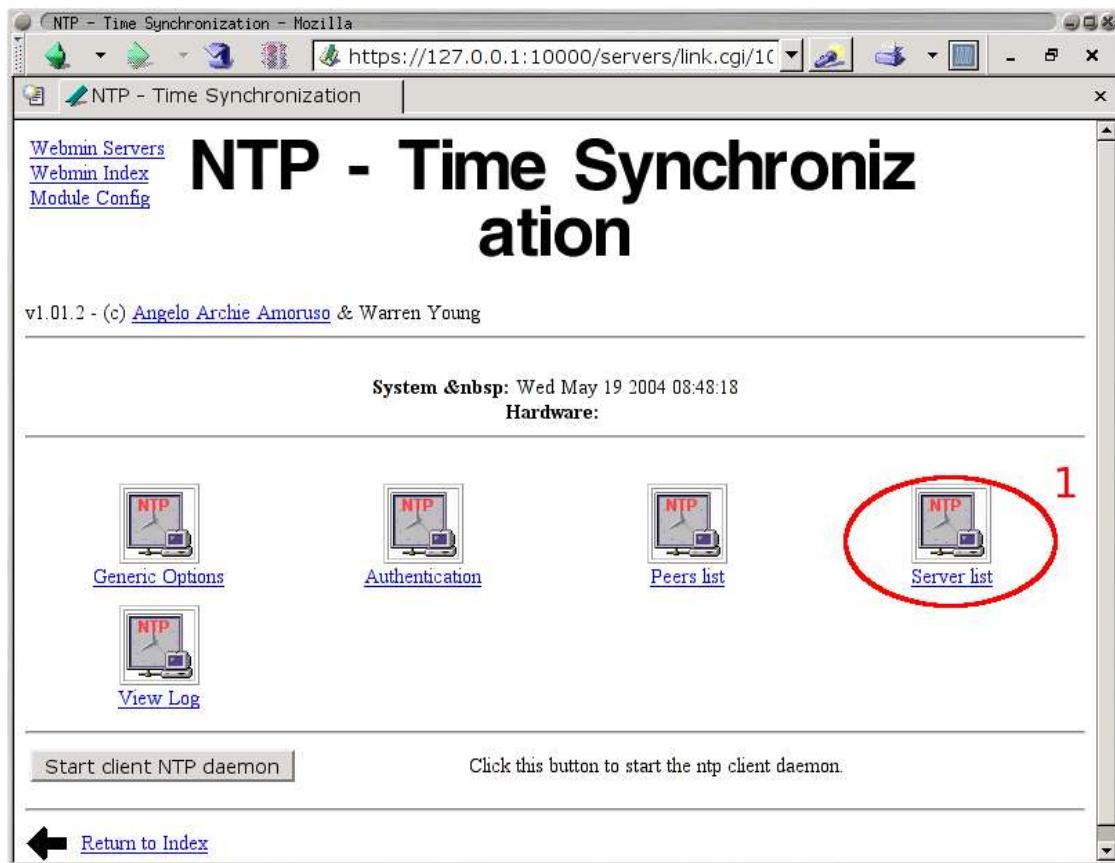


fig 22 - Détail de l'interface gestion du NTP de webmin

1. Le seul paramètre intéressant à configurer est la liste des serveurs sur lesquels se synchroniser

- Gestion de la liste des serveurs

NTP - Server List - Mozilla

https://127.0.0.1:10000/servers/link.cgi/10

# NTP - Server List

v1.01.2 - (c) Angelo Archie Amoruso & Warren Young

IP ADDRESS	VERSION	KEY	PREFERRED	CHECK
<a href="#">ntp.u-psud.fr</a>	Default (0)	None	No	Contact
<a href="#">ntp2.unicaen.fr</a>	Default (0)	None	No	Contact

1 Click on server address to edit

2

Create new

[Return to Module Index](#)

fig 23 - Liste des serveurs NTP contactés

1. Liste des serveurs en cours d'utilisation (un click sur le lien permet de les reconfigurer)
2. Lien permettant de vérifier le fonctionnement de la synchronisation
3. Bouton permettant d'ajouter un nouveau serveur

- Vérification de la synchronisation

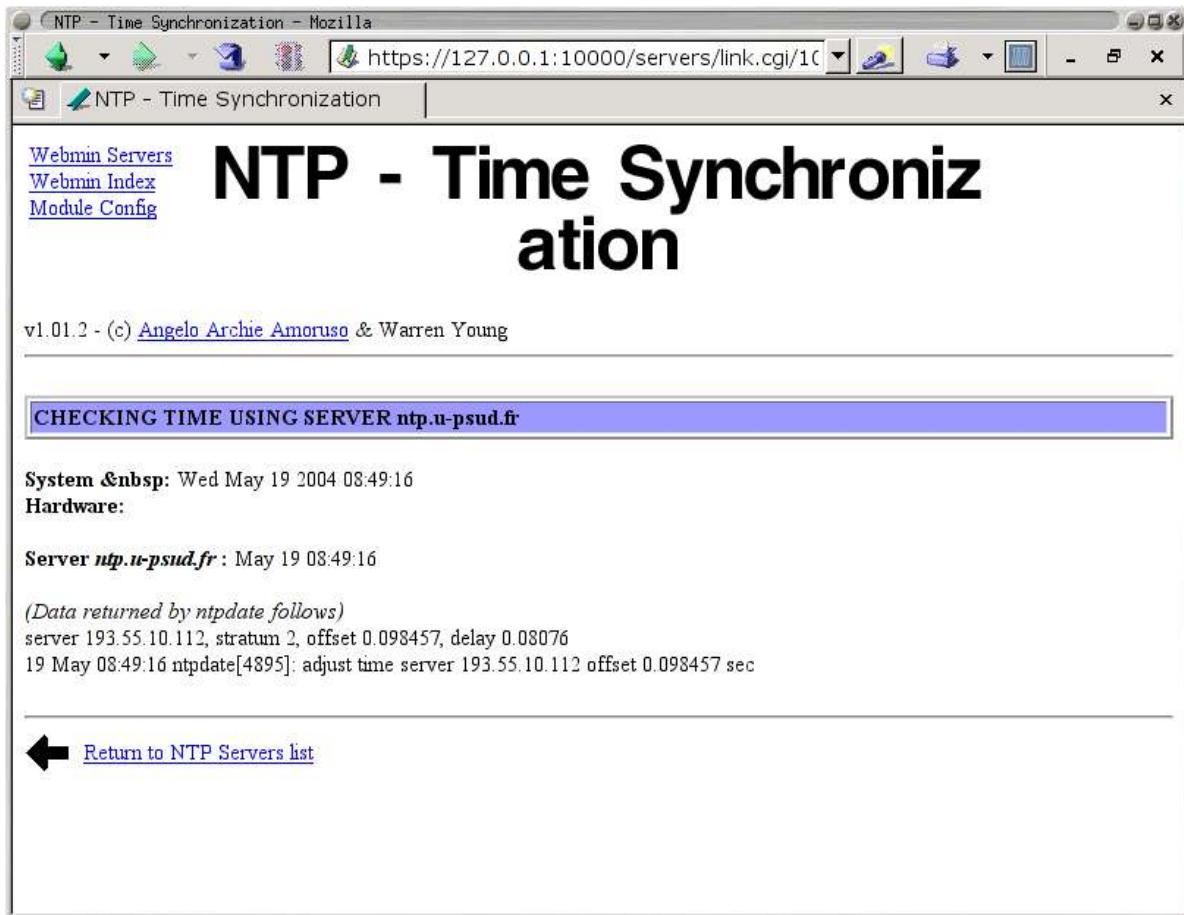


fig 24 - Vérification de la synchronisation

## 17. SERVICE LDAP + SAMBA

*L'administration des utilisateurs d'un domaine Windows est possible grâce à l'interface IDX Ldap Accounts.*

### 17.1. ÉCRANS DE BASE

- Localisation:

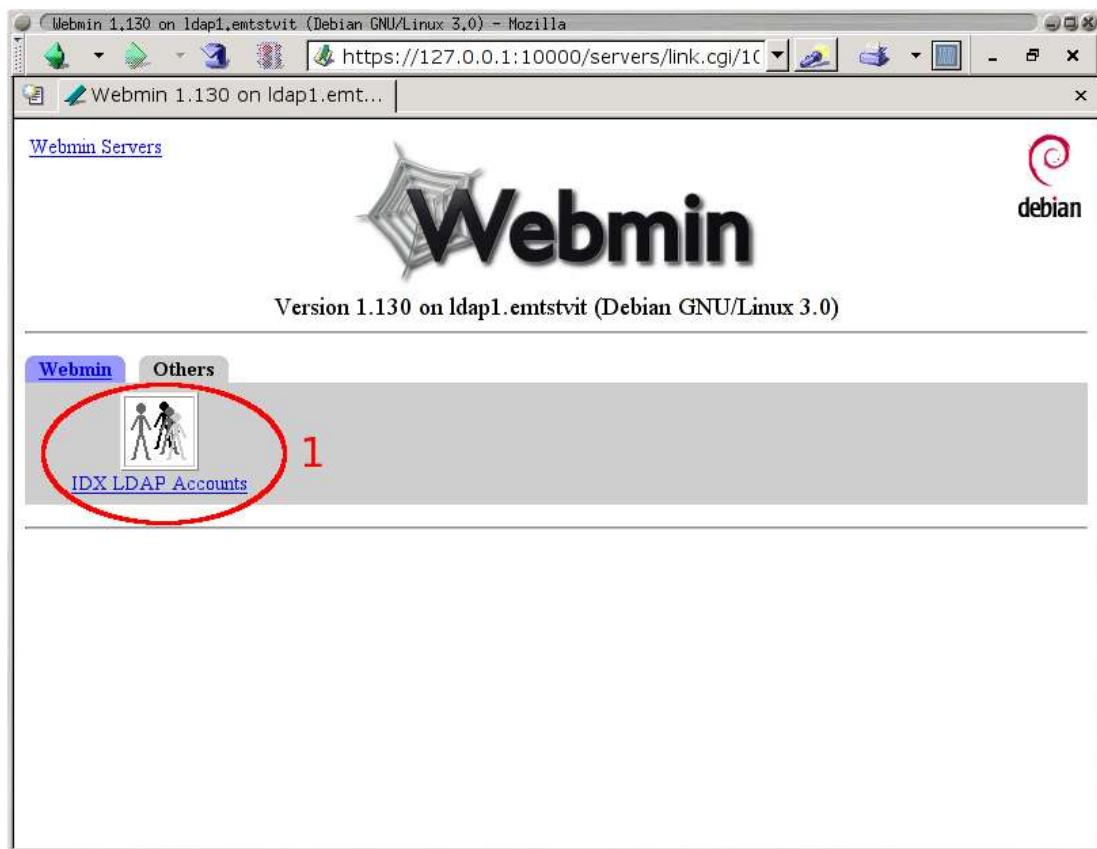


fig 25 - Module webmin pour la gestion du service LDAP

L'interface d'administration des utilisateurs LDAP se trouve dans la catégorie **others**.

- Écran principal
  - 1. Liens pour l'administration des utilisateurs

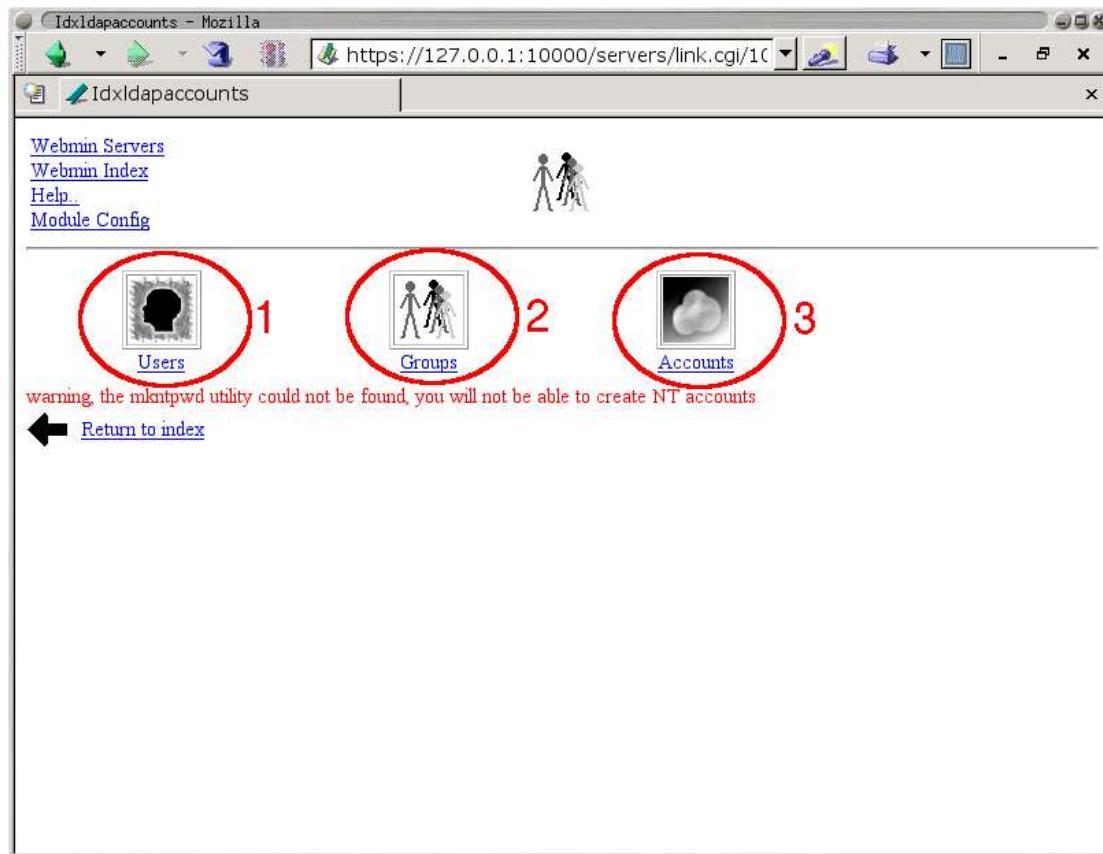


fig 26 - Accès aux fonctions principales de gestion

- 2. Liens pour l'administration des groupes
- 3. Liens pour l'administration des comptes

## 17.2. GESTION DES UTILISATEURS

- L'interface de gestion des utilisateurs présente deux catégories:

The screenshot shows a Mozilla Firefox browser window titled 'Users - Mozilla'. The address bar contains the URL <https://127.0.0.1:10000/servers/link.cgi/1C>. The page title is 'Users'. On the left, there's a sidebar with links: 'Webmin Servers', 'Webmin Index', 'Module Index', 'Help...', and 'Module Config'. Below the sidebar, a search bar is labeled 'Search users' with fields for 'Name:' and 'uid', and a dropdown menu for 'search by'. A red box highlights this search area, with the number '1' next to the 'Name:' field and '2' next to the 'uid' dropdown. To the right of the search bar, a blue link reads '• ou=People, ou=emt25, dc=emtechno, dc=fr'. The main content area is titled 'Users' and displays a table of user information. The table has columns: Name, Status, Number, Full name, Description, and Delete user. Each row shows a user icon, a name like 'acarrey', their status (e.g., 1014), full name (e.g., 'Carrey Alain'), description (e.g., 'System User'), and a 'Delete user' link. A red box highlights the first row ('acarrey'). A red number '1' is placed next to the 'acarrey' entry. A red number '2' is placed next to the 'uid' dropdown in the search bar. At the bottom of the table, there are page navigation links from 1 to 10. A 'Return to index' link with a back arrow is at the bottom left.

Name	Status	Number	Full name	Description	Delete user
acarrey	1	1014	acarrey	Carrey Alain	<a href="#">delete</a>
administrateur		1091	administrateur	System User	<a href="#">delete</a>
apprentibef1		1123	apprentibef1	apprentibef1	<a href="#">delete</a>
apprentibef2		1124	apprentibef2	apprentibef2	<a href="#">delete</a>
arodot		1077	arodot	Rodot Alain	<a href="#">delete</a>
asimplot		1105	asimplot	Simplot Alexandre	<a href="#">delete</a>
atouati		1013	atouati	Touati Abderrahman	<a href="#">delete</a>
bbulle		1133	bbulle	bbulle	<a href="#">delete</a>
bducher		1085	bducher	Dugher Bernard	<a href="#">delete</a>
cbrehier		1021	cbrehier	Brehier Christophe	<a href="#">delete</a>

fig 27 - Interface de gestion des utilisateurs

1. une liste des utilisateurs
2. une interface de recherche

## ● Paramètres généraux

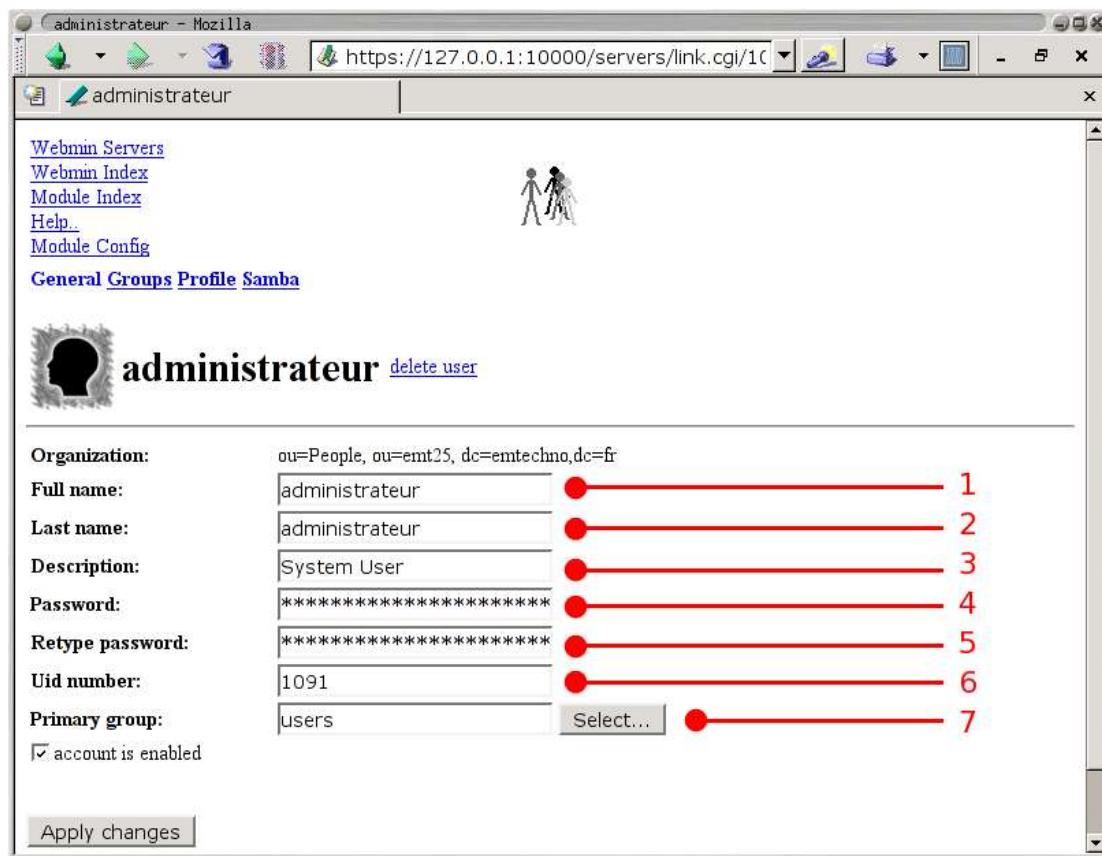


fig 28 - Paramètres généraux d'un utilisateur

1. login de l'utilisateur
2. Nom de l'utilisateur
3. Description de l'utilisateur
4. Mot de passe de l'utilisateur
5. Mot de passe de l'utilisateur (confirmation)
6. Identifiant de l'utilisateur
7. Groupe principal de l'utilisateur

- Groupes d'appartenance de l'utilisateur

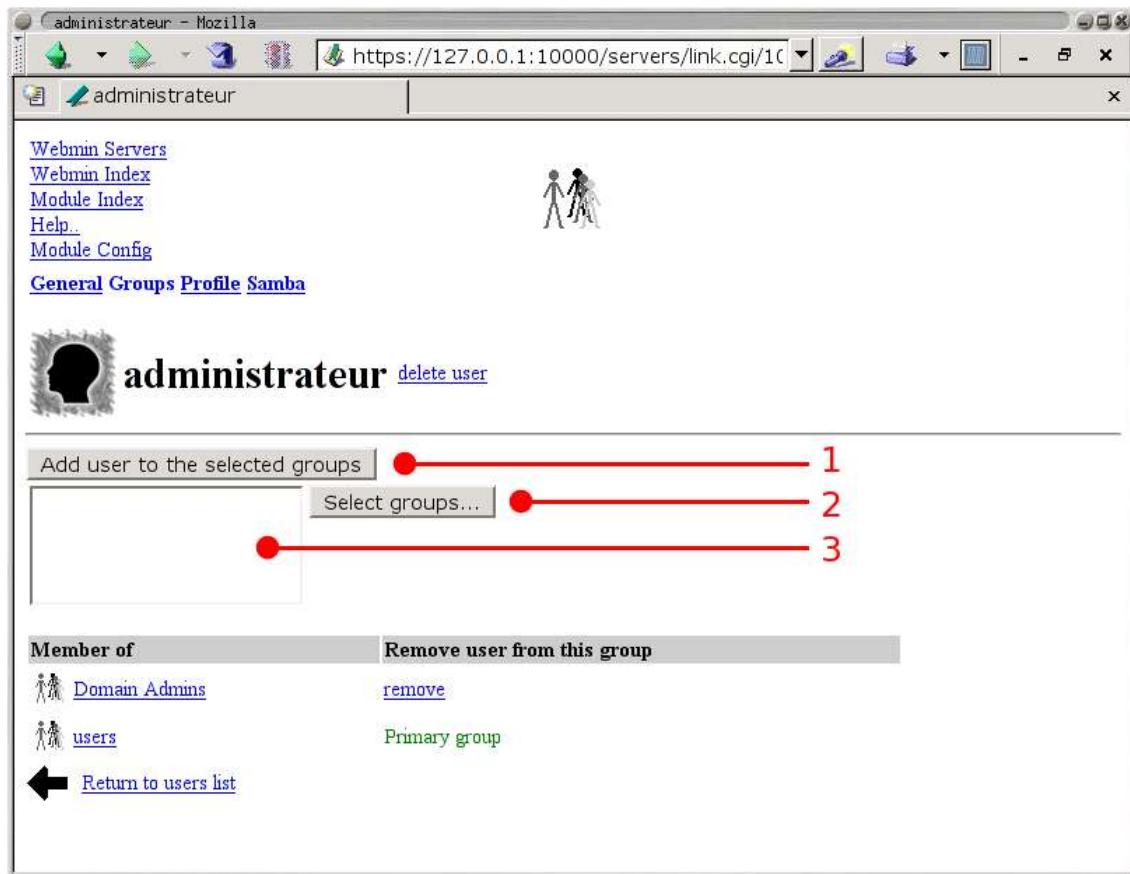


fig 29 - Groupes d'appartenance d'un utilisateur

1. Bouton permettant d'ajouter l'utilisateur à d'autres groupes
2. Bouton permettant de sélectionner les groupes auxquels ajouter l'utilisateur
3. Liste des groupes supplémentaires auquel appartient l'utilisateur

## ● Profil de l'utilisateur



fig 30 - Profil d'un utilisateur

1. Shell de l'utilisateur
2. Répertoire de base de l'utilisateur

- Paramètres samba de l'utilisateur

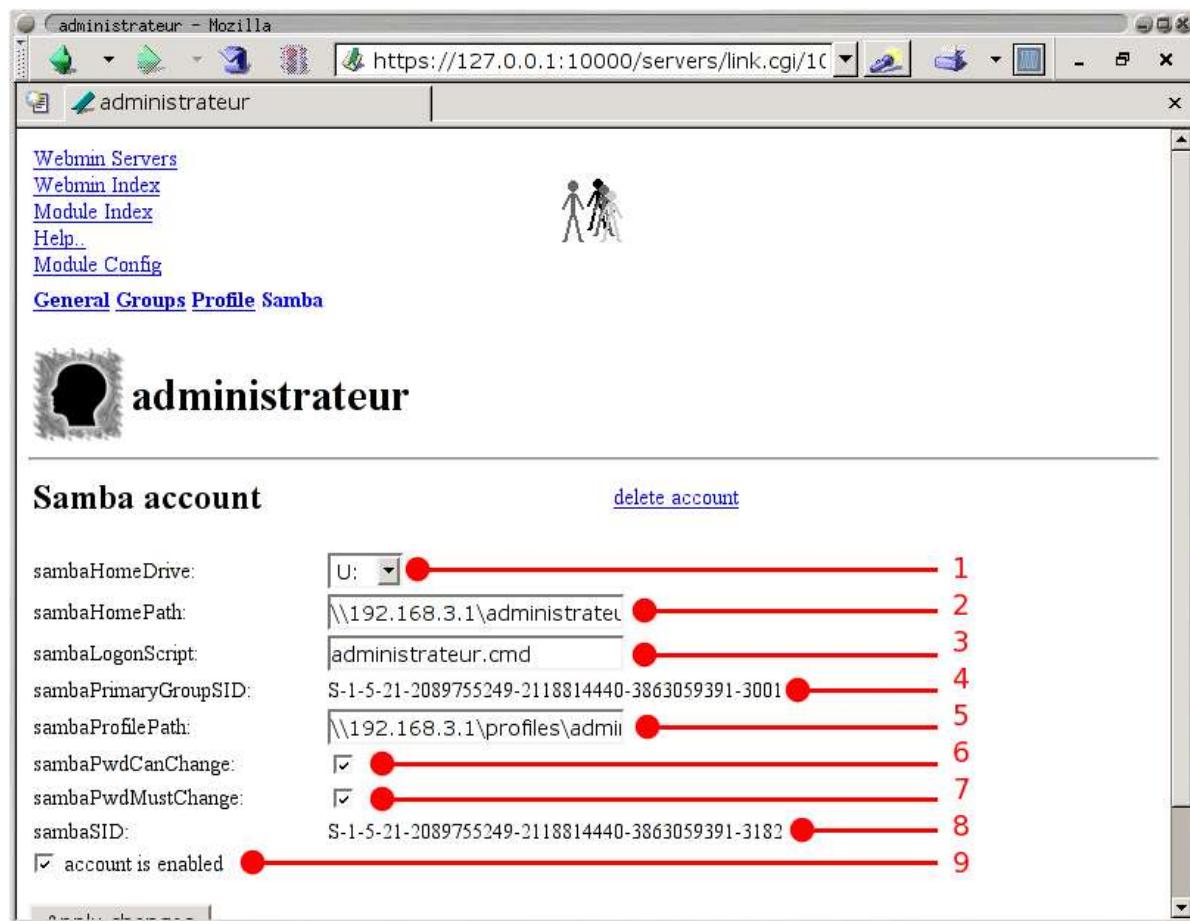


fig 31 - Paramètres samba d'un utilisateur

1. Point de montage du répertoire de base de l'utilisateur
2. Emplacement réseau du répertoire de base de l'utilisateur
3. Script exécuté à la connexion de l'utilisateur
4. GSID (identifiant samba) du groupe de l'utilisateur
5. Emplacement réseau du profil de l'utilisateur
6. Possibilité de l'utilisateur de changer son mot de passe
7. Obligation de l'utilisateur de changer son mot de passe
8. SID (identifiant samba) de l'utilisateur
9. Possibilité de l'utilisateur de se connecter

## 17.3. GESTION DES GROUPES

- L'interface de gestion des utilisateurs est semblable à l'interface de gestion des utilisateurs et dispose de deux zones :

The screenshot shows a Mozilla Firefox browser window with the title 'Groups - Mozilla'. The address bar displays the URL <https://127.0.0.1:10000/servers/link.cgi/10>. The page content is titled 'Search groups' and contains a search form with fields for 'Name:' and 'cn', and a dropdown menu. To the right of the search form, there is a note about LDAP search parameters: '• ou=Group, ou=emt25, dc=emtechno, dc=fr'. Below the search form is a link 'Add group'. The main area is titled 'Groups' and lists ten entries in a table format. The first entry, 'Comptabilite25', is highlighted with a red box and labeled '1'. The table columns are 'Name', 'Group number', 'Description', and 'Delete group'. The entries are:

Name	Group number	Description	Delete group
<a href="#">Comptabilite25</a>	1006	Local Unix group	<a href="#">delete</a>
<a href="#">Domain Admins</a>	200	Local Unix group	<a href="#">delete</a>
<a href="#">Domain Guests</a>	1028	not found	<a href="#">delete</a>
<a href="#">Domain Users</a>	1027	not found	<a href="#">delete</a>
<a href="#">achats25</a>	1002	Local Unix group	<a href="#">delete</a>
<a href="#">administratif25</a>	1003	Local Unix group	<a href="#">delete</a>
<a href="#">as400</a>	1033	not found	<a href="#">delete</a>
<a href="#">autocad_lt</a>	1034	not found	<a href="#">delete</a>
<a href="#">bureau_etude25</a>	1004	Local Unix group	<a href="#">delete</a>
<a href="#">commercial25</a>	1005	Local Unix group	<a href="#">delete</a>

At the bottom of the page, there is a navigation bar with links for 'page: [1] [2] [3] [4] [5]' and a 'Return to index' button.

fig 32 - Interface de gestion des groupes

- Cependant un seul paramètre est modifiable:

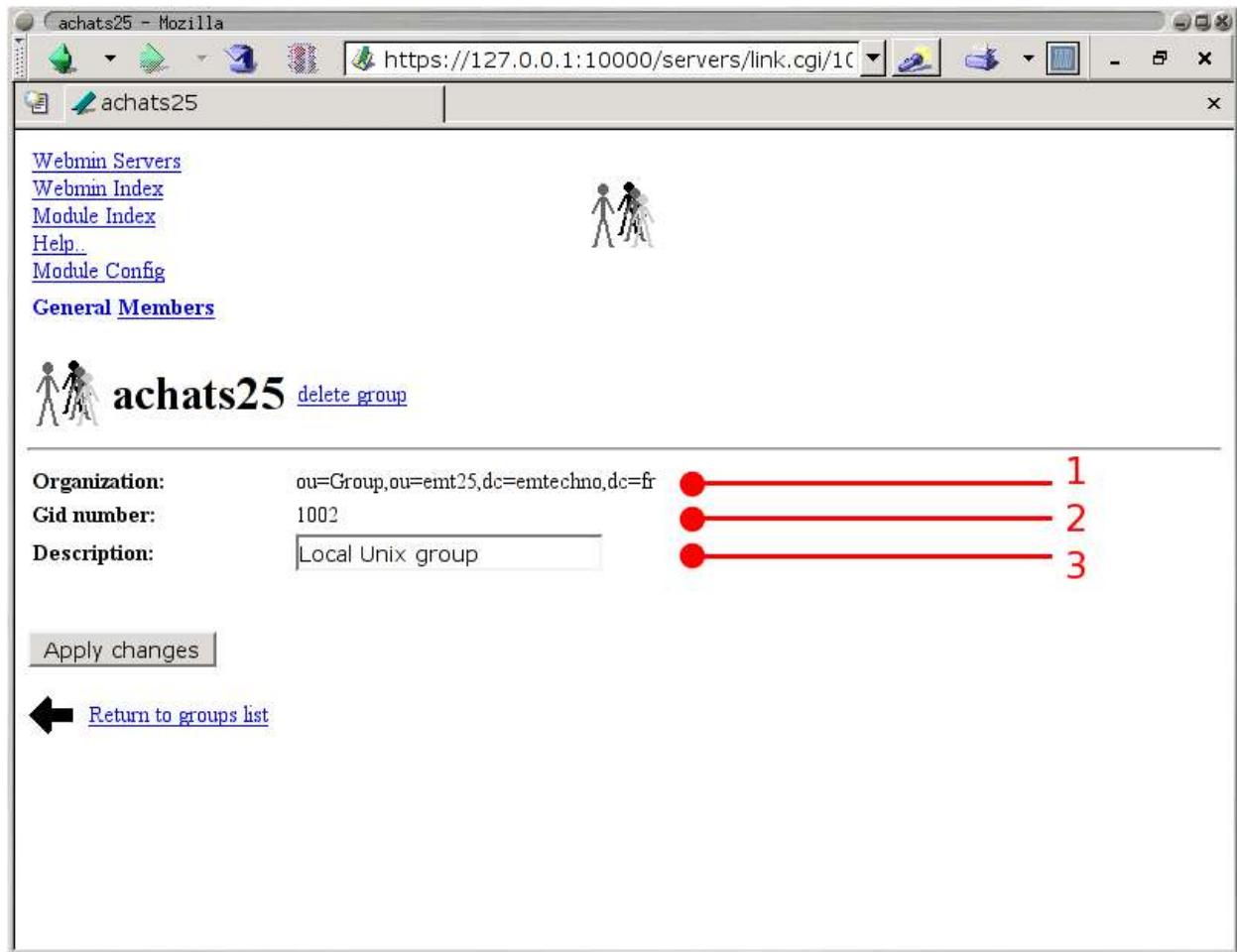


fig 33 - Modification d'un groupe

2. Identifiant du groupe
3. Description du groupe

## 17.4. GESTION DES COMPTES

- Enfin, l'interface permet la gestion des types de compte pour les installations hétérogènes:

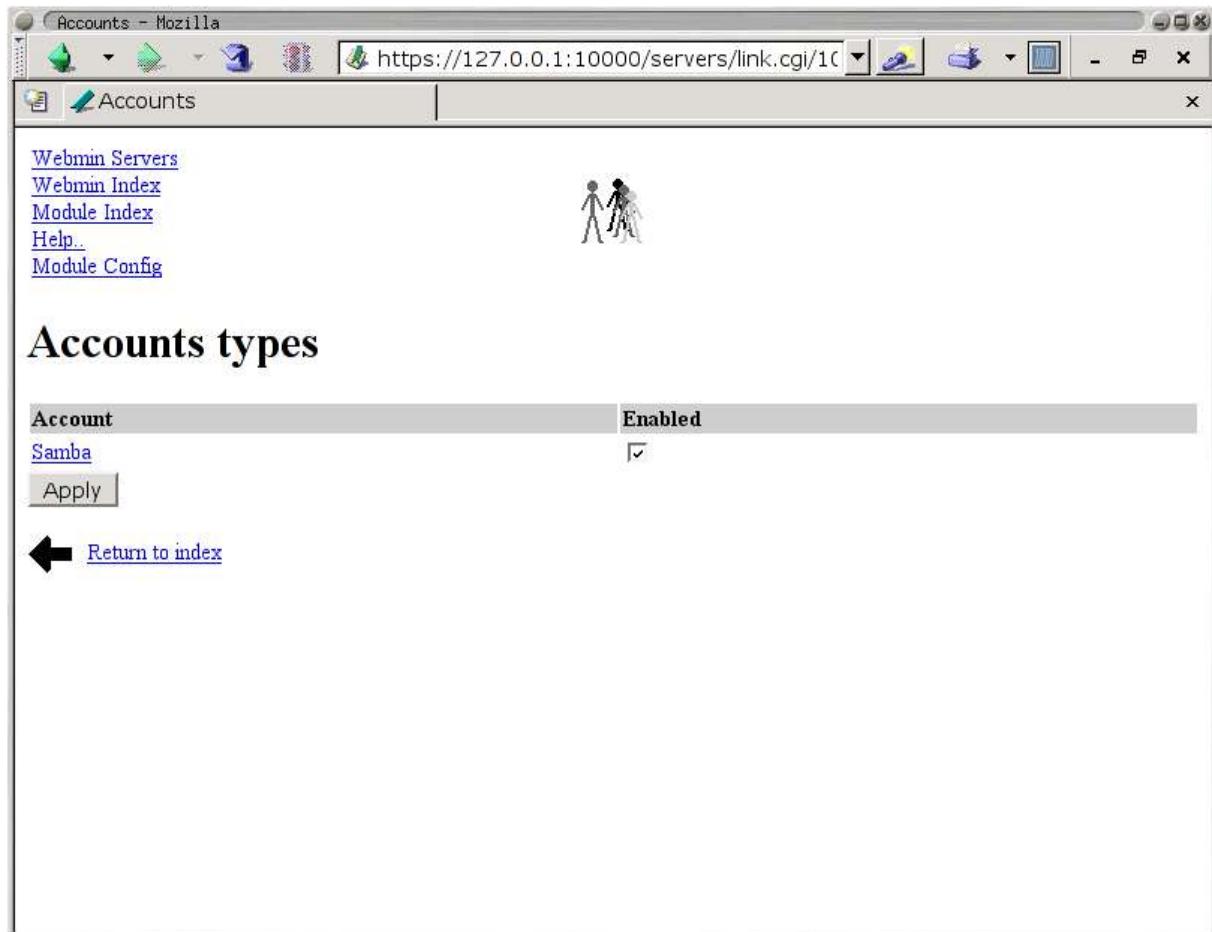


fig 34 - Interface de gestion des types de compte

## 18. SERVICES UML

---

*UML signifie User Mode Linux. Un service UML est en quelque-sorte une machine virtuelle à part entière. Depuis l'intérieur, elle se comporte comme une machine classique à part entière, et vue depuis l'extérieur, elle prend la forme d'un simple programme. Elle peut communiquer avec son environnement par le biais du fichier de la machine hôte et part des interfaces réseau également virtuelles.*

### 18.1. ARCHITECTURE

---

Actuellement les UML sont toutes installées sur **Ina**. Elles sont au nombre de 7:

- **dhcp1**, d'adresses (intérieure) et (extérieure)
- **dhcp2**, d'adresses (intérieure) et (extérieure)
- **dns1**, d'adresses (intérieure) et (extérieure)
- **dns2**, d'adresses (intérieure) et (extérieure)
- **ldap1**, d'adresses (intérieure) et (extérieure)
- **ldap2**, d'adresses (intérieure) et (extérieure)
- **ntp**, d'adresses (intérieure) et (extérieure)

### 18.2. PARAMÈTRES

---

<b>nom</b>	<b>Ina</b>
<b>adresse IP</b>	<b>192.168.3.2</b>

## 18.3. FICHIERS

---

<i>fichier de configuration global</i>	<code>/etc/init.d/uml-servers.sh (sur Ina)</code>
<i>fichiers de configuration de chaque uml</i>	<code>/net/fichier/home/uml-images/confs/&lt;nom de l'uml&gt; (sur Ina)</code>
<i>disque virtuel de chaque uml</i>	<code>/net/fichier/home/uml-images/images/&lt;nom de l'uml&gt; (sur Ina)</code>
<i>logs</i>	<code>/var/log/syslog (sur Ina)</code>

## 18.4. ADMINISTRATION

---

<i>arrêter les UML</i>	<code>/etc/init.d/uml-servers.sh stop</code>
<i>démarrer les UML</i>	<code>/etc/init.d/uml-servers.sh start</code>
<i>redémarrer les UML</i>	<code>/etc/init.d/uml-servers.sh restart</code>
<i>lister les logs</i>	<code>less /var/log/syslog   grep &lt;nom de la machine UML&gt;</code>
<i>tuer le service</i>	<code>killall -9 linux</code>

## 18.5. WEBMIN

- Localisation:

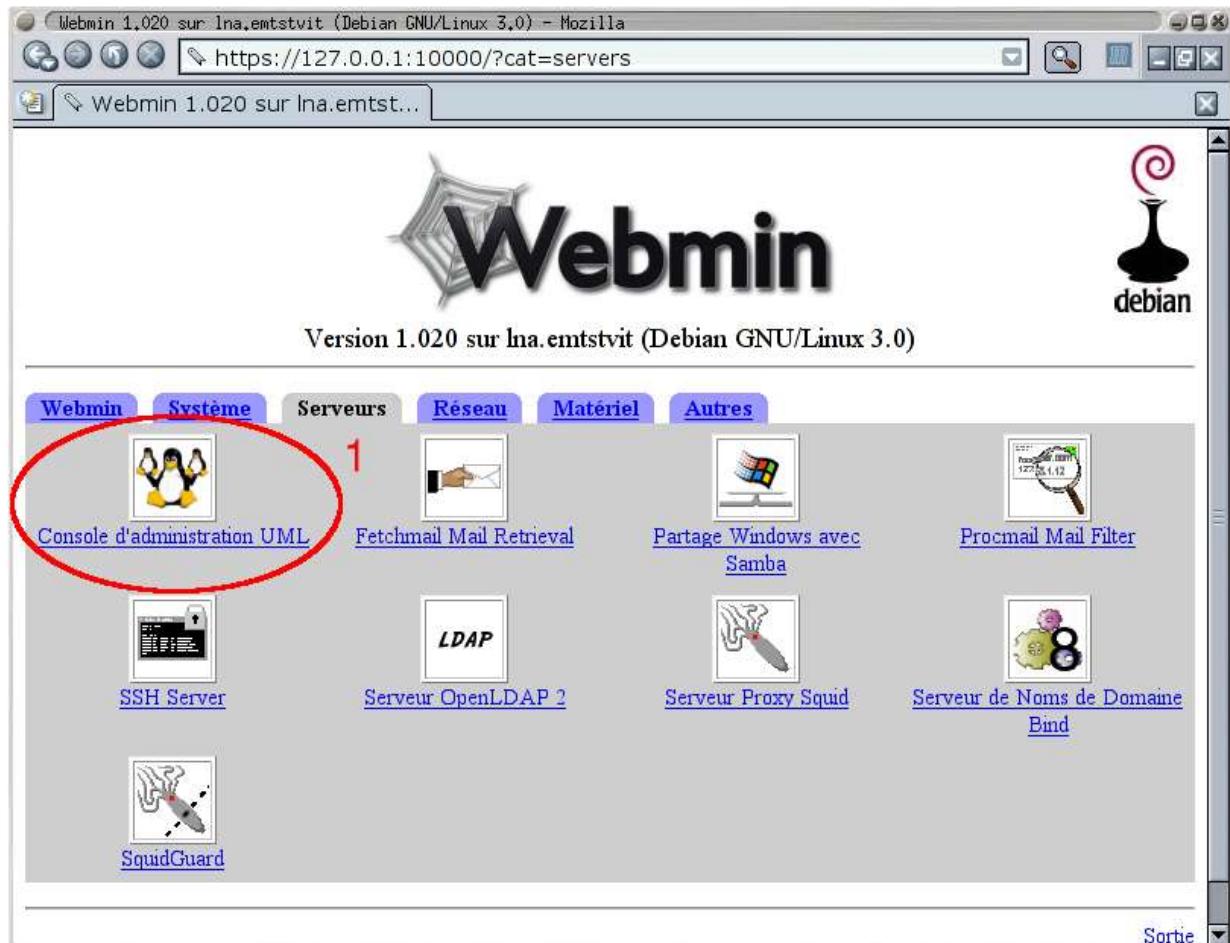


fig 35 - Interface d'administration de User Mode Linux

1. L'interface d'administration du serveur uml se trouve dans la catégorie **servers**.

- Écran principal:

The screenshot shows a Mozilla browser window titled "Console UML - Mozilla" displaying the "Console UML" interface. The URL is https://127.0.0.1:10000/uml-admin/. The page has a red circle around the "Module" link in the top left menu bar, which is highlighted with the number 9. A red box labeled 1 surrounds the first column of the table, which lists UML modules: dhcp1, dhcp2, dns1, dns2, ldap1, ldap2, and ntp. Another red box labeled 2 surrounds the second column, "Status". The third column, "Stats", contains several small charts. Columns 4 through 8 are labeled 3, 4, 5, 6, 7, and 8 respectively, each with a red box around them. The last two columns are "Informations" and "Journaux". At the bottom left is a back arrow and the link "Retourner à l'index".

UML	Status	Stats				Informations	Journaux
dhcp1	lancée		Maintenance	Démarrage	Arrêt	Informations	Journaux
dhcp2	lancée		Maintenance	Démarrage	Arrêt	Informations	Journaux
dns1	lancée		Maintenance	Démarrage	Arrêt	Informations	Journaux
dns2	lancée		Maintenance	Démarrage	Arrêt	Informations	Journaux
ldap1	lancée		Maintenance	Démarrage	Arrêt	Informations	Journaux
ldap2	lancée		Maintenance	Démarrage	Arrêt	Informations	Journaux
ntp	lancée		Maintenance	Démarrage	Arrêt	Informations	Journaux

fig 36 - Console d'administration UML

1. liste des UMLs
2. statut des UMLs. Les valeurs possibles sont:
  - lancée: la machine est en fonctionnement
  - arrêtée: la machine est stoppée
  - suspendue: la machine est en pause
  - bloquée: la machine est dans un état instable

### 3. statistiques d'occupation mémoire:

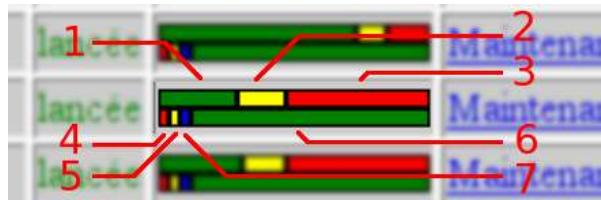


fig 37 - Indicateur graphique d'état d'une machine UML

1. mémoire disponible
2. mémoire attribuée aux caches, buffers, ...
3. mémoire occupée
4. occupation du processeur à des tâches utilisateur
5. occupation du processeur à des tâches système
6. occupation du processuer à ne rien faire
7. occupation du processuer à des tâches de faible priorité
4. lien menant à la page de maintenance des UML
5. lien permettant de démarrer un UML
6. lien permettant de tuer un UML
7. lien menant à une page d'informations à propos d'un UML
8. lien menant à une page des logs d'un UML
9. lien menant à la page de configuration de l'interface

- Écran de configuration de l'interface

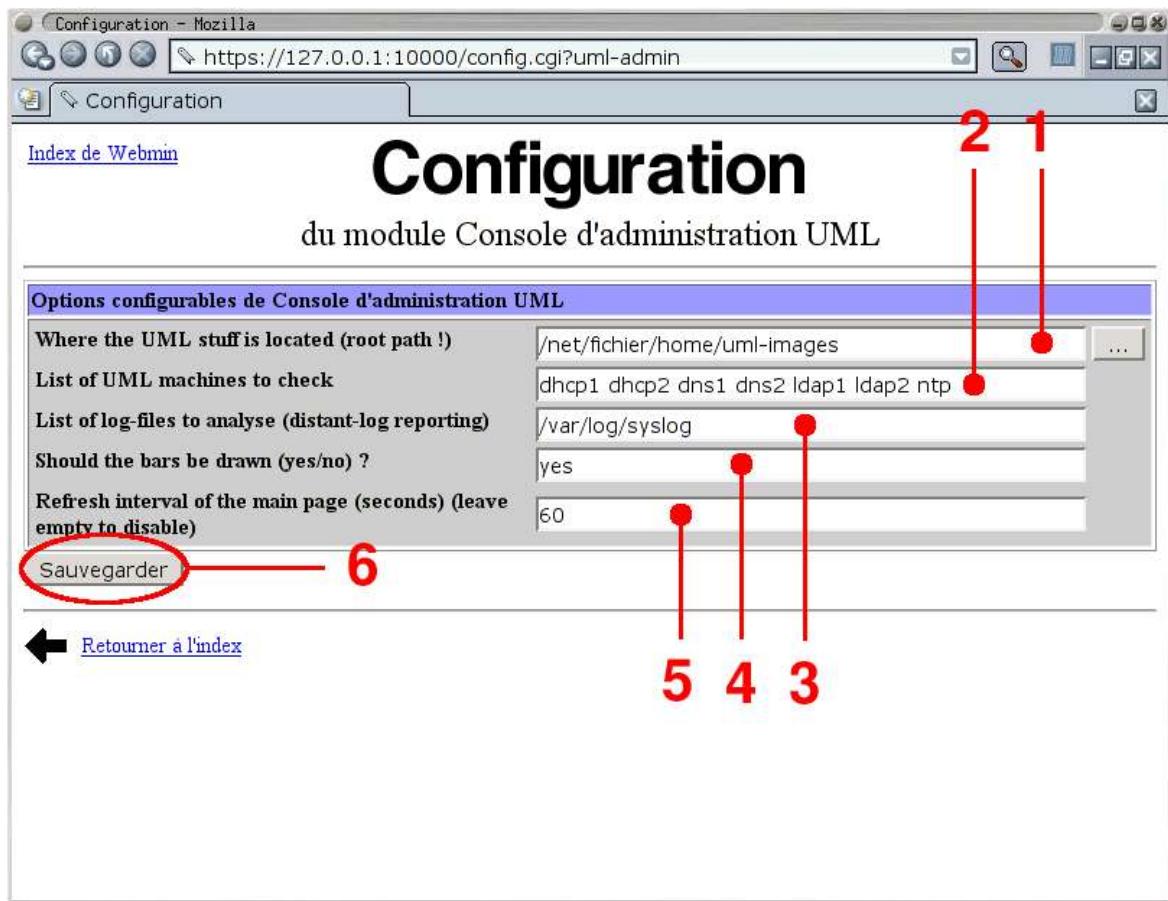


fig 38 - Configuration du module d'administration UML

- répertoire de base des UMLs
- liste des UMLs à surveiller depuis l'interface
- liste des fichiers dans lesquels aller chercher les logs des UMLs
- dessiner ou non les barres de statistiques ?
- intervalle de rafraîchissement de la page principale

● Page de maintenance des UML

Pilotage physique	
1	Démarrer (équivaut à mettre la machine sous tension)
2	Reboot (Équivaut à taper la combinaison de touches <control><alt><del>)
3	Reset (équivaut à appuyer sur le bouton « reset » de la machine)
4	Tuer (équivaut à débrancher la prise de courant de la machine)
5	Pause (équivaut à appuyer sur la touche « pause »)
6	Reprise (équivaut à appuyer sur la touche « pause »)
Pilotage logique	
7	Arrêter (équivaut à taper « halt » à la ligne de commande)
8	Redémarrer (équivaut à taper « reboot » à la ligne de commande)
Commandes avancées	
9	Vérifier le disque Déclenche la vérification du fichier UML
10	Débloquer Réinitialise un fichier UML
11	Sauvegarder le disque Crée une copie de sauvegarde de l'UML
12	Restaurer le disque Mets en place une copie de sauvegarde de l'UML

[Retourner à l'index](#) | [Retourner à Console UML](#)

fig 39 - Page de maintenance d'un UML

1. mise sous tension de la machine virtuelle
2. envoyer la combinaison <ctrl><alt><del> à la machine virtuelle
3. appuyer sur le bouton « reset » de la machine virtuelle
4. débrancher la machine virtuelle
5. mettre en pause la machine virtuelle
6. sortir la machine virtuelle de sa pause
7. arrêter proprement la machine virtuelle
8. redémarrer proprement la machine virtuelle
9. vérifier le disque de la machine virtuelle
10. débloquer une machine virtuelle bloquée
11. sauvegarder le disque d'un machine virtuelle
12. restaurer le disque d'une machine virtuelle

● Démarrage d'une machine virtuelle

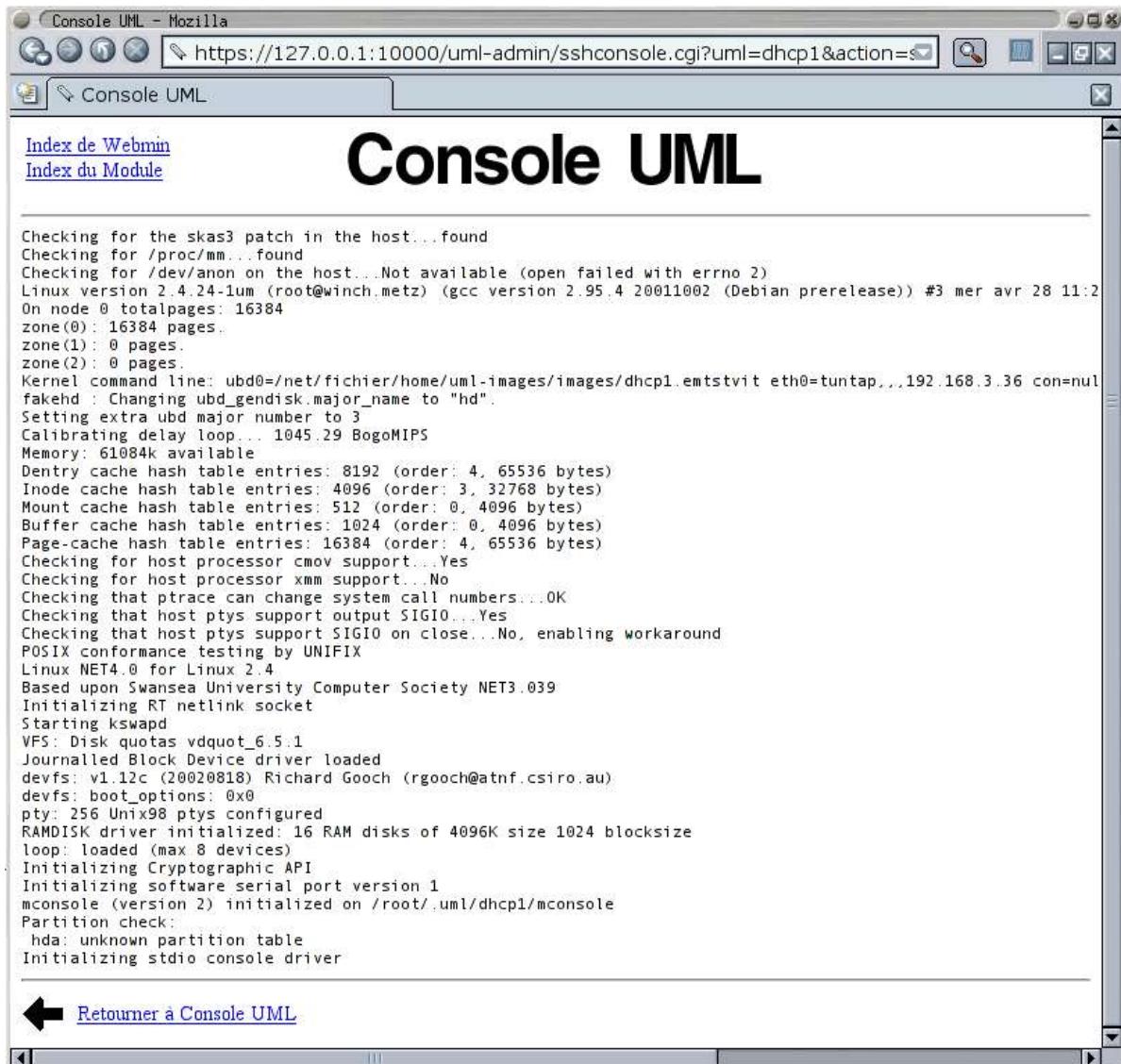


fig 40 - Démarrage d'une machine UML

- Page d'informations d'une machine virtuelle

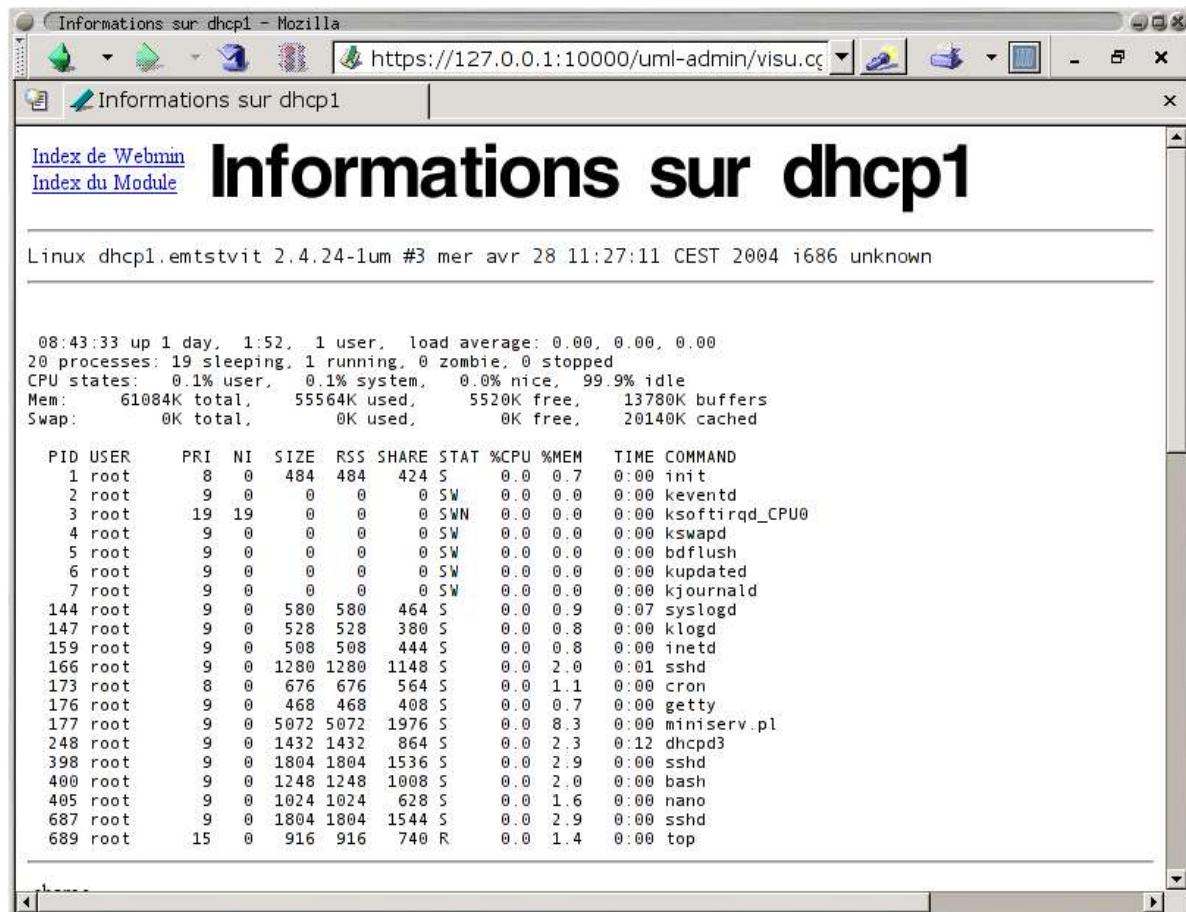


fig 41 - Informations sur une machine UML

● Logs d'une machine virtuelle

```
May 19 06:40:20 dns1 -- MARK --
May 19 07:00:20 dns1 -- MARK --
May 19 07:11:23 dns1 named[947]: Cleaned cache of 4 RRsets
May 19 07:11:23 dns1 named[947]: USAGE 1084943483 1084864283 CPU=6.7u/0.94s CHILDCPU=0u/0s
May 19 07:11:23 dns1 named[947]: NSTATS 1084943483 1084864283 A=9017 SOA=25 PTR=126186 AAAA=2754 SRV=9 AXFR=7
ANY=2
May 19 07:11:23 dns1 named[947]: XSTATS 1084943483 1084864283 RR=1071 RNXD=760 RFwdR=31 RDupR=4 RFail=1
RFErr=3 RErr=0 RAXFR=7 RLame=0 R0pts=0 SSysQ=687 SAns=138566 SFwdQ=347 SDupQ=107 SErr=0 RQ=138000 RIQ=0
RFwdQ=347 RDupQ=29 RTCP=28 SFwdR=31 SFail=0 SErr=0 SNaAns=2003 SNXD=3988 RUQ=0 RURQ=0 RUXFR=0 RUUpd=0
May 19 07:40:20 dns1 -- MARK --
May 19 08:00:20 dns1 -- MARK --
May 19 08:11:23 dns1 named[947]: Cleaned cache of 90 RRsets
May 19 08:11:23 dns1 named[947]: USAGE 1084947083 1084864283 CPU=7.18u/0.94s CHILDCPU=0u/0s
May 19 08:11:23 dns1 named[947]: NSTATS 1084947083 1084864283 A=9720 SOA=27 PTR=131518 AAAA=2832 SRV=9 AXFR=7
ANY=2
May 19 08:11:23 dns1 named[947]: XSTATS 1084947083 1084864283 RR=1135 RNXD=787 RFwdR=38 RDupR=4 RFail=3
RFErr=3 RErr=0 RAXFR=7 RLame=0 R0pts=0 SSysQ=718 SAns=144689 SFwdQ=371 SDupQ=117 SErr=0 RQ=144115 RIQ=0
RFwdQ=371 RDupQ=37 RTCP=28 SFwdR=38 SFail=0 SErr=0 SNaAns=2101 SNXD=4161 RUQ=0 RURQ=0 RUXFR=0 RUUpd=0
May 19 08:25:06 dns1 /USR/SBIN/CRON[970]: (root) CMD (test -e /usr/sbin/anacron || run-parts --report
/etc/cron.daily)
May 19 08:25:35 dns1 syslogd 1.4.1#10: restart...
May 19 08:40:20 dns1 -- MARK --
May 19 09:00:20 dns1 -- MARK --
May 19 09:11:23 dns1 named[947]: Cleaned cache of 40 RRsets
May 19 09:11:23 dns1 named[947]: USAGE 1084950683 1084864283 CPU=7.42u/1.11s CHILDCPU=0u/0s
May 19 09:11:23 dns1 named[947]: NSTATS 1084950683 1084864283 A=10673 SOA=27 PTR=137157 AAAA=2952 SRV=9 AXFR=7
ANY=2
May 19 09:11:23 dns1 named[947]: XSTATS 1084950683 1084864283 RR=1157 RNXD=804 RFwdR=38 RDupR=4 RFail=3
RFErr=3 RErr=0 RAXFR=7 RLame=0 R0pts=0 SSysQ=732 SAns=151411 SFwdQ=379 SDupQ=117 SErr=0 RQ=150827 RIQ=0
RFwdQ=379 RDupQ=37 RTCP=28 SFwdR=38 SFail=0 SErr=0 SNaAns=2158 SNXD=4376 RUQ=0 RURQ=0 RUXFR=0 RUUpd=0
May 19 09:40:20 dns1 -- MARK --
May 19 10:00:20 dns1 -- MARK --
May 19 10:11:23 dns1 named[947]: Cleaned cache of 87 RRsets
May 19 10:11:23 dns1 named[947]: USAGE 1084954283 1084864283 CPU=8.07u/1.13s CHILDCPU=0u/0s
May 19 10:11:23 dns1 named[947]: NSTATS 1084954283 1084864283 A=11859 SOA=27 PTR=143209 AAAA=3298 SRV=14
AXFR=7 ANY=2
May 19 10:11:23 dns1 named[947]: XSTATS 1084954283 1084864283 RR=1587 RNXD=1097 RFwdR=58 RDupR=4 RFail=17
RFErr=3 RErr=0 RAXFR=7 RLame=0 R0pts=0 SSysQ=1057 SAns=159257 SFwdQ=452 SDupQ=185 SErr=0 RQ=158416 RIQ=0
RFwdQ=452 RDupQ=55 RTCP=34 SFwdR=58 SFail=0 SErr=0 SNaAns=2421 SNXD=4847 RUQ=0 RURQ=0 RUXFR=0 RUUpd=0
May 19 10:40:20 dns1 -- MARK --
```

[Retourner à l'index](#) | [Retourner à Console TTYT](#)

fig 42 - Log d'une machine UML

## 19. MAINTENANCE LTSP

Ce guide décrit la méthode utilisée pour le démarrage des clients légers, ainsi qu'un introduction à toutes les erreurs et les problèmes qui peuvent être rencontrés pendant ce démarrage, et les moyens de les corriger.

### 19.1. DÉMARRAGE DE LA MACHINE - CÂBLAGE

Quand le client léger est allumé, la première opération réalisée est de vérifier le matériel.

#### 19.1.1. PROBLÈME 1

Le message suivant peut apparaître:

```
Intel (R) Boot Agent Version 4.0.14
PXE-E61: Media test failure, check câble
PXE-MOF: Exiting Intel PXE ROM
DISK BOOT FAILURE, INSERT SYSTEM DISK AND PRESS ENTER
```

Il s'agit d'un problème matériel de connexion switch et/ou câble. Pour le résoudre:

- Vérifier le branchement ou le fonctionnement de la connectique réseau.
- Utiliser un switch en état de fonctionnement.

### 19.2. OBTENTION DES PARAMÈTRES RÉSEAU - DHCP

Si l'environnement réseau semble sain, la machine va demander une adresse IP, ainsi que l'emplacement réseau de l'image de son système d'exploitation.

#### 19.2.1. PROBLÈME 1

Si la machine n'a pas pu contacter le service distribuant les adresses réseaux (DHCP) - ou être contactée - le message d'erreur suivant apparaît:

```
PXE-E51: No DHCP or proxyDHCP offers were received
PXE-MOF: Exiting Intel PXE ROM
```

**DISK BOOT FAILURE, INSERT SYSTEM DISK AND PRESS ENTER**

C'est probablement un problème de DHCP:

- Vérifier les câbles.
- Vérifier que le **serveur DHCP** est en fonction.
- Vérifier que le **serveur DHCP** est en fonction.
- Vérifier la configuration de DHCP: `dhcpd.conf` est peut être incomplet (l'entrée avec l'adresse **MAC** du client n'est pas présente), voir défectueux. Pour cela, consulter les messages du service DHCP:
  - si les logs ne contiennent pas un message comme « **DHCPDISCOVER from <adresse-mac-du-client> via 10.25.0.2** »: le paquet n'est pas arrivé au service DHCP. Vérifier le réseau entre la station et le service (incluement les switches).
  - si les logs contiennent le message d'erreur « **DHCPDISCOVER from 00:08:83:a5:26:80 via 10.25.0.2: network 10.25.0/16: no free leases** », c'est qu'il manque une entrée correspondant au client léger.

À titre informatif, voici comment une requête doit apparaître dans les logs:

```
DHCPDISCOVER from 00:04:00:4b:58:34 via 10.25.0.2
DHCPoffer on 10.25.2.4 to 00:04:00:4b:58:34 via 10.25.0.2
DHCPREQUEST for 10.25.3.10 from 00:0c:f1:6f:9c:f6 via eth0
DHCPACK on 10.25.3.10 to 00:0c:f1:6f:9c:f6 via eth0
```

Si les symptômes persistent, c'est que la station n'est pas brassée sur le bon réseau. Vérifier qu'elle est branchée sur le switch du réseau auquel elle appartient.

### 19.2.2. PROBLÈME 2

Si le message d'erreur suivant apparaît:

**PXE-E74: Bad or missing PXE menu and/or prompt information**

c'est que l'entrée **vendor-encapsulated-options** du fichier `dhcpd.conf` est défectueuse. Elle doit contenir exactement (sans retour à la ligne):

```
option vendor-encapsulated-options
09:0f:80:00:0c:4e:65:74:77:6f:72:6b:20:62:6f:6f:74:0a:07:00:50
:72:6f:6d:70:74:06:01:02:08:03:80:00:00:47:04:80:00:00:ff;
```

### PROBLÈME 3

Si le message suivant apparaît:

```
PXE-T01: File not found
```

l'erreur vient sans doute du fichier **dhcpd.conf**. Il doit contenir une entré comme celle-ci:

```
filename "/tftpboot/pxelinux.bin";
```

### 19.2.3. PROBLÈME 4

Si vous voyez le message suivant:

```
ERROR ! No root-path. Check your DHCP configuration, to make
sure
that the 'option root-path' is specified
Kernel panic: Attempt to kill init!
```

l'erreur vient sans doute du fichier **dhcpd.conf**. Il doit contenir une entré comme celle-ci:

```
option root-path "192.168.3.1:/home/ltsp/i386";
```

## 19.3. RÉCUPÉRATION DE L'IMAGE DE BOOT - TFTP

Quand le client léger a récupéré ses paramètres réseau, il va charger son système d'exploitation en interrogeant un serveur tftp.

### 19.3.1. PROBLÈME 1

Si le message d'erreur suivant apparaît:

```
PXE-E32 : TFTP open timeout
```

C'est probablement une erreur de configuration du service tftp:

- vérifiez que le fichier **/etc/inetd.conf** contient la ligne suivante

```
tftp    dgram    udp      wait    root    /usr/sbin/in.tftpd  /
tftpboot/revoboot
```

- Vérifiez que le fichier `/home/ltsp/pixelinux.0` existe et a une taille non nulle.

### **19.3.2. PROBLÈME 2**

Le message suivant:

```
PXE-E3B: TFTP Error - File Not Found
```

provient probablement du fait que le fichier indiqué dans `dhcpd.conf` (directive `filename`) n'existe pas.

## **19.4. MONTAGE DU SYSTÈME DE FICHIER - NFS**

Quand le client a chargé son système d'exploitation, il monte le partage NFS sur lequel se trouve sa partition racine (partage NFS).

### **19.4.1. PROBLÈME 1**

Le problème le plus courant est que le serveur NFS soit mal configuré:

```
Root-NFS: Server returned error -13 while mounting /  
tftpboot/lts/ltsroot  
VFS: Unable to mount root fs via NFS, trying floppy.  
kmod: failed to exec /sbin/modprobe -s -k block-major-2, errno  
= 2  
VFS: Cannot open root device "nfs" or 02:00  
Please append a correct "root=" boot option  
Kernel panic: VFS: Unable to mount root fs on 02:0
```

C'est le signe qu'il y a vraisemblablement un problème dans `/etc/exports`, qui est le fichier de configuration de NFS. Ce fichier doit impérativement contenir la ligne suivante:

```
/home *(rw,no_root_squash)
```

## **19.5. LANCEMENT DE LA SESSION GRAPHIQUE - XFREE86**

La dernière étape à franchir est le démarrage de l'interface graphique. Les problèmes les plus souvent rencontrés touchent aux périphériques.

### **19.5.1. PROBLÈME 1**

Certaines machines possèdent une carte graphique non standard:

```
Error:  
Auto probe of the video card failed !  
You need to specify the proper X server in lts.conf  
Press <enter> to continue
```

Il suffit d'ajouter une entrée spécifique à la machine dans le fichier de configuration (dans /home/ltsp/i386/etc/lts.conf). Par exemple:

```
[ltsp34]  
XSERVER = vesa
```

### **19.5.2. PROBLÈME 2**

Certaines machine possèdent des souris PS/2:

```
(EE) xf86OpenSerial : Cannot open device /dev/input/mice  
No such device or address.  
(EE) Mouse0: cannot open input device  
(EE) PreInit failed for input device "Mouse0"  
(WW) No core pointer registered  
No core pointer  
Fatal server error:  
failed to initialize core devices
```

Il suffit d'ajouter une entrée spécifique à la machine dans le fichier de configuration (dans /home/ltsp/i386/etc/lts.conf). Par exemple:

```
[ltsp34]  
X_MOUSE_DEVICE = "/dev/psaux"
```

## 20. MAINTENANCE DE SERVEURS

Ce document se veut être un document synthétique qui vous permettra de détecter et résoudre les problèmes les plus courants d'un serveur Linux.

### 20.1. ESPACE DISQUE DISPONIBLE

Le premier réflexe en cas de problème est de vérifier l'espace disque disponible, à l'aide de la commande df:

```
lna:~# df -h
Système de fichiers Tail. Util. Disp. Uti% Monté sur
/dev/sda1      1.4G  1.3G  117M  92% /
/dev/lvm1/hd1   6.6G  3.9G  2.7G  59% /tftpboot
fichier:/home        121G    59G    62G    49% /
amd/fichier/root/home
```

On peut définir deux niveaux d'alerte:

- quand **l'espace utilisé** (colonne 5) est supérieur à 95%, certains problèmes peuvent toucher des utilisateurs normaux.
- quand **l'espace disponible** (colonne 4) devient nul, la machine (ou certains de ses services) peuvent se bloquer.

En cas de remplissage d'une partition, la seule mesure à prendre est de faire de la place. Le répertoire **/var/log** contient des fichiers de journaux, données non vitales, ce sont donc les premières cible d'une épuration. Éliminer de préférence les plus vieux fichiers. Dans le même esprit, le répertoire **/var/cache** est un bon candidat, ainsi qu'en dernier recours le répertoire **/usr/src**.

L'utilitaire **du** est particulièrement efficace pour juger de la taille de certains fichiers:

```
lna:~# du /var/* -sch
924k    /var/backups
21M     /var/cache
52M     /var/lib
4.0k    /var/local
4.0k    /var/lock
73M    /var/log
548k   /var/mail
4.0k   /var/opt
316k   /var/run
```

22M	/var/spool
12k	/var/state
18M	/var/tmp
1.6M	/var/www
188M	total

Si ce problème d'espace disque revient souvent, il faut probablement envisager de passer à un espace de stockage plus important, ou faire le ménage dans les applicatifs installés.

## 20.2. MÉMOIRE DISPONIBLE

Une autre cause de problème d'instabilité est le manque de mémoire vive. `free` permet rapidement juger de la mémoire restante:

lna:~# free -mt					
	total	used	free	shared	buffers
<b>cached</b>					
Mem:	250	243	6	0	32
142					
-/+ buffers/cache:		68	182		
Swap:	258	54	204		
Total:	509	298	210		

Sous Linux la mémoire est toujours complètement utilisée, comme on le voit sur la première ligne (6 Mo libres). Ceci est dû au fait qu'un système de cache (ici 142 Mo) et de tampons (ici 32 Mo) est mis en place pour accélérer les accès aux autres périphériques. En cas de besoin, cette mémoire est immédiatement disponible, on peut donc considérer que cette mémoire est en fait libre. Le calcul visant à ajouter la mémoire pouvant être disponible à la mémoire vraiment disponible est fait à la ligne 2 (ici, on voit que 182 Mo sont disponibles).

Un autre mécanisme est utilisé sous Linux: le swap. Cet espace, stocké sur disque dur, est utilisé pour augmenter artificiellement la mémoire disponible, et permet à un serveur de continuer de fonctionner même quand la mémoire vive disponible devient nulle (ici ligne 4: 204 Mo sont disponibles).

Concrètement, on distingue deux niveaux d'alerte:

- quand la mémoire vive disponible devient nulle mais que qu'il reste de la place dans le swap (ligne 2: free = 0 et ligne 4: free <> 0), le serveur commencera à ralentir. la commande `top` permet de voir quel processus prend le plus de mémoire (processus qu'il faudra éventuellement redémarrer)
- quand le swap est également rempli (ligne 4: free = 0), le serveur se bloquera probablement dans les minutes qui suivent. le plus pertinent est probablement de tenter d'éliminer le plus gros processus.

À noter: quand une machine semble avoir de la mémoire vive disponible (ligne 2: free <> 0) mais plus de swap (ligne 3: free = 0), c'est probablement que le serveur a eu à un moment un problème de mémoire disponible.

Si ce problème de mémoire revient souvent, il faut probablement envisager d'augmenter la mémoire de la machine concernée.

## 20.3. CHARGE ET OCCUPATION PROCESSEUR

Concrètement, la donnée représentative de la bonne santé d'un serveur est sa charge, affichable à l'aide de l'outil **uptime**:

```
lna:~# uptime
 12:06:20 up 11 days, 19:58, 8 users, load average: 0.00,
 0.01, 0.00
```

Les trois derniers nombres représentent la charge moyenne sur la dernière minute, les cinq dernières et les dix dernières.

Un serveur efficace doit avoir une charge moyenne inférieur à 1. Pendant un pic d'utilisation, cette charge moyenne peut monter à 2, voir 3. Un serveur dépassant 5 présente probablement un dysfonctionnement (mémoire, espace disque ?).

## 20.4. FICHIERS VERROUS (LOCKS)

Quand une application se plaint de ne pas pouvoir à cause d'un verrou posé sur un fichier - ce qui arrive généralement après un arrêt brutal de l'application - il suffit de supprimer le verrou, représenté par un autre fichier, pour démarrer correctement.

### *APPLICATIONS COTÉ UTILISATEUR*

En règle générale, les applications souhaitant marquer le fichier /mon/fichier comme verrouillé créent un fichier vide /mon/fichier.lock.

Ce n'est pas toujours le cas:

- **mozilla** crée un fichier .lock quelque part dans le répertoire ~/.mozilla . Pour le trouver, il faut utiliser la commande **find** (en étant loggué avec le compte de l'utilisateur) :

```
bash-2.05b$ find ~/.mozilla -name "*lock*"
.mozilla/default/46j2zfa1.slt/lock
```

- **OpenOffice**: méthode identique à mozilla, ainsi que les fichiers **OSL\_PIPE\*** du répertoire /tmp.

- En ce qui concerne les **services**, le premier endroit où rechercher ce fichier verrou est **/var/lock**

## 20.5. DÉPANNAGE D'UN SERVEUR AU COMPORTEMENT DOUTEUX

---

Les opérations à réaliser sur un serveur qui semble avoir un problème de fonctionnement - ralentissement en général - sont, dans l'ordre:

1. **vérifier l'espace disque disponible.** S'il est très bas, il faut impérativement partir à la chasse aux gros fichiers. La cible principale de cette chasse est le répertoire **/tmp** (attention de ne rien supprimer de vital), suivi des répertoires **/var/log** et **/var/cache** pour un contrôle visuel immédiat. Si cela ne suffit pas, une commande **find** correctement placée peut permettre de régler le problème également.
2. **vérifier la mémoire disponible.** Un programme peut posséder des fuites, ce qui n'est pas fréquent mais peut arriver. S'il s'agit d'un programme rattaché à un service, un simple démarrage du service suffira. S'il s'agit d'un programme plus critique d'un point de vue utilisateur (OpenOffice par exemple), le tuer est à envisager également: un processus trop gourmand en mémoire risque de fragiliser la machine, autant limiter les dégâts.
3. **lancer l'outil top.** Il permet de connaître rapidement les processus occupant le processeur. Les mêmes précautions d'usage que précédemment s'appliquent également. S'il apparaît que la charge est élevée sans qu'un processus puisse être identifier, le problème viens probablement du système de fichiers: remontez les systèmes NFS.
4. **vérifier les paramètres réseaux.** En particulier l'état des interfaces réseaux (**ifconfig**), la communication avec les serveurs aux alentours (**ping**), le nom de machine (**hostname** et **host**).
5. **consultez les logs.** Beaucoup d'informations y sont inscrites. Si vous ne savez pas quel fichier consulter, alors consultez **/var/log/syslog**.
6. **pensez au matériel.** Un serveur Linux ne devient pas instable sans raison. Des « kernoops » sont signe d'une machine mal refroidie ou de mémoire défectueuse. Des gels brutaux sont signe de processeur ou carte mère défaillante. Des liaisons réseau problématiques sont signe d'un câble réseau vieillissant ...

## 21. ANNEXES

---

## 21.1. CORRECTION TP1 - LIGNE DE COMMANDE

1. Allez dans votre HOME

```
cd ~
```

2. Affichez le nom du répertoire courant

```
pwd
```

3. Créez un répertoire TP

```
mkdir TP
```

4. Allez dans le répertoire créé

```
cd TP
```

5. Affichez le contenu du répertoire courant

```
ls
```

6. Décompressez l'archive du tp 1 dans le répertoire courant

```
tar zxf /chemin/de/1/archive
```

7. Allez dans le répertoire lsg\_cl/long-noms

```
cd lsg_cl/long-noms
```

8. Afficher le nombre de fichiers du répertoire courant

```
ls | wc -l
```

9. Afficher le nombre de fichiers finissant par "89"

```
ls *89 | wc -l
```

10. Déplacez les fichiers finissant par "977" dans ~/TP/lsg\_cl/long-noms.tmp

```
mkdir ../long-noms.tmp; mv *977 ../long-noms.tmp
```

11. Listez le contenu de ce dernier répertoire

```
ls ..../long-noms.tmp
```

12. Supprimez ce dernier répertoire

```
rm -fr ..../long-noms.tmp
```

13. Copiez le répertoire ~/TP/lsg\_cl/long-noms vers ~/TP/lsg\_cl/long-noms.tmp

```
cp -a ..../long-noms ..../long-noms.tmp
```

14. Allez dans ce répertoire

```
cd ..../long-noms.tmp
```

15. Affichez la taille de ce répertoire

```
du
```

16. Supprimez tous les fichiers commençant par « je\_suis\_un\_fichier »

```
find -name "je_suis_un_fichier*" -exec rm {} \;
```

17. Affichez la taille de ce répertoire

```
du
```

18. Allez dans le répertoire ~/TP/lsg\_cl/invalidé

```
cd ~/TP/lsg_cl/invalidé
```

19. Supprimez le fichier « doit etre supprime »

```
rm "doit etre supprime"
```

20. Supprimez le fichier « -h »

```
find -name "-h" -exec rm {} \;
```

21. Allez dans le répertoire ~/TP

```
cd ..
```

22. Trouvez quel fichier du répertoire recherche contient le terme «gagne»

```
grep gagne recherche/*
```

23. Affichez la date

```
date
```

24. Concaténez la sortie de la commande date vers le fichier « date-courante »

```
date > date-courante
```

25. Ajoutez la sortie de la commande cal vers le fichier « date-courante »

```
cal >> date-courante
```

26. Affichez le contenu du fichier « date-courante »

```
cat date-courante
```

27. Affichez les premières et dernières lignes du fichier « date-courante »

```
head -1 date-courante; tail -1 date-courante
```

28. Afficher le contenu trié du fichier « atrier.txt »

```
sort -n atrier.txt
```

29. Affichez le contenu trié du fichier « atrier.txt », uniquement les lignes contenant le mot "LIGNE"

```
sort -n atrier.txt | grep LIGNE
```

30. Enregistrez le contenu trié du fichier « atrier.txt », uniquement les lignes contenant le mot "LIGNE", dans le fichier « tri.txt »

```
sort -n atrier.txt | grep LIGNE > tri.txt
```

31. Affichez avec le pager le contenu du fichier caché du répertoire « invalides »

```
ls -a invalides; less invalides/.fichier-a-trouver
```

32. Allez dans le répertoire parent

```
cd ..
```

33. Comptez le répertoire lsg\_cl dans l'archive « lsg\_cl.tar.gz »

```
tar zc lsg_cl > lsg_cl.tar.gz
```

## 21.2. CORRECTION TP2 - Outils Avancés

1. Lancez **screen**

```
screen
```

2. Lancez **top**

```
top
```

3. Triez l'affichage par occupation mémoire

```
M
```

4. Créez une nouvelle console **screen**

```
<ctrl><a><c>
```

5. Lancez **mc**

```
mc
```

6. Revenez sur la première console

```
<ctrl><a><p>
```

7. Trier par **age**

```
A
```

8. Créez une nouvelle console **screen**

```
<ctrl><a><c>
```

9. Afficher les tâches en cours avec le **pageur**

```
ps aux | less
```

10. Depuis **top**, tuer le pageur (signal 9)

```
<ctrl><a><n> + k <pid du pageur>
```

11. Exploration de l'arborescence à l'aide de mc.

## 21.3. CORRECTION TP3 - RÉSEAU

1. Loguez-vous sur **192.168.3.2**

```
ssh <user>@192.168.3.2
```

2. Déterminez son nom

```
hostname
```

3. Déterminez à quel réseau appartient la machine

```
ifconfig
```

4. Listez les machines sur les réseaux visibles

```
ping <broadcast>
```

5. Déterminez les noms des machines sur tous les réseaux visibles

```
host <adresse-ip>
```

6. Affichez les routes de la machine

```
route
```

7. Listez les passerelles autours de la machine

```
route | grep UG
```

8. Trouvez par quelle machine aller sur internet

```
traceroute www.google.fr
```

9. Affichez quels services écoutent sur la machine

```
netstat -lp
```

10. Affichez les machines connectées en ssh sur Ina

```
12.netstat -p | grep ssh
```

## Index des figures

- fig 1 - vue générale 36  
fig 2 - édition d'un fichier 36  
fig 3 - visualisation de fichiers 37  
fig 4 - copie de fichier 37  
fig 5 - Écran de login à Webmin 56  
fig 6 - Page d'accueil de webmin 57  
fig 7 - Accès aux interfaces webmin de différents serveurs 58  
fig 8 - Interface webmin de dhcp1 depuis l'interface webmin principale 59  
fig 9 - Gestion du service dhcp 62  
fig 10 - détail de l'interface de gestion du dhcp 63  
fig 11 - gestion des sous-réseaux dhcp 64  
fig 12 - Ajout manuel d'un hôte dans le dhcp 65  
fig 13 - icone d'accès à l'interface de gestion du DNS sous webmin 69  
fig 14 - Interface principale de gestion du serveur DNS 70  
fig 15 - Édition d'une zone inverse 71  
fig 16 - Liste des enregistrements d'une zone inverse 72  
fig 17 - Édition des enregistrements inverses 73  
fig 18 - Édition d'une zone directe 74  
fig 19 - Ajout d'un enregistrement en zone directe 75  
fig 20 - Édition d'une adresse directe 76  
fig 21 - Interface d'administration du service ntp sous webmin 80  
fig 22 - Détail de l'interface gestion du NTP de webmin 81  
fig 23 - Liste des serveurs NTP contactés 82  
fig 24 - Vérification de la synchronisation 83  
fig 25 - Module webmin pour la gestion du service LDAP 84  
fig 26 - Accès aux fonctions principales de gestion 85  
fig 27 - Interface de gestion des utilisateurs 86  
fig 28 - Paramètres généraux d'un utilisateur 87  
fig 29 - Groupes d'appartenance d'un utilisateur 88  
fig 30 - Profil d'un utilisateur 89  
fig 31 - Paramètres samba d'un utilisateur 90  
fig 32 - Interface de gestion des groupes 91  
fig 33 - Modification d'un groupe 92  
fig 34 - Interface de gestion des types de compte 93  
fig 35 - Interface d'administration de User Mode Linux 96  
fig 36 - Console d'administration UML 97  
fig 37 - Indicateur graphique d'état d'une machine UML 98  
fig 38 - Configuration du module d'administration UML 99

- fig 39 - Page de maintenance d'un UML 100**
- fig 40 - Démarrage d'une machine UML 101**
- fig 41 - Informations sur une machine UML 102**
- fig 42 - Log d'une machine UML 103**