Guide d'administration serveur

Mandriva Linux 2006

http://www.mandriva.com

Guide d'administration serveurMandriva Linux 2006
Publié septembre 2005

par Camille Bégnis, Fabian Mandelbaum, Christian Roy, Fred Lepied, Nicolas Planel, Daouda Lo, François Pons, John Rye, Pascal Rigaux, Damien Chaumette, Till Kamppeter, Florent Villard, Luca Berra, Florin Grad, Frédéric Crozat, Stew Benedict, Guillaume Cottenceau, Thierry Vignaud, Jean-Michel Dault., et Lunas Moon

Notice légale

Outils utilisés dans la conception de ce manuel

Ce manuel est écrit et mis à jour par NeoDoc (`http://www.neodoc.biz`). Les traductions sont assurées par NeoDoc, Mandriva et d'autres traducteurs.
Ce manuel a été rédigé avec la grammaire XML DocBook. Pour gérer l'ensemble des fichiers, le système collaboratif de création de contenu Borges (`http://sourceforge.net/projects/borges-dms/`) a été utilisé. Les fichiers source XML ont été transformés avec xsltproc et `jadetex` (pour la version électronique), grâce aux feuilles de style personnalisées réalisées par Norman Walsh. Les captures d'écran ont été prises avec `xwd` et GIMP, puis converties avec `convert` (issu du paquetage ImageMagick). Tous ces logiciels sont libres et disponibles sur votre distribution Mandriva Linux.

Table des matières

Liste des tableaux

Préface

1. À propos de Mandriva Linux

Mandriva Linux est une distribution GNU/Linux développée par Mandriva S.A. La société Mandriva est née sur Internet en 1998 ; son ambition première demeure de fournir un système GNU/Linux convivial et facile à utiliser. Les deux piliers de Mandriva sont le logiciel libre et le travail coopératif.

Le 7 avril 2005, la société Mandrakesoft a modifié son nom d'entreprise pour refléter sa fusion avec Conectiva, leader GNU/Linux du Brésil. Par conséquent, le produit phare Mandrakelinux a lui aussi changé de nom pour Mandriva Linux.

1.1. Communiquer avec la communauté Mandriva Linux

Nous présentons ci-dessous plusieurs liens Internet pointant vers de nombreuses ressources liées à Mandriva Linux. Si vous souhaitez en savoir plus sur la société Mandriva, consultez notre site Web (`http://www.mandriva.com/`). Vous pouvez aussi visiter le site dédié à la distribution Mandriva Linux (`http://www.mandrivalinux.com/`) et à tous ses dérivés.

Mandriva Expert (`http://www.mandrivaexpert.com/`) est la plate-forme d'aide en ligne de Mandriva. Elle propose une nouvelle façon de partager les savoirs, basée sur la confiance et le plaisir de récompenser son prochain pour son aide.

Vous êtes également invité à participer aux nombreuses listes de diffusion (`http://www.mandrivalinux.com/fr/flists.php3`), où la communauté Mandriva Linux déploie tout son enthousiasme et sa vivacité.

Enfin, n'oubliez pas de vous connecter sur la page sécurité (`http://www.mandriva.com/security/`) (en anglais). Ce site rassemble tout ce qui traite de la sécurité des distributions Mandriva Linux. Vous y trouverez notamment des avertissements de bogues et de sécurité, ainsi que des procédures de mise à jour du noyau, les différentes listes de diffusion concernant la sécurité auxquelles vous pouvez souscrire et Mandriva Online (`https://online.mandriva.com/`). Bref, voilà un site incontournable pour tout administrateur système, ou tout utilisateur soucieux de sécurité.

1.2. Rejoignez le Club

Mandriva propose une large palette d'avantages à travers son Mandriva Club (`http://club.mandriva.com`) :

- télécharger des logiciels commerciaux, qui ne sont normalement disponibles que dans les packs commerciaux, tels que des pilotes logiciel, des applications commerciales, des gratuiciels (*freeware*) et des versions démo ;
- voter et proposer de nouveaux logiciels à travers un système de vote RPM que des bénévoles maintiennent ;
- accéder à plus de 50 000 paquetages RPM pour toutes les distributions Mandriva Linux ;
- obtenir des remises sur des produits et des services sur le Mandriva Store (`http://store.mandriva.com`) ;
- accéder à une liste de miroirs exclusive pour les membres du Club ;
- lire des forums et articles multilingues.
- accéder à la Base de connaissances (`http://club.mandriva.com/xwiki/bin/view/KB/`) *Knowledge Base* de Mandriva, un site basé sur le travail collaboratif « wiki » qui traite de nombreux sujets tels que l'administration, la connectivité, la résolution de problèmes, et plus encore ;
- discuter avec les développeurs de Mandriva Linux sur le Club Chat (`https://www.mandrivaclub.com/user.php?op=clubchat`) ;
- approfondir ses connaissances de GNU/Linux grâce à Mandriva e-training (`http://etraining.mandriva.com/`).

En finançant Mandriva par le biais du Mandriva Club, vous améliorerez directement la distribution Mandriva Linux et vous nous permettrez de proposer le meilleur poste de travail GNU/Linux possible à nos utilisateurs.

1.3. S'abonner à Mandriva Online

Afin d'éviter la présence de bogues ou de failles de sécurité, Mandriva vous propose un moyen commode permettant de mettre à jour votre système automatiquement. Visitez le site Mandriva Online (`https://online.mandriva.com//`) pour en savoir plus sur ce service.

1.4. Acquérir des produits Mandriva

Vous pouvez acheter des produits Mandriva en ligne sur le Mandriva Store (`http://store.mandriva.com`). Vous y trouverez non seulement des logiciels Mandriva Linux, des systèmes d'exploitation et des CD de démarrage « live » (comme Move), mais aussi des offres spéciales d'abonnement, de l'assistance, des logiciels tiers et des licences, des manuels et des livres GNU/Linux, ainsi que d'autres gadgets Mandriva.

1.5. Contribuer à Mandriva Linux

Quels que soient vos talents, vous êtes encouragé à participer à l'une des nombreuses tâches requises à la construction du système Mandriva Linux :

- **Paquetages.** Un système GNU/Linux est principalement constitué de programmes rassemblés depuis Internet. Ils doivent être mis en forme de façon à ce qu'ils puissent fonctionner ensemble, si tout se passe bien ;
- **Programmation.** Une foule de projets est directement développée par Mandriva : trouvez celui qui vous intéresse le plus et proposez votre aide au développeur principal ;
- **Internationalisation.** vous pouvez nous aider à traduire des pages de nos sites Web, des programmes et leur documentation respective.

Consultez la page des projets de développement (`http://qa.mandriva.com/`) pour en savoir plus sur les différentes façons de contribuer à l'évolution de Mandriva Linux.

2. À propos de ce guide d'administration serveur

Ce *Guide d'administration serveur* a été écrit afin de transmettre des connaissances générales au sujet de la configuration des services les plus utilisés. À travers des outils graphiques, nous vous montrerons comment régler vos serveurs, activer les services nécessaires et sécuriser votre environnement réseau. Les lignes qui suivent présentent les différentes parties de ce manuel.

La première partie (*Assitants de configuration pour services usuels*) abordera les différents services que vous pouvez configurer avec le Centre de contrôle Mandriva Linux (*Les assistants de configuration serveur*, page 9). Après avoir lu ce chapitre, vous devriez être en mesure de configurer des services tels que DHCP, DNS ou Postfix.

Ensuite, *Configurer des clients de passerelle*, page 25, couvre la configuration de clients en mascarade avec votre système Mandriva Linux, ce qui permet de travailler dans un réseau comprenant plusieurs plates-formes telles que Microsoft DOS, Windows® 9x, Windows NT® et Windows® XP. Pour que ce chapitre vous soit utile, votre LAN doit être bien configuré puisque nous nous concentrons sur la passerelle.

La deuxième partie (*Configuration approfondie des services usuels*) explore les différents modules de Webmin qui vous aideront à configurer les services les plus courants.

Dans la dernière partie (*Théorie appliquée*), nous discutons de trois sujets utiles en tant que références : un peu de théorie sur la sécurité et les réseaux pour commencer, puis un chapitre très important détaillant les moyens de prévention des désastres, et comment se sortir de situations délicates.

3. Note des traducteurs

Dans l'esprit de la communauté du libre (*open source*), nous accueillons les collaborations à bras ouverts ! La mise à jour du fonds de documentation sur Mandriva Linux est toute une tâche, et vous pourriez nous aider de plusieurs façons. En fait, l'équipe de documentation est toujours à la recherche de bénévoles talentueux pour accomplir les tâches suivantes :

- écriture et mise à jour ;
- traduction ;
- relecture linguistique ;
- programmation XML/XSLT.

Si vous disposez de beaucoup de temps libre, vous pouvez écrire ou mettre à jour un chapitre entier ; si vous parlez une langue étrangère, vous pouvez nous aider à traduire nos manuels ; si vous avez des idées pour en améliorer le contenu, faites-le nous savoir ; si vous possédez des compétences en programmation et que vous désirez aider au développement du système de production collaboratif de contenu Borges (`http://sourceforge.net/projects/borges-dms`), rejoignez-nous ! Et n'hésitez pas à nous faire part de toute erreur que vous pourriez rencontrer, ainsi nous pourrons les corriger .

Pour toute information sur le projet de documentation de Mandriva Linux, contactez-nous (`mailto:documentation@mandriva.com`) ou visitez notre site Web (`http://qa.mandriva.com/twiki/bin/view/Main/DocumentationTask/`) (en anglais seulement).

Veuillez noter que depuis le mois de juin 2004, la documentation de Mandriva Linux ainsi que le développement de Borges sont gérés par NeoDoc (`http://www.neodoc.biz`).

4. Conventions utilisées dans ce manuel

4.1. Conventions typographiques

Afin d'accentuer clairement certains mots ou groupes de mots, nous avons utilisé certains attributs typographiques. Le tableau suivant en donne la signification symbolique :

Exemple formaté	Signification
inode	Signale un terme technique.
`ls -lta`	Type utilisé pour une commande et ses arguments (voir la section *Synopsis d'une commande*, page 4).
`un_fichier`	Type utilisé pour les noms de fichier. Il peut aussi représenter un nom de paquetage RPM.
ls(1)	Référence à une page de manuel (aussi appelée page de `man`). Pour consulter la page correspondante, tapez `man 1 ls` dans un *shell* (ou ligne de commande).
`$ ls *.pid`	Ce style est utilisé pour une copie d'écran texte de ce que vous êtes censé voir à l'écran comme une interaction utilisateur-ordinateur ou le code source d'un programme, etc.
`localhost`	Données littérales qui ne correspondent généralement pas à une des catégories précédemment définies : un mot clé tiré d'un fichier de configuration, par exemple.
OpenOffice.org	Désigne le nom des applications. Selon le contexte, une application et la commande qui la représente peuvent être formatées différemment. Par exemple, la plupart des noms de commande s'écrivent en minuscule, alors que les noms d'application commencent par une majuscule.

Exemple formaté	Signification
Fichier	Entrée de menu ou label des interfaces graphiques. La lettre soulignée, si présente, indique le raccourci clavier, auquel vous pouvez accéder en appuyant sur la touche **Alt** et la lettre soulignée.
Once upon a time...	Citation en langue étrangère.
Attention !	Type réservé pour les mots que nous voulons accentuer. Lisez-les à voix haute.

Cette icône introduit une note. Il s'agit généralement d'une remarque dans le contexte courant, pour donner une information complémentaire.

Cette icône introduit une astuce. Il peut s'agir d'un conseil d'ordre général sur la meilleure façon d'arriver à un but spécifique ou une fonctionnalité intéressante qui peut vous rendre la vie plus facile, comme les raccourcis clavier.

Soyez très attentif lorsque vous rencontrez cette icône. Il s'agit toujours d'informations très importantes sur le sujet en cours de discussion.

4.2. Conventions générales

4.2.1. Synopsis d'une commande

L'exemple ci-dessous présente les symboles que vous rencontrerez lorsque nous décrirons les arguments d'une commande :

```
commande <argument non littéral> [--option={arg1,arg2,arg3} [argument optionnel...]
```

Ces conventions étant standardisées, vous les retrouverez en bien d'autres occasions (dans les pages de `man`, par exemple).

Les signes « < » (inférieur) et « > » (supérieur) indiquent un argument **obligatoire** qui ne doit pas être recopié tel quel mais remplacé par votre texte spécifique. Par exemple : `<fichier>` désigne le nom d'un fichier ; si ce fichier est `toto.txt`, vous devrez taper `toto.txt`, et non `<toto.txt>` ou `<fichier>`.

Les crochets (« [ ] ») indiquent des arguments optionnels que vous déciderez ou non d'inclure dans la ligne de commande.

Les points de suspension (« ... ») signifient qu'un nombre illimité d'arguments peut être inséré à cet endroit.

Les accolades (« { } ») contiennent les arguments autorisés à cet endroit. Il faudra obligatoirement en insérer un à cet endroit précis.

4.2.2. Notations particulières

De temps à autre, il vous sera demandé d'appuyer sur les touches **Ctrl-R**, cela signifie que vous devez maintenir la touche **Ctrl** enfoncée pendant que vous appuyez sur la touche **R**. Il en va de même pour les touches **Alt** et **Shift**.

Nous utilisons des lettres majuscules pour représenter les touches clavier. Ceci n'implique pas que vous deviez les utiliser en majuscule. Toutefois, dans certaines applications, il est possible que le fait de taper **R** ou **r** n'ait pas le même effet. Nous vous le signalerons lorsque ce sera le cas.

De même, à propos des menus, aller sur l'entrée de menu Fichier→Relire la configuration utilisateur (**Ctrl-R**) signifie : cliquez sur le label Fichier du menu (généralement en haut et à gauche de la fenêtre) puis sur le menu

vertical qui apparaît, cliquez sur Relire la configuration utilisateur. De plus, vous pouvez également utiliser la combinaison de touches **Ctrl**-**R** , comme décrit ci-dessus pour arriver au même résultat.

4.2.3. Utilisateurs système génériques

Chaque fois que cela est possible, nous utiliserons deux utilisateurs génériques dans nos exemples :

Reine Pingusa	reine	C'est notre utilisateur par défaut, que nous utilisons dans la plupart des exemples de ce manuel.
Pierre Pingus	pierre	Cet utilisateur peut ensuite être créé par l'administrateur système. Nous l'utilisons quelques fois afin de varier le texte.

Configuration d'un réseau local et des services associés

Cette partie se divise en deux chapitres : le premier détaille les assistants de configuration serveur Mandriva Linux, tandis que le second traite et approfondit la notion de clients en mascarade (*masqueraded clients*).

1. Assistants de configuration serveur

Ce chapitre (*Les assistants de configuration serveur*, page 9) vous aidera à configurer des serveurs tels que DNS (*Domain Name Server*), DHCP (*Dynamic Host Configuration Protocol*), Samba, HTTP, FTP, etc., avec les assistants graphiques de configuration.

Les assistants vous permettent de configurer ces services facilement afin qu'ils soient intégrés de façon transparente dans votre environnement réseau. Si vous désirez approfondir la configuration de ces services, référez-vous aux chapitres Webmin correspondants (Partie II).

2. Clients derrière une passerelle

Nous vous montrerons comment configurer d'autres machines sur un réseau local en utilisant Mandriva Linux avec un mandataire réglé en tant que passerelle (*gateway*) vers le monde extérieur (*Configurer des clients de passerelle*, page 25). L'information contenue dans ce chapitre couvre plusieurs plates-formes et architectures.

Chapitre 1. Les assistants de configuration serveur

1.1. Préface

Les assistants de configuration fournis avec Mandriva Linux sont conçus pour configurer un serveur situé entre votre réseau local et Internet. Ils vous permettent de configurer de manière rapide et efficace les services les plus courants pour un réseau local, ainsi que des services Internet tels que Web ou FTP. Dans ce chapitre, nous supposons que votre réseau est établi tel qu'illustré à la figure 1-1, et que Mandriva Linux est installé sur le serveur. La configuration et l'activation d'une connexion Internet (si vous en avez une) est hors du cadre de ce chapitre.

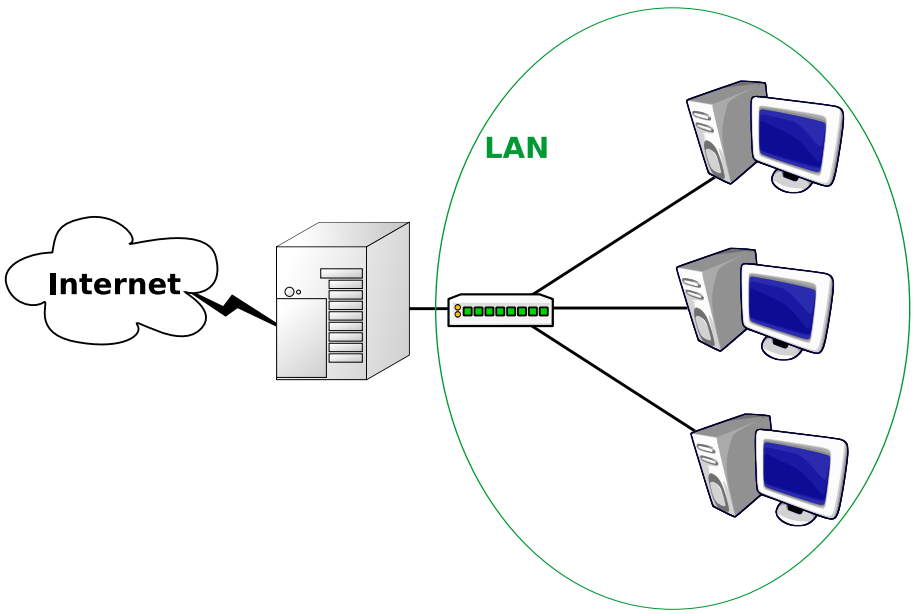


Figure 1-1. Un exemple de réseau interne

Les assistants de configuration serveur sont accessibles depuis le Centre de contrôle Mandriva Linux. Lorsque le paquetage `drakwizard` est installé, une nouvelle catégorie apparaît dans Centre de contrôle Mandriva Linux, et les assistants sont organisés de la manière qui suit :.

Les assistants signalés avec ■ Mode expert uniquement ■ ne sont accessibles que lorsque le mode expert est activé (Options→Mode expert).

Partage de fichiers

- Serveur FTP (voir *Configuration du serveur FTP*, page 15) : configure un serveur FTP et les réseaux d'où il pourra être rejoint.
- Serveur Samba (voir *Configuration de Samba*, page 13) : si le serveur doit agir en tant que serveur de fichiers ou d'impression pour des machines Windows®, cet assistant vous aidera à configurer les fichiers et imprimantes partagées, et le nom du serveur dans le réseau Windows®.
- Serveur Web (voir *Configuration du serveur Web*, page 14) : configure un serveur Web, et les réseaux d'où il pourra être rejoint.
- Un serveur d'installation (*Assistant de serveur d'installation*, page 17) : pour pouvoir lancer des installations de machines par réseau en NFS ou HTTP, et reléguer CDs et DVDs au placard. Mode expert uniquement.

Services réseau

- Serveur DHCP (voir *Configuration du serveur DHCP*, page 10) : votre serveur peut attribuer dynamiquement des adresses IP à de nouvelles machines sur le réseau.
- Un serveur DNS (voir *Configuration du serveur DNS*, page 11) : configuration de la résolution des noms de domaines extérieurs au réseau privé.
- Serveur mandataire (voir *Configuration du serveur mandataire*, page 20) : permet de configurer votre serveur en tant que *proxy*, ce qui accélère la navigation Web et réduit l'utilisation de bande passante.
- Un serveur de temps (voir *Configuration du serveur de temps*, page 22) : votre machine peut aussi donner l'heure aux autres machines en utilisant le protocole NTP (*Network Time Protocol*).

Authentification

- Choix de la méthode d'authentification :: pour choisir la manière dont les utilisateurs locaux sont identifiés : fichiers locaux, LDAP, NIS, Windows Domain. Mode expert uniquement. Mode expert uniquement.
- Un serveur NIS : pour configurer le service *Network Information System*, par exemple pour centraliser l'authentification des utilisateurs.
- Serveur LDAP (*Assistant de configuration LDAP*, page 19) : pour configurer un simple annuaire LDAP à utiliser en tant que mécanisme d'authentification.

Groupware

- Un serveur de forums (voir *Configuration du serveur de forums*, page 20) : vous pouvez faire agir votre serveur en tant que miroir local d'un serveur de forums externe.
- Un serveur de courrier électronique (voir *Configuration du serveur mail Postfix*, page 12) : configuration de votre domaine de courrier pour envoyer et recevoir des courriels de et vers l'extérieur.
- Un serveur *groupware* : cet assistant permet de configurer facilement le serveur Kolab, permettant de partager dans votre entreprise contacts, calendrier, rendez-vous, etc.

Dans ce chapitre, les assistants seront décrits sans ordre préétabli. Notez que les paquetages nécessaires seront automatiquement installés au lancement des assistants.

Note aux utilisateurs expérimentés : les assistants sont limités à la configuration d'un réseau de classe C, et pour chaque service, seule la configuration de base est gérée. Cela devrait suffire dans la plupart des cas, mais si vous voulez une configuration plus personnalisée, vous devrez éditer les fichiers de configuration à la main, ou utiliser un autre outil d'administration tel que Webmin.

1.2. Configuration du serveur DHCP

DHCP signifie *Dynamic Host Configuration Protocol* (protocole de configuration dynamique des hôtes). Il permet aux nouvelles machines se connectant à votre réseau local de se voir attribuer automatiquement tous les paramètres réseau nécessaires, tels que l'adresse IP, les adresses des serveurs de noms et l'adresse de la passerelle.

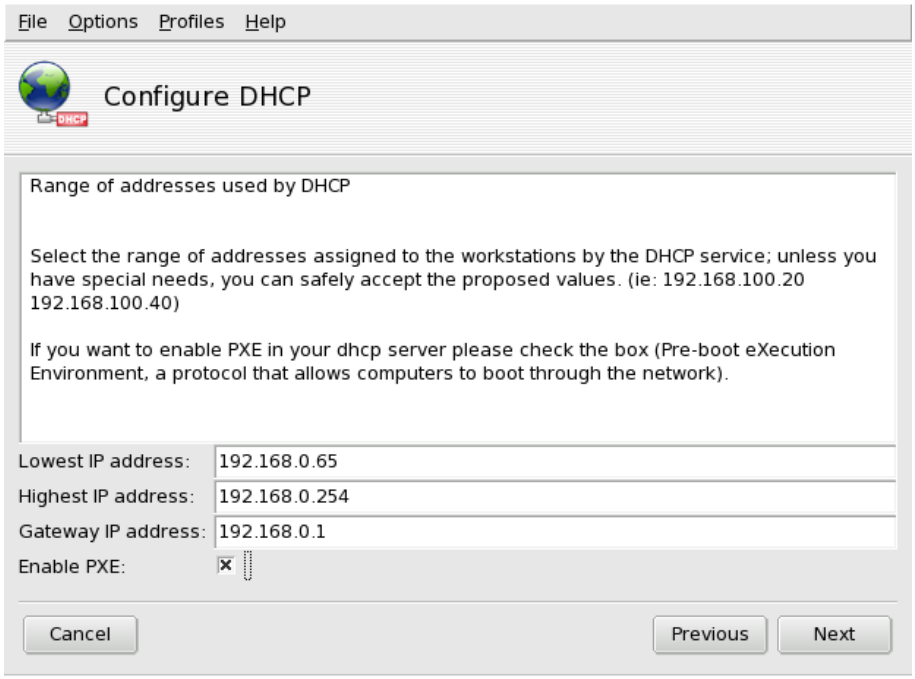


Figure 1-2. Choisir la plage d'adresses disponible depuis votre serveur DHCP

Vous n'avez qu'à spécifier la plage d'adresses[1] que vous voulez rendre disponible par l'entremise du DHCP, comme le montre la figure 1-2. Si votre serveur a plus d'une interface réseau, vous devrez tout d'abord choisir sur laquelle le serveur doit écouter les requêtes DHCP : choisissez l'interface connectée au réseau local. Si vous souhaitez que les machines client puissent accéder à Internet, vous pouvez spécifier ici l'adresse de la passerelle.

Si vous souhaitez utiliser votre serveur comme serveur de démarrage PXE pour le réseau local, n'oubliez pas de cocher la case Permettre PXE.

1.3. Configuration du serveur DNS

DNS est l'acronyme de *Domain Name System* (soit Système de Noms de Domaine en français). DNS vous permet de spécifier une machine par son nom à la place de son adresse IP. Cet assistant permet de configurer un serveur DNS de base, maître ou esclave.

Assurez-vous d'avoir assigné à votre serveur un nom d'hôte qualifié (FQDN), à défaut de quoi l'assistant DNS refusera de démarrer. Vous avez alors la possibilité de lancer l'un de ces assistants :

Serveur DNS Maître

Cet assistant configurera votre machine comme serveur DNS principal. La première étape permet de fournir l'adresse d'un serveur DNS externe auquel seront transmises les requêtes auxquelles le serveur local ne pourra pas répondre directement. Il s'agit généralement de l'adresse du serveur DNS de votre fournisseur d'accès.

La deuxième étape permet de spécifier le nom de domaine pour les recherches. Par exemple, si vous demandez l'adresse IP de la machine `kenobi`, le serveur effectuera la recherche en suffixant à ce nom le nom de domaine spécifié ici.

Serveur DNS secondaire

Cet assistant configure votre machine en tant que serveur esclave d'un autre serveur DNS maître. Il suffit de spécifier l'adresse IP du serveur maître pour que l'esclave en fasse un miroir. Les clients pourront alors être configurés pour interroger les deux serveurs : si le maître est défaillant, l'esclave prendra le relais.

1. Les adresses en dehors de cette plage seront disponibles pour les machines nécessitant une adresse statique, et qui seront déclarées dans *Configuration du serveur DNS*, page 11.

Ajouter un hôte au DNS

Si votre machine est un serveur DNS maître, vous pouvez déclarer ici toutes les machines à adresse fixe (non DHCP) de votre réseau afin que le serveur DNS puisse répondre aux requêtes les concernant.

Enlever un hôte du DNS

Cela est utilisé pour enlever une entrée DNS précédemment ajoutée avec Ajouter un hôte au DNS.

Les assistants Ajouter un hôte au DNS et Enlever un hôte du DNS ne fonctionneront que si la machine est configurée en tant que serveur DNS maître.

1.4. Configuration du serveur mail Postfix

Cet assistant vous aidera à configurer le courrier électronique entrant et sortant. Une fois configuré, ce serveur SMTP permettra aux utilisateurs locaux d'envoyer des messages à des correspondants internes et externes. En outre, si votre serveur est référencé sur Internet en tant que serveur MX pour votre propre domaine, alors il pourra aussi recevoir et gérer le courrier reçu depuis Internet et adressé à vos utilisateurs locaux. Dans ce dernier cas, assurez-vous d'ouvrir les ports correspondants de votre pare-feu.

Votre serveur ne doit pas être en configuration DHCP afin que Postfix fonctionne correctement.

La première étape consiste à choisir si vous utiliserez un relais SMTP externe ou non. Si vous pouvez utiliser un relais fourni par votre fournisseur d'accès, alors choisissez Relay mail server dans la liste déroulante. Sinon, choisissez Main mail server. Dans la procédure qui suit, seule la deuxième étape diffère d'un serveur à l'autre.

1. Configuration générale de Postfix

   Smtpd banner

   L'entête que le serveur envoie lorsqu'il dialogue avec d'autres serveurs ou clients.

   Hostname

   Le nom de votre serveur.

   Domain

   Le nom de domaine géré par ce serveur de courrier.

   Origin

   Les messages postés localement apparaîtront provenir de ce nom de domaine, et seront délivrés à ce même domaine.

2. Relais (pour le serveur Relay mail server uniquement)

   Relay host

   Le serveur de courrier électronique de votre fournisseur d'accès chargé de relayer vos messages sortants.

   Relay domains

   Vers quels domaines destinataires (et sous-domaines correspondants) ce système relaie les messages. Les messages envoyés à un domaine autre que le domaine local sont rejetés (pour empêcher les pourriels ou *spam*).

3. Configuration du serveur principal (pour le serveur Main mail server uniquement)

helo required

Pour des raisons de sécurité, vous pouvez exiger que les clients distants s'identifient avant de démarrer la communication. Choisissez yes dans ce cas.

Disable verify command

La commande `verify` peut être utilisée par un client pour vérifier si un utilisateur en particulier est bien géré par le serveur de courrier. Vous pouvez désactiver cette commande pour empêcher la récolte de courriers électronique par les polluposteurs (*spammers*).

Masquerade domains

Cette option sert à masquer le domaine depuis lequel le courrier interne provient. Par exemple : `foo.exemple.com exemple.com` indique à Postfix de remplacer `toot@foo.example.com` par `toto@example.com`.

4. Options pour les messages

Quelques options qui modifient la façon de gérer les messages, et que vous pouvez laisser inchangées.

Maximal queue life

Si un message ne peut être délivré après ce délai, il est renvoyé en tant qu'indélivrable.

Message size limit

Les messages qui dépassent cette taille (octets) sont rejetés.

Delay warning time

Si un message ne peut être délivré, l'expéditeur reçoit un avertissement au bout de ce nombre d'heures.

5. Configuration réseau

inet interfaces

L'adresse de l'interface réseau sur laquelle le serveur de mail reçoit les messages. Par défaut, seule l'interface locale est activée. Spécifiez `all` pour permettre la réception de messages depuis toutes les interfaces réseau.

my destination

La liste des domaines qui sont gérés par la méthode locale de postage. Le serveur SMTP valide les adresses des destinataires et rejette les destinataires invalides qui n'existent pas.

my networks

La liste des clients SMTP de « confiance » qui ont plus de privilèges que les « étrangers ». Les clients de « confiance » sont notamment autorisés à relayer du courrier à travers Postfix. Spécifiez une liste d'adresses réseaux ou de paires réseau/masque, séparés par une virgule et/ou un espace.

Si la signification d'un paramètre n'est pas claire pour vous, consultez la documentation Postfix : Postfix Configuration Parameters (`http://www.postfix.org/postconf.5.html`).

1.5. Configuration de Samba

Samba est un paquetage logiciel qui permet à GNU/Linux d'agir en tant que serveur de fichiers et d'impression pour des machines Windows®. Cet assistant vous aidera à configurer des contrôleurs de domaines primaires et de sauvegarde, mais nous nous limiterons ici à la configuration plus standard d'un serveur isolé.

Figure 1-3. Choisir le groupe de travail pour vos partages

Vous devez ensuite entrer le nom du groupe de travail pour lequel ces partages seront disponibles (figure 1-3). Vous pouvez soit créer un nouveau groupe de travail, soit en choisir un déjà existant : si vous ne savez que faire, demandez à votre administrateur système.

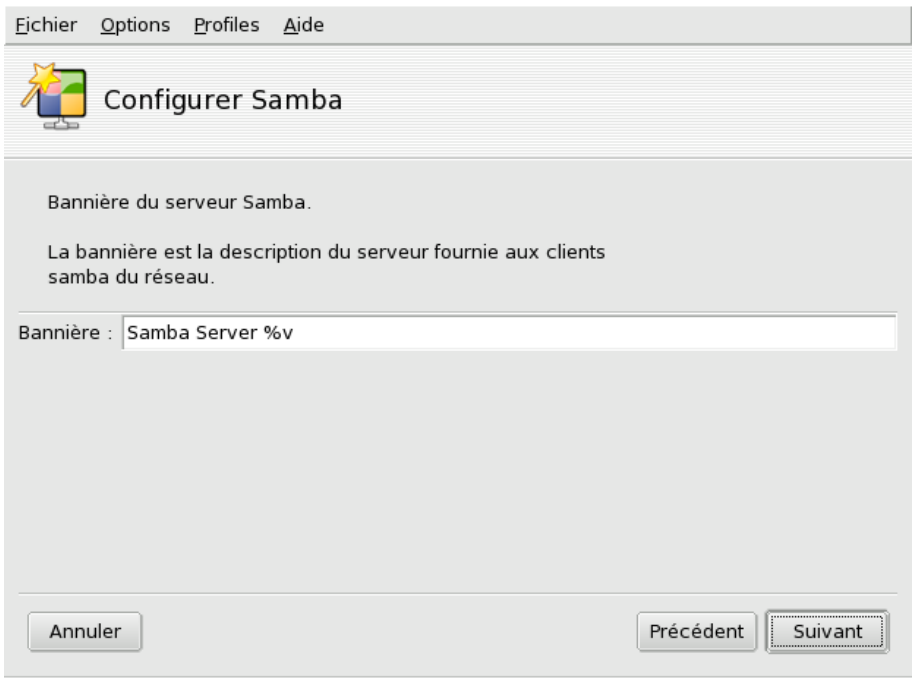


Figure 1-4. Choisir le nom de votre serveur Samba

Ensuite, vous devez spécifier le nom par lequel votre serveur Mandriva Linux sera connu des machines Windows®, tel qu'illustré dans la figure 1-4. Vous pouvez choisir le nom que vous voulez.

Vous pourrez finalement ajuster les paramètres du service de log. Gardez les valeurs par défaut à moins que vous n'ayez des besoins spécifiques.

Une fois que le serveur Samba est configuré, vous pouvez lancer la commande `drakwizard sambashare` en tant que root pour créer de nouveaux partages et configurer les partages existants.

1.6. Configuration du serveur Web

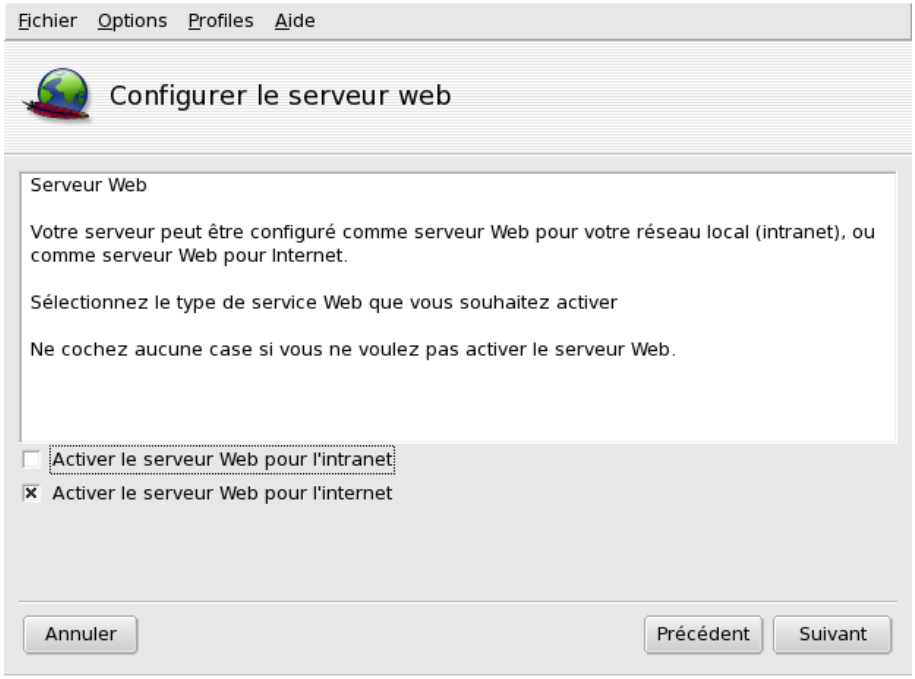


Figure 1-5. Définir d'où votre serveur Web sera visible

Cet assistant vous laissera simplement décider d'où votre serveur Web sera visible. Vous avez le choix de ne pas l'activer, de le rendre visible depuis le réseau interne et/ou externe. Cochez la case appropriée comme le montre la figure 1-5.

Si vos paramètres réseau sont configurés par DHCP, le serveur Web pourrait ne pas fonctionner normalement, notamment depuis Internet.

La seconde étape sert à activer la fonctionnalité permettant aux utilisateurs de publier leur propre site Web. Ceux-ci seront accessibles à l'adresse `http://nom.du.serveur/~utilisateur/`. Le répertoire local où enregistrer les fichiers du site Web pourra être modifié à l'étape suivante.

La dernière étape permet de personnaliser le chemin d'accès au répertoire contenant les fichiers qui seront servis. Pour commencer à garnir votre site Web, placez simplement vos fichiers dans le répertoire choisi. Aussitôt que l'assistant aura terminé son travail, vous pourrez vous connecter directement sur votre site Web à travers l'adresse `http://localhost/`.

1.7. Configuration du serveur FTP

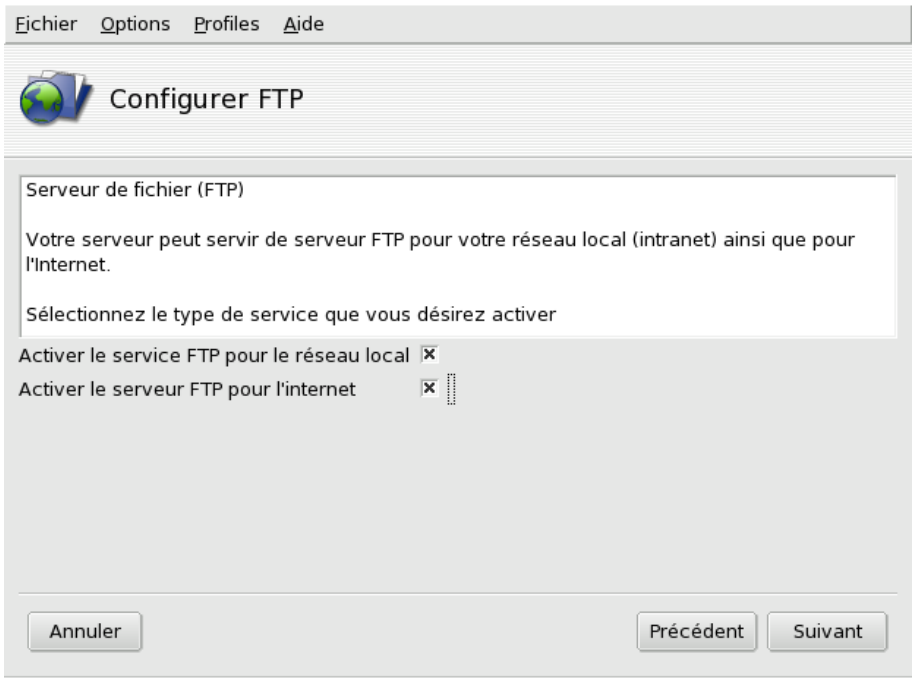


Figure 1-6. Définir d'où voulez-vous rendre visible votre serveur FTP

Si vos paramètres réseau sont configurés par DHCP, le serveur FTP pourrait ne pas fonctionner normalement, notamment depuis Internet.

Cet assistant ressemble à celui utilisé pour la configuration du serveur Web : il vous laissera décider si le serveur FTP doit être désactivé, visible depuis le réseau local seulement, ou bien à la fois sur les réseaux internet et externe.

Figure 1-7. Configuration du serveur FTP

Il s'agit ici de la configuration de base du serveur FTP, il est conseillé de spécifier l'adresse de courrier électronique de l'administrateur afin qu'il reçoive les éventuels messages d'alerte.

Adresse électronique de l'administrateur

Entrez-y l'adresse à laquelle les messages relatifs au serveur FTP seront envoyés.

Autoriser root à se connecter

Cochez cette case si vous souhaitez que l'utilisateur root puisse se connecter au serveur FTP. Si l'authentification FTP est effectuée en clair, cette option est à éviter.

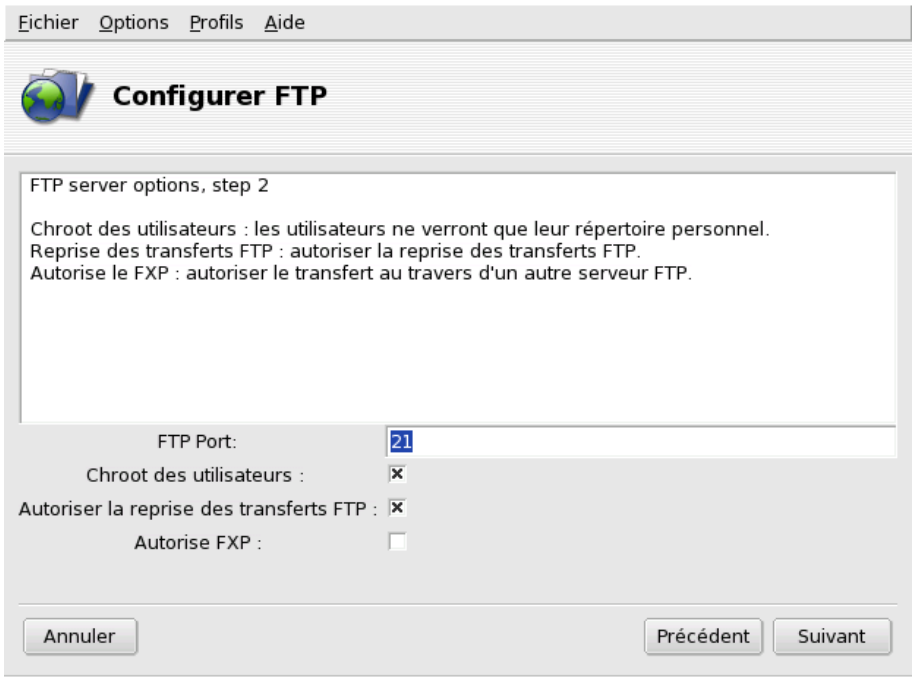


Figure 1-8. Options du serveur FTP

Il est alors possible de changer quelques options :

FTP Port

Le port FTP standard est `21`. Si vous en spécifiez un autre ici, les clients FTP devront être configuré également.

Chroot home user

En cochant cette option, les utilisateurs qui se connectent sur le serveur FTP seront « confinés » à l'intérieur de leur répertoire personnel.

Autoriser la reprise des transferts FTP

Si votre serveur est susceptible de proposer de gros fichiers en téléchargement, il pourrait être judicieux de permettre aux clients de reprendre un téléchargement interrompu.

Autoriser FXP

Cochez cette option si vous souhaitez que le serveur soit capable d'échanger des fichiers avec un autre serveur FTP. Notez que le protocole FXP n'est pas très sécurisé.

Pour commencer à utiliser votre serveur FTP anonyme, ajoutez simplement vos fichiers dans le répertoire `/var/ftp/pub`. Aussitôt que l'assistant aura terminé son travail, vous pourrez vous connecter directement sur votre site FTP à travers l'adresse Web `ftp://localhost`. Les répertoires personnels sont accessibles par défaut à travers une authentification par mot de passe local. Si `reine` veut accéder à son répertoire personnel, elle n'a qu'à utiliser l'adresse `ftp://reine@localhost`.

1.8. Assistant de serveur d'installation

Vous effectuez régulièrement des installations et êtes fatigué de manipuler des CDs ? Cet assistant est fait pour vous. Il configure votre machine pour qu'elle puisse servir de serveur d'installation, de façon à ce que les nouvelles machines puissent obtenir tous les paquetages requis directement par le réseau, que ce soit pour une installation initiale ou pour de la maintenance.

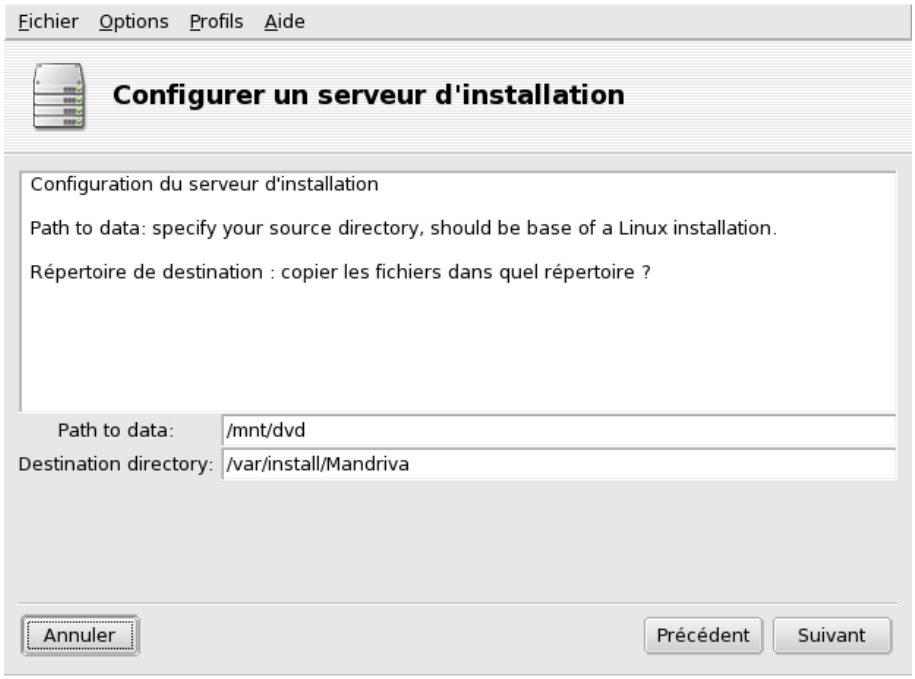


Figure 1-9. Copie des sources de l'installation

Spécifiez le répertoire source depuis lequel copier les CDs ou DVD, puis l'endroit sur le disque local où les fichiers doivent être stockés.

1.9. Assistant de serveurs NIS et Autofs

Lancez cet assistant si vous souhaitez centraliser l'authentification de vos utilisateurs sur le réseau local, ainsi que leurs répertoires personnels. Ceci permet aux utilisateurs de de connecter depuis n'importe quel poste du réseau local et accéder directement à leur environnement propre.

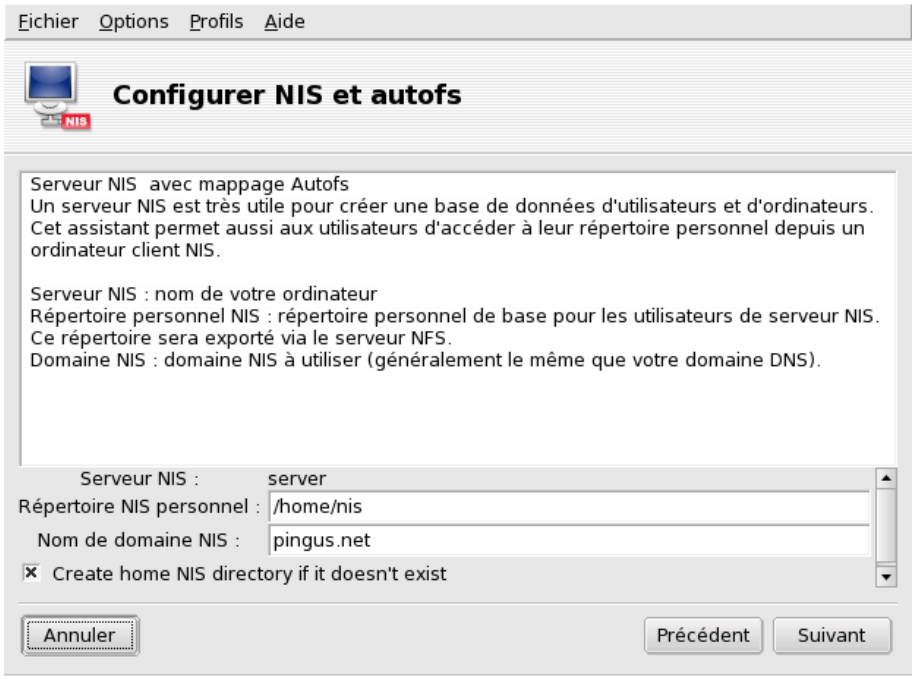


Figure 1-10. Configuration des paramètres du serveur NIS

Il suffit de remplis les paramètres en suivant les instructions de l'assistant. Une fois la configuration terminée, les utilisateurs NIS pourront se connecter depuis toutes les machines du réseau configurées pour se connecter sur votre serveur NIS.

1.10. Assistant de configuration LDAP

Cet assistant simple permet une configuration de base d'un serveur LDAP, et l'ajout de nouvel utilisateurs à celui-ci. Cela est utile pour rapidement mettre en place un mécanisme d'authentification basé sur LDAP.

La première fois que vous lancez l'assistant, le dialogue de configuration du serveur apparaît.

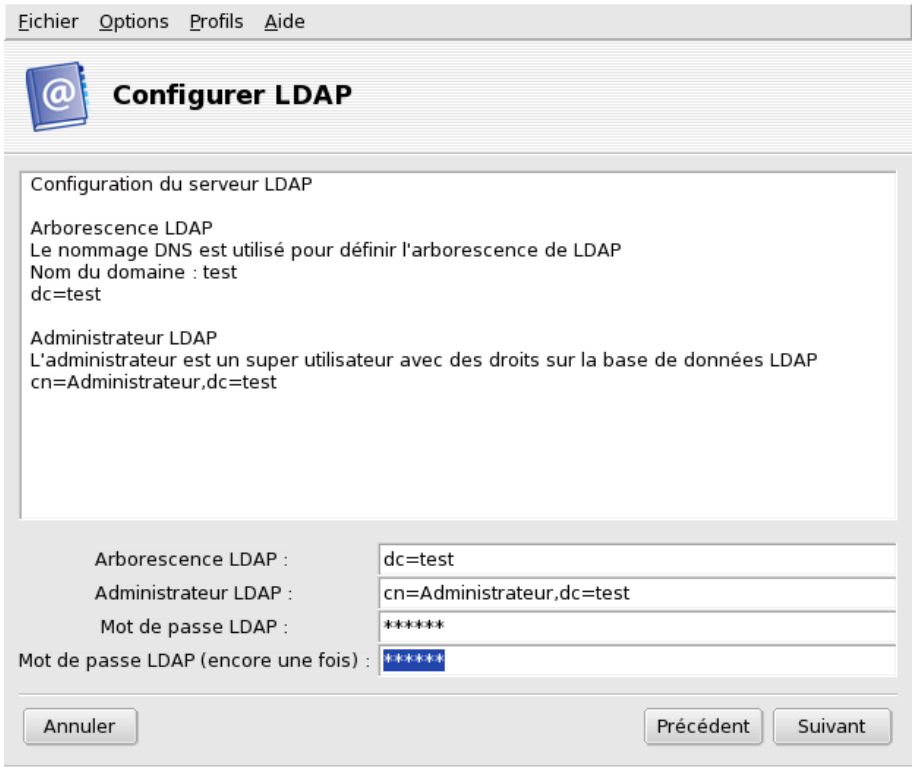


Figure 1-11. Configuration du serveur LDAP

Une fois la configuration effectuée et le serveur démarré, un menu apparaît alors en lançant l'assistant :

Montrer la configuration Ldap

Affiche la configuration actuelle du serveur, utile pour configurer les clients LDAP.

Effacer la configuration Ldap

Efface la configuration du serveur et l'arrête.

Ajouter un utilisateur sur le serveur Ldap

Démarre un petit assistant permettant d'ajouter de nouveaux utilisateur dans l'annuaire.

1.11. Configuration du serveur de forums

Cet assistant configurera une passerelle pour les forums : votre serveur récupérera les forums de discussion depuis un serveur de forums externe (habituellement, celui de votre fournisseur d'accès : `news.domaine-du.fai`) et les rendra visibles sur votre réseau interne. La première chose à faire est donc de spécifier quel serveur de forums vous voulez utiliser.

Vous devez ensuite spécifier l'intervalle (en heures) entre chaque rafraîchissement. Il faudra trouver un équilibre entre un intervalle trop grand entraînant des forums rapidement obsolètes, et un intervalle trop petit entraînant une charge réseau trop importante. Le choix dépendra du trafic sur les forums et de votre bande passante disponible.

1.12. Configuration du serveur mandataire

Le serveur mandataire (*proxy*) squid est très utile pour les réseaux locaux qui accèdent à une grande quantité de pages Web à travers une connexion lente ou relativement lente. Il maintient en cache les pages les plus visitées. Ainsi, elles n'ont pas à être récupérées deux fois sur Internet si une requête sur une même page est faite par plusieurs utilisateurs, le server mandataire utilisé ici est Squid.

Premièrement, vous devez choisir le port sur lequel le mandataire écoutera les requêtes. Les usagers devront configurer leur navigateur Web afin d'utiliser ce port en tant que port mandataire, et le nom de votre serveur en tant que serveur mandataire.

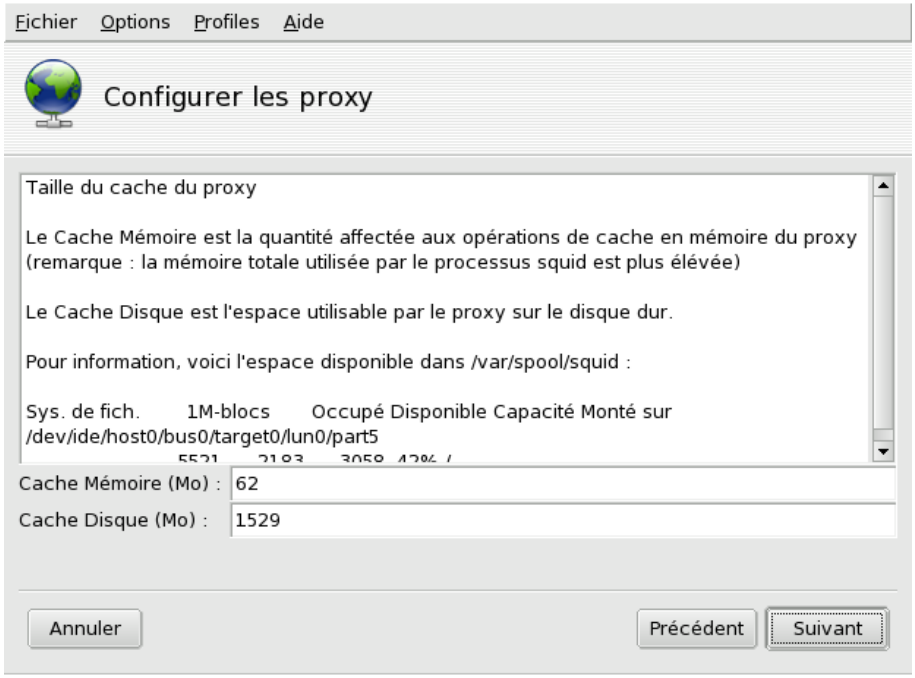


Figure 1-12. Choisir la taille du cache

Selon l'espace mémoire dont vous disposez, vous pouvez en allouer plus ou moins au mandataire. Plus vous utilisez de mémoire cache, moins il y aura d'accès au disque de votre serveur. Et selon l'espace disque disponible, vous pouvez allouer plus ou moins d'espace pour les pages en cache. Plus vous avez d'espace, moins vous aurez à accéder directement à Internet. L'assistant choisit des valeurs moyenne en fonction de votre système, que vous pouvez accepter pour l'instant.

Plusieurs niveaux d'accès sont disponibles pour les clients désirant utiliser le mandataire :

- **Pas de restriction d'accès.** Aucune restriction, tous les ordinateurs auront accès au cache : cette option est peu sûre et donc à éviter.
- **Réseau local.** Seules les machines sur le réseau local auront accès au mandataire. Ceci est l'option recommandée.
- **localhost.** Seules la machine, soit le serveur, pourra accéder à son propre mandataire.

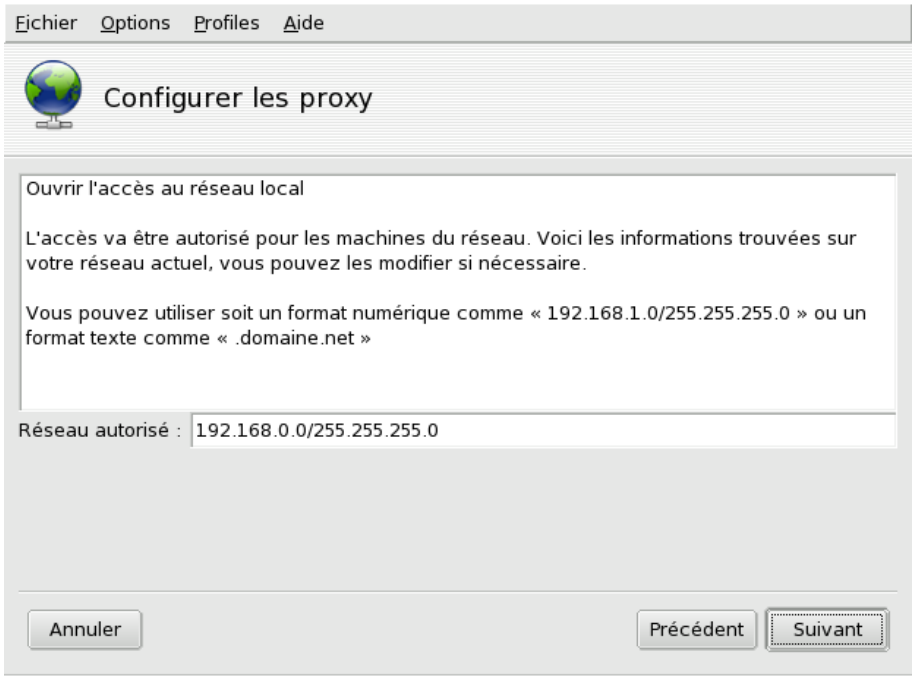


Figure 1-13. Restreindre l'accès à un sous-réseau particulier

Si, précédemment, vous avez choisi la politique d'accès Réseau local, vous pouvez restreindre encore plus l'accès à un sous-réseau ou domaine particulier. L'assistant utilisera l'adresse réseau de votre réseau local par défaut, que vous pouvez modifier si nécessaire.

Enfin, si votre serveur a accès à un autre mandataire de grande taille connecté à Internet, vous pouvez Définir un mandataire de niveau supérieur sur lequel les requêtes seront transférées. Si tel est le cas, à la prochaine étape, il vous sera demandé d'entrer le nom de ce serveur.

1.13. Configuration du serveur de temps

Cet assistant vous aide à configurer un serveur de temps pour votre réseau interne. Le protocole utilisé est NTP. Lorsque vous aurez configuré les serveurs de temps externes sur lesquels votre propre serveur se synchronisera, les machines de votre réseau local pourront à leur tour se synchroniser sur votre serveur.

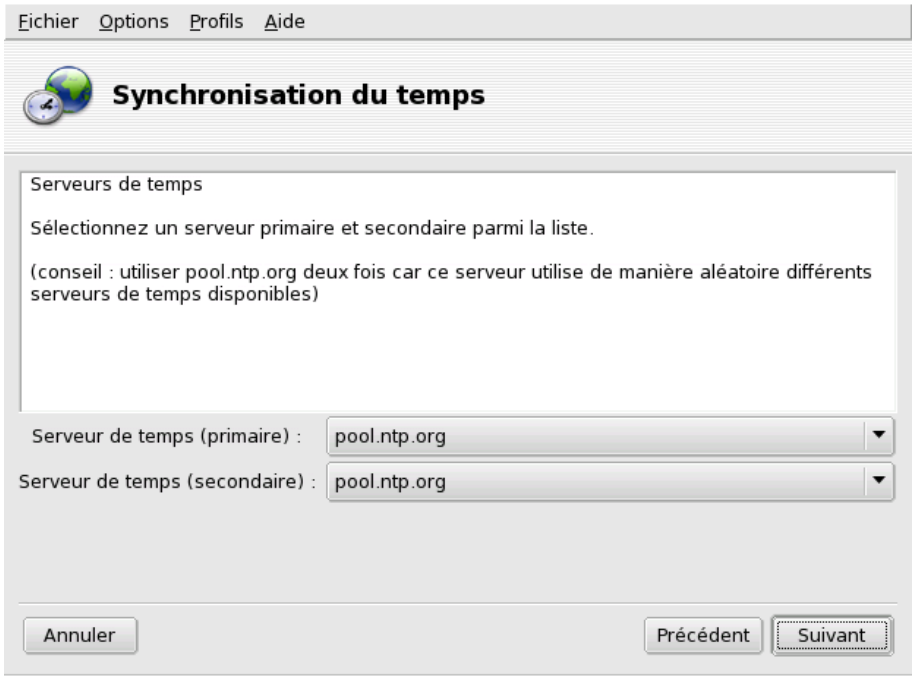


Figure 1-14. Choisir vos serveurs de temps

Il suffit de choisir les serveurs à interroger, par ordre de préférence. Comme il est indiqué, mieux vaut garder le choix initial à moins que cela ne fonctionne pas. Choisissez alors un serveur qui soit le plus proche possible de votre situation géographique. Par défaut, le fuseau horaire sélectionné est celui choisi pendant l'installation.

Chapitre 2. Configurer des clients de passerelle

Ce chapitre vous montrera comment faire interagir différents systèmes d'opération avec une machine Mandriva Linux, laquelle agit comme mandataire (*masquerading*) réglé en tant que passerelle vers le monde extérieur. Les tests de configuration se sont déroulés avec succès sur plusieurs systèmes d'exploitation et architectures.

Si vous craignez que votre OS ne soit pas supporté, une façon simple de procéder est de « simplement signifier au système d'exploitation quelle machine doit être utilisée en tant que passerelle ». Notez qu'ici, nous nous concentrerons sur le côté **passerelle** du réseau : donc, nous n'aborderons pas les problèmes pouvant être liés au DNS, au partage de fichiers ou aux schémas de connexion. Ainsi, pour que ce chapitre vous soit utile, votre réseau local doit être bien configuré. Référez-vous à la documentation de votre système pour le régler de façon adéquate, en accordant une attention particulière aux réglages du DNS.

Pour la suite, nous présumons que vous travaillez avec un réseau de classe C : vos différents postes de travail ont tous une adresse IP ressemblant à `192.168.0.x`, votre masque de réseau (*netmask*) est réglé à `255.255.255.0`, et vous utilisez une interface de réseau `eth0`. Nous prenons également pour acquis que l'adresse IP de votre passerelle est réglée à `192.168.0.1` et que tous vos postes de travail peuvent « parler » à la passerelle (vous pouvez tester ceci avec la commande `ping` ou son équivalent, tout dépendant de l'environnement que vous utilisez).

2.1. Machine Linux

2.1.1. Pour toutes les machines Linux

Nous devons éditer un fichier de configuration. La méthode est différente quand on utilise la configuration automatique du réseau.

Configuration automatique du réseau

Ouvrez le fichier de configuration de l'interface (par exemple `/etc/sysconfig/network-scripts/ifcfg-eth0` sur une machine Mandriva Linux, cela peut être différent sur la vôtre) et vérifiez que le paramètre `BOOTPROTO` est réglé à `BOOTPROTO=dhcp`.

Configuration manuelle

Vous devez éditer le fichier de configuration `network` (`/etc/sysconfig/network` sur une machine Mandriva Linux, ce peut être différent sur la vôtre). Ouvrez ce fichier avec votre éditeur de texte habituel, puis ajoutez les lignes suivantes (en ajustant les valeurs si nécessaire) :

```
GATEWAYDEV=eth0
GATEWAY=192.168.0.1
```

Vous pouvez maintenant relancez votre couche réseau Linux. Sur une machine Mandriva Linux tapez en tant que `root` : `service network restart` ou `/etc/init.d/network restart` dans un terminal.

2.1.2. Sur une machine Mandriva Linux

Vous n'avez qu'à entrer les bons paramètres dans l'outil Gérer les connexions depuis la section Réseau & Internet du Centre de contrôle Mandriva Linux. Référez-vous au chapitre *Configuration des connexions Internet* du *Guide de démarrage* pour plus de renseignements. Il vous est proposé de configurer le réseau en mode manuel ou automatique (DHCP) :

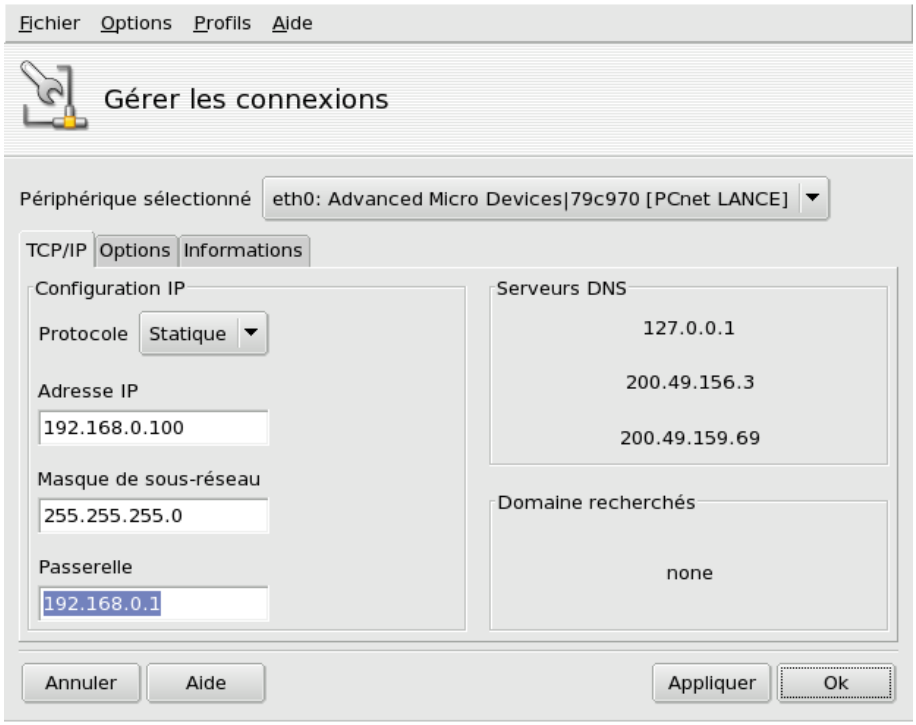


Figure 2-1. Entrer les paramètres réseau manuellement dans drakconnect

Si votre réseau local abrite un serveur DHCP, choisissez l'entrée DHCP. Si votre machine possède une adresse IP fixe, entrez-la dans le premier champ après vous être assuré que l'entrée Statique est bien sélectionnée. Il faut également remplir les champs Masque de sous-réseau et Passerelle en fonction de votre configuration réseau, tel qu'illustré dans la figure 2-1.

Une fois que vous avez appliqué les modifications, votre réseau est correctement configuré et prêt à être utilisé. La configuration est maintenant permanente.

2.2. Machine Windows XP

Nous prenons pour acquis que votre connexion réseau est déjà configurée. figure 2-2 montre les différentes étapes nécessaires pour obtenir le menu contextuel désiré.

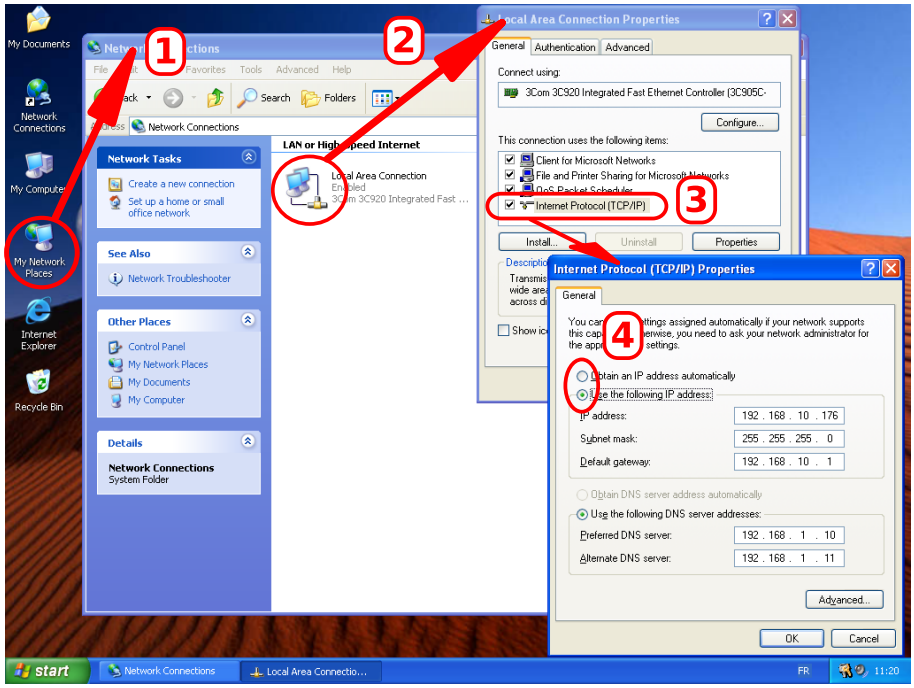


Figure 2-2. Configuration de la passerelle sous Windows XP

Voici les étapes à suivre pour passer d'une fenêtre à l'autre :

1. Sur le bureau, faites un clic droit sur l'icône My network places, et sélectionnez Properties dans le menu contextuel ;
2. Dans la fenêtre Network Connections, faites la même chose avec la connexion liée au réseau où se trouve la passerelle ;
3. Dans le prochain menu, choisissez le champ Internet Protocol (TCP/IP) et cliquez sur le bouton Properties ;
4. Dans ce menu, vous pouvez sélectionner Obtain an IP address automatically si votre réseau abrite un serveur DHCP. Ensuite, tous les paramètres réseau devraient être configurés automatiquement. Si vous préférez régler les paramètres réseau à la main, choisissez Utiliser l'adresse IP suivante et remplissez les champs appropriés.

2.3. Machine Windows 95 ou Windows 98

Premièrement, allez dans le panneau de contrôle (Démarrer ParamètresPanneau de contrôle) et trouvez l'icône de réseau ci-dessus. Double-cliquez dessus et une fenêtre de configuration réseau apparaîtra.

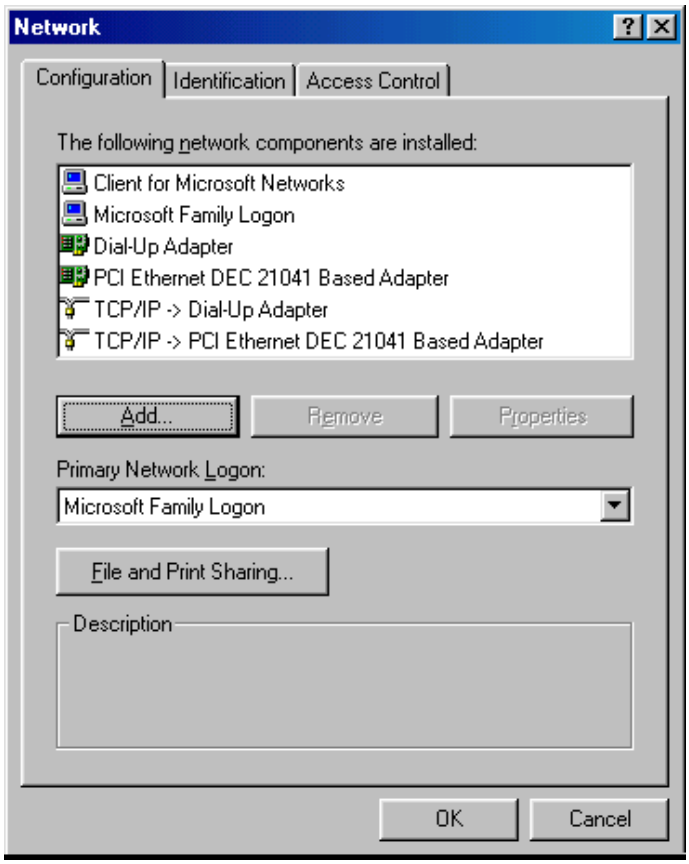


Figure 2-3. La fenêtre de configuration réseau sous Windows 9x

Dans la liste affichée, vous devriez trouver le protocole `TCP/IP`. Sinon, vous devrez vous référer à la documentation de votre système pour savoir comment l'installer. Sélectionnez-le et cliquez sur Propriétés.

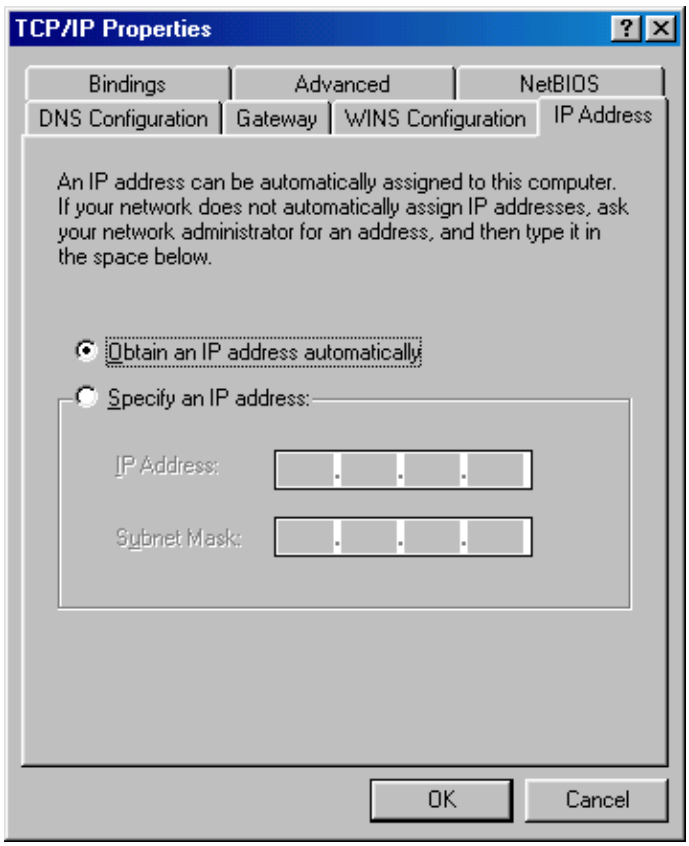


Figure 2-4. La fenêtre de configuration TCP/IP sous Windows 9x

À travers cette fenêtre, vous pourrez régler les paramètres TCP/IP. Votre administrateur système vous dira si vous avez une adresse IP statique ou si vous utilisez un DHCP (paramètres réseau automatique). Cliquez sur l'onglet `Passerelle` (*gateway*).

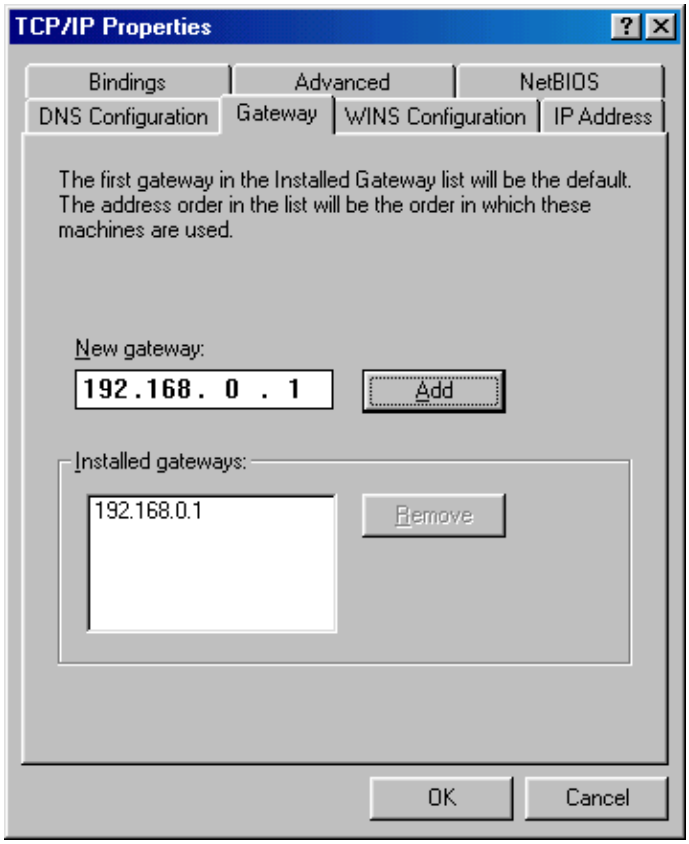


Figure 2-5. La fenêtre de configuration de la passerelle sous Windows 9x

La suite est un jeu d'enfants ! Remplissez les champs vides avec l'adresse IP de votre passerelle (dans notre exemple, 192.168.0.1). Enfin, cliquez sur les boutons Ajouter et OK.

Évidemment, vous devrez redémarrer votre machine. Vérifiez ensuite que vous pouvez rejoindre le reste du monde Internet.

2.4. Machine Windows NT ou Windows 2000

Pour configurer ces systèmes d'exploitation, suivez ces étapes très simples :

1. Allez dans le menu Panneau de contrôle+Réseau→Protocole.

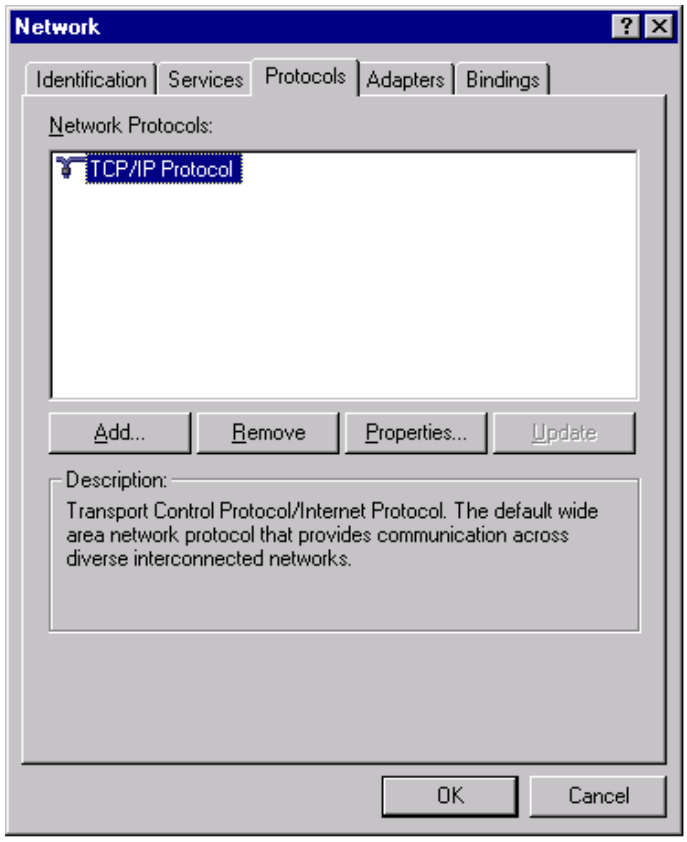


Figure 2-6. La fenêtre de configuration de protocole sous Windows NT/2000

2. Premièrement, sélectionnez le Protocole TCP/IP dans la liste de protocoles réseau. Ensuite, cliquez sur le bouton Propriétés, et choisissez la carte réseau connectée au réseau local (figure 2-7). Dans cet exemple, nous montrons une configuration faite avec un serveur DHCP : l'option Obtenir une adresse IP du serveur DHCP (*Obtain an IP address from a DHCP server*) est sélectionnée.

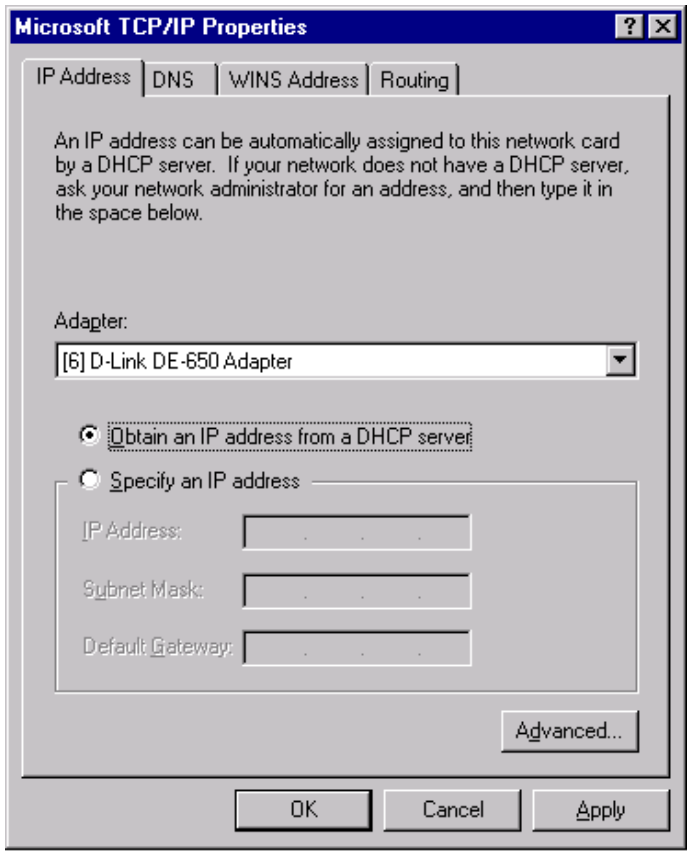


Figure 2-7. Le panneau de logiciel réseau sous Windows NT/2000

Si tel est votre cas, vous n'avez qu'à confirmer tous ces choix et redémarrer votre machine. Sinon, suivez les prochaines étapes.

3. Pour configurer les paramètres réseau manuellement, cochez l'option Spécifiez une adresse IP (figure 2-8).

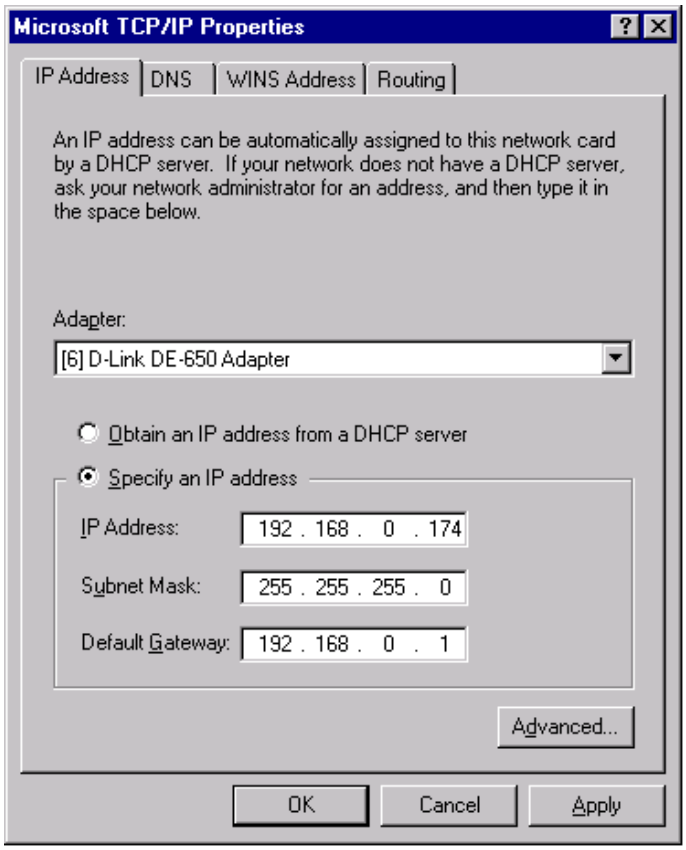


Figure 2-8. La fenêtre de configuration TCP/IP sous Windows NT/2000

Choisissez l'adaptateur approprié : l'adresse IP devrait déjà être la bonne. Sinon, il faut la spécifier.

4. Dans le champ Passerelle par défaut, écrivez `192.168.0.1` (soit l'adresse de la machine Linux partageant la connexion dans notre exemple).
5. Enfin, vous devez spécifier les serveurs DNS que vous utilisez dans l'onglet DNS, tel que montré dans la figure 2-9.

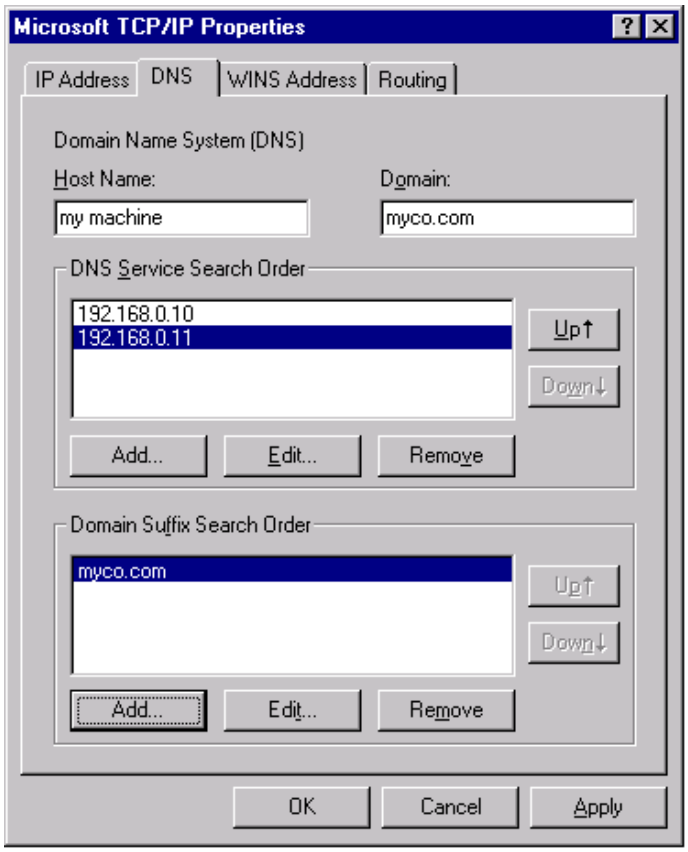


Figure 2-9. La fenêtre de configuration DNS sous Windows NT/2000

Vous devez également fournir le nom d'hôte et le nom de domaine qui y est associé.

Sauf si vous savez exactement ce que vous faites, procédez de façon très minutieuse lors des étapes qui suivent :

- laissez le champ Configuration automatique du DHCP vide, sauf si votre réseau abrite un serveur DHCP ;
- laissez également tous les champs Serveur WINS vides, sauf si vous possédez un ou plus d'un serveur WINS ;
- ne cochez pas le champ Activez le transfert d'IP (*Enable IP Forwarding*) sauf si votre machine NT/2000 est utilisée pour le routage et, encore une fois, que vous savez exactement ce que vous faites ;
- désactivez DNS for Windows Name Resolution et Activez la consultation LMHOSTS (*Enable LMHOSTS lookup*).

Cliquez sur OK dans les menus contextuels qui apparaîtront et redémarrez votre ordinateur pour tester la configuration.

2.5. Machine DOS utilisant le paquetage NCSA Telnet

Dans le répertoire qui contenant le paquetage NCSA, vous trouverez un fichier nommé `config.tel`. Éditez-le avec votre éditeur de texte préféré et ajoutez les lignes suivantes :

```
name=default
host=le_nom_de_la_machine_linux
hostip=192.168.0.1
gateway=1
```

Changez `le_nom_de_la_machine_linux` pour le nom de réel de votre passerelle Linux.

Maintenant, sauvegardez le fichier, essayez de faire un `telnet` sur votre machine Linux, puis sur une machine branchée à Internet.

2.6. Windows pour Workgroup 3.11

Le paquetage `TCP/IP 32b` devrait déjà être installé. Allez dans le menu Principal+Configuration Windows+Configuration réseau→Pilotes et choisissez Microsoft TCP/IP-32 3.11b dans la section Pilotes réseau (*Network Drivers*), puis cliquez sur Réglage (*Setup*.

Ensuite, la procédure est très similaire à celle décrite dans la section *Machine Windows NT ou Windows 2000*, page 29.

2.7. Machine MacOS

2.7.1. MacOS X

La configuration consiste à régler les paramètres corrects de l'interface Ethernet connectée à votre passerelle.

Figure 2-10. Le dock de MacOS X

Avant tout, vous devez ouvrir la fenêtre Préférences Système en cliquant sur son icône dans le dock système.

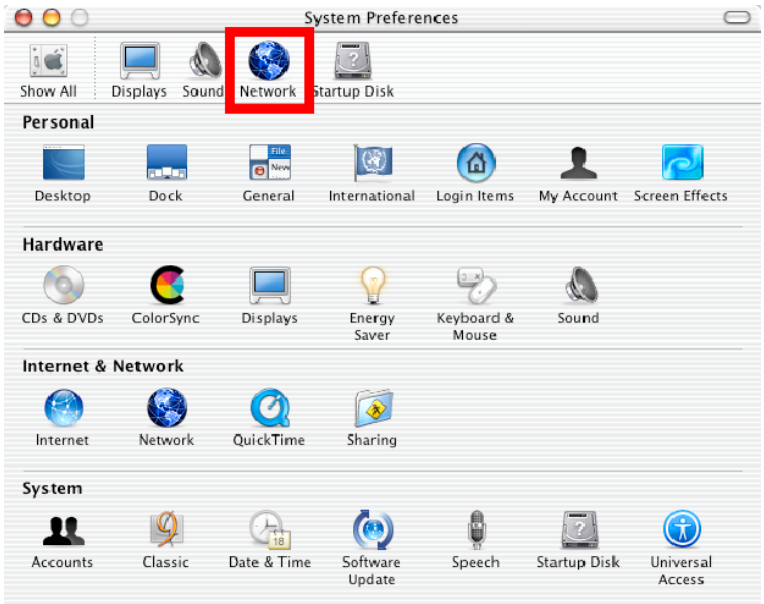


Figure 2-11. Préférences Système de MacOS X

2.7.1.1. Avec une configuration automatique DHCP

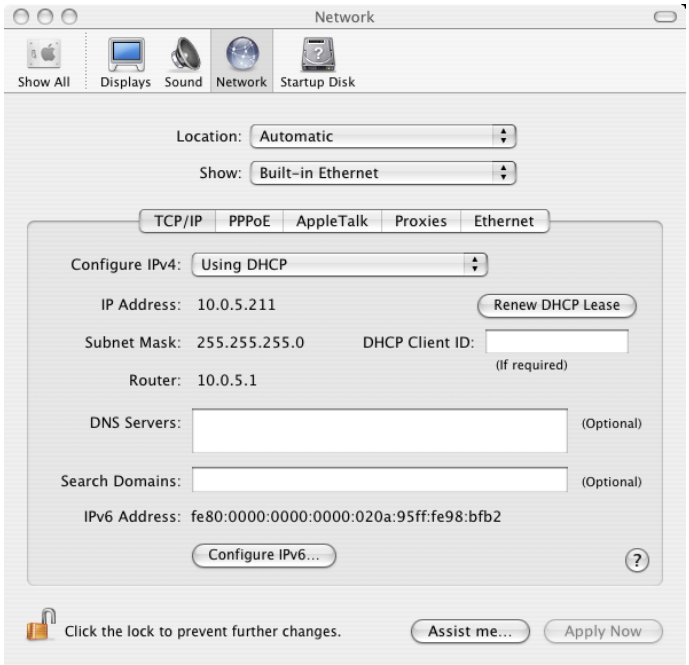


Figure 2-12. Configuration automatique de l'accès Internet pour MacOS X

Dans la fenêtre qui apparaît, sélectionnez Built-In Ethernet ou l'interface actuellement connectée à la passerelle, puis choisissez Utilisez DHCP dans l'onglet TCP/IP comme dans figure 2-12. Puis, cliquez sur Appliquez maintenant, et si tout s'est bien déroulé, le champ Routeur devrait afficher l'adresse IP votre passerelle.

2.7.1.2. Pour une configuration manuelle

Si vous n'avez pas de DHCP sur votre réseau local, suivez cette procédure.

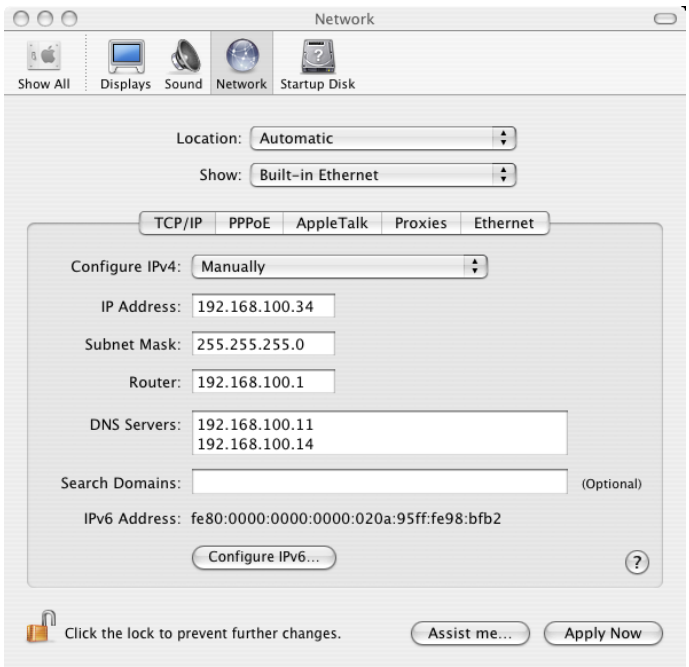


Figure 2-13. Configuration manuelle de l'accès Internet pour MacOS X

Dans la fenêtre qui apparaît, remplissez les champs comme expliqué ici :

- Configuration : Manuelle ;
- Adresse IP :192.168.100.34 (l'adresse IP du client) ;
- Masque de sous-réseau (*Subnet Mask*) : 255.255.255.0 (le masque de sous-réseau du réseau local) ;
- Adresse du routeur : 192.168.100.1 (l'adresse de la passerelle) ;
- Serveurs DNS : 192.168.100.11 ; 192.168.100.14 (l'adresse IP des serveurs DNS).

L'adresse du serveur de noms peut être un serveur DNS interne ou celui de votre fournisseur d'accès.

Une fois que tout est fini, cliquez sur Appliquez maintenant, et si tout s'est bien déroulé, vous pourrez surfer sur Internet.

2.7.2. MacOS 8/9

Premièrement, vous devez ouvrir le panneau de contrôle TCP/IP tel qu'illustré dans le menu Apple.

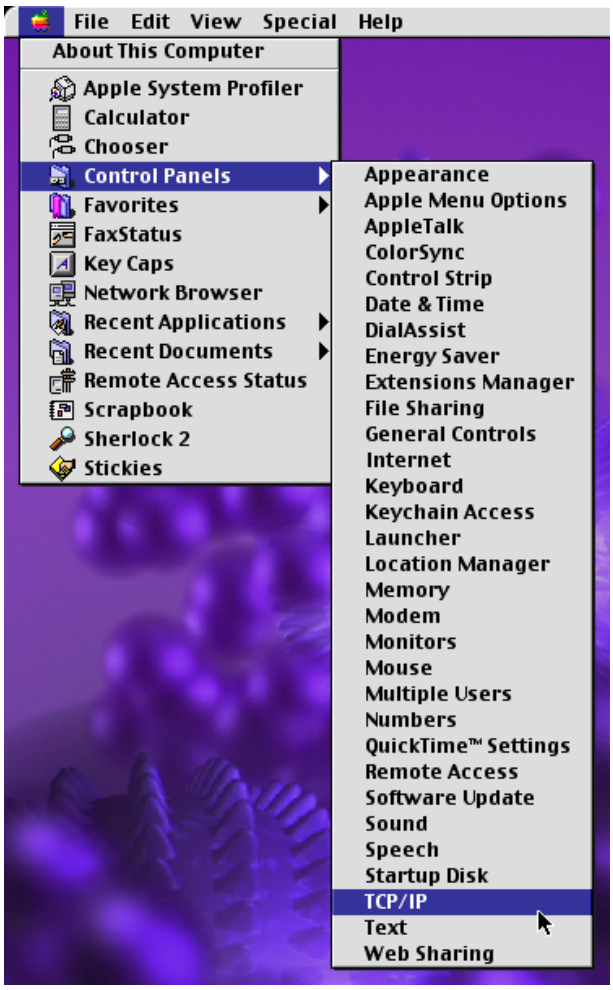


Figure 2-14. Accéder au panneau de contrôle TCP/IP

2.7.2.1. Avec la configuration automatique du DHCP

Si vous configurez votre pare-feu pour qu'il agisse en tant que serveur DHCP, suivez cette procédure à la lettre. Sinon, allez à la section suivante.

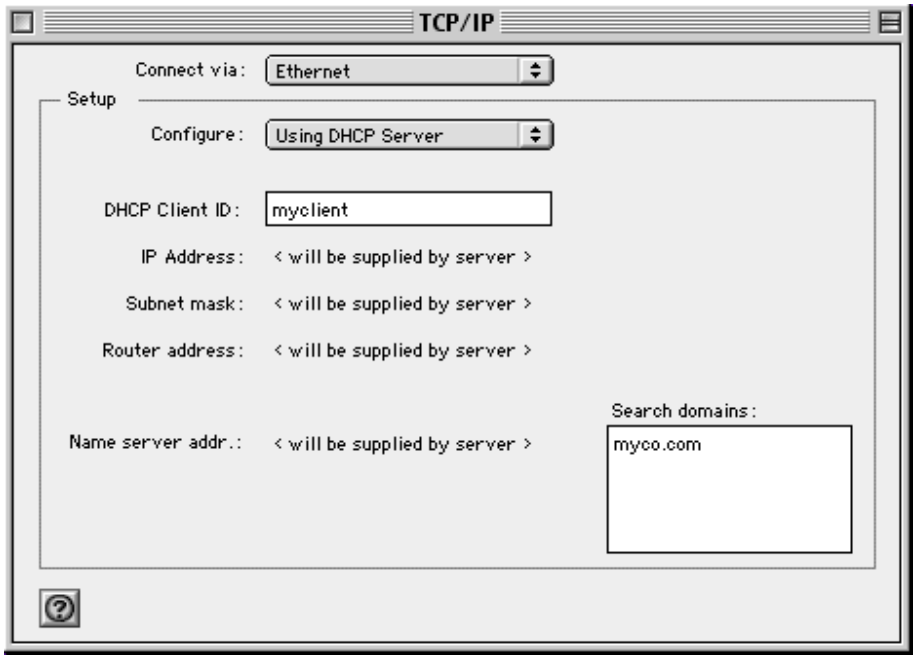


Figure 2-15. Configuration automatique de l'accès à Internet pour MacOS

Dans le menu contextuel qui apparaît, remplissez les champs comme ceci :

- Connect via: Ethernet ;
- Configure : Using DHCP server (soit *Utiliser un serveur DHCP* ;
- DHCP Client ID (soit Identification du client DHCP) : 192.168.0.1.

2.7.2.2. Configuration manuelle

Si votre réseau local n'abrite pas de serveur DHCP, suivez la procédure ci-dessous :

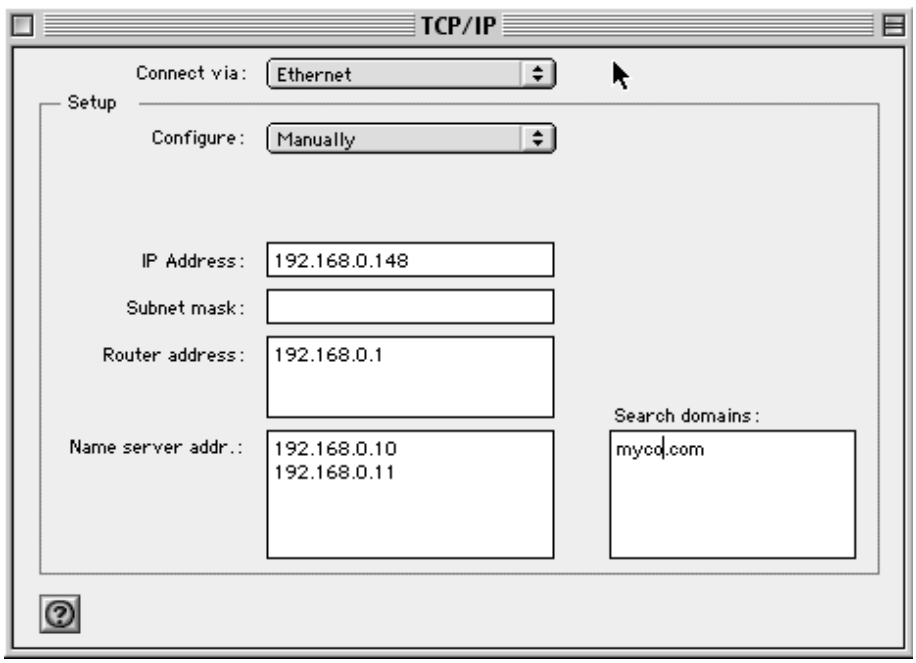


Figure 2-16. Configuration manuelle de l'accès à Internet pour MacOS

Dans le menu contextuel, remplissez les champs ainsi :

- Connect via : Ethernet ;
- Configure : Manuellement ;
- Adresse IP : 192.168.0.248 ;
- Masque de sous-réseau (*Subnet Mask*) : 255.255.255.0 ;
- Adresse du routeur : 192.168.0.1 ;
- Adresses des serveurs de noms de domaine : 192.168.0.10 et 192.168.0.11 ;
- Nom de domaine de recherche : myco.com.

Les adresses des serveurs de noms de domaine peuvent être celles des DNS internes ou celles des serveurs de votre fournisseur d'accès à Internet.

2.7.3. MacTCP

1. Dans le Panneau de contrôle MacTCP, choisissez le pilote de réseau Ethernet (attention, ce n'est pas EtherTalk) puis cliquez sur le bouton Encore (*More*).
2. Dans le champ Adresse de la passerelle, entrez l'adresse de la machine Linux qui partage la connexion (dans notre exemple, `192.168.0.1`).
3. Cliquez sur OK pour sauvegarder les réglages. Peut-être aurez-vous à redémarrer votre système pour tester ces réglages.

2.8. Machine OS/2 Warp

Le protocole TCP/IP devrait déjà être installé. Sinon, installez-le.

1. Allez dans Programmes, puis TCP/IP (LAN), et Réglages TCP/IP.
2. Dans la rubrique Routing, choisissez Ajouter. Pour le Type, sélectionnez Défaut.
3. Remplissez le champ Adresse du routeur avec l'adresse de la machine Linux qui partage la connexion Internet (dans notre exemple, 192.168.0.1).
4. Maintenant, fermez le panneau de contrôle `TCP/IP`, répondez Oui à toutes les questions, et réamorcez votre machine afin de tester les réglages.

Introduction à la configuration des services

Cette partie détaille les services les plus communs dont un administrateur système peut avoir besoin concernant l'utilisation de réseaux externe (Internet) et interne (intranet). Nous mentionnons les services que les entreprises de taille moyenne sont susceptibles d'utiliser. Tous les services sont configurés avec l'outil Webmin.

1. Introduction à Webmin

Webmin permet l'administration distante de votre machine en utilisant uniquement un navigateur qui prend en charge le protocole HTTPS (HTTP sur SSL). Il facilite l'administration à distance tout en favorisant la sécurité des opérations.

Webmin est idéal pour les administrateurs système, puisque toutes les plates-formes importantes possèdent des navigateurs Web qui correspondent ou excèdent les pré-requis susmentionnés. De plus, Webmin abrite son propre « serveur Web » ; il n'a pas besoin de logiciel tiers (comme un serveur Web) pour fonctionner. Tout est inclus.

1.1. Introduction à l'interface

Premièrement, assurez-vous que le paquetage `webmin` est installé. Assurez-vous aussi qu'il fonctionne à travers l'application drakxservices. Une fois ces opérations complétées, vous serez en mesure d'y accéder avec un navigateur, localement ou sur une autre machine du même réseau. Pointez votre navigateur vers `https://NomDuServeurOuIP:10000` pour accéder à l'interface. Acceptez le certificat et l'écran de connexion apparaît. Entrez l'identifiant `root` ainsi que son mot de passe, puis cliquez sur Login afin d'accéder à l'écran principal de Webmin.

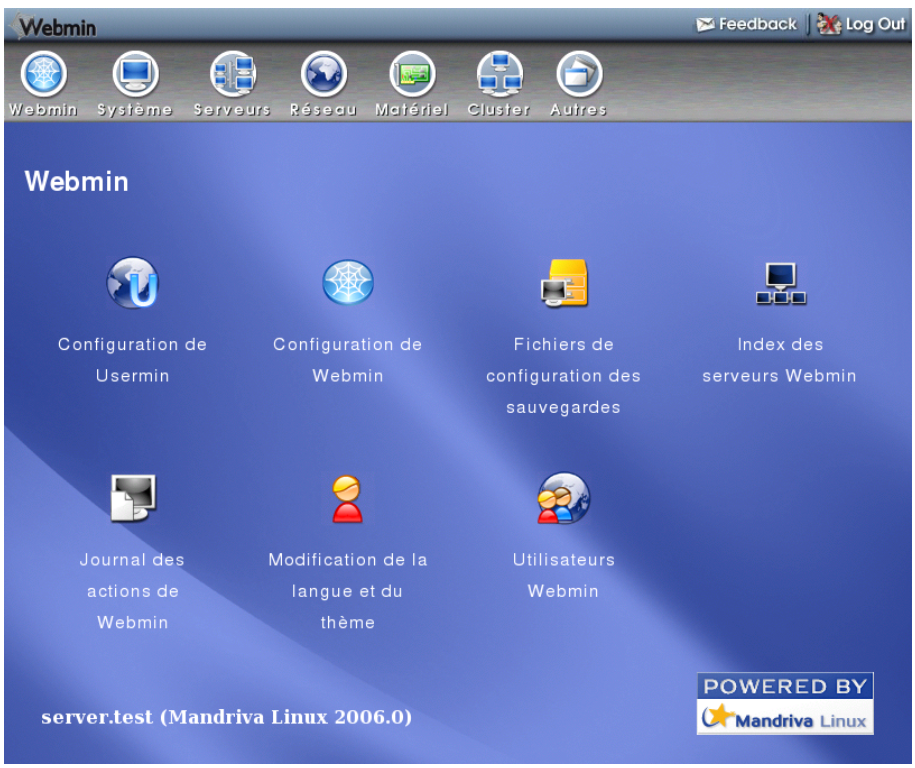


Figure 31. L'interface de Webmin

Cliquez sur le bouton Webmin Configuration puis sur Languages pour obtenir l'interface en français. Depuis la liste déroulante, choisissez French (FR). Malheureusement, certains modules ne sont pas complètement traduits. Donc, vous y retrouverez certains champs ou boutons en anglais.

L'interface présente des sections ou des onglets donnant accès à des modules dédiés à un aspect particulier de la configuration d'une machine.

À titre d'exercice, cliquez sur l'option Contrôle d'accès par adresses IP du module Configuration de Webmin.

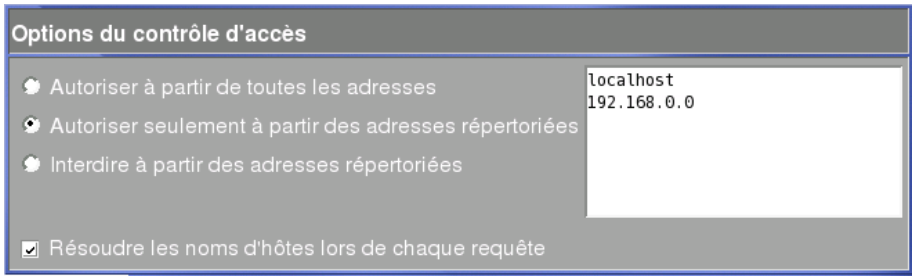


Figure 32. Contrôle d'accès

Notez que si votre serveur est accessible depuis Internet et que vous voulez bien le sécuriser, cette étape est obligatoire. Bien entendu, cela ne vous dispense pas de configurer un pare-feu à travers le Centre de contrôle Mandriva Linux, Webmin (Réseau, Linux Firewall) ou tout autre outil de configuration de pare-feu.

Choisissez l'option Autoriser uniquement depuis les adresses listées. Puis dans le champ texte, listez toutes les machines ou réseaux qui pourront se connecter à Webmin. Pour une sécurité optimisée, cochez également l'option Resolve hostnames on every request (soit résolution des noms d'hôte à chaque requête).

1.2. Comment obtenir de l'aide

Pour la plupart des modules, vous pouvez accéder à de l'aide en ligne par l'entremise d'hyperliens. En cliquant sur ceux-ci, une autre fenêtre apparaît et abrite de l'aide concernant le paramètre choisi. Elle peut vous donner le sens, la syntaxe à utiliser ou même des exemples, tout dépendant du module.

Notez également que la plupart des modules propose un lien Chercher dans la documentation dans le coin supérieur droit de votre écran. En cliquant sur ce bouton, vous lancez une recherche sur le nom de ce module dans la documentation locale, sur Google[tm] (`http://www.google.com`), dans les Documents HOWTO, dans la Documentation des composants, etc. Ainsi, vous avez un accès instantané aux documents pertinents au module que vous voulez configurer. Accédez au formulaire de recherche et à sa configuration à partir du module Système+Pages de manuel.

Le site Web de Webmin (`http://www.webmin.com/index2.html`) propose également des ressources variées, incluant un lien vers le très bon livre The Book of Webmin (`http://www.swelltech.com/support/documentation.html`) écrit par Joe Cooper.

Finalement, à la fin de chaque chapitre discutant d'un service, nous incluons une liste de ressources intéressantes.

2. Services

Voici les services que nous couvrons :

- Le *BIND : serveur DNS*, page 43 traite des serveur de noms de domaine (DNS ou *Domain Name System*) et plus précisément, de BIND.
- Dans le chapitre (*Serveur Web Internet/intranet*, page 51), nous traitons de l'hébergement de sites Web Internet/intranet (HTTP) avec le serveur Web Apache.

- Ensuite, nous traitons de la gestion de courrier (SMTP), nous concentrant sur l'envoi de courrier électronique avec Postfix (*Le serveur de courrier Postfix*, page 57).
- Nous discutons des services de remise de courrier (POP et IMAP) avec le serveur de courrier IMAP dans le *Serveurs de remise de courrier : POP et IMAP*, page 63.
- Le partage de ressources telles que fichiers et imprimantes est le sujet principal du chapitre suivant (*Partage de ressources*, page 65). Il détaille NFS, Samba et le serveur FTP ProFTPD.
- Nous documentons la partie serveur de la solution de travail collaboratif Kroupware dans le *Le serveur Kolab*, page 73.
- Nous abordons l'utilisation d'un serveur de base de données dans le *Serveur de bases de données MySQL*, page 83.
- La gestion décentralisée des utilisateurs et l'hébergement de répertoires personnels est le sujet principal du *Client et serveur NIS*, page 87.

Chapitre 3. BIND : serveur DNS

Un DNS permet d'associer un nom à une adresse IP. Par exemple : `www.mandriva.com` (« un nom ») est associé à `212.85.150.181` (« une adresse » IP). À titre de comparaison, un serveur de nom est un peu comme un annuaire téléphoniqe : vous lui soumettez un nom et il fournit le numéro permettant de joindre votre correspondant. Cette opération est cependant translarente à l'utilisateur : il n'a jamais besoin de taper ou de se rappeller une adresse IP, grâce au serveur DNS.

Nous vous guidons dans ce chapitre pour la configuration des options générales du serveur, et comment définir de nouvelles zones (domaines) pour qu'elles soient gérées par votre serveur DNS. Grâce à cela, les autres machines du réseau local ou même de l'Internet, pourront connaitre l'adresse pour accéder aux machines et services de votre propre domaine.

Le module Serveur de noms de domaine (DNS) BIND 8 de Webmin permet de créer et éditer les domaines, entrées DNS et options BIND pour les versions the 8.x et 9.x. BIND (Berkeley Internet Name Domain) est une implémentation du protocole de Système de Nom de Domaine (DNS) et propose une implémentation de référence ouverte et libre des composants majeurs dy système DNS.

BIND est particulièrement utile pour effectuer des configurations simples, malgré quelques différences entre les versions 8.x et 9.x. Vous devrez donc vous méfier particulièrement du module Webmin puisque les fonctionnalités de BIND 9.x ne sont pas encore toutes prises en charge. En conséquence, si vous tentez d'utiliser les options avancées, vous devrez surveiller les fichiers journaux (*log files*) afin de vous assurer que BIND fonctionne correctement.

Nous couvrons dans ce chapitre la configuration d'un serveur DNS pour les requêtes locales. Nous ne couvrons pas de manière explicite la configuration d'un serveur de noms public.

3.1. Installation et initalisation

Assurez vous que le paquetage `bind` est bien installé.

Arrivé à ce point, Mandriva Linux permet de configurer simplement votre serveur pour un cas très précis. Si vous ne souhaitez pas implémenter vos propres domaines avec le serveur, mais simplement l'utiliser comme relais pour vos clients locaux, il suffit d'installer le paquetage `caching-nameserver`. Celui-ci construira une configuration BIND de base, permettant qu serveur de répondre aux requêtes DNS locales pour des adresses Internet. Le serveur devra pouvoir accéder à Internet.

Une foix ce paquetage installé, démarrez le serveur en lançant la commande `service named restart` en tant que `root`. Vous pouvez alors configurer vos machines locales (*Configuration des postes client*, page 48) pour qu'elle effectuent les requêtes DNS sur votre serveur.

Pour pouvoir utiliser le module Webmin, vous devrez sélectionner la catégorie **Serveurs**, puis cliquer sur le bouton Serveur de Noms de Domaine Bind (avec le chiffre 8 dans l'icône.)

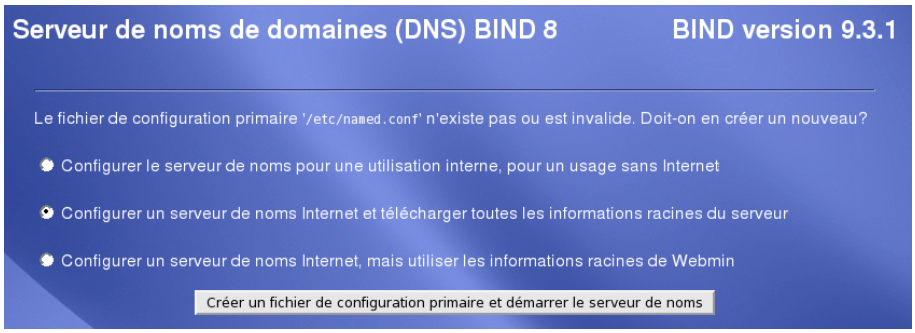


Figure 3-1. Créer un premier fichier de configuration pour Bind

La première fois que vous ouvrez ce module, et si vous n'avez pasz déjà configuré BIND, il faut choisir l'usage que vous comptez faire du serveur de noms.

Configurer le serveur de noms pour une utilisation interne, pour un usage sans Internet

Sélectionnez cette option si vous pensez n'utiliser le serveur que pour servir les requêtes du réseau local, pour les machines du réseau local. Ceci n'est utile que si le réseau n'est pas connecté à Internet.

Configurer un serveur de noms Internet et télécharger toutes les informations racines du serveur

Sélectionnez cette option si le serveur devra répondre à des reqêtes issues de ou pour des machines de l'Internet, et si le serveur est actuellement connecté à Internet.

Configurer un serveur de noms Internet, mais utiliser les informations racines de Webmin

Idem que pour l'option précédente, mais si le serveur **n'a pas accès** à Internet en ce moment.

Cliquez alors que Créer un fichier de configuration primaire et démarrer le serveur de noms pour continuer la configuration.

La page d'accueil est divisée en deux sections : les Options globales du serveur et les Zones existantes, qui vous permet d'accéder à chaque zone déjà définie, représentée par une icône, et permet de créer de nouvelles zones.

Lorsque vous changez des paramètres, que ce soit les options globales du serveur ou les zones, n'oubliez pas de cliquer sur le bouton Appliquer tous les changements pour que le serveur recharge la configuration.

3.2. Exemple de configuration

Si vous avez choisi de configurer votre serveur en tant que serveur Internet, il existe déjà un zone DNS (dans Zone existantes) ; la **Root zone** (soit la zone primaire). Ceele-ci est utilisée par le serveur DNS pour contacter le serveur central afin de résoudre les noms de domaine qui lui sont externes. À moins que votre serveur DNS ne soit utilisé dans un réseau interne exclusivement sans accès à Internet, ou si vous relayez les requêtes vers un autre serveur, il ne faut pas enlever cette zone.

3.2.1. Configuration de base du serveur et sécurité

Plusieurs paramètres peuvent être ajustés pour optimiser et sécuriser votre serveur DNS.

3.2.1.1. Definition des relais DNS

L'écran Redirection et transferts permet de lister les serveurs de noms vers lesquels rediriger les requêtes si le serveur local ne peut y répondre directement.

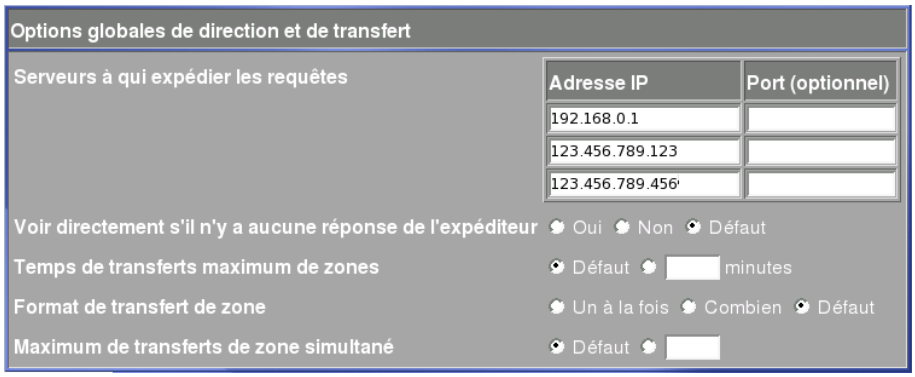


Figure 3-2. Relais DNS

Dans les champs Serveurs à qui expédier les requêtes, vous devrirez listes les adresses IP des autres serveurs de noms de votre réseau local, et au moins deux serveurs de noms Internet : ceux de votre fournisseur d'accès. Cela est susceptible de diminuer la charge du serveur et accélérer le temps de réponse.

3.2.1.2. Sécuriser le serveur

L'écran Topologie et adresses permet de définir les interfaces sur lesquelles le serveur réponds aux requêtes. Mieux vaut ne lister que les interfaces locales si le serveur n'est pas censé répondre aux requêtes externes.

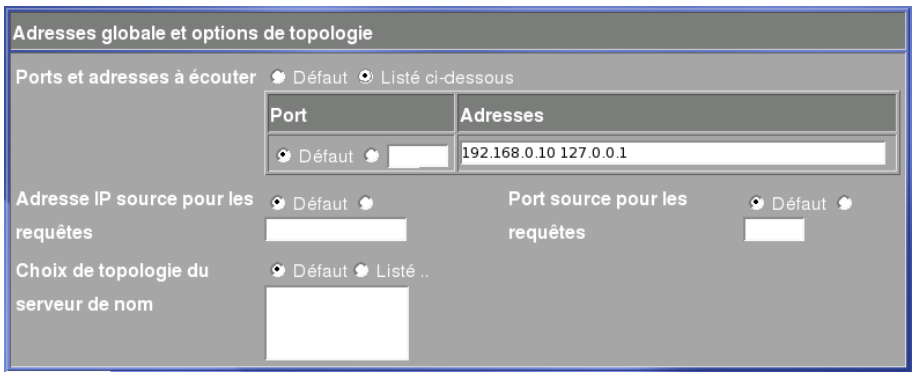


Figure 3-3. Ports et adresses à écouter

Dans le champs Adresses, entrez la liste (separée par des espaces) des adresses des interfaces du serveur sur lequel il doit répondre aux requêtes. Les requêtes faites sur d'autres interfaces seront rejetées.

Ceci ne vous dispense en aucun cas de configurer un pare-feu, indispensable de nos jour pour une installation réseau sécurisée.

3.2.2. Configuration de zones DNS simples

Pour pouvoir utiliser chaque service réseau adéquatement, vous devez créer une zone pour chacun de domaines que le serveur est censé gérer. Nous nous concentrerons ici sur les Zones existantes.

Il convient tout d'abord de créer une zone `Master 127.0.0` minimale pour décrire le réseau en boucle locale (*loopback network*). Cela est utile pour des raisons de sécurité et afin de pouvoir utiliser le serveur comme cache. Cela se réalise en deux étapes simples : création de la zone maître inverse puis configuration de l'hôte. Cliquez sur le lien Créer une nouvelle zone primaire dans l'écran d'accueil.

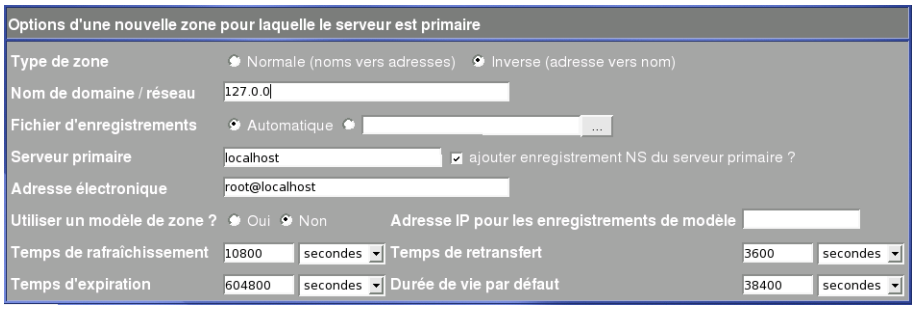


Figure 3-4. Création d'une zone maître directe

Sélectionnez le Type de zone Inverse, puis remplissez les champs Nom de domaine / réseau avec l'adresse réseau locale de l'hôte : `127.0.0` (pas de point final dot). Utilisez `localhost` pour le Serveur primaire et `root@localhost` (ou toute autre adresse) comme Adresse électronique de l'administrateur. Cliquez enfin sur Créer pour valider vos paramètres.

S'affiche alors l'écran corresponding Éditer un serveur primaire de zone. Cliquez sur l'icône Adressage inverse.

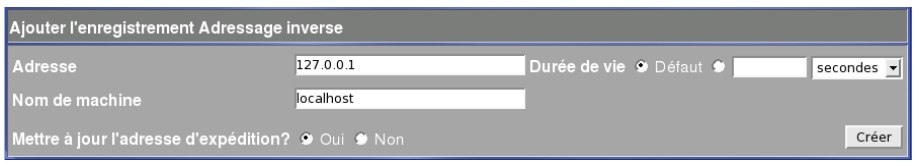


Figure 3-5. Créer un enregistrement d'adressage inverse

Remplissez les champs Adresse et Nom de machine, puis cliquez sur Créer. Votre zone locale est maintenant configurée, et vous pouvez l'oublier. Cliquez sur le lient Retourner liste de zones pour afficher l'écran d'accueil.

3.2.3. Mise en place de zones DNS spécifiques

Notre tâche est maintenant de créer la zone primaire (*Root zone*) qui décrira toutes les machines de notre réseau local. Choisissez **Créer une nouvelle zone primaire** et complétez la page, tel qu'illustré dans la figure 3-6.

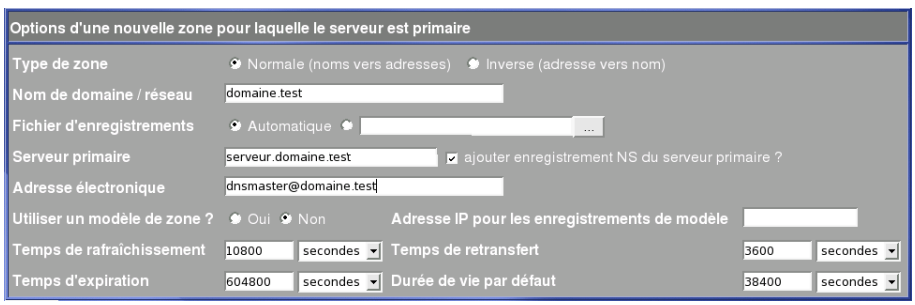


Figure 3-6. Créer une nouvelle zone primaire

Une nouvelle page s'affichera avec de nombreuses icônes : la plupart peuvent être laissées tel quel si vous n'avez pas de configurations complexes à implanter. Vous pourrez ici ajouter tous les noms de vos machines locales, mais vous devriez créer la partie inverse (*reverse*) de votre zone maître en premier lieu. En fait, une zone DNS est composée de deux parties ; la première, dite directe, pour les conversions nom-vers-adresse (*forward*) et l'autre, dite Inverse, adresse-vers-nom (*reverse*).

Puis, sélectionnez Retourner à la liste de zones et choisissez Créer une nouvelle zone primaire, mais cette fois, choisissez une zone Inverse au lieu de Normale. Plutôt que d'écrire le nom de domaine, vous spécifierez la classe réseau. Par exemple, pour la plage d'adresses 192.168.1.0/24, écrivez `192.168.1`.

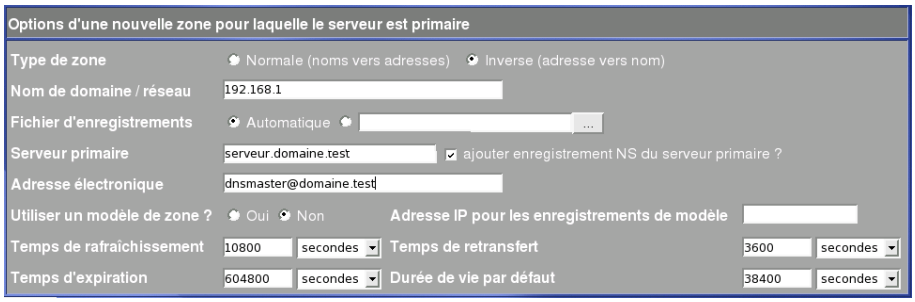


Figure 3-7. Créer une zone maître inversée (Reverse Master Zone)

Souvenez vous de cliquer sur le bouton Créer. La nouvelle zone est maintenant prête à accueillir les enregistrements pour toutes les machines ouservices du réseau local.

3.2.4. Enregistrer les postes de votre réseau

Cette étape est la seule qui doive être reproduite à chaque ajout de machine sur le réseau, tous les autres paramètres sont configurés une fois seulement, tant que votre réseau ne change pas et que vous n'ajoutez pas un second serveur DNS.

Retournez à la liste de zones, celle-ci devrait désormais en comporter quatre).

Figure 3-8. All DNS zones

Choisissez la zone domaine.test et cliquez sur l'icône Adresse. c'est ici que nous allons déclarer tous les noms machines locales et leur adresse IP.

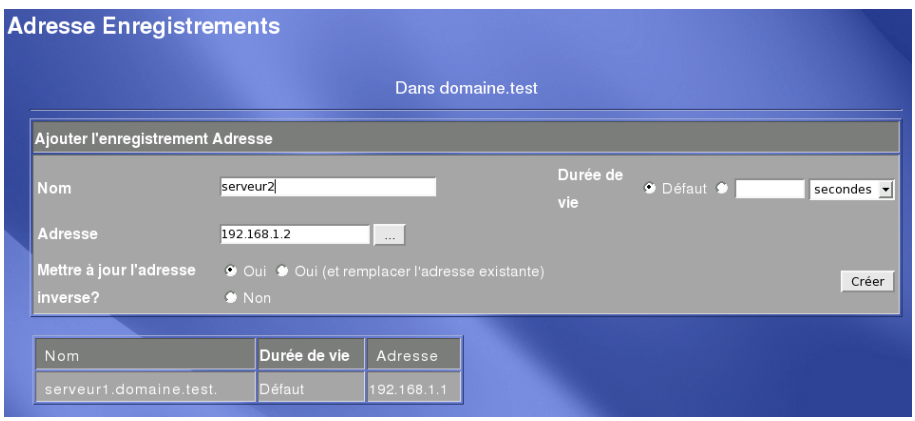


Figure 3-9. Assigner un nom à un poste de travail

Vous pouvez donc ajouter autant de noms que votre plage d'adresses IP le permet (254 dans notre exemple). Cliquez sur Créer pour ajouter le nouvel enregistrement, vous pouvez alorts en rajouter un nouveau. Notez que l'option Mettre à jour l'adresse inverse ? est sélectionnée automatiquement. Avec cette option, la partie inversée de votre adresse est configurée automatiquement.

3.2.5. Démarrage du service

Dans notre exemple, nous avons créé un DNS très simple. Pour que la nouvelle configuration soit prise en compte, revenez à la liste de zones et cliquez sur Démarrer le serveur de noms.

Webmin vérifie les paramètres que vous entrez, de sorete qu'il est difficile de corrompre la configuration de BIND. Cependant si le bouton que vous venez de presser n'est pas remplacé par un autre indiquant Appliquer les changements, ce la indique que le serveur m'a pas démarré à cause d'une erreur de configuration. Dans ce cas, nous vous conseillons de lire *Configuration avancée et résolution de problèmes*, page 48.

3.2.6. Configuration des postes client

Pour pouvoir résoudre les adresses Internet de votre réseau local, vous devez configurer les postes client du réseau pour qu'ils dirigent leurs requêtes au serveur DNS. Cela peut être fait soit grâce à l'outil de configuration réseau du Centre de contrôle Mandriva Linux, soit grâce à Webmin : allez dans la section Réseau, puis sur Configuration Réseau. Choisissez ensuite Client DNS et tapez l'adresse IP de votre serveur DNS si vous êtes sur un poste client, ou `127.0.0.1` si vous êtes sur le serveur.

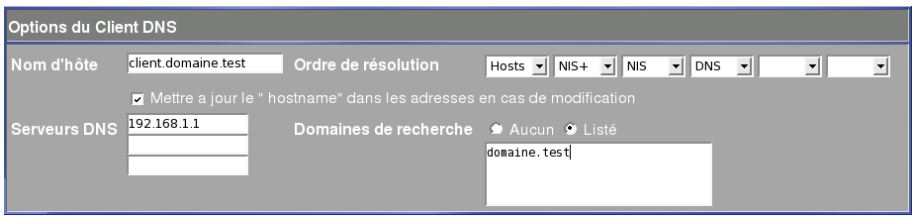


Figure 3-10. Configuration des postes client

3.3. Configuration avancée et résolution de problèmes

3.3.1. Résolution de problèmes

Si le service n'est pas démarré, consultez le fichier `/var/log/messages` pour identifier les informations vous permettant de résoudre votre problème. Si vous ne voyez pas de message d'erreur significatif, vous pouvez utiliser les programmes `named-checkconf` et `named-checkzone` pour vérifier les paramètres de votre configuration.

Dans le paquetage `bind-utils`, vous avez accès à une gamme d'outils vous permettant de tester votre configuration, et notamment `dig` qui permet de faire des requêtes avancées sur les serveurs DNS. Par exemple, pour interroger notre serveur local à propos de la machine `machine2.domaione.test`, nous pourrions exécuter :

```
$ dig serveur1.domaine.test @127.0.0.1

; <<>> DiG 9.3.1 <<>> serveur1.domaine.test @127.0.0.1
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44635
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;serveur1.domaine.test.         IN      A

;; ANSWER SECTION:
serveur1.domaine.test.  38400   IN      A       192.168.1.1

;; AUTHORITY SECTION:
domaine.test.           38400   IN      NS      serveur.domaine.test.

;; Query time: 4 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Sep  8 18:42:25 2005
;; MSG SIZE  rcvd: 77
```

3.3.2. Declarer son serveur de courrier

Si votre serveur de courrier électronique doit prendre en charge les adresses de votre propre domaine, géré par votre propre serveur DNS, alors le serveur de courrier doit être déclaré dans la configuration du domaine. De cette façon, les autres serveurs de courrier sauront quelle machine est responsable de la distribution du courrier adressé aux utilisateurs de ce domaine.

Dans l'écran principal de votre zone, cliquez sur l'icône Serveur de courrier.

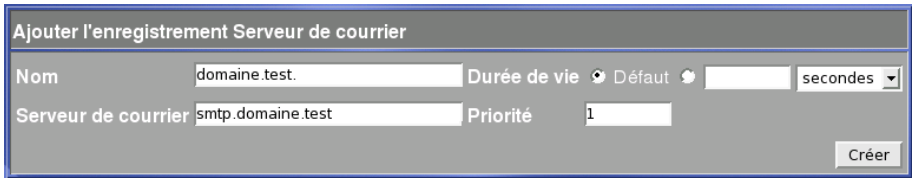


Figure 3-11. Déclarer un serveur de courrier

Remplissez le champs Nom avec le nom du domaine géré par le serveur de courrier (le même que le nom de la zone) et écrivez le nom ou l'adresse du serveur dans le champs Serveur de courrier. Assurez vous que le nom est aussi définit en tant que machine du domaine local s'il fait partie du domaine local. Vous pouvez répéter cette opération pour chacun des serveurs de courrier.

Le Nom de domaine dans le formulaire doit se terminer par un point.

Le champs Priorité (utile lorsque plus d'un serveur de courrier gèrent le même domaine) définit l'ordre dans lequel les serveurs sont contactés si l'un des serveurs à la priorité la plus élevée (numéro de priorité inférieur) est injoignable.

3.3.3. Documentation

Tout un chapitre du livre de Joe Cooper' (The Book of Webmin (`http://www.swelltech.com/support/webminguide/ch08.html`)) est consacré à BIND.

Si vous voulez en faire plus avec BIND, il est fortement recommandé de lire BIND 9 Administrator Reference Manual (`http://www.bind9.net/Bv9ARM.html`) (en anglais seulement). Ce document est aussi disponible localement : Cliquez sur le bouton Chercher dans la documentation dans la page d'accueil du module BIND, pour afficher de nombreux liens locaux et Internet. Notez que le *Manuel de référence* est disponible au format HTML en cliquant sur `bind-9.3.1/html/Bv9ARM.html`. Ce manuel est aussi disponible au formatPDF (`http://www.nominum.com/content/documents/bind9arm.pdf`). Pour finir, n'hésitez pas à consulter le site Web officiel BIND (`http://www.bind9.net/`).

Chapitre 4. Serveur Web Internet/intranet

Apache permet à votre entreprise de créer un site Web et de desservir des pages Web à des navigateurs client tels que Firefox>. Apache peut servir aussi bien des pages statiques que dynamique et utilise des technologies telles que PHP, SSL etc.

4.1. Installation

La première étape consiste à vérifier que le serveur Web Apache est installé sur votre ordinateur. Si ce n'est pas le cas, utilisez Rpmdrake ou tapez `urpmi apache-mpm-prefork` dans une terminal en tant que `root`.

La version Mandriva Linux de la distribution Apache est largement modulaire et permet d'ajouter exactement les fonctionnalités désirées. Le nom des paquetages de modules sont de la forme `apache-mod_xxx`, où `xxx` est le nom du paquetage en question. Assurez vous donc d'installer aussi les modules dont vous auriez besoin.

La configuration serveur est faite à travers le bouton Serveur Web Apache. Vous le trouverez dans la catégorie Serveurs (accessible depuis l'onglet du même nom).

4.2. Exemple de configuration

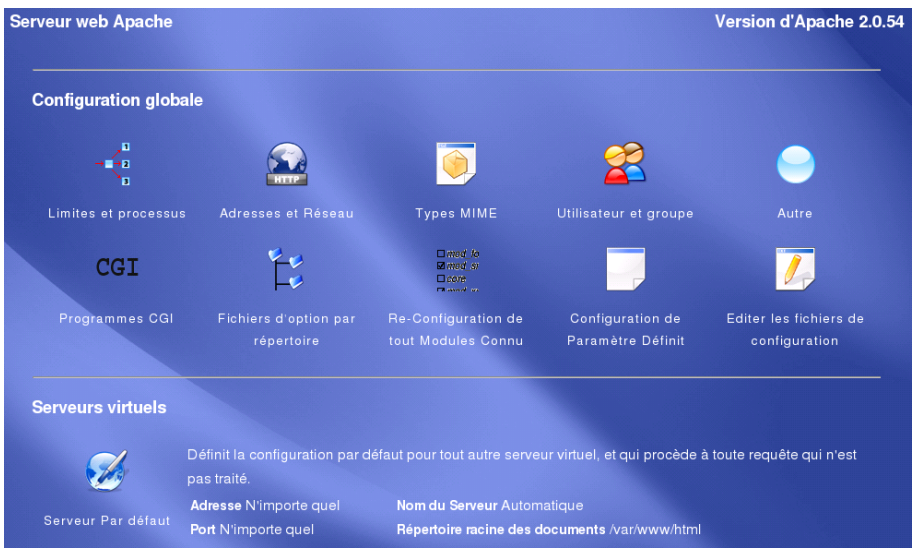


Figure 4-1. Écran principal du module Apache dans Webmin

Vous pouvez héberger plusieurs sites sur un unique serveur Apache : Cette fonction est connue sous le nom de « Serveurs virtuels ». Votre « site principal » est le Serveur par défaut. Les options Configuration Globale s'appliquent à tous les serveurs virtuels. Les options pour chaque serveur virtuel se trouvent dans la section Serveurs virtuels. Nous parlerons des options globales dans *Configuration avancée*, page 53.

Les fichiers de configuration d'Apache se trouvent dans le répertoire `/etc/httpd/conf/`. Les options principales de trouvent dans le fichier `/etc/httpd/conf/httpd.conf` et peuvent être modifiées à partir de l'icône Serveur par défaut.

4.2.1. Options générales du serveur par défaut

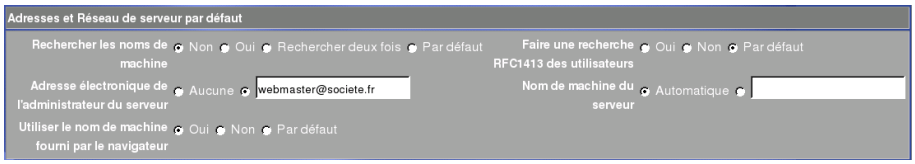


Figure 4-2. Options de réseau et adressage

La section Adresses et réseau contient certaines options importantes. Vous pouvez y spécifier l'adresse de courriel du webmestre dans le champ Adresse électronique de l'administrateur du serveur. Pour éviter les fausses requêtes sur votre serveur Web, configurez les options suivantes : Rechercher les noms de machinet à Oui et Utiliser le nom de machine fourni par le navigateur, à Non.

L'activation de la recherche des noms de machine afin de rendre votre site Web plus sûr a un coût élevé en matière de performance. Une requête DNS est effectivement effectuée à chaque requête sur votre serveur Web.

Tous les accès, erreurs et autres opérations sont enregistrés dans un fichier journal dans le répertoire `/var/log/httpd/`. Ces options de journalisation sont disponibles dans la section Fichier log (*Log File* ou fichier journal) : où envoyer les événements (le système de journaux centralisés, un fichier journal spécifique ou un programme), le format des entrées, etc. n'hésitez pas à explorer les différents options.

Cliquez maintenant sur l'icône Options des documents.

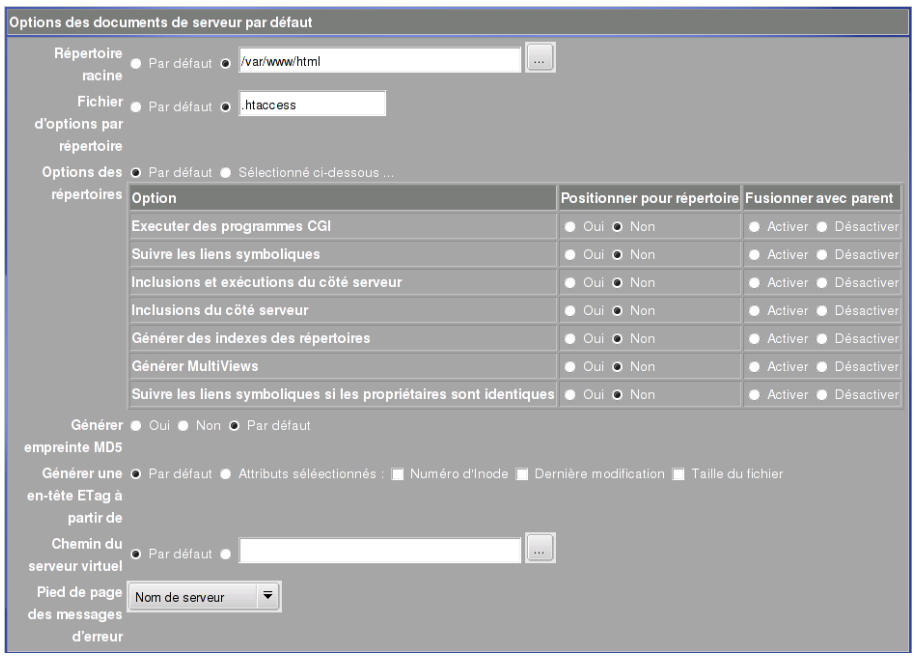


Figure 4-3. Options des documents

Le Répertoire racine est le chemin vers le répertoire contenant les pages Web de votre site. Le champ Options des répertoires contient des options communes pour votre serveur Web, comme la possibilité d'exécuter un programme CGI ou de générer automatiquement un index des fichier du répertoire ci celui-ci ne comporte pas de fichier index spécifique (Generate directory indexes).

Si vous avez une arborescence complexe de répertoires contenant vos pages Web, vous pouvez simplifier la navigation en créant des alias dans Alias de répertoires de documents statiques.

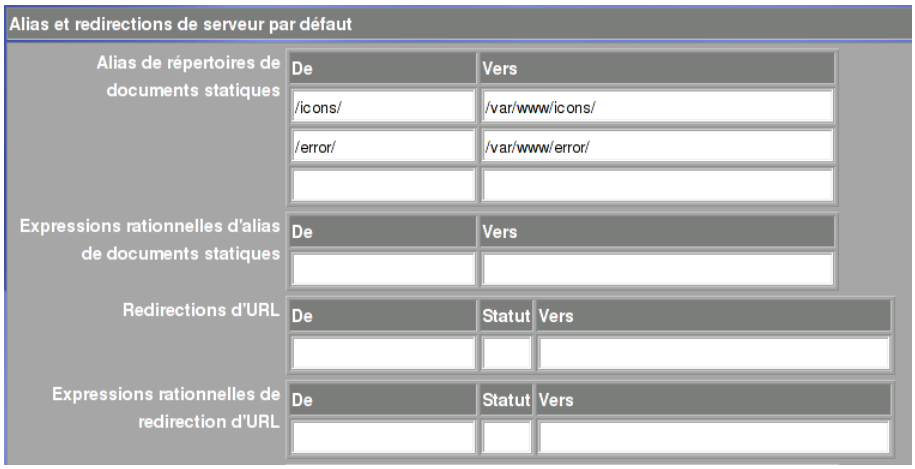


Figure 4-4. Section « Alias et redirections »

L'exemple figure 4-4 montre comment il est possible de faire pointer le navigateur sur `http://www.example.com/mores` au lieu de `http://www.example.com/foo/bar/again/and/more`. La deuxième partie de l'écran est dédiée aux redirections, qui permet de rediriger toute une arborescence.

4.2.2. Options spécifiques à quelques technologies courantes

4.2.2.1. CGI

Si vous pensez utiliser des programmes de Common Gateway Interface (CGI), la section Programmes CGI permet de spécifier quel répertoire contiendra ces CGIs, et de configurer certaines variables à attribuer aux exécutables. Les valeurs par défaut permettent d'utiliser directement vos script CGI dans votre site Web.

4.2.2.2. SSL

SSL permet d'établir un canal de communications cryptées afin de rendre votre site Web plus sûr. Vous pouvez activer SSL simplement en installant le paquetage `apache-mod_ssl`.

Votre serveur sera alors prêt à utiliser des communications cryptées avec SSL, en utilisant le préfixe `https://` au lieu de `http://`.

Pour l'heure, la version standard d'Apache ne prends en charge qu'un seul site en SSL par adresse IP. Si vous aviez besoin d'héberger plusieurs sites sécurises sur la même adresse IP, il faudra alors installer le paquetage `apache-ssl` à la place. Notez cependant que l'architecture de ce serveur (et notamment en ce qui concerne les fichiers de configuration) diffère des autres serveurs.

4.2.2.3. PHP

Il suffit d'installer le paquetage `apache-mod_php` afin que vos pages PHP puissent être interprétées.

4.2.3. Options par répertoire

Si vous cliquez sur le nom d'un répertoire, vous pouvez spécifier les mêmes options générales pour chaque répertoire. Par exemple, vous pouvez configurer des Types MIME pour votre répertoire de téléchargement, ou le Contrôle d'accès pour un répertoire spécifique, etc.

4.3. Configuration avancée

Les options dont nous traitons dans cette section sont accessibles depuis l'index des modules Apache de Webmin.

4.3.1. Limites et processus

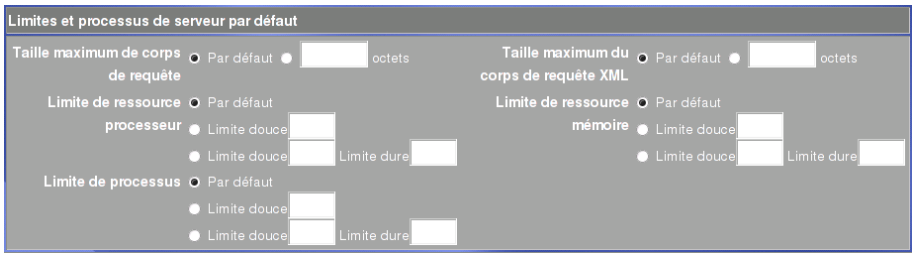


Figure 4-5. L'écran de configuration des processus d'Apache

Il est possible de régler finement la consommation des ressources système par Apache. Vous pouvez configurer le nombre initial de processus d'Apache (Nombre initial de processus et Nombre maximum de processus en attente), la taille des en-têtes et d'une ligne de requête (Entêtes maximum dans une requête et Taille maximum d'une ligne de requête) ou le nombre de clients par processus (Requêtes maximum par processus du serveur).

4.3.2. Adresses et Réseau

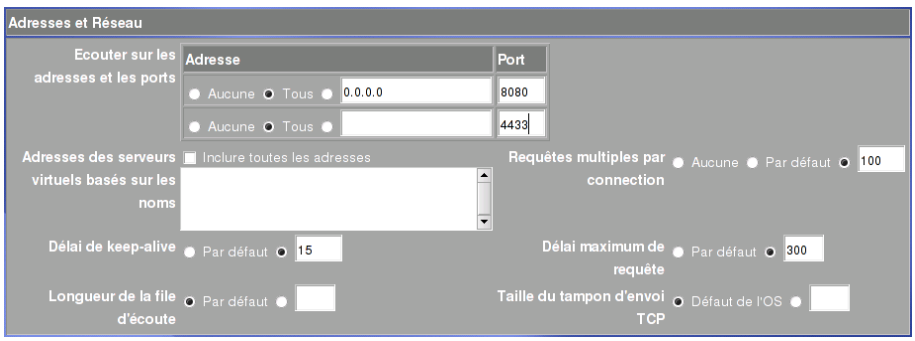


Figure 4-6. Changement des ports sur lesquels Apache écoute

figure 4-6 montre comment il est possible de spécifier les ports qu'Apache écoute pour les sessions standard (`80` par défaut, `8080` dans notre exemple) et cryptées (respectivement `443` et, `4433`).

4.3.3. Contrôle d'accès par authentification simple

L'authentification d'une personne implique généralement l'utilisation d'un identifiant et d'un mot de passe, mais peut inclure aussi d'autres méthodes pour prouver son identité. Vous pouvez contrôler l'accès à certaines parties (répertoires) de votre site en utilisant un fichier de mots de passe contenant une liste de paires identifiant / mot de passe. Voici la procédure pour mettre en place ce mécanisme :

1. Créer un fichier de mots de passe et le remplir.
2. Protéger un répertoire spécifique en créant les directives de configuration idoines faisant référence au fichier de mots de passe.

Imaginons que vous souhaitiez contrôler l'accès au répertoire `/var/www/html/restricted/`.

Pour créer le fichier de mots de passe, tapez `htpasswd -c -m path_to_the_password_file username` dans une console, en tant que `root`. l'option `-c` est utilisée la première fois pour créer le fichier.

```
# htpasswd -c -m /etc/httpd/.htpass queen
```

```
New password: verySecret
Re-type new password: verySecret
Adding password for user queen
```

L'exemple ci-dessus crée le fichier `/etc/httpd/.htpass` contenant le mot de passe (`verySecret`) pour l'utilisateur `queen`. Bien entendu, `verySecret` sera crypté.

Pour optimiser la sécurité, mieux vaut enregistrer le fichier de mots de passe **en dehors** du répertoire des documents Web, et s'assurer que ses droits d'accès sont aussi stricts que possible.

Une fois que les utilisateurs ont été ajoutés au fichier de mots de passe , vous devez indiquer à Apache de l'utiliser. Dans la configuration du serveur (Serveur par défaut par exemple) contenant le répertoire à protéger, un petit formulaire permet de créer des options spécifiques à des répertoires.

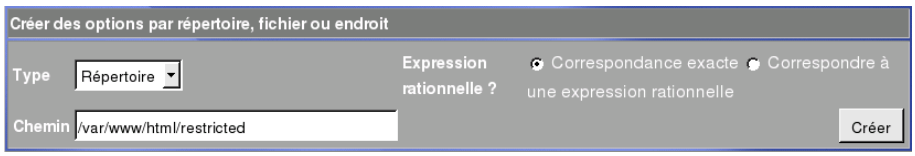


Figure 4-7. Options par répertorie

Une fois cela fait, une icône Directory /var/www/html/restricted apparaît dans la section Options par répertoire. Cliquez dessus, puis sur le bouton Contrôle d'accès sur cette nouvelle page. Vous pourrez alors remplir le formulaire en utilisant l'exemple donné ici (figure 4-8) comme guide.

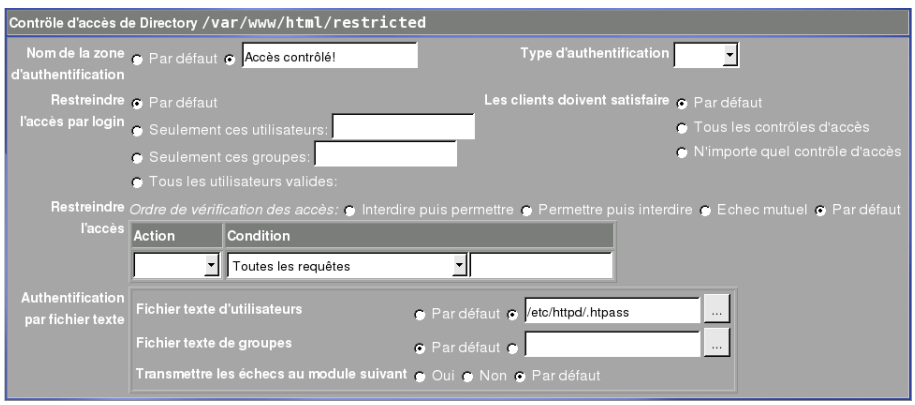


Figure 4-8. Options par répertoire

4.3.4. Servir plusieurs domaines avec un seul serveur

Lorsque vous configurez des hôtes virtuels, le premier d'entre eux reçoit les requêtes qui ne correspondent à aucun autre.

Vous pouvez configurer un serveur Web à domaines multiples grâce au formulaire situé au bas de la section Serveurs virtuels.

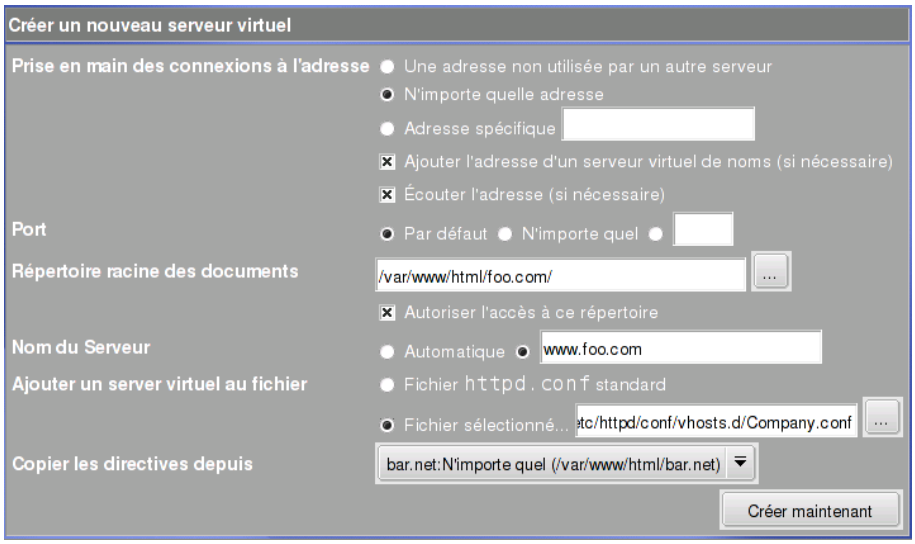


Figure 4-9. Création d'un nouveau serveur virtuel s'appuyant sur un serveur existant

Par exemple, votre société possède les domaines `foo.com` et `bar.net`. Il suffit de spécifier la racine des documents (l'endroit où les fichiers de chaque site sont enregistrés), et le nom du serveur virtuel. Si vous gérez de nombreux sites, vous pouvez copier les directives de configuration de l'un à l'autre (voir figure 4-9). Cela peut faire gagner beaucoup de temps.

Nous utilisons ici la technique ■ hôtes virtuels d'après le nom ■ (■ Name based virtual hosts ■), c'est à dire que nous hébergeons plusieurs serveurs sur la même adresse IP. Afin que cela fonctionne, il convient d'ajouter un directive particulière dans le fichier de configuration principal d'Apache, à l'aide de la commande suivante :

```
# echo "NameVirtualHost *:80" >> /etc/httpd/conf/httpd.conf
```

N'oubliez pas de redémarrer le serveur en cliquant sur le bouton Appliquer tout changement.

Bien entendu, votre serveur de noms (*BIND : serveur DNS*, page 43) devra être configuré de manière à ce que les requêtes sur le nom de domaine (`www.foo.com`), soit dirigées sur la machine qui héberge le site Web.

Chaque serveur virtuel propose des options similaires à celles vues ci-dessus, mais tous partagent un processus parent Apache commun.

4.4. Documentation supplémentaire

Joe Cooper consacre un long chapitre de son livre à Apache dans The Book of Webmin (`http://www.swelltech.com/support/webminguide/ch07.html`). Vous trouverez là des explications pour presque toutes les options disponibles dans le module Apache de Webmin, même si ce livre est relativement ancien.

C'est aussi une bonne idée de consulter le Apache Documentation Project (`http://httpd.apache.org/docs-project/`). Si vous installez le paquetage `apache-doc`, vous pourrez aussi accéder à la documentation Apache sur votre propre système dans le répertoire `/usr/share/doc/apache-doc-*/` ou en pointant votre navigateur sur http://localhost/manual/ (`http://localhost/manual/`).

Chapitre 5. Le serveur de courrier Postfix

Avec Postfix, vous pouvez configurer un serveur de courrier électronique qui vous permettra d'envoyer et de recevoir du courrier. Celui-ci peut communiquer directement avec d'autres serveurs de courrier sur Internet à travers le protocole SMTP. Avec une configuration appropriée, Postfix peut gérer l'ensemble des courriers d'une organisation.

5.1. Fonctions d'un serveur SMTP

Un serveur SMTP (*Simple Mail Transfer Protocol*) peut être comparé à un bureau de tri postal. Le bureau reçoit des lettres du quartier et les trie. Si une lettre s'adresse à quelqu'un habitant le quartier, elle sera déposée dans sa boîte aux lettres. Sinon, la lettre sera envoyée au bureau postal correspondant à l'adresse du destinataire. La même procédure a lieu lorsqu'une lettre d'un autre bureau de poste est relayée.

Les opérations d'un serveur de courrier Postfix standard sont très similaires : il reçoit des courriers électroniques provenant des utilisateurs du réseau local et depuis d'autres serveurs, lesquels ont identifié votre serveur de courrier comme celui étant responsable de la prise en charge des courriers électroniques adressés à un nom de domaine spécifique. Le serveur lit l'adresse du destinataire, puis :

- Si le nom de domaine correspond à celui desservi localement, le courrier sera stocké dans la boîte aux lettres correspondante. Ensuite, l'utilisateur devra prendre ses messages à travers un client de courriel. La livraison des messages aux utilisateurs se fait à travers un autre protocole (*Serveurs de remise de courrier : POP et IMAP*, page 63).
- Sinon, le serveur cherche sur Internet le serveur responsable de la livraison des courriers adressés à ce nom de domaine, puis les lui transfère.

5.2. Installation

Assurez-vous que Postfix est bien installé sur votre machine.

La configuration du serveur s'effectue à partir de l'icône Configuration de Postfix, que vous trouverez sous l'onglet Serveurs.

Si le serveur de courrier est destiné à recevoir les messages d'un domaine spécifique en provenance d'autres serveurs, il devra être configuré ainsi dans la configuration du DNS, soit sur votre serveur DNS local (*BIND : serveur DNS*, page 43) ou sur le site de votre fournisseur de nom de domaine.

5.3. Exemple de configuration

Chaque option de Postfix contenue dans Webmin est documentée. Il vous suffit de cliquer sur le nom d'une option et une nouvelle fenêtre apparaîtra, détaillant l'option en question.

Figure 5-1. Écran de démarrage du module Postfix

Les fichiers de configuration de Postfix sont dans le répertoire `/etc/postfix/`. Les options principales de Postfix que vous devez modifier se trouvent dans le fichier `/etc/postfix/main.cf` et peuvent être modifiées en cliquant sur la première icône : Options générales.

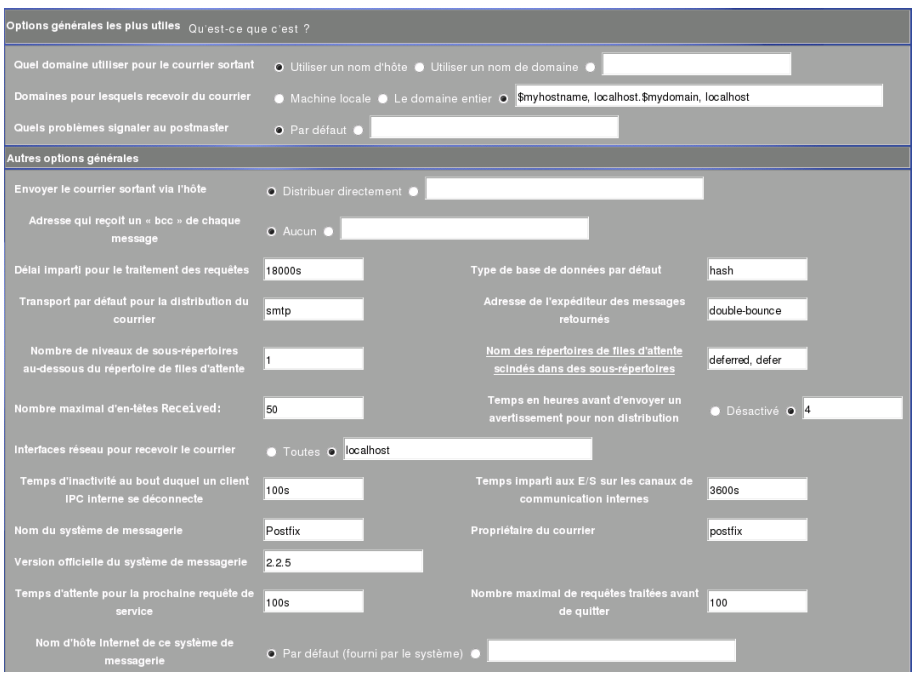


Figure 5-2. L'écran principal de configuration de Postfix

Dans cette section vous devrez configurer les options suivantes :

- La première option (Quel domaine utiliser pour le courrier sortant) concerne le courrier sortant. Vous devriez y spécifier le nom de domaine. Laissez la valeur par défaut (Utiliser le nom de machine) si le nom de domaine de votre serveur est le même que votre nom de domaine de courrier électronique.
- Domaines pour lesquels recevoir le courrier. Ce paramètre est associé au courrier entrant. Vous devriez spécifier les domaines de courrier pour lesquels votre serveur est responsable. Réglez-le à Tout le domaine si votre

ordinateur possède la même valeur que le nom de votre domaine de courrier. Sinon, cochez la troisième option et entrez la liste des domaines dont il a la charge, ainsi que tous les noms que le serveur peut avoir, incluant `$myhostname` et `localhost.$mydomain`, séparés par des virgules.

- Envoyer le courrier sortant via la machine. Cette option est utile si vous accédez à Internet à travers un ISP qui vous fournit un serveur de courrier. Si tel est le cas, vous pouvez choisir de l'utiliser en tant que relais pour répartir vos propres messages à leurs destinataires, ce qui réduira la charge de votre serveur. Toutefois, il est impératif que vous ayez confiance en l'intégrité de votre ISP. Ensuite, tapez le nom du serveur de courrier de votre ISP : `smtp.fournisseur.net` par exemple.
- Nom de machine (hostname) de ce système. Ce paramètre spécifie le nom d'hôte Internet de votre serveur de courrier. La valeur par défaut correspond au FQDN (*Fully-Qualified Domain Name*), soit au nom de domaine qualifié. Par exemple, `passerelle.exemple.com`. Laissez la valeur par Défaut (donné par le système) si votre nom d'hôte est de la forme `nom_machine.nom_domaine_mx`.
- Nom de domaine internet local. Cette option spécifie le nom de domaine Internet local. La valeur par défaut est `$myhostname` auquel on enlève le premier composant. Pour notre exemple, ce serait `exemple.com`. Laissez la valeur par Défaut (donné par le système) si votre nom d'hôte est de la forme `nom_machine.nom_domaine_mx`.
- Réseaux locaux. Ce paramètre est utilisé pour identifier les machines auxquelles vous pouvez faire confiance pour faire le relais de courrier à travers votre serveur de courrier. Les messages provenant de ces machines et se dirigeant vers d'autres serveurs sur le Net seront acceptés et transférés sans restriction. Voici des valeurs typiques à utiliser : `192.168.1.0/24, 127.0.0.0/8`, ce qui signifie que vous acceptez que votre machine locale relaie le courrier, tout comme les systèmes dont l'adresse figure dans l'étendue d'adresses `192.168.1.1-254`. Assurez-vous de spécifier uniquement les réseaux voulus de façon à éviter d'être la cible de polluposteurs (*spammers*) indésirables.

La section Alias de courrier vous aidera à configurer la redirection de courrier vers des boîtes aux lettres existantes et valides. Comme vous pourrez le voir dans le tableau de cette section, plusieurs alias par défaut existent et convergent tous, possiblement après quelques « sauts », vers l'adresse `postfix`. Il est recommandé d'ajouter un alias pour que cette adresse pointe vers votre compte personnel afin que les messages envoyés à un des alias définis (incluant les messages pour root, comme les alertes système) vous soient vraiment transférés, au lieu d'être stockés localement dans la boîte de courrier de l'utilisateur `postfix`.

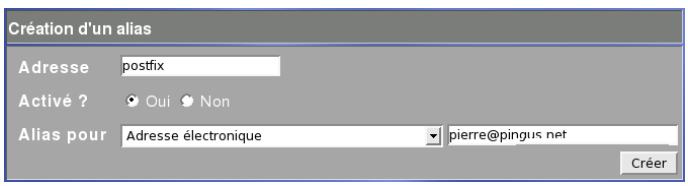


Figure 5-3. Définir un nouvel alias de courrier

Afin de conclure la configuration de base du serveur, il peut être intéressant de jeter un œil à la page Contrôle des ressources. Deux options sont intéressantes :

Taille max d'un message

> Configure la taille maximale (en octets) des courriels acceptés par Postfix. Cette valeur est la taille du message complet, incluant les en-têtes et les pièces jointes. Prenez en compte que le logiciel de courrier électronique encodera les pièces jointes non texte. Donc, la taille totale du message sera plus grande que la taille des pièces jointes lorsque téléchargées sur votre disque dur.

Taille max des messages rebond (bounced)

> Lorsque Postfix ne peut pas livrer le courrier à son destinataire final, il envoie une notification de non-livraison à l'expéditeur original. Cette notification contiendra la cause d'erreur et une partie du message original (vous pouvez configurer la taille du message original à inclure). Ce paramètre indique la taille (en octets) du texte à inclure.

5.4. Configuration avancée

La section Options Générales contient beaucoup de champs, dont voici les plus intéressants. Si vous voulez garder une trace de tous vos messages, ajoutez une adresse dans Adresse qui reçoit un bcc de chaque message. Vous pouvez aussi spécifier le délai avant d'envoyer un avertissement de non-livraison dans Temps en heures avant d'envoyer un avertissement pour non-livraison. Les autres options sont spécifiques à chaque système et ne sont pas cruciales pour la configuration de Postfix. Ne changez ces paramètres seulement si vous comprenez pleinement leur signification.

5.4.1. Mise en correspondance d'adresse

Dans la section Correspondances canoniques, vous pouvez identifier une table d'équivalence qui permet de réécrire les en-têtes de messages gérées par Postfix. Par exemple, dans le champ Tables de correspondances canoniques, vous pourriez associé le nom d'un employé à son adresse de courriel : `John.Doe@exemple.com` et `jdoe@exemple.com`.

5.4.2. Mise en correspondance des domaines virtuels

Si vous desservez plus d'un domaine de courrier avec un même serveur, vous devrez peut-être configurer des Domaines virtuels additionnels. En effet, si vous gérez les courriers des domaines `pingus.org` et `icy.org`, les courriers envoyés à `pierre@pingus.org` et à `pierre@icy.org` seront livrés dans la même et unique boîte aux lettres de `pierre`. Si c'est la même personne, il n'y a évidemment pas de problème. Mais si ce sont deux personnes différentes, les messages devront être livrés à deux comptes de courrier différents.

Premièrement, vous devrez spécifier la Tables de correspondances de domaines. Vous devez taper `hash:/etc/postfix/vir` et cliquer sur Sauvegarder et Appliquer. La prochaine étape est de créer un nouvelle table de correspondance en cliquant sur Nouvelle entrée. Par exemple, nous pouvons vouloir attribuer les messages adressés à `pierre@icy.org` à l'utilisateur local `icypierre`, au lieu de `pierre`.

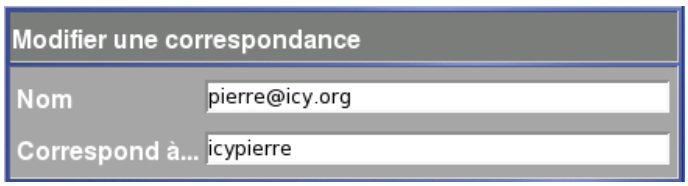


Figure 5-4. Configurer des domaines virtuels

De cette façon, vous pouvez rediriger le courrier d'utilisateurs isolés, d'usagers d'autres domaines ou serveurs, ou même, un domaine entier vers un seul utilisateur.

5.4.3. D'autres options diverses

La section Livraison du courrier contient des options qui peuvent vous aider à configurer la gestion des courriers après que Postfix les ait reçus.

Dans Options du serveur SMTP, vous pouvez prévenir la réception de pourriels (*spam*) en configurant Domaines DNS pour la recherche de blacklist. Certains serveurs Internet utilisent un serveur DNS qui possède des adresses sur une liste noire. Ceux-ci relaient des pourriels. En configurant cette option, Postfix vérifie dans cette base de données avant d'accepter le courrier.

Si LDAP est installé sur votre système, vous pouvez accéder et configurer les options dans la section Recherches LDAP.

Enfin, vous pouvez utiliser la section de Réécriture et masquage d'adresses pour cacher toutes les machines à l'intérieur de votre réseau local derrière la passerelle de courrier, et faire croire que tout le courrier provient de la passerelle elle-même et non pas de machines individuelles. Notez que cette option est activée par défaut.

5.4.4. Accès aux boîtes aux lettres

Enfin, la section User Mailboxes vous permet de naviguer à travers les boîtes aux lettres locales. Par exemple, vous pourriez vouloir y faire des tâches d'entretien en manipulant des messages.

Il peut être intéressant d'avoir accès aux messages d'un utilisateur si ce dernier ne peut plus accéder à sa boîte aux lettres, ou pour effacer des pièces jointes énormes qui surchargeraient l'ordinateur.

Si vous utilisez cette fonctionnalité, gardez à l'esprit votre sens de l'éthique et n'abusez pas de vos droits d'administrateur en lisant les messages de vos utilisateurs...

5.5. Pour en savoir plus

Un long chapitre traite de Postfix dans The Book of Webmin (`http://www.swelltech.com/support/webminguide/ch10.html`) écrit par Joe Cooper. Vous trouverez des explications pour presque toutes les options disponibles dans le module Postfix de Webmin.

C'est également une bonne idée de lire les Postfix Documentation pages (`http://www.postfix.org/docs.html`) (en anglais). Vous pouvez aussi accéder à cette documentation dans le répertoire `/usr/share/doc/postfix-*/`.

Chapitre 6. Serveurs de remise de courrier : POP et IMAP

En utilisant POP (*Post Office Protocol*) ou IMAP (*Internet Message Access Protocol*), un utilisateur peut accéder à sa boîte aux lettres électronique et récupérer ses courriels de façon à pouvoir les lire sur sa machine locale.

6.1. Avant-propos, installation

Si vous avez fait une installation standard de Mandriva Linux, les serveurs d'accès au courrier (POP3 ou IMAP) sont démarrés à la demande : dès qu'une requête est reçue sur un port POP3 ou IMAP, le programme approprié pour répondre à la requête est lancé.

Un utilisateur POP3 récupère ses courriels sur son poste, d'où il peut ensuite les lire avec un logiciel comme KMail ou Evolution. Par contre, le protocole IMAP permet aux utilisateurs de laisser leur courrier électronique sur le serveur pour une gestion à distance. IMAP est particulièrement adapté aux utilisateurs mobiles. Du côté de l'administrateur système, il devra vérifier régulièrement l'état de son espace disque, puisque les courriers IMAP consomment habituellement beaucoup d'espace sur le serveur. Une politique de quota d'espace peut également être mise en place.

Assurez vous que le paquetage `imap` est bien installé.

6.2. Exemple de configuration

La première étape consiste à décider avec les utilisateurs du service qu'ils souhaitent utiliser : POP, IMAP ou les deux. Mieux vaut ne configurer et activer que les services qui seront effectivement utilisés.

En cliquant sur Services Internet étendus, vous verrez une liste de services accessibles sur votre poste gérés par xinetd. Ces services peuvent être activés ou non.

	Nom de service	Type	Port / numéro	Protocole	Utilisateur	Programme du serveur	Activé ?
☐	ftp	Internet	21	TCP	root	/usr/sbin/in.ftpd	Non
☐	ssh	Internet	22	TCP	root	/usr/sbin/sshd	Non
☐	imap	Internet	143	TCP	root	/usr/sbin/imapd	Non
☐	imaps	Internet	993	TCP	root	/usr/sbin/imapsd	Non
☐	pop2	Internet	109	TCP	root	/usr/sbin/ipop2d	Non
☐	pop3	Internet	110	TCP	root	/usr/sbin/ipop3d	Oui
☐	pop3s	Internet	995	TCP	root	/usr/sbin/ipop3sd	Non

Figure 6-1. Écran de démarrage du module xinetd

Chacun des protocoles POP et IMAP possède un équivalent sécurisé, POP3S et IMAPS, qui chiffrent les données lors de la transmission. Si les utilisateurs sont amenés à consulter leur courrier sur Internet (et non pas uniquement depuis le réseau local), il est plus sûr d'utiliser les protocoles sécurisés et de désactiver les autres. Assurez-vous alors que les clients de courrier électronique permettent l'utilisation de ces protocoles.

Le paquetage `imap` installe les services et démarre le serveur POP avec les options par défaut. Cliquez sur un service pour le configurer et contrôler son état.

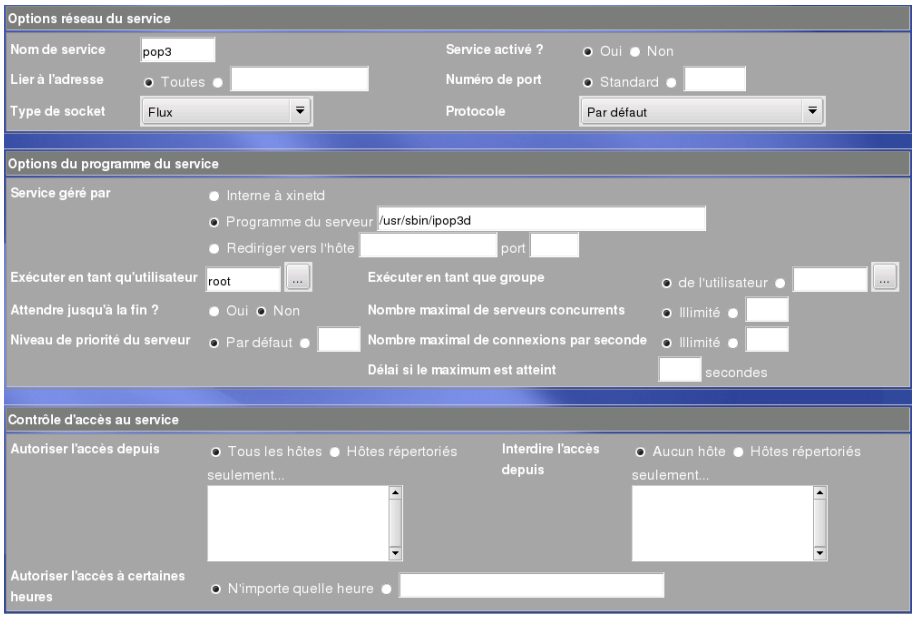


Figure 6-2. Configuration du module POP3

Pour qu'un service soit activé, choisissez Oui dans la case Service activé ?. Ensuite, vous pouvez restreindre l'accès à ce service dans le : Contrôle d'accès au service. Ajoutez les adresses IP des postes ayant accès au service dans la case Permettre l'accès depuis et sélectionnez Machines listées seulement.

Puis, cliquer sur Sauvegarder pour enregistrer vos changements et, sur la page précédente, cliquez sur Appliquer les changements pour que xinetd prenne en compte la nouvelle configuration.

Cet écran de configuration est le même pour tous les services gérés par xinetd.

6.3. Configuration avancée

De nombreuses options existent mais ne sont pas requises pour une configuration standard. Dans la section Options réseau du service, les options Lier à l'adresse et Numéro de port permettent de forcer le service à écouter sur un couple spécifique adresse/port. Si vous avez de nombreuses interfaces réseau et que vous voulez faire circuler le trafic de courrier sur une interface spécifique, vous pouvez le spécifier ici en entrant son adresse IP.

Dans la table intitulée Options du programme du service, vous pouvez rediriger toutes vos requêtes vers un autre système. Dans le champ Service effectué par, choisissez Rediriger vers la machine et entrez l'adresse IP et le port de la machine. Les options Exécuter en tant qu'utilisateur et Exécuter en tant que groupe permettent d'exécuter le service sous un nom d'utilisateur spécifique.

Xinetd permet également de définir des limites ou des quotas pour chaque service. L'option Nombre maximal de serveurs concurrents détermine le nombre maximum de démons qui peuvent être exécutés en concurrence. Pour sa part, le champ Nombre maximum de connexions par seconde spécifie le nombre de requêtes que pourra soutenir le serveur en même temps. Si le nombre maximum est atteint, alors l'option Délai si le maximum est atteint établit l'intervalle en secondes avant que le serveur soit de nouveau accessible. Dans notre exemple avec POP3, vous pourriez décider que seulement trois serveurs peuvent être démarrés pour répondre à 5 connexions par seconde, ce qui peut être utile pour des serveurs surchargés.

La dernière option très utile est Niveau de nice pour le serveur (« niveau de gentillesse ») qui indique la priorité du programme à l'échelle du système. Si plusieurs services sont disponibles sur le même serveur, et que certains d'entre eux sont plus importants que d'autres, cette option permet de demander au système d'allouer plus de ressources aux processus critiques. Le Niveau de nice est à `0` par défaut et peut prendre des valeurs entre `-20` (la plus haute priorité) et `19` (la plus basse). Si vous considérez que le service POP3 est de moindre importance par rapport aux autres services hébergés sur cette machine, vous pouvez lui assigner un niveau de « nice » de `10`, par exemple.

Chapitre 7. Partage de ressources

7.1. Samba : intégrer Linux dans un réseau Windows

Le serveur Samba permet d'intégrer facilement un système Mandriva Linux dans un réseau hétérogène. À travers Samba, votre ordinateur peut être vu dans le réseau d'autres utilisateurs et agir en tant que serveur Microsoft Windows® en partageant des fichiers, des comptes d'utilisateurs distants, des imprimantes, etc.

7.1.1. Installer Samba

Vérifiez que le paquetage `samba-server` est installé sur votre système.

La configuration du serveur se trouve dans l'outil Partage de fichiers Windows avec Samba de la catégorie Serveurs.

7.1.2. Exemple de configuration

Figure 7-1. La fenêtre principale du module de Samba

Les fichiers de configuration de Samba sont enregistrés dans `/etc/samba/`. Les options Samba principales sont situées dans le fichier `/etc/samba/smb.conf` et sont accessibles par l'icône Réseau Windows.

Samba recharge sa configuration chaque minute, il n'est donc pas nécessaire de redémarrer le serveur Samba pour chaque changement de configuration.

7.1.2.1. Configuration générale

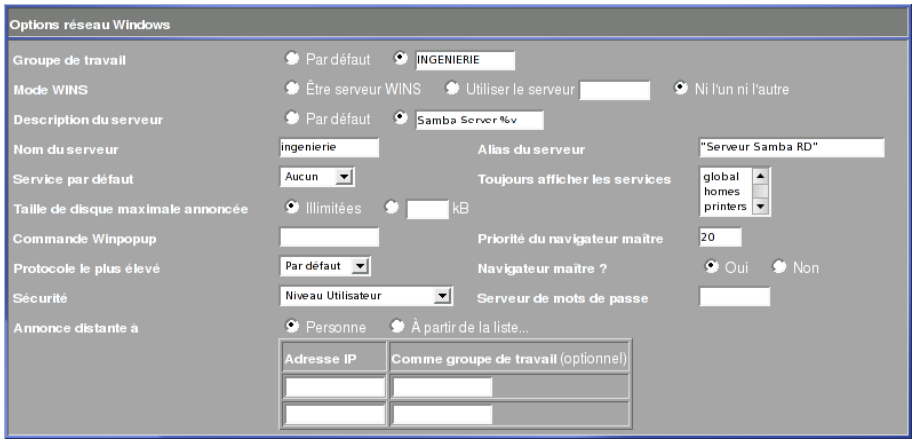


Figure 7-2. Configurer les options communes de réseau

Définissez un Groupe de travail pour votre serveur (`RetD` dans notre exemple). De plus, vous pouvez modifier le Nom du serveur et la Description du serveur. Vous pouvez aussi demander au serveur Samba de se comporter comme le serveur WINS de votre réseau grâce à l'option Mode WINS[1] Ensuite, sélectionnez le niveau de sécurité Niveau Utilisateur et validez votre choix en cliquant sur Sauvegarder (voir figure 7-2).

7.1.2.2. Méthode d'authentification

Figure 7-3. Configurer la méthode d'authentification pour les clients Windows 95

Si vous voulez utiliser un serveur de fichiers avec un client Windows® 95, vous devez modifier une valeur par défaut dans la section Authentification : réglez Utiliser des mots de passe chiffrés ? à Non tel qu'illustré dans la figure 7-3.

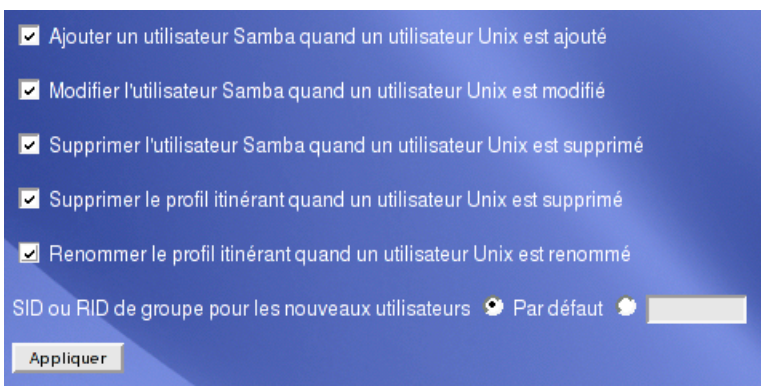


Figure 7-4. Synchronisation des utilisateurs Samba et Unix

Si votre réseau ne comporte pas de clients Windows® 95, cliquez sur l'icône Configurer la synchronisation automatique d'Unix et de Samba, cochez chacune des options comme montré (figure 7-4) et cliquez sur le bouton Appliquer.

Pour ajouter les utilisateurs actuels Linux du système en tant qu'utilisateur Samba, cliquez sur Convertir les utilisateurs Unix vers des utilisateurs Samba, vérifiez les options et cliquez sur le bouton Convertir les utilisateurs. Après cela, vous devriez cliquer sur Éditer les utilisateurs et les mots de passe Samba pour modifier ou supprimer les utilisateurs non souhaités.

1. Il faut éviter de mélanger des serveurs WINS Windows® et Samba sur votre réseau.

7.1.2.3. Ajouter des partages

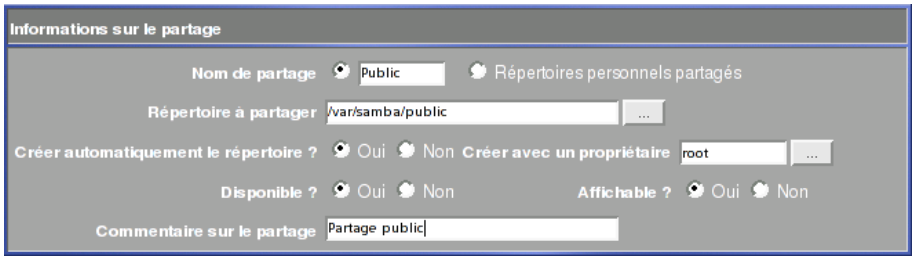


Figure 7-5. Configurer un partage public

Pour créer un partage public sur lequel **tous** les utilisateurs locaux pourront lire et écrire des fichiers, cliquez sur le lien Créer un nouveau répertoire partagé et remplissez les options comme indiqué (figure 7-5). Cliquez ensuite sur le nom du partage (`Public` dans notre exemple) puis sur le bouton Sécurité et contrôle d'accès pour changer les options En écriture et Accès invité à Oui. Sauvegardez vos changements et répétez l'opération pour rajouter d'autres dossiers partagés avec les contrôles d'accès appropriés.

Rappelez-vous que les répertoires partagés devront posséder des droits d'accès Linux appropriés afin d'être lisibles, accessibles et modifiables par les utilisateurs Windows®.

7.1.3. Configuration avancée

7.1.3.1. Accès aux partages

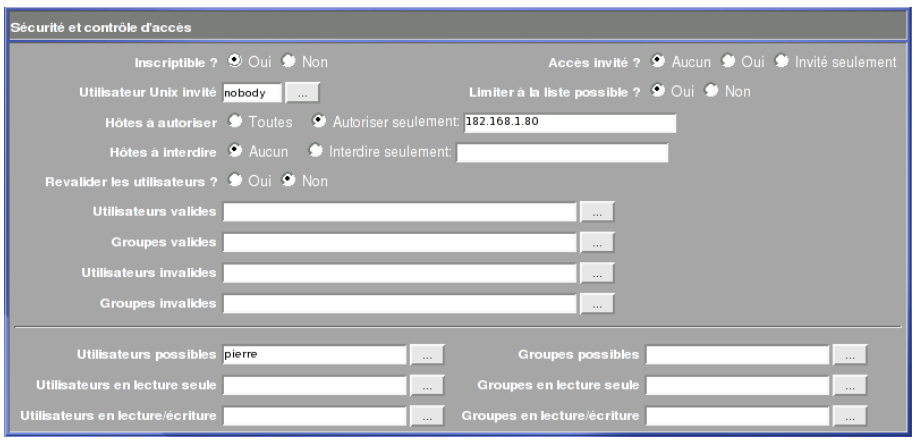


Figure 7-6. Limiter l'accès

Sélectionnez un partage à modifier dans la liste de partages puis cliquez sur le bouton Sécurité et Contrôle d'Accès. Utilisez les options Machines autorisées et Machines refusées pour spécifier une liste d'adresses IP (séparées par des espaces) des machines autorisées à se connecter, ou non, à ce partage. Si vous placez l'option Limiter à liste possible à Oui, vous pourrez alors remplir les champs Utilisateurs possible et Groups possibles. Voir figure 7-6.

7.1.3.2. Imprimante par défaut

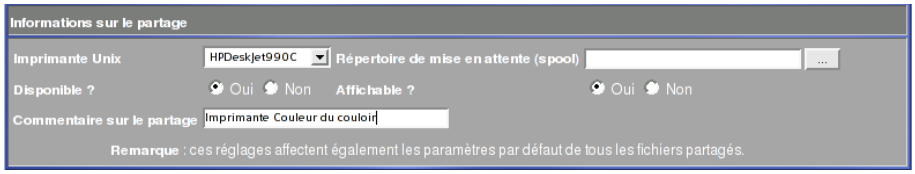


Figure 7-7. Options par défaut pour l'imprimante partagée

Toutes les imprimantes du serveur Samba seront disponibles et vous voudrez peut-être définir une imprimante par défaut en cliquant sur Réglages par défaut des imprimantes partagées (voir figure 7-7). Utilisez la liste déroulante Imprimante Unix pour sélectionner l'imprimante par défaut et spécifier sa disponibilité, ainsi que certaines options de contrôle d'accès.

7.1.4. Documentation additionnelle

C'est une bonne idée de consulter la Documentation Samba (`http://samba.org/samba/docs/`). Si vous avez installé le paquetage `samba-doc`, vous pouvez aussi accéder à la documentation Samba installée sur votre machine dans le répertoire `/usr/share/doc/samba-doc-*/`.

7.2. Partage de ressources : FTP

ProFTPD permet de créer et de paramétrer un serveur FTP. À travers cette application, votre entreprise peut partager des fichiers avec des utilisateurs connectés à Internet (ou à votre intranet). Selon votre configuration, ils pourraient éventuellement télécharger des fichiers sur votre serveur.

7.2.1. Installation

Assurez vous en premier lieu que le paquetage proftpd est installé sur votre système.

La configuration du serveur se fait à travers le module ProFTPD Server de Webmin, dans la catégorie Serveurs.

7.2.2. Exemples de configuration

Le protocole FTP n'est pas sécurisé, car ni l'authentification ni les communications ne sont cryptées. Les identifiants et mots de passe circulant en clair. Utilisez les connexions autres qu'anonymes seulement à l'intérieur de réseaux sécurisés.

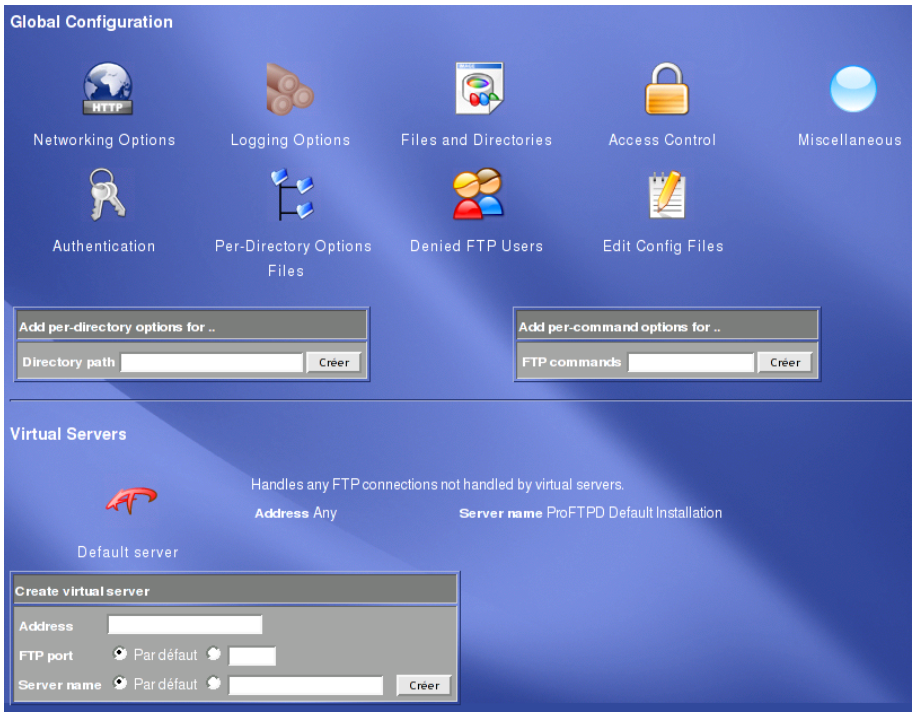


Figure 7-8. Page de démarrage du module ProFTPD

Toute la configuration du serveur ProFTPD est enregistrée dans le fichier `/etc/proftpd.conf`. La configuration de ProFTPD par défaut (juste après l'installation) ne permet que la connexion des utilisateurs de votre système ayant un compte local. Dans les sections qui viennent, nous présenterons quelques exemples de configuration courante de serveurs FTP.

Tout comme Apache, ProFTPD peut être utilisé pour servir plusieurs sites FTP sur une même machine par le biais de serveurs virtuels. Les options de configuration « globales » s'appliqueront à tous les serveurs virtuels. Les options de configuration globales se trouvent dans la section Virtual Servers.

Les valeurs par défaut sont optimisées pour la plupart des configurations. Inutile de les changer si vous n'avez pas de besoins spécifiques.

7.2.2.1. Simple serveur FTP anonyme

Il suffit d'installer le paquetage `proftpd-anonymous`. Celui-ci rajoute un fichier de configuration contenant toutes les directives nécessaires pour que les connections anonymes soient acceptées sur le serveur FTP.

Pour tester un accès anonyme sur le serveur FTP :

1. Pointez votre client FTP sur l'adresse ou le nom de votre serveur.
2. Entrez le mot `anonymous` comme identifiant et votre adresse électronique comme mot de passe.
3. Si tout se passe bien, tous les fichiers et sous-répertoires situés dans le répertoire `/var/ftp` (le répertoire racine de de l'utilisateur `ftp`) devraient alors être disponibles au téléchargement.

7.2.2.2. Serveur FTP anonyme avec répertoire de chargement (upload)

Si vous souhaitez que les utilisateurs puissent aussi charger des fichiers sur le serveur, vous devrez créer une zone spéciale à cet effet. Ajoutons cette fonctionnalité à notre serveur.

Lancez les commandes suivantes dans un terminal en tant que `root`, pour créer l'espace de stockage, et lui donner les droits d'accès adéquats.

```
# mkdir /var/ftp/uploads
# chown ftp:ftp /var/ftp/uploads
# chmod g+w /var/ftp/uploads
```

Allez alors dans la section Anonymous FTP de la configuration Default server et entrez `uploads/*` dans le champ Directory path type de la section Add per-directory options for.

Nous souhaitons que les utilisateur de notre réseau puissent lire et écrire des fichiers dans ce répertoire. Utilisez la section Per-command options. Puis, créez et configurez les deux FTP commands suivantes :

- Entrez `STOR` dans la table Add per-command options for..., puis cliquez sur Create. Ensuite cliquez sur Access Control et remplissez le formulaire tel qu'illustré (figure 7-9) :

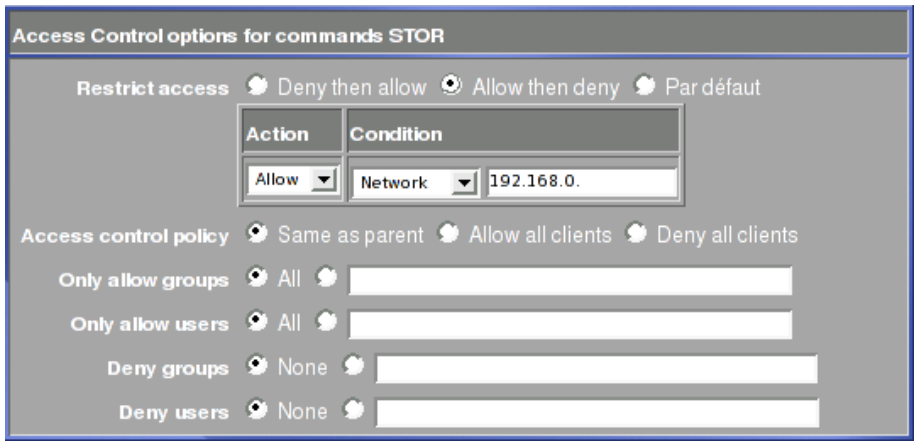


Figure 7-9. Contrôle d'accès pour les commandes répertoire

  Dans notre exemple, nous autorisons les chargements anonymes de fichiers dans ce répertoire, uniquement pour le réseau `192.168.1.`, et les bloquons pour tous les autres réseaux. Vous pouvez aussi contrôler l'accès sur la base d'un nom de machine, adresses IP, utilisateurs ou groupes d'utilisateurs.

- Cliquez sur le lien Return to per-directory options, créez la commande `READ` et répétez les mêmes opérations, mais cette fois pour l'autorisation en lecture du répertoire `uploads/*`.

Retournez au menu principal puis cliquez sur Apply Changes pour redémarrer le serveur FTP avec la nouvelle configuration. Tous les fichiers du répertoire `/var/ftp/uploads/` seront disponibles sur le réseau local en lecture et écriture anonymes.

Vous pouvez désormais répéter la procédure de test susmentionnée, cette fois pour le répertoire `/var/ftp/uploads/`.

7.2.3. Configuration avancée

Voici la liste des options les plus utiles :

- Dans la section Miscellaneous des serveurs virtuels, vous pouvez changer le Server administrator's email address pour spécifier l'adresse électronique de l'administrateur système du serveur ; et le Server name displayed to users pour personnaliser le nom de votre serveur. Par exemple, `Serveur principal FTP de ma société`.
- Dans la section Networking Options, vous pouvez changer la valeur Maximum concurrent logins pour que votre serveur ne soit pas surchargé par un trop grand nombre de connexions simultanées[2]. La valeur initiale est de 10 connexions simultanées. Vous pourrez aussi modifier le message d'erreur de connexion (Login error message), par exemple : `Désolé, le nombre maximal d'utilisateurs (%m) a été atteint -- réessayez plus tard` ; où `%m` représente le nombre que nous venons de choisir. Vous pouvez aussi personnaliser le port sur lequel le serveur virtuel va écouter les requêtes (`21` pour le serveur principal).
- Dans la section Files and Directories, vous pouvez spécifier les répertoires initiaux (Initial login directory). C'est le répertoire racine par défaut et peut être utilisé pour cantonner les utilisateurs dans un environnement hermétique. Si vous souhaitez mettre tous les utilisateurs dans leur propre environnement cage (Limit users

2. Positionner cette valeur à `0` revient à empêcher toute connexion sur le serveur FTP.

to directories), en limitant leur accès à leur propre répertoire personnel par exemple. New file umask peut être utilisé pour contrôler les permissions des fichiers qui seront créés (*upload*) sur le serveur.

Vous pouvez toujours utiliser la section Edit Config files de l'écran principal (figure 7-8) si vous souhaitez modifier les fichiers de configuration du serveur ProFTPD à la main.

7.2.4. Documentation additionnelle

Consulter la Documentation ProFTPd (`http://proftpd.linux.co.uk/docs/`), vous y trouverez aussi de nombreux exemples de configuration.

7.3. NFS: Partage de dossiers pour les hôtes UNIX/Linux

Le service Network File System (NFS) permet de partager très facilement des répertoires de votre ordinateur sur d'autres ordinateurs du même réseau. Ainsi, vous pouvez partager des fichiers entre plusieurs utilisateurs. Ce type de partage est beaucoup plus facile à configurer que Samba, mais il n'est utilisé que sur des systèmes GNU/Linux et UNIX®. NFS n'est pas un protocole sécurisé et doit être utilisé seulement dans un réseau local bien sécurisé.

7.3.1. Installation

Assurez vous que les paquetages `nfs-utils` et `nfs-utils-clients` sont bien installés.

7.3.2. Exemple de configuration

Le bouton de configuration Partage NFS se trouve dans la section **Réseau**. Cliquez simplement sur le lien Ajouter un nouveau partage et la page de configuration s'affichera.

Cliquez sur un paramètre que vous ne comprenez pas et un message contextuel s'affichera sur la signification de celui-ci.

Figure 7-10. Créer un nouveau partage NFS

L'écran de création d'un nouveau partage (figure 7-10) est divisé en deux parties. Dans Détails du partage, vous devrez spécifier le nom du Répertoire partagé que vous voulez exporter vers d'autres ordinateurs. Vous pourrez aussi spécifier les hôtes autorisés à accéder à ce répertoire (Partager à). Par défaut, le partage est accessible à Tous. Ceci devrait être changé pour le sous-réseau que vous utilisez (par exemple : `192.168.1.0/255.255.255.0`) ou un Groupe de réseau.

Dans Sécurité de l'export, vous pourrez restreindre un peu plus l'accès au répertoire partagé. Par exemple, vous pouvez choisir les ID auxquelles vous voulez faire confiance (ou non), ainsi que permettre la lecture ou la lecture et l'écriture dans vos répertoires.

Une fois que tout est configuré, cliquez sur le bouton Créer pour retourner à l'écran principal de configuration des partages NFS. Vous verrez alors dans la liste le partage que vous venez de créer. Vous pouvez ensuite créer de nouveaux partages, ou modifier ceux existant en cliquant sur le lien correspondant dans la colonne Partager à. Cliquez sur le bouton Appliquer tous changements pour rendre vos partages effectivement accessibles.

7.3.3. Accéder au répertoire partagé

Il faut désormais configurer les clients pour qu'ils « montent » les partages que nous venons de créer. La configuration varie d'un système à l'autre. Nous verrons donc ici la configuration d'un client Mandriva Linux.

La manière la plus simple consiste à utiliser le Centre de contrôle Mandriva Linux, dans le module Points de montage NFS de la section Points de montage.

Il est aussi possible de faire cela grâce à Webmin par l'interface Montages disques et réseau de la section Système. Vous pouvez y Ajouter un montage du type Network filesystem (nfs).

7.3.4. Documentation additionnelle

Un chapitre dédié aux partages NFS se trouve dans le livre de Joe Cooper The Book of Webmin (`http://www.swelltech.com/support/webminguide/ch13.html#exports`). Bien que s'appuyant sur une version ancienne de Webmin, cette lecture sera sûrement profitable.

Chapitre 8. Le serveur Kolab

8.1. Introduction

Kolab est la partie serveur de Kroupware, la solution de travail collaboratif de KDE. Kolab stocke les informations de synchronisation telles que les adresses, le calendrier et les fichiers utiles aux groupes d'utilisateurs. Vous pouvez accéder aux informations stockées au niveau du serveur Kolab en utilisant la partie cliente Kontact du projet Kroupware. Kontact est une combinaison de plusieurs outils: KMail, KOrganizer, KAddressbook, KNotes, KPilot et KNode. Ce chapitre vous donnera un aperçu technique du serveur Kolab, de même que l'installation, la configuration et l'administration de ce type de serveur. Les informations utilisateur pour le client Kontact se trouvent dans la documentation *Guide de démarrage* de Mandriva Linux. Celles relatives au projet Kroupware, peuvent directement être consultées sur le site web de Kroupware (`http://kroupware.kde.org`).

8.2. Aperçu

L'interface administration de Kolab repose sur le serveur HTTP amélioré Apache. L'authentification au niveau du module d'administration n'est possible que via une connexion sécurisée.

Kolab liste trois catégories d'utilisateurs:

- Utilisateur. Peut changer les informations utilisateurs.
- *Maintainer* (utilisateur évolué). A les droits Utilisateur plus des droits d'administration sur les utilisateurs, groupes et dossiers partagés.
- Administrateur. Possède les droits Maintainer plus les droits sur tout l'arborescence LDAP ainsi que les droits de basculer les services hérités et de consulter les journaux(logs).

Toutes les catégories d'utilisateurs accèdent au module d'administration Kolab avec la même interface Web. Après l'authentification de l'accès grâce aux lettres de créances de LDAP, l'utilisateur se retrouve face à une interface Web reflétant sa catégorie et ses permissions. Les nouveaux utilisateurs sont créés automatiquement en tant qu'utilisateurs normaux.

Le serveur LDAP est hébergé physiquement sur la même machine que Kolab. Toutes les données utilisées par Kolab, aussi bien les données utilisateurs et les données de configuration, sont stockées sur le serveur LDAP, qui est configuré à l'aide du script d'amorce de Kolab, kolab_bootstrap -b. En sauvegardant régulièrement les données LDAP sur une autre machine, il est possible de restaurer un serveur Kolab après un crash matériel.

Kolab utilise un compte **manager** spécial, créé à l'installation pour permettre aux utilisateurs de type administrateur de manipuler toutes les données de Kolab du serveur LDAP. Les Maintainers et les Utilisateurs ont des droits d'accès différents sur l'arborescence LDAP. Ce qui signifie qu'une potentielle attaque sur le serveur Apache ne pourrait pas manipuler ou altérer les données des comptes utilisateurs sur la machine tant que le mot de passe du **manager** n'est pas fourni.

8.3. Installation

Pour installer le serveur Kolab, utiliser Rpmdrake (voir *Rpmdrake: Gestionnaire de paquetages* du *Guide de démarrage*) de Mandriva Linux Control Center. Vous pouvez aussi installer Kolab en lançant une console en tant que root et en tapant la commande `urpmi --auto kolab-server`.

Après l'installation de Kolab, le serveur doit être configuré en exécutant la commande `/usr/sbin/kolab_bootstrap -b`. Le script d'amorce va configurer le serveur LDAP utilisé pour stocker les informations de configuration de Kolab et les données utilisateur. Lors de l'initialisation du serveur, `kolab_bootstrap` vous demande de fournir un mot de passe pour le compte manager du serveur LDAP. Vous devez garder cette information puisqu'elle sert à la fois pour le compte Administrateur de Kolab et pour l'accès à l'interface d'administration lors de la première connexion.

Vous aurez besoin d'une entrée de nom d'hôte valide dans le DNS ainsi qu'un enregistrement MX valide pour votre domaine mail. Si vous n'utilisez que `/etc/hosts`, vous pouvez accéder à la majorité des fonctionnalités, mais vous ne pourrez pas recevoir de courriel venant de l'extérieur. Une solution serait d'utiliser fetchmail ou un outil similaire pour aller chercher les mails sur un serveur POP externe, mais l'idéal serait d'avoir votre propre nom de domaine et une adresse IP fixe accessible de l'extérieur.

Quand le script d'amorce a fini de s'exécuter, Démarrez le serveur Kolab en lançant la commande `service kolab-server start`. Kolab tourne et est maintenant en attente du premier accès.

Pour configurer le client Kontact en conjonction avec Kolab, vous avez besoin d'informations de connexion de LDAP que vous trouverez dans `/etc/openldap/slapd.conf`. Par exemple:

```
# grep suffix /etc/openldap/slapd.conf
suffix      "dc=kolab,dc=yourdomain,dc=com"
```

Vous fournit la chaîne `Base DN`: `dc=kolab,dc=yourdomain,dc=com` Ainsi pour l'utilisateur `peter`, la chaîne `Bind DN` sera `cn=peter,dc=kolab,dc=yourdomain,dc=com`

8.4. L'interface d'administration de Kolab

Tous les utilisateurs qui sont connectés dans le module d'administration de Kolab utilisent la même interface Web. Si votre navigateur Internet se trouve sur la même machine que le serveur Kolab, vous pouvez le charger à `https://localhost/kolab/`. Si vous accédez à partir du réseau, l'URL serait de la forme `https://hostname/kolab/`.

A cause du certificat SSL factice et auto-signé, votre navigateur vous affichera le message "certificate failed the authenticity test". Ne vous en souciez pas, ceci est tout à fait normal. Cliquez juste sur Continuer, puis Accepter toujours. En fonction de votre configuration DNS, vous pouvez être amené à repasser par cet étape une deuxième fois.

Le premier accès au serveur Kolab doit être fait en utilisant le compte `manager` avec le mot de passe que vous aviez choisi lors de l'exécution du script `kolab_bootstrap`. Une fois connecté, l'administrateur peut créer un compte utilisateur Kolab, des comptes Maintainer et administrateurs. Pour plus d'informations sur ce point, voir *Maintainers*, page 76.

Si la base de données LDAP est déjà pré-remplie, l'administrateur verra les informations des utilisateurs existants. Ces utilisateurs LDAP ne pourront pas se connecter au module administration de Kolab automatiquement. Les utilisateurs Kolab doivent être créés de façon explicite à l'aide du module d'administration.

Lorsqu'un nouveau compte est créé, il est fonctionnel. L'utilisateur Kolab peut accéder au module d'administration.

Après s'être connecté dans le module administration, la page d'accueil de Kolab s'affiche. Une liste de formulaires Web, disponible pour l'utilisateur, est accessible sur le cadre de gauche. Les sections suivantes expliquent ces formulaires pour les différents types d'utilisateurs et les informations nécessaires à leur bonne utilisation.

8.4.1. Utilisateurs

Les membres du groupe d'utilisateurs régulier ont le droit de:

- modifier leurs données utilisateur personnels;

- ajouter une adresse courriel supplémentaire pour leur compte;
- activer un service de notification d'absence (vacances);
- activer un service de redirection de courriel.

Figure 8-1. L'interface utilisateur du serveur Kolab

Les services de notification d'absence (vacances) et de redirection de courriel sont mutuellement exclusifs. L'utilisateur doit explicitement désactiver un service pour activer l'autre.

8.4.1.1. Changer les données Utilisateur

les membres du groupe d'utilisateurs régulier ne peuvent pas:

- changer leur nom d'utilisateur;
- changer leur identifiant unique utilisateur (UID);
- changer leur adresse courriel primaire;

Pour changer les données utilisateur :

Figure 8-2. Modifier les données utilisateur existantes

1. Connectez vous dans Administration Interface de Kolab.
2. Cliquez sur **My User Settings** sur le panneau de gauche sur l'interface administration de Kolab.
3. Dans le formulaire Modify Existing User changer les informations de l'utilisateur.
4. Cliquez sur OK.

8.4.1.2. Activer les paramètres d'absence (vacances)

Dans certains cas, quand un utilisateur est en vacances et ne peut pas consulter son courriel, c'est souvent utile d'informer ses interlocuteurs de la personne à contacter en son absence. Le service de message d'absence de Kolab permet de configurer les paramètres d'absence.

Pour activer le service de message d'absence de Kolab:

1. Connectez vous dans l'interface Administration de Kolab.
2. Cliquez sur My User Settings sur le panneau de gauche de l'interface d'administration de Kolab.
3. Cliquez sur Vacation. la page User Vacations Settings s'affichera.
4. Sélectionnez la durée de votre absence dans le menu déroulant.
5. Tapez votre message d'absence dans la zone de texte Vacation.
6. Cliquez OK.

8.4.1.3. Activer la redirection de courriel

Kolab fournit un service de redirection de courriel pour permettre aux utilisateurs, en mission externe et ne pouvant pas accéder directement à leurs boîtes aux lettres, de spécifier une adresse de courriel où leurs courriels seront redirigés. Une copie du courriel redirigé peut être stocké sur le serveur mail local (en option).

Pour activer le service de redirection de courriel de Kolab:

1. Connectez vous dans l'interface Administration de Kolab.
2. Cliquez sur My User Settings sur sur le panneau de gauche de l'interface d'administration de Kolab.
3. Cliquez sur Forward E-Mail et la page User Forward Settings s'affichera.
4. Tapez l'adresse où le courriel sera redirigé.
5. Si vous voulez conserver une copie des courriels sur le serveur local, cliquez sur la case à cocherKeep.
6. Cliquez OK.

8.4.2. Maintainers

Le rôle du Maintainer de groupe est d'administrer les utilisateurs et les dossiers partagés sur le serveur Kolab. Les droits suivants sont accessibles aux Maintainers en plus des droits de l'utilisateur de base :

- ajouter, modifier et effacer les utilisateurs de Kroupware;
- ajouter, modifier et effacer les contacts du carnet d'adresses, pour désigner les utilisateurs dans le répertoire LDAP qui ne sont pas enregistrés sur le serveur Kolab;
- ajouter, modifier et effacer les dossiers partagés.

Les activités relatives aux droits utilisateur du Maintainer sont documentés à *Utilisateurs*, page 74.

Figure 8-3. L'interface Maintainer du serveur Kolab

8.4.2.1. Utilisateurs Kroupware

Les utilisateurs Kroupware sont des utilisateurs Kolab dûment enregistrés et ont accès à tous les services de travail collaboratif de Kolab. les Maintainers de Kolab peuvent gérer les données utilisateur de Kroupware et créer de nouvelles entrées du carnet d'adresses.

8.4.2.1.1. Créer de nouveaux utilisateurs.

Pour ajouter un nouvel utilisateur:

1. Cliquez sur Create New User dans la section Users du cadre de gauche.
2. Remplissez les informations utilisateur dans le formulaire Create New User.
3. Cliquez sur OK.

Sélectionnez la case à cocher Addressbook pour rendre l'adresse de l'utilisateur Kroupware visible dans le carnet d'adresses.

8.4.2.1.2. Gérer les Utilisateurs existants

Si un membre du groupe des Maintainers clique sur le bouton Users situé sur le cadre de gauche de l'interface administration de Kolab, une liste alphabétique de tous les utilisateurs courants de Kroupware apparaît dans le cadre de droite. Pour chaque utilisateur, un choix de modification ou de suppression est proposé.

- Pour modifier les informations de l'utilisateur, cliquez sur le bouton Modify. La page Modify Existing User s'affichera. Cette page est expliquée plus en détails dans *Utilisateurs*, page 74.
- Pour effacer un utilisateur, cliquez sur le bouton Delete.

8.4.2.2. Contacts du carnet d'adresses

Les contacts du carnet d'adresses sont les personnes présentes dans le répertoire LDAP mais qui ne sont pas des utilisateurs enregistrés Kolab. Ces derniers peuvent accéder à leurs données du carnet d'adresses; les Maintainers Kolab peuvent gérer les données des contacts du carnet d'adresses et en créer des nouveaux.

8.4.2.2.1. Créer de nouveaux contacts

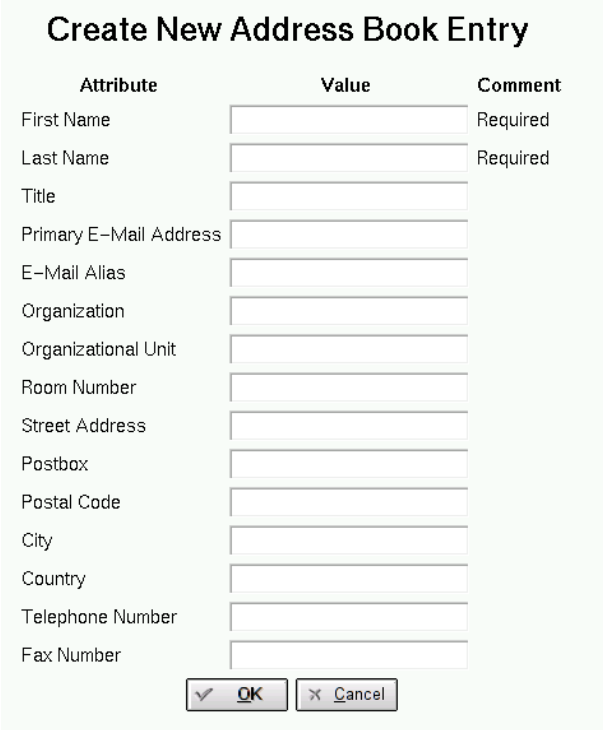


Figure 8-4. Le formulaire de création de carnet d'adresses

Pour créer un contact de carnet d'adresses:

1. Cliquez sur Create new vCard dans la section Users du cadre de gauche.
2. Remplissez les informations requises pour le contact dans le formulaire Create New Address Book Entry.
3. Cliquez sur OK.

8.4.2.2.2. Gérer les utilisateurs existants

Quand un membre du groupe de Maintainers clique sur le bouton Addressbook sur le cadre de gauche du module d'administration de Kolab, une liste alphabétique de tous les utilisateurs de carnet d'adresses s'affiche dans le cadre de droite. Pour chaque utilisateur, un choix de modification ou de suppression est proposé.

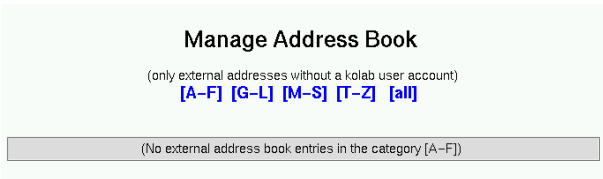


Figure 8-5. La table de gestion des utilisateurs de carnet d'adresses

Les actions suivantes peuvent être menées sur le formulaire Manage Address Book Users:

- Pour modifier les informations de l'utilisateur:
  1. Cliquez sur le bouton Modify.
  2. Sur la page Modify Address Book Users, changer les informations désirées.
  3. Cliquez sur OK.

- Pour supprimer un utilisateur, cliquez sur le bouton Delete.

8.4.2.3. Gérer les dossiers partagés

les Maintainers peuvent reconfigurer les dossiers partagés existants et en créer de nouveaux.

8.4.2.3.1. Créer de nouveaux dossiers partagés

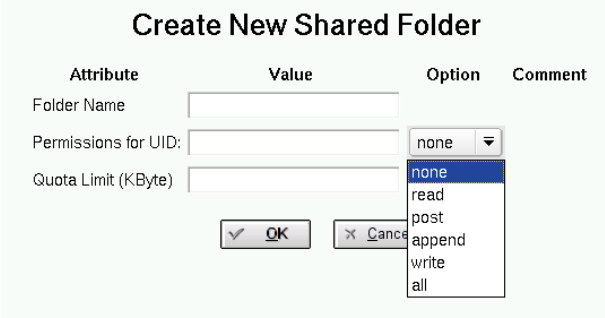


Figure 8-6. Le formulaire de création de nouveaux dossiers partagés

Pour ajouter un nouveau dossier partagé:

1. Cliquez sur Add Folder dans la section Shared Folder sur le cadre de gauche.
2. Remplissez les informations requises dans le formulaire Create New Shared Folder.
3. Cliquez sur OK.

8.4.2.3.2. Configurer les dossiers partagés

Quand un membre du groupe de Maintainers clique sur le bouton Shared Folder sur le cadre de gauche du module d'administration de Kolab, une liste alphabétique de tous les dossiers partagés courants s'affiche dans le cadre de droite. Pour chaque dossier, un choix de modification ou de suppression est proposé.

- Pour modifier un dossier:
  1. Cliquez sur le bouton Modify.
  2. Sur la page du dossier Modify Shared, changer les informations désirées.
  3. Cliquez sur OK.

- Pour effacer un dossier, cliquez sur le bouton Delete.

8.4.3. Administrateurs

Le groupe administrateur a un contrôle total sur tous les objets du serveur LDAP et des services hérités non sécurisés tels que FTP, HTTP, IMAP et POP3. Les administrateurs peuvent accomplir toutes les fonctions du groupe des Maintainers. En plus de pouvoir ajouter, modifier ou supprimer les utilisateurs, les entrées du carnet d'adresses et les dossiers partagés. Les administrateurs ont les droits suivants:

- ajouter, modifier ou supprimer les comptes des utilisateurs des groupes Maintainer ou administrateur;
- changer les caractéristiques du serveur (Nom d'hôte et domaine mail);
- Basculer les services hérités non sécurisés (FTP, HTTP, IMAP et POP3).

Les activités relatives au Maintainer du groupe administrateur et des droits basiques d'utilisateur sont documentés à *Utilisateurs*, page 74, et *Maintainers*, page 76.

8.4.3.1. Gérer les comptes Maintainers

Les administrateurs ont le droit de modifier ou de supprimer les comptes Maintainers existants ou d'en créer de nouveaux.

8.4.3.1.1. Créer de nouveaux Maintainers

Pour ajouter un nouveau Maintainer:

1. Cliquez sur Add Maintainer dans la section Maintainer sur le cadre de gauche.
2. Remplissez les informations requises dans le formulaire.
3. Cliquez sur OK.

8.4.3.1.2. Gérer les Maintainers existants

Quand un membre du groupe d'administrateurs clique sur le bouton Maintainers sur le cadre de gauche du module d'administration de Kolab, une liste alphabétique de tous les utilisateurs ou Maintainers courants s'affiche dans le cadre de droite. Pour chaque utilisateurs ou Maintainers, un choix de modification ou de suppression est proposé.

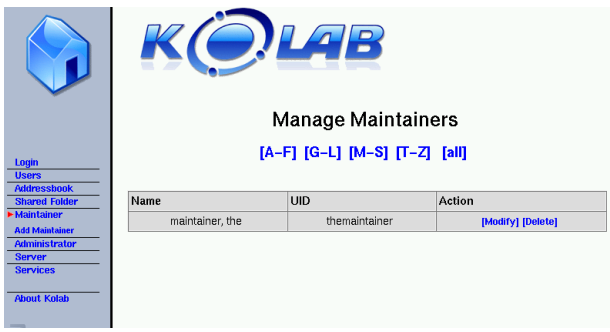


Figure 8-7. La table de gestion des Maintainers

- Pour modifier les informations d'un Maintainer:
  1. Cliquez sur le bouton Modify du Maintainer désiré.
  2. Cet action affichera la page Modify Existing User.
  3. Mettez à jour les informations désirées.
  4. Cliquez sur OK.

- Pour supprimer un Maintainer, cliquez sur le bouton Delete.

8.4.3.2. Créer de nouveaux administrateurs

Il est toujours prudent d'avoir au moins un administrateur de secours pour chaque serveur. Kolab permet la création de plusieurs administrateurs.

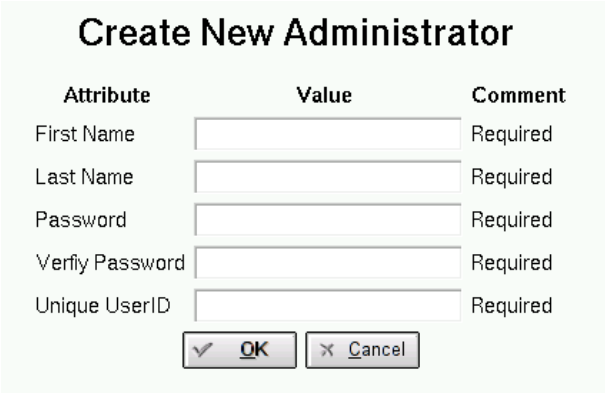


Figure 8-8. Le formulaire de création de nouveaux administrateurs

Pour ajouter un nouvel administrateur:

1. Cliquez sur Administrator dans le panneau de gauche du module d'administration.
2. Cliquez sur Add Administrator.
3. Remplissez les cases pour le nouvel administrateur.
4. Cliquez sur OK.

8.4.3.3. Changer les caractéristiques du Serveur

Les membres du groupe administrateur peuvent changer le nom d'hôte, le nom de domaine du domaine courriel sur le serveur hôte.

Les changements de ces caractéristiques peuvent affecter directement le système de transport du courriel et causer des problèmes sur son acheminement.

Pour changer les paramètres du serveur, cliquez sur Server dans le cadre de gauche du module d'administration, donnez les informations nécessaires comme indique sur la figure ci-dessous puis cliquez sur OK.

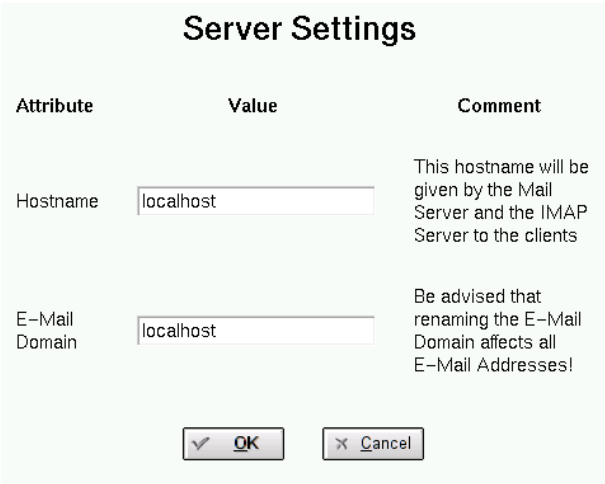


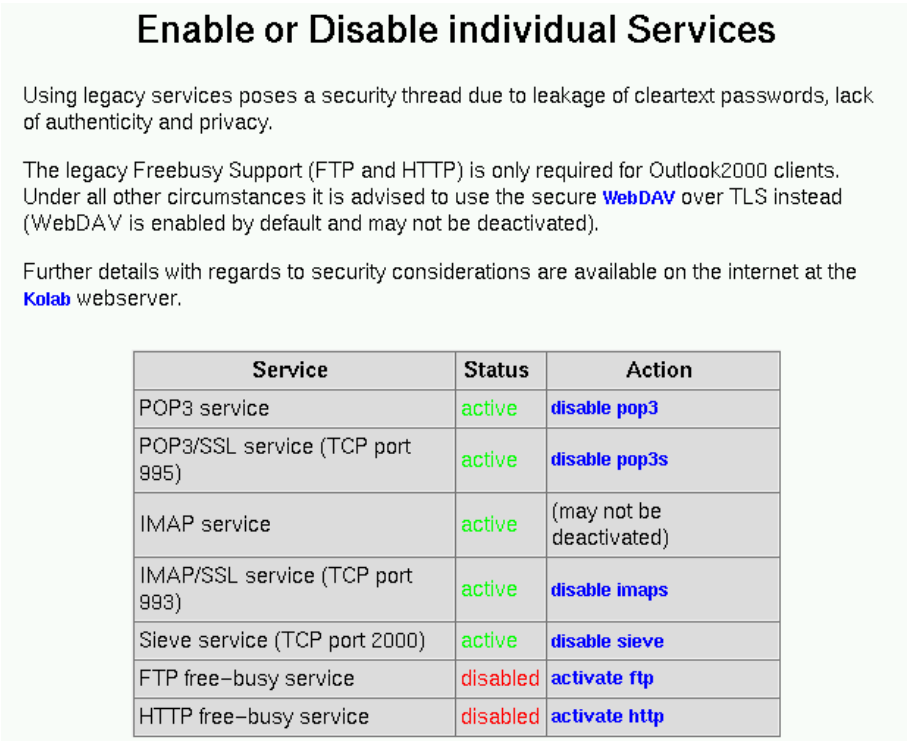
Figure 8-9. Le formulaire de paramétrage du serveur

8.4.3.4. Basculer les services

L'administrateur de Kolab a le droit d'activer ou de désactiver les services suivants sur la machine hôte:

- POP3;
- service POP3/TLS (TCP port 995);
- service IMAP/TLS (TCP port 993);
- service FTP *free-busy* (publication des disponibilités);
- service HTTP *free-busy* (publication des disponibilités).

Pour activer ou désactiver les services, cliquez sur Services dans le panneau de gauche du module d'administration. Vous verrez alors le formulaire Web suivant.



Enable or Disable individual Services

Using legacy services poses a security thread due to leakage of cleartext passwords, lack of authenticity and privacy.

The legacy Freebusy Support (FTP and HTTP) is only required for Outlook2000 clients. Under all other circumstances it is advised to use the secure **WebDAV** over TLS instead (WebDAV is enabled by default and may not be deactivated).

Further details with regards to security considerations are available on the internet at the **Kolab** webserver.

Service	Status	Action
POP3 service	active	**disable pop3**
POP3/SSL service (TCP port 995)	active	**disable pop3s**
IMAP service	active	(may not be deactivated)
IMAP/SSL service (TCP port 993)	active	**disable imaps**
Sieve service (TCP port 2000)	active	**disable sieve**
FTP free-busy service	disabled	**activate ftp**
HTTP free-busy service	disabled	**activate http**

Figure 8-10. Le formulaire des Services

Dans ce formulaire vous pouvez voir le statut des différents services. Pour les activer ou les désactiver, cliquez sur l'URL requis dans la colonne des actions.

Chapitre 9. Serveur de bases de données MySQL

Une base de données est une application dédiée au stockage des données (principalement texte et nombres) et à leur restitution de manière efficace. Elle est généralement utilisée par d'autres applications qui ont besoin d'accéder rapidement à des données pour les afficher ou les manipuler.

MySQL est un véritable serveur de bases de données SQL (*Structured Query Language*, soit un langage d'interrogation, de mise à jour et de gestion des bases de données relationnelles) multiutilisateurs et multiprocesseurs (*multi-threaded*). MySQL est une implantation client/serveur qui consiste en un démon serveur (`mysqld`) et plusieurs programmes/librairies client différents. Les visées principales de MySQL sont la vitesse, la robustesse et la convivialité.

9.1. Pour commencer

Nous aborderons ici la configuration de base de MySQL et son utilisation à travers l'interface Webmin. Assurez vous que le paquetage `MySQL` est bien installé.

Le bouton de configuration MySQL Database Server se trouve dans la section Serveurs. Si vous venez d'installer MySQL, il vous sera proposé de le démarrer : faites-le en cliquant sur le bouton Start MySQL Server.

Si vous obtenez une erreur lorsque vous essayez de démarrer ou arrêter le serveur, ouvrez l'onglet Configuration du module, et assurez vous que les champs Command to start/stop MySQL server utilisent bien la commande `/etc/rc.d/init.d/mysqld`.

Notez qu'il y a trois bases de données par défaut dans l'écran principal (mysql, test et tmp). Vous ne devriez **ni les modifier, ni les effacer**.

Votre première tâche est de choisir un mot de passe pour l'administrateur. **Cela est obligatoire pour empêcher que les autres utilisateurs puissent avoir un accès illimité à la base de données.** Pour ce faire, cliquez sur l'icône User Permissions puis effectuez les opérations suivantes pour chacun des liens `root` dans la table des utilisateurs.

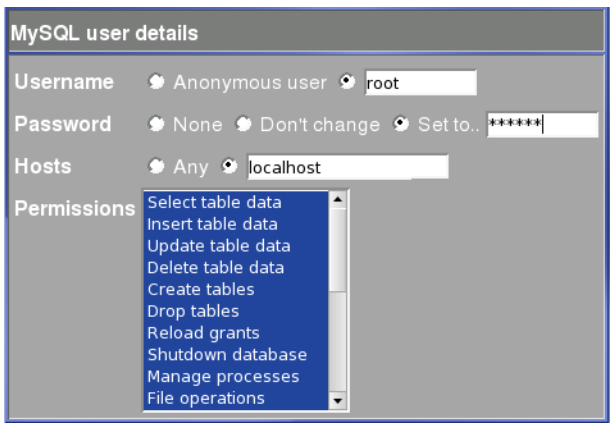


Figure 9-1. Modifier le mot de passe de l'administrateur

Après avoir cliqué sur un utilisateur, cochez le bouton Set to de la ligne Password. Dans le champ correspondant, entrez le nouveau mot de passe pour l'administrateur. Confirmez vos changements en cliquant sur le bouton Sauvegarder.

Pour des raisons de sécurité, l'accès réseau au serveur MySQL est désactivé par défaut. Si vous avez besoin que des applications d'une autre machine puissent accéder à la base de données, supprimez le fichier `/etc/sysconfig/mysqld` du système serveur.

Dans certains cas, les applications locales effectuent systématiquement des requêtes réseau pour interagir avec la base de données, et sont alors bloquées même si l'application tourne sur la même machine que le serveur.

9.2. Créer un utilisateur pour la base de données

Un utilisateur de base de données n'a rien à voir avec un utilisateur UNIX. Cette notion signifie plutôt que vous devez gérer les utilisateurs de façon différente. Depuis la page d'index MySQL Database Server, cliquez sur le bouton User Permissions puis sur Create new user. Les utilisateurs de la base de données peuvent avoir des permissions différentes, lesquelles sont listées dans l'image qui suit. Sélectionnez dans la liste les permissions qui seront accordées à l'utilisateur pour une machine spécifique.

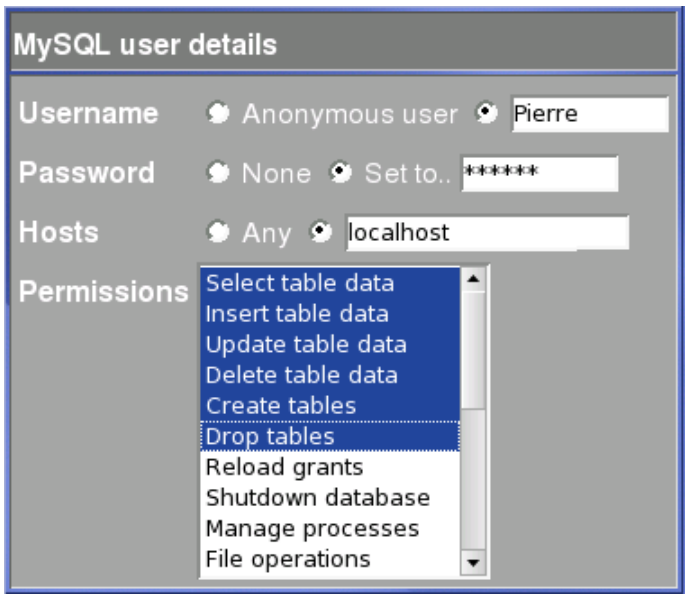


Figure 9-2. Créer un utilisateur MySQL

Pour des raisons de sécurité, mieux vaut ne pas laisser la valeur Hosts à **Any**. Spécifiez plutôt les noms des machines depuis lesquelles l'utilisateur pourra se connecter à la base MySQL.

9.3. Créer une base de données

Premièrement, créons une base de données qui contiendra nos tables. Cliquez sur Create a new database depuis la page principale, et nommez votre base de données.

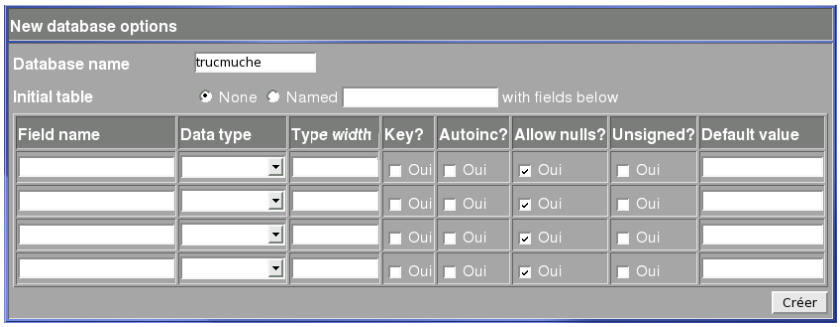


Figure 9-3. Créer une base de données MySQL

Il est possible de définir une première table sur cette nouvelle base de données et d'y spécifier jusqu'à quatre champs. Pour notre exemple nous avons décidé cependant de faire cela dans l'étape suivante. Remarquez que si vous envisagez d'utiliser votre base de données avec une application tierce comme une interface Web, tout ce dont vous avez besoin est désormais disponible: un utilisateur et son mot de passe, ainsi qu'une base de données prête à accueillir des informations.

9.4. Créer une table

Lorsque la base de données aura été créée, il est possible de définir sa structure manuellement avec Webmin. Cliquez sur son icône pour accéder à la page Edit Database. Notez que cette nouvelle base de données ne contient aucune table pour le moment, mais nous pouvons créer de nouvelles tables (Create a new table), supprimer la base de données (Drop Database) ou faire des copies de sauvegarde (Backup Database). Vous pouvez aussi exécuter des requêtes SQL directement (Execute SQL) en entrant des commandes SQL à la main ou en envoyant un fichier de commandes SQL. Vous pouvez sélectionner le nombre de champs que vous voulez que la nouvelle table contienne (4 par défaut) avant de cliquer sur Create a new table.

Sur la page **Create Table**, vous devez écrire le nom de la table et des champs et cliquer sur Créer.

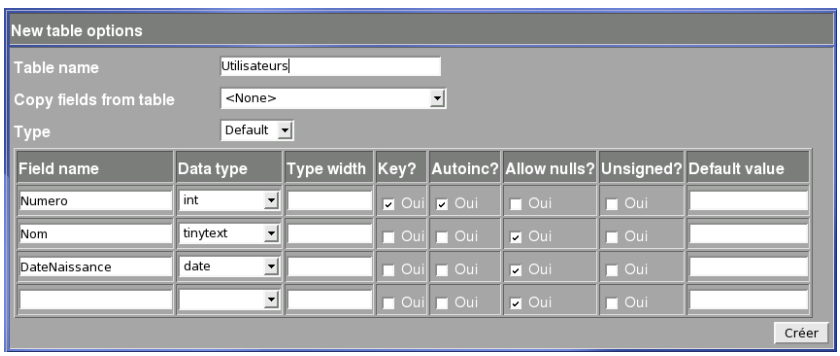


Figure 9-4. Créer une nouvelle table MySQL

Si vous voulez modifier les paramètres d'une table ou ajouter des nouveaux champs, vous pouvez cliquer sur le nom de la table à la page Edit Database.

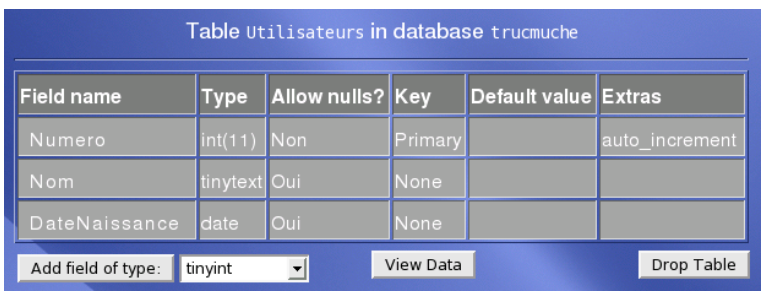


Figure 9-5. Modifier une table MySQL

À partir d'ici, vous pourrez modifier ou supprimer un champ existant, ou en créer un nouveau, visualiser les données ou supprimer la table (Drop Table) et ses données.

9.5. Gestion de données dans une table

Tout est prêt pour que la base de données MySQL commence à recevoir des données. Plusieurs programmes client permettent de se connecter au serveur MySQL, et plusieurs programmes ont besoin d'une telle base de données. Vous pouvez également utiliser Webmin pour gérer vos données. Sur la page Edit Table, vous pouvez cliquer sur le bouton View Data pour ajouter, modifier ou supprimer des données.

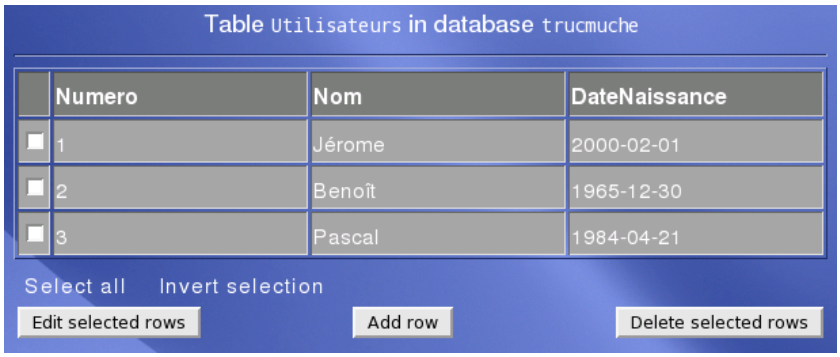


Figure 9-6. Gérer des données avec Webmin

9.6. Pour en savoir plus

Vous trouverez tout un ensemble de documents sur le site Web de MySQL (`http://www.mysql.com/documentation/`), y compris en français.

Chapitre 10. Client et serveur NIS

Pour simplifier la gestion d'usagers sur un réseau local, il est possible de centraliser l'information réseau, telle que les listes d'usagers et de mots de passe sur un domaine NIS (*Network Information System*).

Avec NIS, les usagers peuvent se connecter sur n'importe quel ordinateur en utilisant un identifiant (*login*) et un mot de passe uniques. Le partage d'information permet de distribuer des fichiers tels que `/etc/passwd`, `/etc/shadow` ou `/etc/hosts` pour partager des mots de passe ou des alias d'ordinateurs. Pour distribuer les données, vous devez configurer un serveur de Partage de ressources comme NFS (voir *NFS: Partage de dossiers pour les hôtes UNIX/Linux*, page 71) ou Samba (voir *Samba : intégrer Linux dans un réseau Windows*, page 65).

10.1. Installation

D'abord, assurez-vous que le serveur ypserv est installé correctement sur votre machine. Si ce n'est pas le cas, utilisez Rpmdrake ou tapez `urpmi ypserv` dans un terminal pour l'installer.

La configuration du serveur NIS se fait en 2 étapes : la première est la configuration des Tables NIS[1] du serveur ; la deuxième est la configuration de chaque client :

- sur le serveur, vous devez installer le paquetage RPM `ypserv` ;
- pour chaque poste de travail, vous aurez besoin des paquetages RPM `portmap`, `yp-tools` et `ypbind`.

Pour l'utiliser, sélectionnez la catégorie Réseau, puis le bouton Client et serveur NIS.

10.2. Configuration

10.2.1. Serveur NIS

Après avoir cliqué sur l'icône Serveur NIS, vous devez configurer votre domaine NIS en utilisant votre nom de domaine (tel que `mondomaine.test`). Ensuite, choisissez les `Tables NIS à servir`. Dans notre exemple, nous avons sélectionné les fichiers `passwd`, `group` et `shadow` (utilisez la touche **`Ctrl`** pour choisir plusieurs fichiers de la liste).

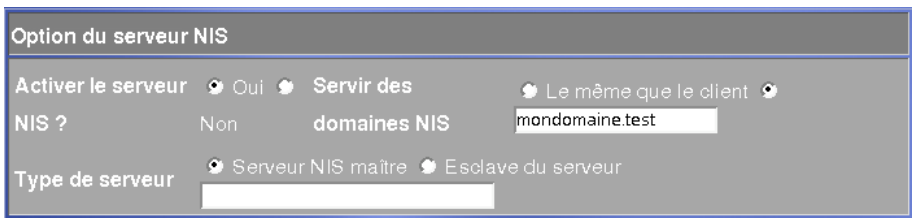


Figure 10-1. Serveur NIS

Vous n'avez pas à modifier la description du fichier qui est faite dans la section Fichiers NIS maîtres. Sur le menu Client et serveur NIS, l'icône Tables NIS vous permet de modifier les tables servies. L'icône Sécurité du serveur vous donne la possibilité de choisir les clients que vous voulez servir, ou non.

10.2.2. Client NIS

Pour chaque client, allez dans le module NIS et dans l'écran de configuration Client NIS, configurez le paramètre de Domaine NIS avec le nom de domaine utilisé par le serveur. Vous devez également spécifier l'adresse IP. C'est tout.

1. Les tables NIS sont les fichiers que vous avez choisis de partager ou d'exporter.

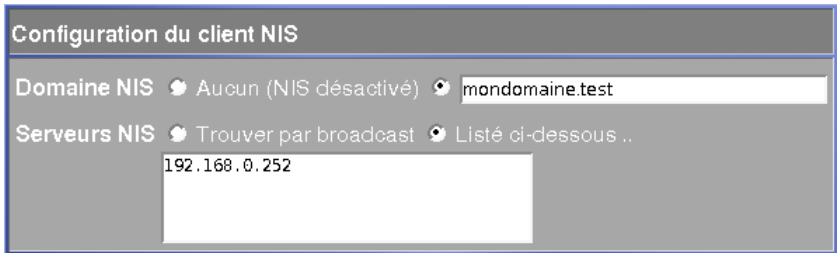


Figure 10-2. Client NIS

10.3. Configuration avancée pour les clients

Parmi toutes les données exportées, certaines d'entre elles peuvent être redondantes en rapport avec la configuration locale. Vous pouvez allouer une priorité à toutes les sources (localement, par NIS, ou autre). Pour ce faire, utilisez le bouton Services client pour chacun des clients NIS. Il vous permet de choisir l'ordre préféré pour chercher des données. Par exemple, vous pouvez choisir de résoudre l'adresse de l'hôte en utilisant :

1. le fichier `/etc/hosts` ;
2. l'hôte NIS desservi (si vous l'avez sélectionné dans les tables NIS) ;
3. et finalement (si le client ne peut plus faire de résolution), utilisez le serveur DNS.

Pour vérifier que le client communique bien avec le serveur, vous pouvez utiliser la commande `ypcat passwd` pour lire les données de mot de passe desservies par le serveur.

10.4. Importation de répertoire personnel (home) avec autofs

Si vous partagez les répertoires de vos utilisateurs (par l'entremise de NFS par exemple) et si vous démarrez le service **autofs** sur votre client NIS, les répertoires personnels des utilisateurs sont montés automatiquement lorsqu'ils se connectent au client. Ainsi, tout le monde peut se connecter automatiquement sur tous les clients, et accéder à ses données personnelles et fichiers de configuration.

Sécurité, réseau et résolution de problèmes

Pour vous aider à gérer des problèmes complexes, nous avons ajouter les trois chapitres suivants pour parfaire vos connaissances de Mandriva Linux.

- Le chapitre qui traite de sécurité (*Au sujet de la sécurité sous GNU/Linux*, page 91) est **une lecture impérative** pour tout administrateur système. Même si vous pouvez sécuriser de façon raisonnable votre système Mandriva Linux avec les outils par défaut, un système n'est vraiment sécurisé que lorsqu'il est administré de manière proactive, en prenant soin d'entretenir la sécurité globale, autant physique que logique de votre système. Ce chapitre vous aidera à choisir une politique de sécurité appropriée pour vos serveurs, les bons outils pour sécuriser votre infrastructure réseau, comment déterminer si votre système a été altéré ou compromis, etc.
- Nous discutons de la configuration réseau et de certains concepts liés au protocole TCP/IP — le plus utilisé des protocoles réseau — dans le chapitre *Le réseau sous GNU/Linux*, page 129. Lorsque possible, nous vous guidons vers d'autres sources d'information au sujet de divers protocoles réseau.
- Afin de tenter de combattre la Loi de Murphy, nous avons écrit un chapitre sur la résolution de problèmes (*Faire face aux problèmes*, page 143) pour vous épargner des nuits blanches. Il couvre aussi la prévention de désastre informatiques, alors lisez ce chapitre avant lorsqu'il ne soit trop tard !

Chapitre 11. Au sujet de la sécurité sous GNU/Linux

Ce document est un aperçu général des problèmes de sécurité auxquels pourrait être confronté un administrateur de système GNU/Linux. Il traite de la philosophie de la sécurité en général et aborde quelques exemples spécifiques pour mieux sécuriser votre système GNU/Linux des intrus. De nombreux liens vers de la documentation et des programmes relatifs à la sécurité sont aussi fournis.

Le document original (voir ci-dessous) a été adapté pour la distribution Mandriva Linux, des parties ont été enlevées ou modifiées.

11.1. Préambule

Ce chapitre est basé sur un *HOWTO* de Kevin Fenzi et Dave Wreski dont l'original est hébergé par The Linux Documentation Project (`http://www.tldp.org`).

11.1.1. Information sur le copyright

11.1.2. Introduction

Ce chapitre traite certains des principaux problèmes affectant la sécurité de GNU/Linux. La philosophie générale ainsi que les ressources réseau sont aussi abordées.

Un certain nombre d'autres *HOWTO*s débordent sur les questions de sécurité et ces documents ont été référencés chaque fois qu'ils s'y prêtaient.

Ce chapitre n'est **pas** destiné à recenser tous les trous de sécurité. Un grand nombre de nouvelles techniques sont sans arrêt utilisées. Ce chapitre vous apprendra où rechercher ce type d'information mise à jour, et donnera des méthodes générales pour empêcher de telles exactions d'avoir lieu.

11.2. Aperçu

Ce chapitre tentera d'expliquer certaines procédures et programmes communément employés pour vous aider à rendre votre système plus sûr. Il est important de discuter de certains des concepts de base en premier, et créer une base de sécurité, avant de commencer.

11.2.1. Pourquoi a-t-on besoin de sécurité ?

Dans le monde en ébullition des communications mondiales de données, connexions Internet peu chères, et développement de programmes accéléré, la sécurité devient une question de plus en plus importante. La sécurité est maintenant une nécessité de base, parce que l'informatique mondiale est intrinsèquement exposée au danger. Alors que vos données circulent d'un point A vers un point B sur Internet, par exemple, elles peuvent transiter par plusieurs autres points sur le trajet, donnant à d'autres la possibilité de les intercepter ou même de les modifier. Même d'autres utilisateurs sur votre système peuvent intentionnellement modifier vos données à votre insu. Les accès non autorisés à votre système peuvent êtres obtenus par des intrus, aussi appelés *crackers*, qui utilisent alors des techniques avancées pour se faire passer pour vous, vous voler de l'information, ou même vous empêcher d'accéder à vos propres ressources. Si vous vous demandez quelle est la différence entre un « hacker » et un « cracker », lisez le document *How to Become a Hacker* (`http://www.catb.org/~esr/faqs/hacker-howto.html`) de Eric Raymond.

11.2.2. Degré de sécurité

Il convient de garder à l'esprit qu'aucun système ne peut jamais être absolument sûr. Tout ce que vous pouvez faire, est de rendre la tâche de plus en plus difficile à quiconque tenterait de compromettre votre système. Pour l'utilisateur moyen de GNU/Linux, il suffit de peu pour garder le *cracker* à l'écart. Néanmoins, pour les utilisateurs GNU/Linux de renom (banques, compagnies de télécommunications, etc), beaucoup plus de travail est nécessaire.

Un autre facteur à prendre en compte est que au plus votre système est sécurisé, au plus votre sécurité devient intrusive. Vous devez décider un juste milieu, compromis entre la sécurité et la facilité d'utilisation. En fait, vous pourriez exiger que toute personne se connectant à votre système utilise un modem à retour d'appel (*call-back)* pour les rappeler à leur propre numéro de téléphone. Cela est plus sûr, mais si quelqu'un n'est pas chez lui, cela devient difficile pour lui de se connecter. Vous pouvez aussi configurer votre système GNU/Linux sans réseau ou connexion Internet, mais cela réduit son utilité.

Si vous êtes en charge d'un site de taille moyenne à grande, vous devriez établir une politique de sécurité faisant état du degré de sécurité requis pour votre site, et de quel outil d'audit est en place pour le contrôler. Vous pouvez trouver un exemple bien connu de politique de sécurité sur le site faqs.org (`http://www.faqs.org/rfcs/rfc2196.html`). Il propose un modèle exhaustif pour établir un plan de sécurité pour votre société.

11.2.3. Qu'essayez-vous de protéger ?

Avant d'essayer de sécuriser votre système, vous devriez déterminer de quel niveau de menace vous avez à vous protéger, quels risques vous pouvez ou ne pouvez pas prendre, et comme résultat, quel sera le degré de vulnérabilité de votre système. Vous devriez analyser votre système pour savoir ce que vous protégez, pourquoi vous le protégez, quelle est sa valeur, et qui est responsable pour vos données et autres biens.

- Le **risque** est la possibilité qu'un intrus puisse réussir à accéder à votre ordinateur. Un intrus peut-il lire ou écrire des fichiers, ou exécuter des programmes qui pourraient faire des dégâts ? Peut il détruire des données critiques ? Peut-il vous empêcher vous ou votre compagnie de réaliser un travail important ? N'oubliez pas : quelqu'un ayant accès à votre compte ou votre système peut se faire passer pour vous.

  Mais aussi, un seul compte non sécurisé sur votre système peut conduire à compromettre le réseau tout entier. Si vous autorisez un seul utilisateur à se connecter en utilisant un fichier `.rhosts`, ou à utiliser un service non sécurisé tel que `tftp`, vous prenez le risque de voir un intrus « mettre un pied dans la porte ». Une fois que l'intrus a un compte utilisateur sur votre système, ou le système de quelqu'un d'autre, il peut être utilisé pour obtenir l'accès à un autre système ou un autre compte.
- Le **danger** vient généralement de quelqu'un ayant des motivations pour obtenir un accès pervers à votre réseau ou ordinateur. Vous devez décider en qui vous avez confiance pour leur donner accès à votre système, et quelle menace ils représentent.

  Il y a plusieurs types d'intrus, et il est utile d'avoir à l'esprit leurs différentes caractéristiques pendant que vous mettez en place la sécurité de votre système.

  - **Le Curieux** - Ce type d'intrus est surtout intéressé par le type de votre système et les données qui s'y trouvent.

- **Le Malveillant** - Cet intrus est là pour faire écrouler votre système, modifier vos pages Web, ou même vous obliger à dépenser du temps et de l'argent pour vous remettre des dommages causés.
- **L'intrus Célèbre** - Ce type d'intrus essaye d'utiliser votre système pour augmenter sa côte de popularité et d'infamie. Il est susceptible d'utiliser la popularité de votre système pour afficher ses capacités.
- **Le Concurrent** - Cet intrus est intéressé par les données qui se trouvent sur votre système. Il peut d'agir de quelqu'un qui pense que vous possédez des informations dont il pourrait tirer profit, financièrement ou autre.
- **Le Locataire** - Ce type d'intrus souhaite s'installer sur votre système, et utiliser ses ressources pour son propre compte. Il fait généralement tourner des serveurs *chat* ou IRC, site d'archives pornographiques, ou même des serveurs DNS.
- **Le Passager** - Cet intrus n'est intéressé par votre système que pour obtenir l'accès à d'autres systèmes. Si votre système est bien connecté, ou une passerelle vers certains hôtes internes, vous êtes directement exposé à ce type d'individu.

- La vulnérabilité décrit le degré de protection de votre ordinateur depuis d'autres réseaux, et la possibilité pour quelqu'un d'obtenir un accès non autorisé.

  Qu'y a-t-il en jeu si quelqu'un casse votre système ? Bien sûr, les soucis d'un particulier en connexion PPP seront différents d'une société connectant leurs machines à Internet, ou un autre grand réseau.

  Combien de temps cela prendrait-il de récupérer/recréer des données qui seraient perdues ? Un investissement de temps maintenant peut économiser dix fois plus de temps plus tard, si vous devez recréer des données perdues. Avez vous vérifié votre stratégie de sauvegarde, et vérifié vos donnés récemment ?

11.2.4. Développer une politique de sécurité

Créez une politique simple, générique, que vos utilisateurs pourront aisément comprendre et suivre. Cela devrait protéger les données et l'intimité des utilisateurs. Certains aspects que vous pouvez aborder sont : Qui a accès au système (ma fiancée peut-elle utiliser mon compte ?) Qui est autorisé à installer des programmes sur le système, qui possède quelle donnée, récupération des catastrophes, et utilisation appropriée du système.

Une politique de sécurité généralement acceptée commence par la phrase

« **Ce qui n'est pas permis est interdit** »

Ceci signifie que, à moins que vous n'autorisiez l'accès à un service pour un utilisateur, cet utilisateur ne devrait pas utiliser ce service jusqu'à ce que vous l'y autorisiez. Assurez vous que les règles fonctionnent pour votre compte d'utilisateur normal. Vous dire « Ah, je n'arrive pas à résoudre ce problème de permissions, je vais le faire comme root » peut conduire à des trous de sécurité évidents et d'autres n'ayant pas encore été exploités.

RFC 1244 (`ftp://www.faqs.org/rfcs/rfc1244.html`) est un document décrivant comment créer votre propre politique de sécurité réseau.

RFC 1281 (`ftp://www.faqs.org/rfcs/rfc1281.html`) est un document qui décrit un exemple de politique de sécurité avec des descriptions détaillées de chaque étape.

Enfin, vous pourrez jeter un coup d'oeil à la bibliothèque COAST (`ftp://coast.cs.purdue.edu/pub/doc/policy`) pour voir de quoi ont l'air de véritables politiques de sécurité.

11.2.5. Moyens pour sécuriser votre site

Cette section va aborder plusieurs moyens grâce auxquels vous pourrez sécuriser les entités pour lesquelles vous avez travaillé dur : votre propre machine, vos données, vos utilisateurs, votre réseau, et même votre réputation. Qu'arriverait il à votre réputation si un intrus effaçait des données de vos utilisateurs ? Ou défigure votre site Web ? Ou publie le projet trimestriel de votre compagnie ? Si vous envisagez une installation réseau, il y a beaucoup de facteurs dont vous devez tenir compte avant d'ajouter une simple machine à votre réseau.

Même si vous avez un simple compte PPP , ou juste un petit site, cela ne signifie pas que les intrus se désintéresseront de votre système. Les grands sites célèbres ne sont pas les uniques cibles, beaucoup d'intrus veulent simplement pénétrer le plus de sites possibles, sans égard à leur taille. De plus, ils peuvent utiliser un trou de sécurité de votre site pour obtenir l'accès à d'autres sites auxquels vous êtes connectés.

Les intrus ont beaucoup de temps devant eux, et peuvent s'économiser de deviner comment vous avez bouché les trous, simplement en essayant toutes les possibilités. Il y a aussi plusieurs raisons pour lesquelles un intrus peut être intéressé par votre système, ce que nous traiterons plus tard.

11.2.5.1. Sécurité de l'hôte

Sans doute le domaine de sécurité sur lequel les administrateurs se concentrent le plus. Cela implique généralement de vous assurer que votre propre système est sûr, et espérer que tous les autres sur votre réseau font de même. Choisir de bons mots de passe, sécuriser les services réseau de votre hôte local, garder de bons registres de comptes et mettre à jour les programmes qui résolvent des trous de sécurité sont parmi les tâches dont est responsable l'administrateur sécurité local. Bien que cela soit absolument nécessaire, cette tâche peut devenir harassante dés que votre réseau dépasse la taille de quelques machines.

11.2.5.2. Sécurité du réseau local

La sécurité réseau est tout autant nécessaire que la sécurité de l'hôte local. Avec des centaines, des milliers, ou plus, d'ordinateurs sur le même réseau, vous ne pouvez supposer que chacun de ces systèmes soit sûr. Vous assurer que seuls les utilisateurs autorisés peuvent utiliser votre réseau, construire des pare-feu, utiliser du cryptage lourd, et s'assurer qu'il n'y a pas de machine « crapuleuse » (non sûre) sur votre réseau font partie des devoirs de l'administrateur de la sécurité du réseau.

Ce document va aborder certaines des techniques utilisées pour sécuriser votre site, et ainsi vous montrer certaines façons de prévenir qu'un intrus obtienne l'accès à ce que vous essayez de protéger.

11.2.5.3. La sécurité par l'obscurité

Un certain type de sécurité qui doit être abordé est « La sécurité par l'obscurité ». Cela signifie par exemple, déplacer un service qui est vulnérable vers un port non standard, en espérant que cela déroutera les attaquants. Un temps suffira pour qu'ils découvrent la supercherie et exploitent le vulnérabilité. La sécurité par l'obscurité signifie aucune sécurité. Simplement parce que vous avez un petit site ou peu de notoriété, ne signifie pas qu'un intrus ne sera pas intéressé par ce que vous avez. Nous discuterons de ce que vous protégez dans les prochaines sections.

11.2.6. Organisation de ce chapitre

Ce chapitre a été divisé en un certain nombre de sections. Elles couvrent plusieurs larges problèmes de sécurité. La première *Sécurité physique*, page 94, explique comment vous devez protéger votre machine physique de violations. La seconde, *Sécurité locale*, page 98, décrit comment protéger votre système de violations par des utilisateurs locaux. La troisième, *Sécurité des fichiers et des systèmes de fichiers*, page 99, vous enseigne comment configurer votre système de fichiers et les permissions sur les fichiers. La suivante, *Sécurité des mots de passe et cryptage*, page 104, traite des moyens de cryptage pour mieux sécuriser machines et réseaux. *Sécurité du noyau*, page 110 débat des options du noyau (*kernel*) que vous pouvez utiliser pour un système plus sûr. *Sécurité réseau*, page 113, décrit comment mieux sécuriser votre système GNU/Linux d'attaques réseau. *Préparation de sécurité (avant de vous connecter)*, page 120, vous informe de la préparation des machines avant leur connexion. Ensuite, *Que faire, avant et pendant une effraction*, page 121, conseille l'attitude à avoir lors d une intrusion en cours et comment détecter une intrusion récente. Dans *Documents de base*, page 123, quelques documents de base sur la sécurité sont recensés. La section Questions et Réponses *Foire aux questions*, page 125, répond à quelques questions fréquentes, et enfin une section *Conclusion*, page 127.

Les deux points principaux à réaliser lors de la lecture de ce chapitre sont :

- Soyez conscient de votre système. Consultez les logs système `/var/log/messages`, gardez un oeil sur votre système, et
- Gardez votre système à jour en vous assurant que soient installées les dernières versions des programmes mis à jour pour les alertes de sécurité. Cette simple précaution rendra votre système notablement plus sûr.

11.3. Sécurité physique

Le premier niveau de sécurité que vous devez prendre en compte est la sécurité physique de vos systèmes d'ordinateurs. Qui a un accès physique direct à votre machine ? Devrait-il ? Pouvez-vous protéger votre machine d'une intrusion de leur part ? Devez vous ?

le degré de sécurité physique dont vous avez besoin sur votre système dépend beaucoup de votre situation et/ou de votre budget.

Si vous êtes un particulier, vous n'en aurez sans doute pas trop besoin (cependant vous pourriez avoir besoin de protéger votre machine de vos enfants ou de visiteurs gênants. Si vous êtes dans un laboratoire, vous en avez besoin de beaucoup plus, mais les utilisateurs devront néanmoins pouvoir travailler sur les machines. Beaucoup des sections suivantes vous y aideront. Si vous êtes dans des bureaux, vous aurez ou non besoin de protéger votre machine pendant les heures de pause ou lorsque vous êtes absent. Dans certaines sociétés, laisser votre console non sécurisée est un crime grave.

Des méthodes de sécurité physiques comme des serrures sur les portes, câbles, armoires fermées, et vidéo surveillance sont de bonnes idées, mais en dehors de la portée de ce chapitre.

11.3.1. Verrouillage de l'ordinateur

De nombreux boîtiers d'ordinateur proposent une option de « verrouillage ». Cela se présente généralement sous la forme d'une serrure sur l'avant du boîtier vous permettent de passer d'un état déverrouillé à verrouillé à l'aide d'une clé. Ce type de verrouillage peut empêcher quelqu'un de voler votre ordinateur, ou ouvrir le boîtier pour directement manipuler ou voler votre matériel. Il peut aussi parfois empêcher le redémarrage de la machine par une disquette ou autre.

Ces verrouillages de boîtier font différentes choses selon le support par la carte mère et la conception du boîtier. Sur beaucoup d'ordinateurs ils font en sorte que vous devez casser le boîtier pour pouvoir l'ouvrir. Sur d'autres, ils empêchent la connexion de nouveaux claviers ou souris. Consultez les caractéristiques de votre carte mère ou du boîtier pour plus de renseignements. Ils peuvent être parfois une caractéristique très utile, même si la serrure est parfois de très mauvaise qualité, et facile à forcer avec un passe-partout.

Certains boîtiers (particulièrement des SPARCs et macs) possèdent un anneau à l'arrière, de sorte que si vous y passez un câble l'attaquant devra couper le câble ou casser le boîtier pour pouvoir l'ouvrir. Y mettre un cadenas ou une chaîne peut avoir un bon effet dissuasif sur quelqu'un essayant de voler votre machine.

11.3.2. Sécurité au niveau du BIOS

Le BIOS est le niveau logiciel le plus bas qui configure ou manipule votre matériel x86. LILO ou d'autres méthodes de boot GNU/Linux accèdent au BIOS pour déterminer comment démarrer votre machine GNU/Linux. Les autres architectures sur lesquelles GNU/Linux tourne ont des programmes similaires (OpenFirmware sur Mac et nouveaux Sun, Sun boot PROM, etc.). Vous pouvez utiliser votre BIOS pour empêcher les attaquants de redémarrer votre machine et y manipuler votre système GNU/Linux.

La plupart des BIOS de PC permettent la configuration d'un mot de passe. Cela ne garantit pas beaucoup de sécurité (le BIOS peut être réinitialisé, ou enlevé si quelqu'un a accès au boîtier), mais peut être une bonne dissuasion (c'est à dire que cela prendra du temps et laissera des traces d'effraction).Cela ralentira les attaquants potentiels.

Le mot de passe par défaut s'avère un autre risque lorsque vous faites confiance au mot de passe du BIOS pour sécuriser votre système. La plupart des fabricants de BIOS ne s'attendent pas à ce que les utilisateurs ouvrent leur ordinateur et déconnectent les batteries s'ils oublient leur mot de passe et ont muni leurs BIOS de mots de passe par défaut qui fonctionnent, nonobstant le mot de passe que **vous** avez choisi. Voici certains des mots de passe les plus communs :

```
j262
AWARD_SW
AWARD_PW
lkwpeter
Biostar
AMI
Award
bios
BIOS
setup
```

```
cmos
AMI!SW1
AMI?SW1
password
hewittrand
shift + s y x z
```

J'ai testé un BIOS Award et AWARD_PW ont fonctionné. Ces mots de passe sont assez faciles à obtenir sur les sites Web des fabricants ou sur astalavista (`http://astalavista.box.sk`) et en tant que tel, un mot de passe de BIOS ne peut pas être considéré comme une protection adéquate contre les attaquants informés.

Beaucoup de BIOS x86 vous permettent aussi de spécifier plusieurs autres bons paramètres de sécurité. Consultez le manuel de votre BIOS ou explorez le la prochaine fois que vous redémarrez. Par exemple, certains BIOS désactivent le démarrage depuis une disquette et d'autres demandent un mot de passe pour pouvoir accéder aux caractéristiques du BIOS.

Si votre machine est un serveur, et vous configurez un mot de passe de démarrage, votre machine ne pourra pas redémarrer toute seule. Gardez à l'esprit que vous aurez besoin de vous déplacer et fournir le mot de passe en cas de coupure de courant.

11.3.3. Sécurité du chargeur de démarrage

Gardez à l'esprit lorsque vous mettez en place tous ces mots de passe, que vous devez vous en souvenir ! Rappelez-vous aussi que ces mots de passe vont seulement ralentir un intrus déterminé. Ils ne vont pas empêcher quelqu'un de démarrer à partir d'une disquette et monter votre partition racine.

Si vous utilisez la sécurité en conjonction avec votre chargeur de démarrage, vous devriez aussi désactiver le démarrage depuis une disquette, ainsi que protéger l'accès au BIOS.

Si vous utilisez la sécurité en conjonction avec votre chargeur de démarrage, vous devriez aussi protéger l'accès au PROM.

Une fois encore, si votre machine est un serveur, et vous configurez un mot de passe de démarrage, votre machine ne pourra pas redémarrer toute seule. Gardez à l'esprit que vous aurez besoin de vous déplacer et fournir le mot de passe en cas de coupure de courant.

11.3.3.1. Avec LILO

LILO propose les paramètres `password` et `restricted`; `password` exige un mot de passe à chaque redémarrage, alors que `restricted` demande un mot de passe seulement si vous spécifiez des options au prompt (comme `single`) au prompt `LILO` .

Référez-vous à lilo.conf(5) pour de plus amples informations sur les paramètres `password` et `restricted`.

Gardez aussi en tête que `/etc/lilo.conf` devra être en mode `600` (lecture et écriture pour `root` seulement), sinon d'autres personnes pourront lire vos mots de passe de démarrage !

11.3.3.2. Avec GRUB

GRUB est assez flexible en ce qui concerne la configuration d'un mot de passe au démarrage : le fichier de configuration par défaut (`/boot/grub/menu.lst`) peut contenir une ligne permettant de charger un nouveau fichier de configuration contenant des options différentes. Ce nouveau fichier peut abriter un nouveau mot de passe permettant d'accéder à un troisième fichier de configuration, et ainsi de suite.

Donc, dans votre fichier `/boot/grub/menu.lst`, vous devez ajouter une ligne ressemblant à :

```
password très_secret /boot/grub/menu2.lst
```

et bien entendu, vous devez générer un nouveau fichier de configuration du nom de `/boot/grub/menu2.lst` vers lequel vous déplacerez les entrées non sécurisées, précédemment enlevées du fichier `/boot/grub/menu.lst`.

Référez-vous à la page GRUB `info` pour plus d'informations.

11.3.4. kxlock et vlock

Si vous vous éloignez de votre machine de temps à autre, il est bon de « verrouiller » votre console afin que personne ne puisse manipuler ou regarder votre travail. Pour ce faire, vous pouvez utiliser les programmes `klock` ou `vlock`.

`klock` est un verrouilleur d'écran X;. Vous pouvez lancer `klock` depuis n'importe quel terminal X, il verrouillera alors l'affichage et exigera un mot de passe pour pouvoir y retourner. La plupart des environnements graphiques proposent aussi cette option dans leurs menus respectifs.

`vlock` est un simple petit programme qui vous permet de verrouiller quelques unes ou toutes les consoles de votre machine GNU/Linux. vous pouvez bloquer juste celle que vous utilisez ou bien toutes. Si vous n'en bloquez qu'une, d'autres peuvent venir et utiliser la console ; ils ne seront simplement pas autorisés à utiliser votre console jusqu'à ce que vous la déverrouilliez.

Bien sûr, verrouiller votre console empêchera quelqu'un de falsifier votre travail, mais ne les empêchera pas de redémarrer la machine, et ainsi interrompre votre travail. Ça ne les empêche pas non plus d'accéder à votre machine depuis une autre et y faire des dégâts.

Plus important, cela n'empêche personne de quitter complètement X Window System et d'aller sur un prompt de console virtuelle normale, ou à la console (VC) depuis laquelle X (X11) a été démarré et la suspendre, obtenant ainsi vos privilèges. Pour cette raison, vous ne devriez utiliser cela que sous le contrôle de KDM (ou autre).

11.3.5. La sécurité des périphériques locaux

Si une webcam ou un microphone est relié à votre système, vous devriez analyser s'il est possible qu'un attaquant gagne l'accès à votre système par leur entremise. Lorsqu'ils ne sont pas utilisés, débrancher ou carrément enlever ces périphériques s'avère une option intelligente. Sinon, vous devriez lire la documentation et examiner tout logiciel qui pourrait donner accès à ces périphériques.

11.3.6. Détecter des violations physiques de sécurité

La première chose à toujours noter, est quand la machine est redémarrée. Du fait que GNU/Linux est un système d'exploitation stable et robuste, les seules fois où votre machine devrait redémarrer, est lorsque **vous** l'arrêtez pour des mises à jour majeure, changement de matériel, ou des actions de cet ordre. Si votre machine a redémarré sans votre intervention, cela pourrait être un signe qu'un intrus l'a violée. Beaucoup des manières de violer votre machines impliquent en effet le redémarrage ou l'arrêt de celle-ci.

Vérifier qu'il n'y a aucune trace d'effraction sur le boîtier et dans la zone de la machine. Bien que la plupart des intrus nettoient les traces de leur passage des logs, c'est une bonne idée de les vérifier et noter toute irrégularité.

C'est aussi une bonne idée de garder les données de logs en un endroit sûr, comme un serveur de logs dédié, à l'intérieur de votre réseau bien protégé. Lorsque une machine a été violée, les données de logs deviennent de peu d'utilité, car il est fort probable qu'ils aient aussi étés modifiés par l'intrus.

Le démon syslog peut être configuré pour envoyer automatiquement les données de logs vers un serveur syslog central, mais les données sont généralement envoyées en clair, permettant à un intrus de consulter les logs lors du transfert. Cela pourrait révéler des informations sur votre réseau qui ne devraient pas être dévoilées. Il y a des démons syslog disponibles qui cryptent les données lorsqu'elles sont envoyées.

Soyez aussi conscient que falsifier les messages de syslog est facile - avec un programme de craquage ayant été publié. syslog accepte même les entrées de logs réseau qui prétendent venir de l'hôte local sans même indiquer leur origine réelle.

Quelques points à vérifier dans vos logs :

- Logs courts ou incomplets.
- Logs contenant des dates étranges.

- Logs avec des permissions ou propriétaire incorrects.
- traces de redémarrage de la machine ou de services.
- Logs manquants.
- Entrées `su` ou connections depuis des origines inhabituelles.

Nous parlerons des données logs système dans le chapitre *Gardez trace des données de journalisation du système*, page 120.

11.4. Sécurité locale

L'aspect suivant à regarder est la sécurité de votre système vis-à-vis des utilisateurs locaux. Avons-nous dit utilisateurs **locaux** ? Oui !

Obtenir l'accès au compte d'un utilisateur local est la première chose que fait un intrus, sur le chemin de l'exploitation du compte `root`. Avec une sécurité locale laxiste, il peut alors « améliorer » ses privilèges du compte normal vers des privilèges de `root` en utilisant un certain nombre de bogues et de services locaux mal configurés. Si vous vous assurez que votre sécurité locales est serrée, alors l'intrus suera un peu plus pour passer la barre.

Les utilisateurs locaux peuvent aussi causer beaucoup de dégâts sur votre système, même (et surtout) s'ils sont vraiment qui ils prétendent être. Donner des comptes à des gens que vous ne connaissez pas ou pour lesquels vous n'avez pas de renseignements est une très mauvaise idée.

11.4.1. Créer de nouveaux comptes

Vous devriez vous assurer de fournir aux comptes utilisateurs le strict minimum requis pour leur tâche. Si vous donnez un compte à votre fils (10 ans), vous voudrez peut-être qu'il puisse accéder à un traitement de textes et un programme de dessin, mais qu'il ne puisse pas effacer des données qui ne sont pas les siennes.

Plusieurs bonnes règles à suivre lorsque vous autorisez des gens à accéder à votre machine GNU/Linux :

- Leur donner la plus exacte quantité de privilèges dont ils ont besoin.
- S'assurer de quand/où ils se connectent, ou devraient se connecter.
- S'assurer de supprimer les comptes inutilisés, que vous trouverez aisément en utilisant la commande `last` ou en vérifiant les fichiers journaux pour déterminer si ces utilisateurs sont encore actifs.
- Pour faciliter la maintenance des comptes et l'analyse des données de logs, il est conseillé d'utiliser le même numéro d'usager (`userid`) sur tous les ordinateurs et réseaux.
- La création de groupes de `userids` devrait être strictement interdite. Les comptes d'utilisateurs permettent aussi la responsabilisation, ce qui est rendu impossible par les comptes groupés.

Beaucoup de comptes d'utilisateurs locaux qui sont utilisés dans des effractions de sécurité n'ont pas été utilisés pendant des mois ou des années. Comme personne ne les utilise, ils sont des vecteurs d'attaque idéaux.

11.4.2. Sécurité pour `root`

Le compte le plus sollicité sur votre machine est le compte `root` (super-utilisateur). Ce compte a l'autorité sur toute la machine, ce qui peut aussi inclure l'autorité sur d'autres machines du réseau. Rappelez vous que vous ne devriez utiliser le compte `root` que pour de très courtes tâches particulières, et être le plus souvent sous votre compte normal. Même de petites erreurs commises lorsque vous êtes connecté en tant que `root` peuvent causer des problèmes. Moins vous êtes connecté avec les privilèges de `root`, plus sûr ce sera.

Plusieurs astuces pour éviter de bousiller votre propre machine en tant que `root` :

- Lorsque vous effectuez des commandes complexes, essayer de les faire tourner d'abord de manière non destructive... tout particulièrement les commandes qui utilisent l'englobement. C'est-à-dire, si vous voulez faire `rm -f foo*.bak`, lancez d'abord `ls foo*.bak` et assurez vous que vous allez effectivement effacer les fichiers que vous pensiez. Utiliser `echo` à la place d'une commande destructive marche aussi parfois.
- Ne devenez `root` que pour lancer des tâches spécifiques. Si vous vous retrouvez en train de vous demandez comment faire pour résoudre un problème, revenez sous votre compte normal, jusqu'à ce que vous soyez **sûr** de ce que vous avez besoin de faire en tant que `root`.
- Le chemin de commandes pour l'utilisateur `root` est très important. Ce chemin de commandes (c'est a dire, la variable d' environnement PATH) désigne les répertoires dans lesquels le *shell* cherche les programmes. Essayez de limiter le chemin de commandes pour l'utilisateur `root` le plus possible, et n'y incluez **jamais** `.` (qui signifie « le répertoire courant ») dans votre PATH. De plus, n'ayez jamais de répertoires en écriture dans votre chemin de recherche, car cela pourrait permettre aux attaquants de modifier ou placer de nouveaux binaires dans votre chemin de recherche, leur permettant de se lancer comme `root` la prochaine fois que vous utilisez la commande.
- N'utilisez jamais la suite d'outils `rlogin/rsh/rexec` (appelés les « r-utilitaire ») en tant que `root`. Ils sont sujets de plusieurs attaques, et sont cruellement dangereux utilisés comme `root`. Ne créez jamais un fichier `.rhosts` pour `root`.
- Le fichier `/etc/securetty` contient la liste des terminaux depuis lesquels `root` peut se connecter. Par défaut, cela est arrêté aux consoles virtuelles locales (ttys). Soyez très prudent lors de l'ajout de nouvelles choses à ce fichier. Vous devriez être capable de vous connecter à distance avec votre compte normal, puis utiliser `su` si nécessaire (de préférence sous couvert de ssh ou un autre tube crypté), il n'y a donc pas de besoin de se connecter directement sous `root`.
- Soyez toujours lent et réfléchi sous `root`. Vos actions peuvent modifier beaucoup de choses, faites sept fois le tour du clavier avant de taper!

Si vous avez absolument besoin d'autoriser quelqu'un (de préférence de toute confiance) à avoir un accès `root` sur votre machine, il y a un certain nombre d'outils qui peuvent vous y aider. `sudo` autorise les utilisateurs à accéder à un certain nombre de commandes comme `root` avec leur propre mot de passe. Cela devrait vous permettre ainsi de laisser un utilisateur éjecter et monter un support amovible, sans aucun autre privilège `root`. `sudo` garde aussi une trace de toutes les tentatives réussies ou non d'utilisation, vous permettant de savoir qui a utilisé quelle commande pour faire quoi. Pour cette raison `sudo` marche bien même à des endroits où certaines personnes ont des accès `root`, car il vous aide à suivre les changements apportés.

Bien que `sudo` puisse être utilisé pour donner à certains utilisateurs des privilèges pour effectuer certaines tâches, il présente quelques inconvénients. Il devrait être utilisé uniquement pour un ensemble de tâches limitées, comme redémarrer un serveur ou ajouter de nouveaux utilisateurs. Tout programme offrant une fuite vers un *shell* donnera l'accès `root` à un utilisateur l'invoquant depuis `sudo`. Cela inclut la plupart des éditeurs, par exemple. De même, un programme aussi inoffensif que `/bin/cat` peut être utilisé pour écraser des fichiers, ce qui pourrait être utilisé pour exploiter `root`. Envisagez `sudo` comme un moyen de responsabilisation, mais n'espérez pas qu'il remplace l'utilisateur `root` tout en étant sûr.

11.5. Sécurité des fichiers et des systèmes de fichiers

Quelques minutes de préparation et de planification avant de mettre votre système en ligne peut vous aider à le protéger ainsi que les données qu'il contient.

- Il ne devrait y avoir aucune raison pour que le répertoire « maison » d'un utilisateur y autorise l'exécution de programmes SUID/SGID. Utiliser l'option `nosuid` dans `/etc/fstab` pour les partitions en écriture par d'autres que `root`. vous pourrez aussi souhaiter utiliser `nodev` et `noexec` sur la partition des répertoires des utilisateurs, ainsi que sur `/var`, interdisant ainsi l'exécution de programmes, et la création de périphériques caractère ou bloc, qui ne devraient jamais être nécessaires de toute façon.
- Si vous exportez des systèmes de fichier via NFS, assurez vous de configurer `/etc/exports` avec le plus de restrictions d'accès possibles. Cela signifie ne pas utiliser de caractères d'englobement (`* ?`) ni autoriser un accès pour `root` en écriture, et exporter en lecture seule chaque fois que c'est possible.

- Configurez le `umask` de création de fichier des utilisateurs le plus restrictif possible, voir *Paramètres umask*, page 101.
- Si vous montez des systèmes de fichier en utilisant un système de fichier réseau comme NFS, assurez vous de configurer `/etc/exports` avec des restrictions appropriées. Généralement, utiliser 'nodev', 'nosuid', et même 'noexec', est souhaitable.
- Fixer les limites du système de fichier, au lieu de le laisser **illimité** comme il est par défaut. Vous pouvez contrôler des limites par utilisateurs en utilisant le module de limites de ressources PAM et le fichier `/etc/pam.d/limits.conf`. Par exemple, les limites pour le groupe `users` pourraient ressembler à cela :

  ```
  @users     hard  core    0
  @users     hard  nproc   50
  @users     hard  rss     5000
  ```

  Cela interdit la création de fichiers « core », limite le nombre de processus à 50, et limite l'utilisation de la mémoire par utilisateur à 5Mo.

  Vous pouvez aussi utiliser le fichier de configuration `/etc/login.defs` pour régler les mêmes limites.
- Les fichiers `/var/log/wtmp` et `/var/run/utmp` contiennent les registres de connexion pour tous les utilisateurs de votre système. Leur intégrité doit être assurée, car ils peuvent être utilisés pour déterminer quand et d'où un utilisateur (ou un possible intrus) est entré sur le système. Ces fichiers devraient aussi avoir des permissions en `644`, sans affecter la marche normale du système.
- Le bit « inaltérable » peut être utilisé pour empêcher l'effacement ou l'écrasement accidentel d'un fichier qui doit être protégé. Cela empêche aussi quelqu'un de créer un lien dur vers le fichier. Voir la page chattr(1) pour plus d'information sur le bit « inaltérable ».
- Les fichiers SUID et SGID sur votre système présentent un risque potentiel de sécurité, et devraient être surveillés de près. Du fait que ces programmes donnent des privilèges particuliers aux utilisateurs qui les exécutent, il est nécessaire de s'assurer que des programmes non sûrs ne sont pas installés. Un coup favori des « crackers » est d'exploiter les programmes `SUID-root`, puis laisser un programme SUID comme porte dérobée (*backdoor*) pour rentrer à nouveau plus tard, même si le trou original a été bouché.

  Cherchez tous les programmes SUID/SGID sur votre système, et gardez une trace de ce qu'ils sont, de sorte que vous puissiez vous rendre compte de tout changement, ce qui pourrait indiquer un intrus potentiel. Utilisez les commandes suivantes pour trouver tous les programmes SUID/SGID de votre système :

  ```
  root#  find / -type f \( -perm -04000 -o -perm -02000 \)
  ```

  Vous pouvez supprimer la permission SUID ou SGID sur un programme suspect avec la commande `chmod`, puis changez-la à nouveau si vous vous rendez compte que c'est absolument nécessaire.
- Les fichiers en écriture non restreinte (*world-writable*), plus particulièrement les fichiers systèmes, peuvent être un trou de sécurité si un cracker obtient l'accès à votre système, et les modifie. De plus, les répertoires en écriture non restreinte sont dangereux, car ils autorisent à un cracker de créer ou effacer des fichiers à volonté. pour localiser de tels fichiers sur votre système, utilisez la commande suivante :

  ```
  root# find / -perm -2 ! -type l -ls
  ```

  et assurez-vous de la cause de l'existence de tels fichiers. En utilisation normale, plusieurs fichiers seront en écriture non restreinte, même certains fichiers de `/dev`, et les liens symboliques, d'où le `! -type l` qui exclut ces derniers de la commande `find`.
- Les fichiers sans propriétaire peuvent aussi être un signe qu'un intrus est passé par là. Vous pouvez localiser les fichiers qui n'ont pas de propriétaire ou de groupe propriétaire grâce à la commande :

  ```
  root# find / \( -nouser -o -nogroup \) -print
  ```

- Trouver les fichiers `.rhosts` devrait faire partie de vos devoirs d'administrateur système, car ils devraient être bannis de votre système. Rappelez-vous qu'un cracker n'a besoin que d'un compte ouvert pour avoir l'opportunité d'accéder au réseau entier. Vous pouvez localiser les fichiers `.rhosts` avec la commande :

  ```
  root# find /home -name .rhosts -print
  ```

- Enfin, avant de changer les permissions d'un fichier système, assurez-vous que vous comprenez ce que vous faites, ne changez jamais les permissions d'un fichier parce que cela semble être une manière facile pour que tout marche bien. Cherchez toujours à savoir pourquoi ce fichier a ces permissions avant de les modifier.

11.5.1. Paramètres umask

La commande `umask` peut être utilisée pour connaître le mode de création des fichiers par défaut sur votre système. C'est le complément octal du mode du fichier en question. Si les fichiers sont créés sans égard à leurs permissions, l'utilisateur pourrait donner des permissions en lecture ou en écriture par inadvertance à quelqu'un qui ne devrait pas avoir ces permissions. Généralement, les paramètres `umask` sont `022`, `027`, ou `077` (qui est le plus restrictif). Normalement, le umask est fixé dans `/etc/profile`, de sorte qu'il s'applique à tous les utilisateurs du système. le masque de création de fichiers peut être calculé en soustrayant la valeur souhaitée de `777`. En d'autres termes, un umask de `777` implique que les fichiers nouvellement créés de contiennent des permissions sans lecture, ni écriture, ni exécution pour tout le monde. Un masque de `666` implique que les fichiers nouvellement créés ont un masque de `111`. Par exemple, vous pourriez avoir une ligne comme celle-ci :

```
# Fixer le umask utilisateur par défaut
umask 033
```

Assurez-vous d'utiliser un `umask` pour `root`'s de `077`, qui interdira lecture, écriture, et exécution pour les autres utilisateurs a moins que vous ne changiez cela explicitement avec la commande `chmod`. Dans ce cas, les répertoires nouvellement créés devraient avoir des permissions de `744`, obtenues en soustrayant `033` de `777`. Les fichiers nouvellement créés avec un `umask` de `033` devraient avoir des permissions de `644`.

Pour Mandriva Linux, il est juste nécessaire d'utiliser un `umask` de `002`. Cela est dû au fait que la configuration de base utilise un groupe par utilisateur.

11.5.2. Permissions des fichiers

Il est important de vous assurer que vos fichiers système ne sont pas ouverts à des modifications accidentelles des utilisateurs et des groupes qui ne devraient pas faire de maintenance système.

UNIX différencie le contrôle d'accès aux fichiers et répertoire selon trois critères : propriétaire, groupe, et autres. Il y a toujours un seul propriétaire, un nombre quelconque de membres du groupe et tous les autres.

Une explication rapide des permissions sous UNIX :

Propriété – Quels utilisateurs et groupes ont le contrôle des paramètres de permission du noeud et du parent du noeud

Permissions – Bits susceptibles d'être mis ou enlevés pour permettre un certain type d'accès. Les permissions pour les répertoires peuvent avoir une signification différente des mêmes paramètres de permissions sur un fichier.

Lecture :

- Être capable de lire le contenu d'un fichier
- Être capable de lire un répertoire

Écriture:

- Être capable d'ajouter ou modifier un fichier
- Être capable de supprimer ou de déplacer des fichiers d'un répertoire

Exécution:

- Être capable de lancer un programme binaire ou un script *shell*
- Être capable de chercher dans un répertoire, en accord avec la permission de lecture

Attribut de sauvegarde du texte : (Pour les répertoires)

Le « *sticky bit* » (bit de conservation) a aussi un comportement différent lorsqu'il est appliqué aux répertoires. Si le bit de conservation est mis sur un répertoire, alors un utilisateur pourra seulement supprimer les fichiers qu'il y possède, ou pour lesquels il a des droits explicites en écriture, même s'il a les droits en écriture sur ce répertoire. Cela est conçu pour des répertoires tels que `/tmp`, qui sont `world-writable` (écriture par tout le monde), mais où il ne vaut mieux pas que les utilisateurs puissent effacer des fichiers à l'envie. Le `sticky bit` est vu comme un `t` dans un listing de répertoire détaillé.

Attribut SUID : (Pour les fichiers)

Il s'agit de la permission « *set-user-id* » (utiliser ID utilisateur) sur le fichier. Quand le mode d'utilisation de l'ID utilisateur est mis dans les permissions du propriétaire, et si le fichier est exécutable, les processus qui l'utilisent obtiennent les ressources systèmes de l'utilisateur qui possède le fichier, et non plus de l'utilisateur qui a lancé le processus. Cela est la cause de beaucoup de violations de type *buffer overflow* (dépassement de mémoire tampon).

Attribut SGID : (Pour fichiers)

S'il est utilisé dans les permissions du groupe, ce bit contrôle le statut « *set group id* » d'un fichier. Il se comporte comme pour suid, à part que c'est le groupe qui en est bénéficiaire. Le fichier doit être exécutable pour faire effet.

Attribut SGID : (Pour répertoires)

Si vous activez le bitSGID sur un répertoire (avec `chmod g+s directory`), les fichiers qui y seront créés auront leur groupe mis au groupe du répertoire.

Vous – Le propriétaire du fichier

Groupe – Le groupe auquel vous appartenez

Tous – Quiconque sur le système qui n'est ni propriétaire, ni membre du groupe

Exemple de fichier :

```
        -rw-r--r--  1 kevin  users         114 Aug 28  1997 .zlogin
1st bit - répertoire?                (non)
2nd bit - lecture propriétaire?      (oui, par kevin)
3rd bit - écriture par propriétaire? (oui, par kevin)
4th bit - exécution propriétaire?    (non)
5th bit - lecture groupe?            (oui, par users)
6th bit - écriture groupe?           (non)
7th bit - exécution groupe?          (non)
8th bit - lecture tous?              (oui, par tous)
9th bit - lecture tous?              (non)
10th bit - exécution tous?           (non)
```

Les lignes suivantes sont des exemples d'ensembles de permissions qui sont nécessaires pour avoir l'accès décrit. Vous voudrez sans doute donner plus de permissions que celles données ici, mais on ne décrit ici que l'effet de ces permissions minimales :

```
-r--------  Autoriser l'accès en lecture au fichier par le propriétaire
--w-------  Autoriser le propriétaire à modifier ou effacer le fichier
 (Notez que quiconque ayant les droits d'écriture sur le répertoire
```

```
 dans lequel se trouve le fichier peut l'écraser/effacer)
---x------  Le propriétaire peut exécuter ce programme, mais pas de
 script shell, qui de plus nécessite un droit en lecture
---s------  Sera exécuté avec l'UID du propriétaire
------s---  Sera exécuté avec le GID du groupe
-rw------T  Pas de mise à jour du "last modified time"
 (Heure de dernièremodification).
 Généralement utilisé pour le fichiers d'échange (swap)
---------t  Aucun effet. (anciennement bit de conservation)
```

Exemple de répertoires :

```
drwxr-xr-x  3 kevin  users         512 Sep 19 13:47 .public_html/
1e bit - répertoire?             (oui, il contient de nombreux fichiers)
2e bit - lecture propriétaire?   (oui, par kevin)
3e bit - écriture propriétaire?  (oui, par kevin)
4e bit - exécution propriétaire? (oui, par kevin)
5e bit - lecture groupe?         (oui, par users)
6e bit - écriture groupe?        (non)
7e bit - exécution groupe?       (oui, par users)
8e bit - lecture par tous?       (oui, par tous)
9e bit - écriture par tous?      (non)
10e bit - exécution par tous?    (oui, par tous)
```

Les lignes qui suivent sont des exemples des ensembles de permissions minimum requis pour autoriser l'accès décrit. Vous voudrez sans doute donner plus de permissions que celles données ici, mais on ne décrit ici que l'effet de ces permissions minimales :

```
dr--------  Le contenu peut être listé, mais l'attribut des fichiers ne peut être lu
d--x------  Le répertoire est accessible, et utilisé comme chemin en exécution complète
dr-x------  Les attributs de fichiers peuvent être lus par le propriétaire
d-wx------  Les fichiers peuvent être créés/effacés, même si le répertoire  n'est pas le répertoire courant
d-----x--t  Empêche l'effacement de fichiers par "tous" ceux ayant un droit d'écriture. Utilisé pour /tmp
d--s--s---  Aucun effet
```

Les fichiers de configuration système (généralement dans `/etc`) ont souvent un mode de `640` (`-rw-r-----`), et sont possédés par `root`. Selon les besoins en sécurité de votre site, vous pouvez les ajuster. Ne laissez jamais un fichier système en écriture pour un groupe ou pour tous. Certains fichiers de configuration, dont `/etc/shadow`, devraient n'être en lecture que par `root`, et les répertoires de `/etc` ne devraient pas être accessibles par tous, au moins.

Scripts Shell SUID

les scripts *shell* suid représentent un sérieux risque de sécurité, et pour cette raison, le noyau n'en tiendra pas compte. Quel que soit le degré de sécurité que vous supposez pour ces scripts, ils peuvent être exploités par le cracker pour lui fournir un *shell* `root`.

11.5.3. Contrôles d'intégrité

Une autre très bonne manière de détecter des attaques locales (et réseau) sur votre système est de lancer un contrôleur d'intégrité comme Tripwire, Aide ou Osiris. Ces contrôleurs d'intégrité génèrent un certain nombre de sommes de contrôle sur tous vos binaires et fichiers systèmes importants et les comparent à une base de données précédemment générée de valeurs références bien connues. Ainsi, tout changement dans un fichier sera détecté.

C'est un bon réflexe d'installer ce genre de programmes sur une disquette, puis d'empêcher physiquement l'écriture sur celle-ci. De cette façon. les intrus ne pourront pas altérer le contrôleur d'intégrité lui-même ou modifier sa base de données. Une fois que vous avez une application de ce style configurée, il est conseillé de l'ajouter à vos devoirs d'administrateurs système pour vérifier que rien n'a changé.

Vous pouvez même ajouter un entrée `crontab` pour lancer le contrôleur depuis votre disquette toute les nuits et vous envoyer un message le matin. Quelque chose comme :

```
# set mailto
MAILTO=kevin
# run Tripwire
```

```
15 05 * * * root /usr/local/adm/tcheck/tripwire
```

Vous enverra un rapport tous les matins à 5H15.

Les contrôleurs d'intégrité peuvent être une aubaine pour détecter des intrusions avant même que vous ne puissiez les remarquer. Comme beaucoup de fichiers changent sur un système moyen, vous devrez faire le discernement entre des activités de cracker et vos propres agissements.

Vous pouvez trouver une version libre et non prise en charge de Tripwire sur le site tripwire.org (`http://www.tripwire.org`), gratuitement. Des manuels et de l'assistance technique peuvent être achetés.

Aide peut être trouvé sur Sourceforge (`http://sourceforge.net/projects/aide`).

Osiris peut être trouvé à OSIRIS — Host Integrity Management (`http://osiris.shmoo.com/`).

11.5.4. Chevaux de Troie

Les « Chevaux de Troie » tirent leur nom du célèbre stratagème décrit dans l'Iliade d'Homère. L'idée est qu'un cracker distribue un programme ou binaire qui semble intéressant, et encourage d'autres personnes à le télécharger et le lancer en tant que `root`. Alors, le programme peut compromettre leur système pendant qu'ils n'y prêtent pas attention. Alors qu'ils pensent que le logiciel qu'ils viennent de charger ne fait qu'une seule chose (et parfois très bien), il compromet aussi leur sécurité.

Vous devez prendre garde aux programmes que vous installez sur votre machine. Mandriva fournit les sommes de contrôle MD5 et les signatures PGP de chacun des RPM qu'il fournit, de sorte que vous puissiez vérifier que vous installez la bonne chose. Vous ne devriez jamais lancer un binaire que vous ne connaissez pas, pour lequel vous n'avez pas les sources comme `root` ! Peu d'attaquants souhaitent publier leur code source pour sondage public.

Bien que cela puisse être complexe, assurez-vous que vous obtenez le code source d'un programme depuis son site réel de distribution. Si le programme doit être lancé par `root`, assurez vous que vous ou quelqu'un de confiance a regardé les sources et les a vérifiées.

11.6. Sécurité des mots de passe et cryptage

La plupart des programmes de cryptage décrits dans ce chapitre sont disponibles dans votre distribution Mandriva Linux.

Une des caractéristiques de sécurité les plus importantes utilisée aujourd'hui est le mot de passe. Il est important que vous et vos utilisateurs ayez des mots de passe sûrs et impossibles à deviner. Votre distribution Mandriva Linux fournit le programme `passwd` qui interdit l'utilisation d'un mot de passe trop simple. Assurez vous que votre version de `passwd` est à jour.

Une discussion en profondeur du thème du cryptage est au delà de la portée de ce document, mais une introduction est de rigueur. Le cryptage est très utile, parfois même nécessaire à notre époque. Il y a toutes sortes de méthodes de cryptage des données, chacune avec ses propres caractéristiques.

La plupart des UNIXs (et GNU/Linux n'y fait pas exception) utilisent principalement un algorithme de chiffrement à sens unique appelé DES (*Data Encryption Standard*, soit Standard de cryptage de données) pour crypter vos mots de passe. Ce mot de passe crypté est alors gardé dans le fichier `/etc/shadow`. Quand vous essayez de vous connecter, le mot de passe que vous tapez est crypté à nouveau et comparé avec l'entrée contenue dans le fichier qui contient les mots de passe. S'ils coïncident, cela doit être le même mot de passe, et l'accès est alors autorisé. Bien que DES soit un algorithme de cryptage à double sens (vous pouvez coder puis décoder un message, la bonne clé étant fournie), les variantes utilisées par la plupart des UNIXs sont à sens unique. Cela signifie qu'il ne devrait pas être possible de renverser le chiffrement pour récupérer le mot de passe d'après le contenu du fichier `/etc/shadow`.

Des attaques en force, du type « Crack » ou « John the Ripper » (voir la section *"Crack" et "John the Ripper"*, page 109) peuvent souvent deviner vos mots de passe, à moins qu'ils ne soient suffisamment aléatoires. Les modules PAM (voir ci-dessous) vous permettent d'utiliser différentes routines de cryptage pour vos mots de passe (MD5 ou similaire). Vous pouvez aussi utiliser Crack à votre avantage. Envisagez de le lancer périodiquement

sur votre propre base de mots de passe, pour trouver les mots de passe non sûrs. Contactez alors l'utilisateur en infraction, et demandez lui de changer son mot de passe.

Vous pouvez vous rendre sur le site du CERN (`http://consult.cern.ch/writeup/security/security_3.html`) pour des conseils sur le choix d'un bon mot de passe.

11.6.1. PGP et la cryptographie à clé publique

La cryptographie à clé publique, comme celle utilisée par PGP, utilise une clé pour le cryptage, et une autre pour le décryptage. La cryptographie traditionnelle, pourtant, utilise la même clé pour le cryptage, et le décryptage ; cette clé doit être connue des deux côtés, et quelqu'un a donc dû transférer de manière sûre la clé d'un côté à l'autre.

pour soulager le besoin de transférer de manière sûre la clé de chiffrement, la clé publique de cryptage utilise deux clés séparées : Une clé publique et une clé privée. La clé publique de chacun est disponible pour quiconque pour faire le cryptage, alors que cependant, chacun garde sa clé privée pour décrypter les messages cryptés avec la clé publique.

Il y a des avantages aux deux méthodes de cryptage, clé publique ou clé privée, et vous pouvez lire à propos de leurs différences : La FAQ pour la cryptographie RSA, citée à la fin de cette section.

PGP (*Pretty Good Privacy*, soit intimité plutôt bonne) est bien toléré par GNU/Linux. Les versions 2.6.2 et 5.0 sont reconnues pour leur stabilité. Pour des nouvelles de PGP et comment l'utiliser, jetez un coup d'oeil aux différentes FAQs de PGP : faqs.org (`http://www.faqs.org/faqs/pgp-faq/`)

Veillez à utiliser la version autorisée dans votre pays. Du fait des restrictions d'exportation du gouvernement américain, il est interdit de transférer hors de ce pays de la cryptographie lourde sous forme électronique.

Les contrôles d'exportation des US sont maintenant gérés par EAR (*Export Administration Regulations*), et non plus par ITAR.

Il y a aussi un guide pas à pas pour configurer PGP sous GNU/Linux disponible sur LinuxFocus (`http://mercury.chem.pitt.edu/~angel/LinuxFocus/English/November1997/article7.html`). Il a été écrit pour la version internationale de PGP, mais est aisément transposable à la version des États-Unis. Vous pourriez aussi avoir besoin de correctifs pour certaines des dernières versions de GNU/Linux; le correctif (*patch*) est disponible chez metalab (`ftp://metalab.unc.edu/pub/Linux/apps/crypto`).

Il y a un projet travaillant sur une réimplantation libre de PGP sous licence « *open source* ». GnuPG est un remplaçant complet et libre pour PGP. Du fait qu'il n'utilise pas IDEA ou RSA il peut être utilisé sans aucune restriction. GnuPG respecte pratiquement OpenPGP (`http://www.faqs.org/rfcs/rfc2440.html`). Voir la page Web GNU Privacy Guard (`http://www.gnupg.org`) pour plus d'information.

Vous trouverez plus de renseignements au sujet de la cryptographie dans la FAQ du site de la cryptographie RSA (`http://www.rsasecurity.com/rsalabs/faq/`). Vous trouverez ici toute l'information sur des sujets tels que « Diffie-Hellman », « cryptographie à clé publique », « certificats électroniques », etc.

11.6.2. SSL, S-HTTP, et S/MIME

Les utilisateurs se demandent souvent ce qui différencient les différents protocoles de cryptage, et comment les utiliser. Bien que ce document ne soit pas consacré au cryptage, il est bon d'expliquer brièvement ce qu'est chaque protocole, et où trouver plus d'information.

- SSL : - SSL (*Secure Sockets Layer*) est une méthode de cryptage développée par Netscape pour fournir de la sécurité sur Internet. Il prend en charge plusieurs protocoles de cryptage et fournit l'authentification du client et du serveur. SSL agit sur la couche transport, crée un canal crypté de données et peut ainsi encoder des données de diverses natures. Vous constaterez cela lorsque vous visiterez un site sécurisé pour consulter un document en ligne avec Communicator. C'est également la base des communications sécuritaires avec Communicator, ainsi qu'avec plusieurs composantes de chiffrement de données de Netscape Communications. Vous trouverez plus de renseignements sur le site Openssl.org (`http://www.openssl.org`). Des informations sur les autres implémentations de sécurité de Netscape et un bon point de départ pour ces protocoles sont disponibles sur le site de Netscape (`http://wp.netscape.com/security/index.html`). Mentionnons aussi que le protocole SSL peut être utilisé pour passer nombre de protocoles communs, en les **enveloppant** par sécurité. Voir le site de Quiltaholic (`http://www.quiltaholic.com/rickk/sslwrap/`).

- S-HTTP : - S-HTTP est un autre protocole qui fournit des services de sécurité par Internet. Il a été conçu pour pourvoir, aux deux parties impliquées dans les transactions, confidentialité, authentification, intégrité, et non répudiation [ne pas pouvoir être pris pour un autre] tout en gérant des mécanismes à clés multiples et des algorithmes de cryptographie à négociation d'options. S-HTTP est limité au logiciel spécifique qui l'implémente et crypte chaque message individuellement. [extrait de « RSA Cryptography FAQ », page 138]
- S/MIME : - S/MIME (*Secure Multipurpose Internet Mail Extension*, soit extension de courrier électronique sécurisé à portée multiple) est un standard de cryptage utilisé pour crypter le courrier électronique et autres types de messages sur Internet. C'est un standard ouvert développé par la RSA, de sorte qu'il est probable qu'il apparaisse sous GNU/Linux un jour ou l'autre. plus de renseignements sur S/MIME peuvent être trouvés sur RFC2311 (`http://www.ietf.org/rfc/rfc2311.txt`).

11.6.3. Implémentations IPSEC

A côté de CIPE, et d'autres formes de cryptage de données, il y a aussi plusieurs implémentations de IPSEC pour GNU/Linux. IPSEC est une tentative de l'IETF de création de communications cryptées, donc sûres, au niveau du réseau IP, pour assurer authentification, intégrité, contrôle d'accès, et confidentialité. Des informations sur IPSEC le projet Internet peuvent être consultées sur : ipsec Charter (`http://www.ietf.org/html.charters/ipsec-charter.html`). Vous pouvez aussi trouver des liens vers d'autres protocoles impliquant la gestion de clés, et une *mailing list* IPSEC et son archive.

L'implémentation de GNU/Linux x-kernel, qui était développée à la University of Arizona, utilise une base orientée objet pour implémenter les protocoles réseau appelés x-kernel. En clair, le x-kernel est une méthode pour passer les messages au niveau du noyau, ce qui facilite l'implémentation. Ce projet n'est plus en développement mais des renseignements peuvent être trouvés sur le site The x-Kernel Project (`http://openresource.com/openres/orgs/DP/P/x-Kernel.shtml`).

Une autre implémentation de IPSEC est l'IPSEC « FreeS/WAN » GNU/Linux, qui est librement disponible. Leur page Web indique : « Ces services vous permettent de monter un tuyau sécurisé à travers des réseaux non fiables. Tout ce qui passe à travers le réseau non fiable est crypté par la machine passerelle IPSEC et décrypté par la passerelle à l'autre bout. Cela conduit à un réseau privé virtuel ou VPN (*Virtual Private Network*). C'est un réseau qui est effectivement privé, même s'il inclut des machines de plusieurs sites différents interconnectés par Internet, non sûrs. »

Elle est disponible en téléchargement sur le site Linux FreeS/WAN (`http://www.freeswan.org/`).

De même que d'autres formes de cryptographie, elle n'est pas distribuée dans le noyau par défaut, à cause des restrictions à l'exportation.

11.6.4. ssh (shell sécurisé) et stelnet

`ssh` et `stelnet` sont des suites de programmes qui permettent de se connecter à un système distant avec des échanges cryptés.

`ssh` est une suite de programmes utilisée comme remplacement sécurisé de `rlogin`, `rsh` et `rcp`. Elle utilise la cryptographie à clé publique pour crypter les communications entre deux hôtes, ainsi que l'authentification des utilisateurs. Ces outils peuvent être utilisés pour se connecter à un serveur distant ou copier des données entre deux hôtes, tout en empêchant des attaques de tiers (« *session hijacking* ») et « *DNS spoofing* ». Ils assurent la compression de données sur vos connections et les communications X11 sécurisées.

Il y a à l'heure actuelle plusieurs implémentations de ssh. L'implémentation commerciale originale par Data Fellows peut être trouvée sur la page `ssh` de datafellows.com (`http://www.datafellows.com`).

L'excellente implémentation Openssh est basée sur une ancienne version de DataFellows ssh et a été entièrement retravaillée pour n'inclure aucun brevet ou partie propriétaire. Elle est libre et sous licence BSD. Elle peut être trouvée sur : http://www.openssh.com (`http://www.openssh.com`).

Il y a aussi un projet « *open source* » pour réimplémenter ssh depuis le néant appelé « lsh ». Pour plus de renseignements, consulter : LSH (`http://www.lysator.liu.se/~nisse/lsh/`).

Vous pouvez aussi utiliser `ssh` depuis vos stations Windows® vers votre serveur `ssh` GNU/Linux. Il y a plusieurs implémentations de clients Windows® librement disponibles, dont celui de PuTTY (`http://www.`

`chiark.greenend.org.uk/~sgtatham/putty/`), ainsi qu'une version commerciale de DataFellows, sur le site DataFellows (`http://www.datafellows.com`).

SSLeay (obsolète, voir OpenSSL plus loin) est une implémentation libre du protocole `Secure Sockets Layer` de Netscape, développé par Eric Young. Elle comporte plusieurs applications, comme « Secure telnet », un module pour Apache, plusieurs bases de données, ainsi que plusieurs algorithmes dont DES, IDEA et « Blowfish ».

En utilisant cette bibliothèque, un remplacement de `telnet` sécurisé qui fait du cryptage par dessus une connexion `telnet`. Au contraire de SSH, `stelnet` utilise SSL, le protocole `Secure Sockets Layer` développé par Netscape. Vous pourrez trouver « Secure telnet » et « Secure FTP » en commençant par la FAQ SSLeay et SSLapps (`http://www.psy.uq.oz.au/~ftp/Crypto/`) (en anglais).

Le projet OpenSSL basé sur SSLeay a pour but de développer une boîte à outils robuste, de qualité commerciale, entièrement fonctionnelle, et *Open Source* qui implémente les protocoles *Secure Sockets Layer* (SSL v2/v3) et *Transport Layer Security* (TLS v1) ainsi qu'une librairie de cryptographie forte d'usage général. Pour plus d'informations sur ce projet, consultez les Pages OpenSSL (`www.openssl.org`). Il y a aussi une liste conséquente d'applications basées sur OpenSSL sur Applications en relation avec OpenSSL (`http://www.openssl.org/related/apps.html`).

SRP est une autre implémentation sécurisée de `telnet/ftp`. Extrait de leur page Web :

« Le projet SRP développe des logiciels Internet sûrs pour une utilisation mondiale gratuite. À partir d'une distribution de Telnet et FTP totalement sécurisés, nous espérons supplanter les systèmes d'authentification réseau vulnérables par des substituts solides qui ne sacrifient en rien la facilité d'utilisation pour la sécurité. La sécurité devrait être de fait et non pas une option ! »

Pour plus de renseignements, visiter stanford.edu (`http://srp.stanford.edu/srp`).

11.6.5. PAM - modules additionnels d'authentification

Votre version de Mandriva Linux est fournie avec une combinaison d'authentifications unifiée appelée PAM. PAM vous permet de changer vos méthodes d'authentification et exigences à la volée, et encapsule toutes les méthodes locales d'authentification sans besoin de recompiler un quelconque binaire. La configuration de PAM est au delà de la portée de ce chapitre, mais allez faire un tour du côté du site Web de PAM : kernel.org (`http://www.kernel.org/pub/linux/libs/pam/index.html`).

Juste un aperçu des possibilités de PAM :

- Utilisez un cryptage autre que DES pour vos mots de passe. (Les rendant plus résistants aux décodages par la force)
- Fixez des limites de ressources pour tous vos utilisateurs, de sorte qu'ils ne puissent mener des attaques de type dénis de service (*denial of service*) (nombre de processus, quantité de mémoire, etc.)
- Activez les mots de passe fantôme (*shadow*) (voir ci-dessous) à la volée
- Autorisez certains utilisateurs à se connecter uniquement à certaines heures depuis des sites spécifiques

En quelques heures d'installation et de configuration de votre système, vous pouvez empêcher plusieurs attaques avant qu'elles ne surviennent. Par exemple, utilisez PAM pour désactiver l'utilisation sur tout le système des fichiers `.rhosts` dans les répertoires des utilisateurs en ajoutant ces lignes dans `/etc/pam.d/rlogin` :

```
#
# Désactiver rsh/rlogin/rexec pour les utilisateurs
#
login auth required pam_rhosts_auth.so no_rhosts
```

11.6.6. Encapsulation IP Cryptographique (CIPE)

Le premier objectif de ce logiciel est de fournir un moyen de sécuriser (contre l'espionnage, y compris l'analyse de trafic, et l'injection de message truqué) des interconnexions de sous-réseaux au travers d'un réseau par paquets non sûr tel que Internet.

CIPE crypte les données au niveau du réseau. Les paquets voyageant entre les hôtes sur le réseau sont cryptés. Le moteur de cryptage est placé près du périphérique qui envoie et reçoit les paquets.

Cela est différent de SSH, qui crypte les données par connexion, au niveau du port (*socket*). Une connexion logique entre des programmes tournant sur des hôtes différents est cryptée.

CIPE peut être utilisé pour faire du pontage (*tunnelling*), afin de créer un réseau privé virtuel (VPN). Le cryptage de bas niveau a l'avantage de pouvoir être rendu transparent entre deux réseaux connectés dans le VPN, sans besoin de changer une quelconque application.

Résumé depuis la documentation de CIPE :

« Le standard IPSEC définit un ensemble de protocoles qui peuvent être utilisés (entre autre) pour monter des VPN cryptés. Cependant, IPSEC est un protocole plutôt lourd et compliqué possédant un grand nombre d'options, les implémentations de l'ensemble complet du protocole sont encore rarement utilisés et plusieurs problèmes (tel que la gestion des clés) ne sont toujours pas complètement résolus. CIPE utilise une approche simple, dans laquelle beaucoup de choses modifiables (comme le choix de l'algorithme de cryptage effectivement utilisé) sont fixées à l'installation. Cela limite la flexibilité, mais permet une implémentation simple (et par là même efficace, facile à déboguer...). »

Plus d'informations peuvent être trouvées chez CIPE Project (`http://sites.inka.de/sites/bigred/devel/cipe.html`)

De même que d'autres formes de cryptographie, il n'est pas distribué avec le noyau par défaut du fait de restrictions à l'exportation.

11.6.7. Kerberos

Kerberos est un système d'authentification développé par The Athena Project au MIT. Quand un utilisateur se connecte, Kerberos authentifie cet utilisateur (en utilisant un mot de passe), et fournit à cet utilisateur un moyen de prouver son identité aux autres serveurs et hôtes disséminés sur le réseau.

Cette authentification est alors utilisée par des programmes tels que `rlogin` pour autoriser l'utilisateur à se connecter à d'autres hôtes sans mot de passe (au lieu du fichier `.rhosts`). Cette méthode d'authentification peut aussi être utilisée par le système de courrier électronique pour garantir que les messages seront délivrés à la bonne personne, ainsi que pour garantir l'authenticité de l'expéditeur.

Kerberos et les programmes qui l'accompagnent, empêchent les utilisateurs de tromper le système en lui faisant croire qu'ils sont quelqu'un d'autre (« *spoofing* »). Malheureusement, installer Kerberos est très intrusif, et demande le remplacement ou la modification de nombreux programmes standards.

Vous pourrez trouver plus d'informations à propos de Kerberos en visitant la FAQ Kerberos (`http://www.faqs.org/faqs/kerberos-faq/general/`), et le code peut être obtenu depuis le site mit.edu (`http://web.mit.edu/kerberos/www/`).

[Stein, Jennifer G., Clifford Neuman, and Jeffrey L. Schiller. "Kerberos : An Authentication Service for Open Network Systems." USENIX Conference Proceedings, Dallas, Texas, Winter 1998.]

Kerberos ne devrait pas être votre premier pas pour améliorer la sécurité de votre hôte. Il est plutôt compliqué, et pas aussi répandu que, disons SSH.

11.6.8. Les mots de passe Shadow

Les mots de passe Shadow sont un moyen de cacher vos informations de cryptage de mots de passe aux utilisateurs normaux. Votre système d'exploitation Mandriva Linux utilise les mots de passe Shadow par défaut, mais d'autres systèmes stockent les mots de passe cryptés dans le fichier `/etc/passwd` où tout le monde peut les lire. N'importe qui peut alors exécuter des programmes de cassage de mots de passe et ainsi les déterminer. Les mots de passe Shadow, à l'inverse, sont sauvegardés dans le fichier `/etc/shadow`, que seuls les utilisateurs autorisés peuvent lire. Vous pouvez lire Shadow-Password HOWTO (`http://www.tldp.org/`

HOWTO/Shadow-Password-HOWTO.html) pour obtenir plus de renseignements, si nécessaire. Il date un peu et n'est pas requis pour des distributions supportant PAM, comme votre système Mandriva Linux.

11.6.9. "Crack" et "John the Ripper"

Si pour une raison quelconque votre programme `passwd` ne force pas l'utilisation de mots de passe difficiles à deviner, vous pourrez souhaiter utiliser un programme de cassage de mots de passe pour vous assurer que les mots de passe de vos utilisateurs sont sûrs.

Les programmes de cassage de mots de passe reposent sur une idée simple : ils essayent tous les mots du dictionnaire, puis des variations sur ces mots, en cryptant chacun d'eux et les comparant à vos mots de passe cryptés. S'ils obtiennent une correspondance, ils ont trouvé le mot de passe

Il y a plusieurs programmes de ce type les deux les plus connus sont Crack et John the Ripper (voir OpenWall (`http://www.openwall.com/john/`)). Malheureusement, ils consomment beaucoup de temps CPU, mais vous devriez être capable de vérifier si un attaquant est susceptible de pénétrer en les utilisant vous-même, puis en avertissant les utilisateurs dont le mot de passe est trop faible. Notez qu'un attaquant devra d'abord utiliser un autre trou pour pouvoir lire votre fichier `/etc/shadow`, mais de tels trous sont plus courants que vous ne le pensez.

Parce que la sécurité n'est aussi forte que si le plus faible des hôtes est protégé, il est bon de mentionner que si vous avez des machines Windows® sur votre réseau, vous devriez jeter un coup d'œil à L0phtCrack, une implantation de Crack sous Windows®. Il est disponible depuis le site atstake.com (`http://www.atstake.com/research/lc3/`).

11.6.10. CFS - Système de Fichiers Crypté et TCFS - Transparent

CFS (*Cryptographic File System*) permet de chiffrer une arborescence complète ; pour leur part, les utilisateurs peuvent y enregistrer des fichiers cryptés. Il utilise un serveur NFS tournant sur la machine locale. Pour obtenir plus de renseignements ainsi que les sources visitez le site de att.com (`ftp://ftp.research.att.com/dist/mab/`).

TCFS (*Transparent Cryptographic File System*) améliore CFS en lui ajoutant une meilleure intégration dans le système de fichiers, de sorte qu'il devient transparent aux utilisateurs quand le système de fichier est crypté. Plus d'informations sur le site de tcfs.it (`http://www.tcfs.it/`).

Il n'a pas non plus besoin d'être utilisé sur des systèmes de fichiers complets. Il fonctionne aussi bien sur de simples arborescences.

11.6.11. X11, SVGA et sécurité de l'affichage

11.6.11.1. X11

Il est important de sécuriser votre affichage graphique pour empêcher les attaquants de saisir vos mots de passe lorsque vous les tapez, lire des documents ou des informations que vous consultez à l'écran, ou même utiliser un trou de sécurité pour obtenir l'accès `root`. Lancer des applications X par réseau peut aussi être dangereux, en autorisant des « *sniffers* » à voir votre interaction avec le système distant.

X possède un certain nombre de mécanismes d'accès de contrôle. Le plus simple d'entre eux est basé sur l'hôte : vous utilisez `xhost` pour spécifier quels hôtes sont autorisés à accéder à votre affichage. Cela n'est pas du tout sûr, car si quelqu'un a accès à votre machine, il peut `xhost + sa.machine` et rentrer aisément. Ainsi, si vous devez autoriser l'accès à une machine peu sûre, quiconque là bas peut violer votre affichage.

Si vous utilisez `xdm` (*X Display Manager*), ou son équivalent pour KDE KDM, pour vous connecter, vous disposez d'une bien meilleure méthode d'accès : MIT-MAGIC-COOKIE-1. Un « cookie » de 128 bits est généré et placé dans votre fichier `.Xauthority`. Si vous avez besoin d'autoriser un accès distant à votre affichage, vous pouvez alors utiliser la commande `xauth` et l'information qui se trouve dans votre fichier `.Xauthority` pour fournir l'accès à cette seule connexion. Voyez le Remote-X-Apps mini-howto : The Linux Documentation Project (`http://www.tldp.org/HOWTO/Remote-X-Apps.html`).

Vous pouvez aussi utiliser `ssh` (voir *ssh (shell sécurisé) et stelnet*, page 106, ci-dessus) pour permettre des connexions X sécurisées. Cela possède aussi l'avantage d'être totalement transparent pour l'utilisateur, et signifie qu'aucune donnée en clair ne circule sur le réseau.

Vous pouvez aussi désactiver toute connexion distante à votre serveur X en utilisant l'option `-nolisten tcp` vers votre serveur X. Ainsi, vous préviendrez toutes les connexions réseau vers votre serveur sur des interfaces de connexion (*sockets*) TCP.

Jetez un coup d'œil à Xsecurity(7x) pour plus de renseignements concernant la sécurité sous X. La bonne manière est d'utiliser `xdm` pour vous connecter à la console, puis d'utiliser `ssh` pour aller sur un site distant sur lequel vous lancez votre application X.

11.6.11.2. SVGA

Les programmes `SVGAlib` sont généralement suid-`root` de façon à pouvoir accéder à tous vos périphériques vidéo. Cela les rend très dangereux. S'ils plantent, Vous devez généralement redémarrer la machine pour récupérer une console utilisable. Assurez-vous que chaque programme SVGA que vous utilisez est authentique, et que vous pouvez leur faire confiance. Ou mieux, ne les utilisez pas du tout.

11.6.11.3. GGI (Projet d'Interface Graphique Générique)

Le projet GNU/Linux GGI essaye de résoudre plusieurs des problèmes de l'interface graphique de GNU/Linux. GGI déplace une petite partie du code vidéo dans le noyau de GNU/Linux, et contrôle alors l'accès au système vidéo. Ce qui signifie que GGI sera capable de récupérer votre console à tout instant vers un état stable connu. Cela permet aussi d'utiliser une clé de sécurité qui empêche l'utilisation de programmes `login` de type « cheval de Troie » (*Trojan*) sur votre console. Projet GGI (`http://www.ggi-project.org`)

11.7. Sécurité du noyau

Ceci constitue une description des options de configuration du noyau en rapport avec la sécurité, une explication de leur effet, et comment les utiliser.

Du fait que le noyau contrôle les communications réseau de votre ordinateur, il est important qu'il soit très sûr, et inviolable. Pour empêcher quelques unes des dernières attaques réseau, vous devriez essayer de garder votre noyau à jour. Vous pouvez trouver les nouvelles versions sur kernel.org (`ftp://ftp.kernel.org`) ou grâce aux mises à jour du paquetage du noyau avec `MandrivaUpdate`.

Il y a là aussi un groupe international qui propose un unique correctif cryptographique unifié pour le noyau GNU/Linux. Ce correctif (*patch*) fournit le support pour plusieurs sous-systèmes cryptographiques et d'autres choses qui ne peuvent pas être inclues dans le noyau principal, à cause des restrictions à l'export. Pour plus d'informations, consulter : GNU/Linux Crypto API (`http://www.kerneli.org`)

11.7.1. Options de compilation du noyau

Lorsque ce document a été écrit, le noyau 2.2 était le nec plus ultra. Encore aujourd'hui, la plupart des pare-feu l'utilisent encore. Toutefois, avec le noyau 2.4, beaucoup de choses ont changé. La plupart des options de compilation contenues dans ce chapitre sont encore valides, mais le masquage et le transfert de port ont été remplacés par les tables IP. Vous obtiendrez de plus amples renseignements en visitant le Linux iptables HOWTO (`http://www.linuxguruz.org/iptables/howto/iptables-HOWTO.html`).

Pour les noyaux 2.2.x, les options suivantes s'appliquent. Vous devriez voir ces options pendant le processus de configuration du noyau. La plupart des commentaires sont issus de `/usr/src/linux/Documentation/Configure.help`, soit le même document utilisé dans l'aide en ligne pendant l'étape `make config` de la compilation du noyau. Consultez le chapitre Compilation et mise en place de nouveaux noyaux du *Manuel de Référence* pour obtenir une description du processus de compilation d'un nouveau noyau.

- Pare-feu réseau (CONFIG_FIREWALL)

Cette option devrait être activée si vous envisagez d'utiliser un pare-feu (*firewalling*) ou le masquage d'IP (*masquerading*) sur votre machine GNU/Linux. Si vous ne configurez qu'une simple machine cliente, il est plus sûr de répondre non.

- IP : reroutage/passerelle (CONFIG_IP_FORWARD)

  Si vous activez le reroutage IP (*IP forwarding*) ; votre machine devient essentiellement un routeur. Si votre machine est sur un réseau, vous pourriez réexpédier des données d'un réseau à un autre, et même subvertir un pare-feu qui était la justement pour empêcher cela. Les utilisateurs normaux en connexion par modem devraient désactiver cette option, et les autres se focaliser sur les implications au niveau de la sécurité d'une telle décision. Les machines pare-feu devront activer cela, en conjonction avec un logiciel de pare-feu.

  Vous pouvez activer le reroutage IP en utilisant la commande :

  ```
  root#  echo 1 > /proc/sys/net/ipv4/ip_forward
  ```

  et le désactiver avec la commande :

  ```
  root#  echo 0 > /proc/sys/net/ipv4/ip_forward
  ```

- IP : cookies syn (CONFIG_SYN_COOKIES)

  Une « attaque SYN » est une attaque du type dénis de service (DoS) qui consomme toutes les ressources de votre machine, vous forçant au redémarrage. Nous ne voyons pas de raisons pour ne pas activer cela. Dans la série de noyaux 2.1, cette option de configuration accepte simplement les cookies « syn », mais ne les active pas. Pour les activer, vous devez faire :

  ```
  root# echo 1 > /proc/sys/net/ipv4/tcp_syncookies <P>
  ```

- IP : Pare-feu (CONFIG_IP_FIREWALL)

  Cette option est nécessaire si vous envisagez de configurer votre machine comme pare-feu, faire du reroutage IP, ou souhaitez protéger votre station en connexion par modem de quelqu'un qui souhaiterait y pénétrer.

- IP : noter les paquets pare-feu (CONFIG_IP_FIREWALL_VERBOSE)

  Cette option vous donne des informations sur les paquets que votre pare-feu a reçu comme l'expéditeur, le destinataire, le port, etc.

- IP : Refuser les structures routées à la source (CONFIG_IP_NOSR)

  Ceci devrait être activé. Les structures routées à la source contiennent le chemin complet vers leur destination à l'intérieur du paquet. Cela signifie que les routeurs n'ont pas besoin de les vérifier et ne font que les réexpédier. Cela pourrait conduire à laisser entrer des données sur votre système qui pourraient représenter une possible violation.

- IP : masquage (CONFIG_IP_MASQUERADE)

  Si l'un des ordinateurs de votre réseau local, pour lequel votre machine GNU/Linux agit comme pare-feu, veut envoyer quelque chose à l'extérieur, votre machine peut « masquer » cet hôte, c'est à dire qu'elle réexpédie le trafic vers la destination mais le fait comme s'il venait de lui-même. Consultez indyramp.com (`http://www.indyramp.com/masq`) et le chapitre *Configurer des clients de passerelle*, page 25 pour plus d'informations.

- IP : masquage ICMP (CONFIG_IP_MASQUERADE_ICMP)

  Cette option ajoute le masquage ICMP à l'option précédente qui ne masque que le trafic TCP ou UDP.

- IP : support de mandataire (*proxy*) transparent (CONFIG_IP_TRANSPARENT_PROXY)

  Cela autorise votre pare-feu GNU/Linux à rediriger de manière transparente tout le trafic réseau provenant du réseau local destiné à un hôte distant depuis un serveur local, appelé « serveur proxy transparent ». Cela fait croire aux ordinateurs locaux qu'ils communiquent avec l'hôte distant, alors qu'ils sont connectés au proxy local. Consultez le document IP Masquerade HOWTO (`http://www.tldp.org/HOWTO/IP-Masquerade-HOWTO/index.html`) pour plus de renseignements.

- IP : défragmenter toujours (CONFIG_IP_ALWAYS_DEFRAG)

  Cette option est normalement désactivée, mais si vous construisez un pare-feu, ou un hôte de masquage, vous devrez l'activer. Lorsque des données sont envoyées d'un hôte à un autre, elles ne sont pas toujours en-

voyées comme un seul paquet de données, mais plutôt fragmentées en plusieurs morceaux. Le problème de cela est que les numéros de ports ne sont connus que du seul premier fragment. Cela signifie que quelqu'un pourrait insérer dans les paquets suivants, des informations erronées. Cela est aussi susceptible d'empêcher une attaque de type « *teardrop* » contre un serveur interne qui ne serait lui même pas immunisé contre cela.

- Signatures de paquets (CONFIG_NCPFS_PACKET_SIGNING)

  Cela est une option qui va signer les paquets NCP pour une sécurité accrue. Vous pouvez normalement la laisser désactivée, mais elle est là si vous en avez besoin.

- IP : Périphérique pare-feu de paquets `netlink`(CONFIG_IP_FIREWALL_NETLINK)

  Voilà une option bien pensée qui vous permet d'analyser les 128 premiers octets des paquets dans un programme utilisateur, pour déterminer si vous souhaitez accepter ou refuser le paquet, selon sa validité.

- Filtrage de `Socket` (CONFIG_FILTER)

  Pour le plus grand nombre, il est bon de répondre non à cette option. Celle-ci vous permet de connecter un filtre utilisateur à n'importe quel `Socket` et choisir les paquets à accepter ou refuser. À moins que vous n'ayez un besoin très spécifique et que vous soyez capable de programmer un tel filtre, vous devriez dire non. Notez aussi que à l'heure d'écrire cette section, tous les protocoles sont supportés, sauf TCP.

- Redirection de port

  La redirection de port (`Port Forwarding`) est une extension du masquage IP qui autorise la redirection de paquets depuis l'intérieur d'un pare-feu sur des ports spécifiques. Cela peut être utile si, par exemple, vous voulez utiliser un serveur Web derrière le pare-feu ou hôte de masquage et ce serveur Web doit être accessible du monde externe. Un client externe envoie une requête au port 80 du pare-feu, le pare-feu fait suivre la requête au serveur Web, le serveur Web traite la requête et les résultats sont envoyés par le réseau au client original. Le client croit que c'est le pare-feu lui-même qui est le serveur Web. Cela peut aussi être utilisé pour répartir la charge si vous avez une « ferme » de serveurs identiques en deçà du pare-feu. Toute l'information à propos de cette caractéristique est disponible sur monmouth (`http://www.monmouth.demon.co.uk/ipsubs/portforwarding.html`).

- Filtrage de ports `Socket` (CONFIG_FILTER)

  En utilisant cette option, un programme utilisateur peut affecter un filtre à chaque `socket`, et indiquer par là au noyau s'il peut accepter ou refuser à certains types de données de passer à travers le `socket`. Le filtrage de `socket` GNU/Linux marche sur tous les types de `socket` sauf les TCP pour l'instant. Consultez le fichier texte `./linux/Documentation/networking/filter.txt` pour plus d'information.

- IP : Masquage

  Le masquage pour les noyaux 2.2 a été amélioré. Il propose des supports additionnels pour masquer des protocoles particuliers, etc. Assurez-vous de lire le *HOWTO* `ipchains` pour plus d'informations.

11.7.2. Périphériques noyau

Il y a plusieurs périphériques en mode bloc et caractère disponibles sous GNU/Linux qui vous aideront aussi pour la sécurité.

Les deux fichiers `/dev/random` et `/dev/urandom` sont fournis par le noyau pour offrir des données aléatoires à tout instant.

Aussi bien `/dev/random` que `/dev/urandom` devraient être assez sûrs pour générer des clés PGP, des `challenges ssh`, et autres applications où des nombres aléatoires sont requis. Les attaquants devraient être incapables de prédire le nombre suivant, connaissant une séquence initiale de nombres provenant de ces sources. Beaucoup d'efforts ont étés consentis pour s'assurer que les nombres fournis par ces sources sont aléatoires, dans tous les sens du terme.

La seule différence entre ces deux périphériques, est que `/dev/random` s'épuise en octets aléatoires, et vous fait attendre jusqu'à ce que d'autres ce soient accumulés. Notez que sur certains systèmes, il peut se bloquer pendant un long moment, attendant que de la nouvelle entropie, générée par l'utilisateur entre dans le système. Vous devez donc faire attention avant d'utiliser `/dev/random`. (La meilleure chose à faire est sans doute de l'utiliser lorsque vous générez des informations de clés sensibles, et vous demandez à l'utilisateur d'utiliser le clavier intensément jusqu'à ce que vous estimiez que cela suffit.)

`/dev/random` est de haute qualité entropique, généré en mesurant les temps inter-interruptions, etc. Il se bloquera jusqu'à ce que suffisamment de bits aléatoires aient été générés.

`/dev/urandom` est semblable, mais lorsque la réserve d'entropie baisse, il retournera un mélange d'un niveau cryptographique élevé de ce qu'il reste. Ce n'est pas aussi sûr, mais cela suffit pour la plupart des applications.

Vous pouvez lire depuis ces périphériques en utilisant quelque chose comme :

```
root#  head -c 6 /dev/urandom | mimencode
```

Cela imprimera six caractères aléatoires à la console, convenables pour un mot de passe. Vous pourrez trouver `mimencode` dans le paquetage `metamail`.

Consultez `/usr/src/linux/drivers/char/random.c` pour une description de l'algorithme.

11.8. Sécurité réseau

La sécurité du réseau devient de plus en plus importante, au fur et à mesure que les utilisateurs passent de plus en plus de temps connectés. Violer la sécurité du réseau est souvent beaucoup plus facile que violer la sécurité physique ou locale, tout en étant beaucoup plus répandue.

Il y a plusieurs bons outils pour vous assister dans la sécurité du réseau, et ils sont de plus en plus fournis avec les distributions GNU/Linux.

11.8.1. Renifleurs de paquets (Packet Sniffers)

Une des manières les plus répandues parmi les intrus pour obtenir l'accès à plus de systèmes sur votre réseau, est d'employer un renifleur de paquets sur un hôte déjà violé. Ce *sniffer* écoute simplement sur les ports Ethernet et repère des choses comme `passwd`, `login` ou `su` dans le corps du paquet et enregistre alors le trafic qui suit. De cette façon, les attaquants obtiennent des mots de passe pour des systèmes qu'ils n'essayent même pas de casser. Les mots de passe en clair sont évidemment très vulnérables à cette attaque.

Exemple : Un hôte A a été violé. L'attaquant y installe un *sniffer*. Ce dernier tombe sur l'administrateur en train de se connecter de l'hôte B à l'hôte C. Il obtient alors le mot de passe personnel de l'administrateur sur B. Puis l'administrateur fait un `su` pour corriger un problème. Il a maintenant le mot de passe de `root` pour l'hôte B. Plus tard, l'administrateur laisse quelqu'un faire un `telnet` depuis sa machine vers l'hôte Z sur un autre site, L'attaquant possède désormais un *login* et mot de passe sur Z...

A l'heure actuelle, les attaquants n'ont même pas besoin de violer un système pour faire cela : Ils peuvent aussi amener un ordinateur (portable ou non) dans un bâtiment et se brancher sur votre réseau.

Utiliser `ssh` ou une autre méthode pour crypter les mots de passe déjoue cette attaque. Des outils comme comptes APOP au lieu de POP pour le courrier électronique préviennent aussi ces attaques. (Les log (Les logins normaux POP sont très vulnérables à cela, de même que tout ce qui envoie des mots de passe en clair à travers le réseau.)

11.8.2. Services système et encapsuleurs tcp

Avant que vous ne connectiez votre système GNU/Linux sur un **QUELCONQUE** réseau, la première chose à déterminer ce sont les services que vous souhaitez offrir. Les services que vous n'avez pas besoin d'offrir devraient être désactivés de sorte que vous aurez moins de choses pour lesquelles vous préoccuper et les attaquants auront moins de chances de pouvoir trouver un trou.

Il y a plusieurs façons de désactiver des services sous GNU/Linux. Vous pouvez regarder le fichier `/etc/inetd.conf` et noter les fichiers qui sont offerts par `inetd`. Désactivez tous ceux dont vous n'avez pas besoin en les commentant (`#` au début de la ligne), et redémarrez alors votre service `inetd`.

Vous pouvez aussi supprimer (ou commenter) des services dans votre fichier `/etc/services`. Cela signifiera que les clients locaux seront aussi incapables de trouver ces services (i.e., si vous supprimez `ftp`, et essayez de faire une connexion FTP vers un site distant depuis cette machine, cela échouera avec un message `service inconnu`). Cela ne vaut généralement pas la peine de supprimer les services à partir de `/etc/services`, vu que cela ne fournit pas de sécurité supplémentaire. Si un utilisateur veut utiliser `ftp` même si vous l'avez commenté, il pourrait faire son propre client qui utilise le port FTP standard, et cela fonctionnerait.

Certains des services que vous pourriez souhaiter activer sont :

- `ftp`
- `telnet` (ou `ssh`)
- courrier électronique, comme `pop-3` ou `imap`
- `identd`

Si vous savez que vous n'allez pas utiliser un paquetage en particulier, vous pouvez aussi le supprimer complètement. `rpm -e nom_du_paquetage`ou `urpme nom_du_paquetage` effacera un paquetage entier.

De plus, vous devriez vraiment désactiver les utilitaires `rsh/rlogin/rcp`, y compris `login` (utilisé par `rlogin`), *shell* (utilisé par `rcp`),et `exec` (utilisé par `rsh`) depuis `/etc/inetd.conf`. Ces protocoles sont extrêmement vulnérables et ont été la cause de violations dans le passé.

Vous devriez vérifier les répertoires `/etc/rc.d/rc[0-9].d`, et regarder si des serveurs présents ne sont pas superflus. Les fichiers de ces répertoires sont en fait des liens symboliques vers des fichiers de `/etc/rc.d/init.d`. Renommez ces fichiers dans `init.d` désactive tous les liens symboliques qui pointent vers ce fichier. Si vous ne souhaitez désactiver un service que pour un niveau d'exécution (*runlevel*) particulier, renommez le lien symbolique approprié en remplaçant le `S` avec un `K`, comme cela :

```
root#  cd /etc/rc6.d
root#  mv S45dhcpd K45dhcpd
```

Vous pouvez aussi utiliser un petit utilitaire pour faire cela : `chkconfig` ou l'interface graphique sous KDE : `ksysv`.

Votre distribution de Mandriva Linux est fournie avec un encapsuleur (*wrapper*) TCP « encapsulant » tous vos services TCP. L'encapsuleur TCP (`tcpd`) est appelé depuis `inetd` au lieu du service réel. `tcpd` vérifie alors l'hôte demandant le service, et soit exécute le vrai serveur, soit refuse l'accès à cet hôte. `tcpd` vous permet de restreindre l'accès aux services TCP. Vous devriez éditer `/etc/hosts.allow` et y ajouter uniquement les hôtes qui ont besoin d'avoir accès aux services de votre machine.

Si vous possédez une connexion par simple modem, nous vous suggérons de refuser tous (`ALL`). `tcpd` enregistre aussi les tentatives échouées pour accéder aux services, de sorte que cela peut vous alerter si on est en train de vous attaquer. Si vous ajoutez de nouveaux services, vous devriez vous assurer de les configurer pour utiliser l'encapsuleur TCP s'ils sont basés sur TCP. Par exemple, une machine connectée par modem peut être protégée de l'extérieur, tout en pouvant charger son courrier électronique, et faire des connexions réseau à Internet. Pour faire cela, vous devez ajouter ce qui suit à votre `/etc/hosts.allow` :

ALL: 127.

Et bien sûr, `/etc/hosts.deny` contiendra :

ALL: ALL

Ce qui empêchera des connexions extérieures à votre machine, vous permettant néanmoins de vous connecter depuis l'intérieur aux services Internet.

Gardez à l'esprit que les encapsuleurs TCP ne protègent que les services exécutés depuis `inetd`, et quelques rares autres. Il y a sûrement d'autres serveurs tournant sur votre machine. Vous pouvez utiliser `netstat -ta` pour afficher la liste de tous les services que votre machine offre.

11.8.3. Vérifiez votre information de DNS

Garder des informations DNS à jour sur tous les hôtes de votre réseau peut vous aider à améliorer la sécurité. Si un hôte non autorisé se connecte à votre réseau, vous pouvez l'identifier grâce à son absence d'entrées DNS. Beaucoup de services peuvent être configurés de façon à ne pas accepter de connexions d'hôtes qui n'ont pas d'entrées DNS valides.

11.8.4. `identd`

`identd` est un petit programme qui est lancé typiquement depuis votre serveur `inetd`. Il garde la trace de qui utilise quel service TCPet le rapporte alors à qui en fait la demande.

Beaucoup de gens ne comprennent pas l'utilité de `identd`, et le désactivent ou bloquent toutes le requêtes de l'extérieur qui lui sont destinées. `identd` n'est pas là pour aider les sites distants. Il n'y a pas moyen de savoir si l'information que vous obtenez de l'`identd` distant est correcte ou non. Il n'y a pas d'authentification dans les requêtes `identd`.

Pourquoi voudriez-vous l'utiliser alors ? Parce qu'il **vous** aide, et est une autre source pour le suivi. Si votre `identd` n'est pas corrompu, alors, vous savez qu'il informe les sites distants des noms d'utilisateur ou UID des personnes utilisant les services TCP. Si l'administrateur du site distant revient et vous dit que l'utilisateur untel essayait de pénétrer dans leur site, vous pouvez facilement prendre des mesures contre cet utilisateur. Si vous n'utilisez pas `identd`, vous devrez chercher dans un grand nombre de « *logs* », deviner qui était connecté à ce moment, et en général prendre beaucoup de temps pour rechercher l'utilisateur.

L' `identd` fourni est plus facile à configurer que beaucoup de gens ne le pensent. Vous pouvez le désactiver pour certains utilisateurs (Ils peuvent créer un fichier `.noident` file), vous pouvez garder trace de toutes les requêtes `identd` (recommandé), vous pouvez même faire en sorte que `identd` retourne un UID au lieu du nom de l'utilisateur, ou même `NO-USER`.

11.8.5. Configuration et sécurisation du MTA de Postfix

Le serveur de courrier Postfix a été écrit par Wietse Venema, auteur de Postfix et de plusieurs autres produits de sécurité Internet, afin « d'essayer de fournir une alternative au programme Sendmail, grandement utilisé. Postfix tente d'être plus rapide, plus facile à administrer et, nous l'espérons, plus sécuritaire. Il essaie également d'être compatible avec Sendmail, au moins de façon à ne pas fâcher les utilisateurs. »

Vous obtiendrez plus de renseignements au sujet de Postfix sur le site de Postfix (`http://www.postfix.org`) ainsi que sur le site *Configuring and Securing Postfix* (`http://www.linuxsecurity.com/feature_stories/feature_story-91.html`).

11.8.6. SATAN, ISS, et autres scanners réseau

Il y a plusieurs paquetages de logiciels qui font du balayage de ports et de services sur machines et réseaux. SATAN, ISS, SAINT, et Nessus en sont quelques-uns des plus connus. Ces logiciels se connectent à la machine cible (ou toutes les cibles machines et réseaux) sur tous les ports qui sont ouverts, et essayent de déterminer quels services tournent dessus. Sur la base de ces informations, vous pouvez dire si la machine est vulnérable a une attaque spécifique et sur quels services.

SATAN (*Security Administrator's Tool for Analyzing Networks*, soit Outil d'administrateur sécurité pour l'analyse de réseaux) est un analyseur de port avec une interface Web. Il peut être configuré pour effectuer des vérifications légères, moyennes, ou lourdes sur une machine ou un réseau de machines. C'est une bonne idée de se procurer SATAN et de scanner votre machine ou réseau, et de régler les problèmes qu'il rencontre. Assurez-vous d'obtenir une copie de SATAN sur le site metalab (`http://metalab.unc.edu/pub/packages/security/Satan-for-Linux/`) ou un site FTP ou Web réputé. Il y avait une copie de SATAN « cheval de Troie » qui était distribuée sur Internet (voir Le site Internet de Trouble (`http://www.trouble.org/~zen/satan/satan.html`)). Notez que SATAN n'a pas été mis à jour depuis longtemps et certains des outils ci-dessous pourraient faire du meilleur boulot.

ISS (Scanner de Sécurité Internet) est un autre scanner de port. Il est plus rapide que SATAN, et devrait donc être meilleur pour de grands réseaux. Néanmoins, SATAN tend à fournir plus d'informations.

SAINT™ est une version mise a jour de SATAN. Il a une interface Web et possède des tests bien plus récents que SATAN. Vous pouvez en apprendre plus sur lui : SAINT (`http://www.wwdsi.com/saint`)

Nessus est un scanner sécurité libre. Il propose une interface graphique GTK pour en faciliter l'utilisation. Il est aussi conçu avec un très bon créateur de modules additionnels pour de nouveaux tests de balayage de ports. Pour plus d'informations, visiter le site Web de Nessus (`http://www.nessus.org/`)

11.8.6.1. Détecter les balayages de ports

Il y a quelques outils conçus pour vous alerter de sondages par SATAN, ISS ou d'autres logiciels de balayage. Néanmoins, une utilisation étendue des encapsuleurs TCP, et la consultation régulière des fichiers de *logs*, devraient vous avertir de telles tentatives. Même avec les paramètres les plus faibles, SATAN laisse encore des traces dans les *logs*.

Il y a aussi des scanners de ports « furtifs ». Un paquet avec le bit TCP ACK activé (comme pour les connexions actives) passera vraisemblablement à travers un pare-feu de filtrage de paquets. Le paquet RST de retour d'un port « **_had no established session_** » (**n'a pas de session établie**) peut être la preuve d'activité sur ce port. Je ne pense pas que les encapsuleurs TCP puissent détecter cela.

Vous pourriez également essayer SNORT™ (`http://www.snort.org`), soit un IDS (*Intrusion Detection System*) libre, dont la fonction est de détecter les intrusions réseau.

11.8.7. sendmail, qmail et les MTA [1]

Un des services les plus importants que vous puissiez fournir est un serveur de courrier électronique. Malheureusement, c'est aussi un des plus vulnérables aux attaques, simplement à cause du grand nombre de tâches qu'il doit effectuer et des privilèges dont il a besoin.

Si vous utilisez `sendmail` il est très important de garder votre version à jour. `sendmail` a une très longue tradition d'attaques. Assurez vous de toujours utiliser la version la plus récente de sendmail, disponible sur le sitesendmail (`http://www.sendmail.org/`).

Gardez à l'esprit que vous n'avez pas forcément besoin de sendmail pour envoyer du courrier. Si vous êtes un particulier, vous pouvez désactiver complètement sendmail, et utiliser simplement votre client de courrier pour envoyer vos messages. Vous pouvez aussi choisir d'enlever l'option `-bd` du fichier de démarrage de sendmail, désactivant ainsi les requêtes pour le courrier rentrant. En d'autres termes, vous pouvez exécuter sendmail depuis vos fichiers de démarrage en utilisant plutôt :

```
# /usr/lib/sendmail -q15m
```

De la sorte, sendmail videra la file de courrier toutes les quinze minutes pour tous les messages n'ayant pu être délivrés à la première tentative.

Beaucoup d'administrateurs choisissent de ne pas utiliser sendmail, et choisissent à la place un des autres agents de transport de courrier. `qmail` par exemple a été conçu dans un but de sécurité, depuis le néant. Il est plus rapide, stable, et sûr. Qmail peut être trouvé à qmail.org (`http://www.qmail.org`)

En compétition directe avec Qmail, on trouve Postfix, écrit par Wietse Venema, l'auteur des encapsuleurs TCP et d'autres outils de sécurité. Anciennement nommé vmailer, et soutenu par IBM, il est aussi un agent de transport de courrier complètement réécrit avec la sécurité à l'esprit. Vous pouvez trouver plus d'informations à propos de Postfix sur postfix.org (`http:/www.postfix.org`)

Postfix est l'agent de transport de courrier installé par défaut avec votre distribution de Mandriva Linux. Consultez à ce sujet le chapitre *Le serveur de courrier Postfix*, page 57 de ce manuel.

11.8.8. Attaques en dénis de service[2]

Un attaque en « Dénis de service » (DoS) essaye de saturer les ressources de sorte que le système ne puisse plus répondre aux requêtes légitimes, ou de refuser l'accès à votre machine aux utilisateurs légitimes.

Les attaques en dénis de service ont beaucoup progressé ces dernières années. Certaines des plus récentes et connues sont listées ci-dessous. Notez que de nouvelles naissent sans arrêt, de sorte qu'il n'y a ici que quelques exemples. Lisez les archives de listes de courriers GNU/Linux sur la sécurité et la liste et les archives de bugtraq pour une information plus à jour.

1. Agents de transport de courrier
2. Denial of Service

- **SYN Flooding** - Inondation `SYN` est une attaque de dénis de service réseau. Il exploite une ouverture dans la façon dont sont créées les connexions TCP. Les derniers noyaux GNU/Linux (2.0.30 et au delà) proposent plusieurs options de configuration pour empêcher ce type d'attaque en refusant aux gens l'accès à votre machine ou services. Consultez *Sécurité du noyau*, page 110 pour les options de noyaux en question.
- **Ping Flooding** - Inondation de `Ping` est une attaque simple en force brute de dénis de service. L'attaquant envoie une « vague » de paquets ICMP à votre machine. S'ils font cela depuis un hôte qui possède plus de largeur de bande que le votre, votre machine sera incapable d'envoyer quoi que ce soit vers le réseau. Une variation de cette attaque, appelée « smurfing », envoie les paquets ICMP à un hôte avec l'IP de retour de **votre** machine, leur permettant de vous inonder de manière moins détectable. vous pouvez trouver plus d'informations sur l'attaque « smurf » sur le site de linuxsecurity.com (`http://www.linuxsecurity.com/articles/network_security_article-4258.html`).

  Si vous êtes en train de subir une attaque en inondation de `ping`, utilisez un outil comme `tcpdump` pour déterminer l'origine des paquets (ou l'origine apparente), puis contactez votre fournisseur d'accès avec cette information. Les inondations `ping` peuvent être le plus facilement stoppées au niveau du routeur ou en utilisant un pare-feu.
- **Ping o' Death** - L'attaque en `ping` mortel envoie des paquets `ICMP ECHO REQUEST` qui sont trop grands pour être contenus dans les structures de données du noyau prévues pour les accueillir. Parce que envoyer un seul, gros (65.510 octets) paquet `ping` à plusieurs système les fera s'arrêter ou même planter, ce problème a rapidement été surnommé « Ping o' Death » (*ping mortel*). Celui-ci a été contourné depuis longtemps, et il n'y a plus à s'en préoccuper.

Vous pouvez trouver le code pour la plupart de ces attaques, et une description plus détaillée de leur fonctionnement sur le site Insecure (`http://www.insecure.org/sploits.html`) en utilisant leur moteur de recherche.

11.8.9. Sécurité NFS (Système de Fichiers Réseau)

NFS est un protocole de partage de fichiers largement utilisé. Il permet a des serveurs qui utilisent `nfsd` et `mountd` d'« exporter » des systèmes de fichiers entiers vers d'autres machines en utilisant le support de systèmes de fichiers NFS inclus dans leurs noyaux. `mountd` suit les systèmes de fichiers montés dans `/etc/mtab`, et peut les afficher avec `showmount`.

Beaucoup de sites utilisent NFS pour fournir les répertoires racines des utilisateurs, de sorte que quelle que soit la machine du réseau sur laquelle ils se connectent, ils auront tous leurs fichiers personnels.

Il y a peu de sécurité possible lorsqu'on exporte un système de fichiers. Vous pouvez faire en sorte que `nfsd` remplace l'utilisateur `root` distant (UID=0) par l'utilisateur `nobody`, en leur empêchant totalement l'accès aux fichiers exportés. Néanmoins, puisque les utilisateurs individuels peuvent accéder à leur propres fichiers (ou tout au moins ayant le même UID), l'utilisateur `root` distant peut se connecter ou faire un `su` depuis son compte et avoir un accès total à ses fichiers. Ce n'est qu'un léger obstacle pour un attaquant qui peut monter votre système de fichier distant.

Si vous devez utiliser NFS, assurez-vous de n'exporter que vers des machines qui en ont vraiment besoin. N'exportez jamais votre répertoire racine entier; mais seulement les répertoires qui ont besoin d'être exportés.

Consultez NFS HOWTO (`http://www.tldp.org/HOWTO/NFS-HOWTO/`) pour plus de renseignements sur NFS.

11.8.10. NIS (Service d'information réseau) (anciennement YP)

NIS (*Network Information Service*) est un moyen de distribuer de l'information à d'autres machines. Le maître NIS détient les tables d'information et les convertit en fichiers cartes NIS. Ces cartes sont alors servies sur le réseau, permettant aux machines clientes NIS d'obtenir les noms de connexion, mots de passe, répertoires utilisateurs et information *shell* (tout ce qui se trouve dans un fichier `/etc/passwd` standard). Cela permet aux utilisateurs de changer leur mot de passe une seule fois et prendre pourtant effet sur toutes les machines du domaine NIS.

NIS n'est pas vraiment sûr. Il n'a jamais été censé l'être. Il était censé être pratique et utile. Quiconque capable de deviner votre nom de domaine NIS (où que ce soit sur le réseau) peut obtenir une copie de votre fichier de mots de passe, et utiliser crack et John the Ripper contre les mots de passe de vos utilisateurs. Il est aussi possible de se faire passer pour NIS et faire toutes sortes de vilaines choses. Si vous devez utiliser NIS, soyez avertis des dangers.

Il y a un remplaçant beaucoup plus sûr à NIS, appelé NIS+. Consultez le *HOWTO* NIS pour plus d'information : NIS HOWTO (`http://www.tldp.org/HOWTO/NIS-HOWTO/`).

11.8.11. Pare-feu

Les pare-feu sont un moyen de contrôler les informations autorisées à sortir et à rentrer dans votre réseau local. Généralement, l'hôte pare-feu est connecté à Internet et à votre réseau local, et le seul accès depuis votre réseau vers Internet est à travers le pare-feu. De cette façon, le pare-feu peut contrôler ce qui rentre et sort d'Internet et de votre réseau local.

Plusieurs types de pare-feu et de méthodes pour les mettre en place existent. Les machines GNU/Linux constituent de bons pare-feu. Le code pare-feu peut être inséré directement dans les noyaux 2.0 et supérieurs. Les outils utilisateur `ipchains` pour les noyaux 2.2, et `iptables` pour noyau 2.4 vous permettent de changer, à la volée, les types de trafics réseau que vous autorisez. Vous pouvez aussi garder trace de certains trafics réseau.

Les pare-feu sont une technique utile et importante pour sécuriser votre réseau. Néanmoins, ne pensez jamais que, parce que vous avec un pare-feu, vous n'avez pas besoin de sécuriser les machines derrière lui. C'est une erreur fatale. Consultez le très bon Firewall-HOWTO (`http://www.ibiblio.org/mdw/HOWTO/Firewall-HOWTO.html`) pour plus d'informations sur les pare-feu et GNU/Linux.

Si vous n'avez aucune expérience avec les pare-feu, et envisagez d'en mettre un en place pour plus qu'une simple politique de sécurité, le livre *Firewalls* de chez O'Reilly and Associates ou tout autre document en ligne sur les pare-feu est indispensable. Consultez O'Reilly (`http://www.ora.com`) pour plus d'informations. Le NIST (*National Institute of Standards and Technology*) a rassemblé un excellent document sur les pare-feu. Bien que daté de 1995, il est toujours très bon. Vous pouvez le trouver sur nist.gov (`http://cs-www.ncsl.nist.gov/publications/nistpubs/800-10/main.html`). Il y a aussi :

- Le projet `Freefire` — une liste d'outils de pare-feu libres, disponible sur le site de freefire (`http://sites.inka.de/sites/lina/freefire-l/index_en.html`)
- *Mason — the automated firewall builder for Linux* (Mason, le bâtisseur de pare-feu automatiques pour GNU/Linux). C'est un script de pare-feu qui apprend quand vous faites les choses dont vous avez besoin sur votre réseau ! Plus de renseignements sur le site de Mason (`http://www.stearns.org/mason/`).

11.8.12. IP Chains - pare-feu pour les noyaux GNU/Linux 2.2.x

Les chaînes pare-feu IP GNU/Linux sont une mise à jour du code de pare-feu des noyaux 2.0, Il y a un bon nombre de nouvelles caractéristiques, dont :

- Manipulation des paquets plus flexible
- Gestion des comptes plus complexe
- Changements de politique simple possible automatiquement
- Les fragments peuvent être explicitement bloqués, refusés, etc.
- Enregistre les paquets suspects
- Peut gérer des protocoles autres que `ICMP/TCP/UDP`.

Assurez-vous de lire IP Chains HOWTO (`http://www.tldp.org/HOWTO/IPCHAINS-HOWTO.html`)pour plus d'informations.

11.8.13. Netfilter - pare-feu pour les noyaux Linux 2.4.x

Netfilter se veut un ensemble d'ajout au code de filtrage de paquets IP du noyau. Il permet aux utilisateurs de configurer, d'entretenir et d'inspecter les règles de filtrage de paquets dans le nouveau noyau 2.4.

Le sous-système netfilter est une réécriture complète des implantations de filtrage de paquets, incluant ipchains et ipfwadm. Netfilter procure un large éventail d'améliorations, et est devenu une solution encore plus mature et robuste pour protéger les réseaux professionnels.

`iptables` se veut l'interface de ligne de commande pour manipuler les tables de pare-feu à l'intérieur même du noyau.

Netfilter procure également une architecture brute pour manipuler les paquets tandis qu'ils traversent les différentes parties du noyau. Cette architecture inclut la prise en charge du masquage, le filtrage standard de paquets ainsi qu'une traduction d'adresses de réseau plus complète. La prise en charge des requêtes de charge balancée pour un service en particulier parmi un groupe de serveurs, situés derrière un pare-feu, a également été améliorée.

La fonctionnalité de l'inspection contextuelle des paquets (*stateful inspection*) est particulièrement puissante. Elle permet de tracer et de contrôler le flux de communications passant à travers le filtre. La possibilité de garder une trace des états et le contexte pertinent à une session ne font pas que rendre les règles plus simples ; cela permet également de mieux interpréter les protocoles de niveau supérieur.

De plus, de petits modules peuvent être développés pour produire des fonctions supplémentaires spécifiques, telles que le passage de paquets à des programmes dans l'espace utilisateur pour traitement, puis leur réintroduction dans le flux normal de paquets. La possibilité de développer ces programmes dans l'espace utilisateur réduit le niveau de complexité y étant associé précédemment : les changements n'ont plus à être faits directement au niveau du noyau.

Voici d'autres références en matière de tables IP :

- Oskar Andreasson IP Tables Tutorial (`http://www.linuxsecurity.com/feature_stories/feature_story-94.html`) — Oskar Andreasson, de pair avec LinuxSecurity.com, discute de son tutoriel sur les tables IP et de l'utilité de ce document pour construire un pare-feu robuste pour votre entreprise ;
- Hal Burgiss Introduces Linux Security Quick-Start Guides (`http://www.linuxsecurity.com/feature_stories/feature_story-93.html`) — Hal Burgiss a écrit deux guides officiels sur la sécurité sous Linux, y compris la gestion de pare-feu ;
- Page d'accueil de Netfilter (`http://www.netfilter.org`) — la page d'accueil concernant netfilter et iptables ;
- Linux Kernel 2.4 Firewalling Matures: netfilter (`http://www.linuxsecurity.com/feature_stories/kernel-netfilter.html`) — cet article de LinuxSecurity.com décrit les bases du filtrage de paquets, comment commencer à utiliser les tables IP, ainsi qu'une liste des nouvelles fonctionnalités disponibles dans les plus récentes générations de pare-feu pour Linux.

11.8.14. VPN : Réseaux privés virtuels (Virtual Private Network)

Les VPNs (*Virtual Private Networks*) sont un des moyens d'établir un réseau « virtuel » par dessus un réseau déjà existant. Ce réseau virtuel est souvent crypté et transmet les données uniquement de et vers certaines entités qui ont rejoint le réseau. Les VPNs sont souvent utilisés pour connecter quelqu'un travaillant chez lui par dessus Internet public sur le réseau interne de sa compagnie.

Il y a plusieurs solutions GNU/Linux VPN disponibles:

- vpnd. Voir VPN Daemon (`http://sunsite.auc.dk/vpnd/`).
- Free S/Wan, disponible sur freeswan.org/ (`http://www.freeswan.org/`)
- `ssh` peut être utilisé pour construire un VPN. Voir VPN PPP-SSH mini-HOWTO (`http://www.tldp.org/HOWTO/ppp-ssh/index.html`) pour plus d'informations.
- vps (serveur privé virtuel) sur http://www.strongcrypto.com (`http://www.strongcrypto.com`).
- vtun (tunnel virtuel) sur le site Web sourceforge (`http://vtun.sourceforge.net/`).

- yavipin (`http://yavipin.sourceforge.net`).

Consultez aussi la section sur IPSEC pour des références vers plus d'informations.

11.9. Préparation de sécurité (avant de vous connecter)

OK, vous avez vérifié tout votre système, et estimé qu'il était aussi sûr que possible, et vous êtes prêt à le mettre en ligne. Il y a quelques petites choses que vous devriez faire maintenant pour vous préparer à une intrusion, de sorte que vous puissiez rapidement déjouer l'intrus, récupérer le système et sa bonne marche.

11.9.1. Faites une sauvegarde complète de votre machine

Discuter des méthodes de sauvegarde et de stockage est hors de la portée de ce chapitre mais voici quelques mots au sujet des sauvegardes et de la sécurité :

Si vous avez moins de 650Mo de données sur une partition, une copie sur CD-R de vos données est un bon moyen (difficile à modifier ensuite, et, si stocké correctement, peut durer longtemps). Bandes et autres médias réinscriptibles devraient être protégés contre l'écriture dès que la sauvegarde est complète, puis vérifiés pour empêcher la modification. Assurez vous de stocker vos sauvegardes dans un endroit sûr hors ligne. Une bonne sauvegarde vous fournira un bon point de départ pour restaurer votre système.

11.9.2. Choisir un bon planning de sauvegardes

Un cycle à six bandes est facile à gérer. Il comprend quatre bandes pour la semaine, une pour chaque vendredi pair, et une dernière pour les vendredis impairs. Faites une sauvegarde incrémentale chaque jour, et une sauvegarde complète sur la bande du vendredi appropriée. Si vous faites un changement particulièrement important ou ajoutez des données importantes à votre système, une sauvegarde complète est recommandée.

11.9.3. Tester vos sauvegardes

Vous devriez faire des tests périodiques de vos copies de sauvegarde pour vous assurer qu'elles fonctionnent correctement. Les restaurations de fichiers et leur vérification auprès des données réelles, la taille et le listage des copies, et la lecture de vieilles copies de sauvegarde devraient être faites sur une base régulière.

11.9.4. Sauvegardez votre base de données RPM

Dans l'éventualité d'une intrusion, vous pouvez utiliser votre base de données RPM comme vous utiliseriez `tripwire`, mais uniquement si vous pouvez être sûr qu'elle n'a pas été modifiée elle non plus. Vous devriez copier votre base de données RPM sur une disquette, et garder tout le temps cette dernière hors-ligne.

Les fichiers `/var/lib/rpm/fileindex.rpm` et `/var/lib/rpm/packages.rpm` ne tiendront sans doute pas sur une seule disquette. Mais compressés, ils devraient tenir chacun sur une.

Maintenant, si votre système est corrompu, vous pouvez utiliser la commande :

```
root#  rpm -Va
```

pour vérifier tous les fichiers du système. Consultez la page de `man` de `rpm`, car il y a quelques autres options qui peuvent être incluses pour le rendre moins verbeux. Gardez à l'esprit que vous devez aussi être sûr que votre binaire RPM n'a pas lui aussi été corrompu.

Cela signifie que chaque fois qu'un nouveau RPM est ajouté au système, la base de données RPM devra être archivée à nouveau. Vous devrez peser les avantages et les inconvénients.

11.9.5. Gardez trace des données de journalisation du système

Il est très important que l'information générée par `syslog` ne soit pas corrompue. Rendre les fichiers de `/var/log` en lecture et écriture par un seul petit nombre d'utilisateurs est un bon début.

Assurez-vous de garder un œil sur ce qui y est écrit, spécialement sous la rubrique `auth`. Des échecs de connexion répétés par exemple, peuvent révéler une tentative de viol.

Vous pourrez regarder dans `/var/log` et consulter `messages`, `mail.log`, etc.

Vous voudrez aussi configurer votre script de rotation des *logs* pour les garder plus longtemps de sorte que vous ayez le temps de les examiner. Jetez un coup d'œil à logrotate(8).

Si vos fichiers de logs ont été corrompus, essayez de déterminer à partir de quand commence la corruption, et quelles choses semblent être corrompues. Y a-t-il de longues périodes sans logs? Regarder dans les sauvegardes les fichiers de logs originels est une bonne idée.

Les intrus modifient généralement les fichiers de logs pour effacer leurs traces, mais on devrait néanmoins y chercher des événements inhabituels. Vous pourriez remarquer l'intrus en train d'essayer d'obtenir l'accès, ou exploiter un programme pour obtenir le compte `root`. Vous devriez voir des entrées de logs avant que l'intrus n'ait eu le temps de les modifier.

Vous devriez aussi vous assurer de bien séparer les entrées `auth` des autres données de logs, y compris les tentatives de changer d'utilisateur en utilisant `su`, tentatives de connexion, et autres informations des comptes utilisateurs.

Si possible, configurez `syslog` pour envoyer une copie des données les plus importantes vers un système sûr. Cela empêchera un intrus d'effacer ses traces en effaçant ses tentatives de `login/su/ftp/etc`. Voir la page de man de `syslog.conf`, et consulter l'option `@`.

Il y a plusieurs programmes `syslogd` plus évolués. Consultez security.sdsc.edu (`http://security.sdsc.edu/software/sdsc-syslog/`) pour Secure Syslog. Secure Syslog vous permet de crypter vos entrées `syslog` et vous assure que personne ne les a modifiées.

Un autre `syslogd` avec plus de fonctions est syslog-ng (`http://www.balabit.hu/en/downloads/syslog-ng/`). Il permet beaucoup plus de flexibilité dans la journalisation et peut crypter vos flots `syslog` distants pour empêcher leur corruption.

Enfin, les fichiers de logs sont encore plus inutiles lorsque personne ne les lit. Prenez un peu de temps régulièrement pour parcourir vos fichiers de logs, et imprégnez vous de ce à quoi ils ressemblent les jours normaux. Cela peut vous aider à repérer les choses anormales.

11.9.6. Appliquez toutes les nouvelles mises à jour système.

La majorité des utilisateurs installent leur système à partir d'un CD-ROM. A cause du rythme rapide des correctifs de sécurité, de nouveaux programmes (corrigés) sont sans arrêt publiés. Avant de connecter votre machine au réseau, c'est une bonne idée de lancer `MandrivaUpdate` (sur une autre machine connectées à Internet bien sûr) et installer tous les paquetages mis à jour depuis que vous avez reçu vos CD-ROM. Souvent, ces paquetages contiennent d'importants correctifs de sécurité, c'est donc une bonne idée de les installer.

11.10. Que faire, avant et pendant une effraction

Alors vous avez suivi les conseils donnés ici (ou ailleurs) et avez détecté une effraction? La première chose à faire est de garder votre calme. Des actions précipitées peuvent causer plus de dégâts que ce qu'aurait fait l'attaquant.

11.10.1. Violation de sécurité sur le vif.

Repérer une violation de sécurité sur le vif peut être une expérience stressante. Comment vous réagissez peut avoir de graves conséquences.

Si la violation que vous voyez est physique, il y a des chances que vous voyiez quelqu'un en train de violer votre maison, bureau ou laboratoire. Vous devriez avertir les autorités locales. Dans un laboratoire, vous

pourriez voir quelqu'un en train d'essayer d'ouvrir un boîtier ou de redémarrer une machine. Suivant votre compétence et le règlement, vous pouvez leur demander d'arrêter ou contacter le personnel de sécurité local.

Si vous avez détecté un utilisateur local en train d'essayer de compromettre votre sécurité, la première chose à faire est de confirmer qu'il est bien celui que vous pensez. Vérifiez le site depuis lequel il est connecté. Est-ce le site habituel? Non? Alors utilisez un moyen non électronique pour rentrer en contact. En l'occurrence, appelez le par téléphone ou allez à leur bureau/maison pour lui parler. S'ils admettent qu'ils sont connectés, vous pouvez leur demander d'expliquer ce qu'ils étaient en train de faire ou leur intimer d'arrêter. S'ils ne sont pas connectés, et n'ont aucune idée de ce dont vous parlez, l'incident demandera sans doute plus d'investigations. Examinez bien chaque incident, et récoltez le plus d'informations possibles avant de faire une quelconque accusation.

Si vous avez détecté une violation réseau, la première chose à faire (si vous le pouvez) est de déconnecter votre réseau. S'ils sont connectés par modem, débranchez le câble du modem; s'ils sont connectés par Ethernet, déconnectez le câble Ethernet. Cela les empêchera de faire plus de dommages, et ils interpréteront cela comme un problème réseau plutôt qu'une détection.

Si vous ne pouvez pas déconnecter le réseau (si vous avez un site occupé, ou n'avez pas le contrôle physique des machines), la meilleure étape suivante est d'utiliser quelque chose comme les encapsuleurs TCP ou `ipfwadm` pour refuser l'accès au site de l'intrus.

Si vous ne pouvez pas refuser tous les utilisateurs du même hôte que celui de l'intrus, bloquer le compte de cet utilisateur devrait fonctionner. Notez que bloquer un compte n'est pas chose aisée. Vous devez prendre en compte les fichiers `.rhosts`, accès FTP, et une foule de portes dérobées possibles.

Après que vous ayez fait l'une des choses précédentes (déconnecté le réseau, refusé l'accès depuis leur site, et/ou désactivé leur compte), vous devez tuer tous leurs processus utilisateurs et les déconnecter.

Vous devriez soigneusement surveiller votre site dans les minutes qui suivent, car l'attaquant pourra essayer de revenir. Peut-être en utilisant un autre compte, et/ou en utilisant une autre adresse réseau.

11.10.2. La violation de sécurité a déjà eu lieu

Alors vous avez détecté une violation qui a déjà eu lieu ou vous l'avez détectée et avez mis dehors (espérons-le) l'intrus. Et maintenant?

11.10.2.1. Fermer le trou

Si vous pouvez trouver le moyen qu'a utilisé l'attaquant pour pénétrer votre système, vous devriez essayer de boucher ce trou. En l'occurrence, vous verrez peut-être plusieurs entrées FTP juste avant que l'utilisateur ne se connecte. Désactivez le service FTP et recherchez s'il existe une version mise à jour, ou si une liste quelconque connaît un remède.

Consultez tous vos fichiers de logs, et faites une visite à vos listes de sécurité et sites Web pour voir s'il n'y a pas un nouveau trou que vous pourriez boucher. Vous pouvez trouver les mises à jour de sécurité de Mandriva Linux en lançant `MandrakeUpdate` régulièrement.

Il y a maintenant un projet d'audit de sécurité GNU/Linux. ils explorent méthodiquement tous les utilitaires utilisateurs à la recherche de possibles exploitations détournées et débordements. Extrait de leur annonce :

« Nous tentons un audit systématique des sources GNU/Linux avec le but de devenir aussi sûr que OpenBSD. Nous avons déjà découvert (et résolu) quelques problèmes, mais plus d'aide serait la bienvenue. La liste n'est pas modérée et est aussi une source utile pour des discussions générales de sécurité. La liste de l'adresse est : `security-audit@ferret.lmh.ox.ac.uk`. Pour vous inscrire, envoyez un message à : `security-audit-subscribe@ferret.lmh.ox.ac.uk` »

Si vous ne gardez pas l'intrus hors de portée, il reviendra sans doute. Pas seulement sur votre machine, mais quelque part sur votre réseau. S'il utilisait un renifleur de paquets, il y a de bonnes chances qu'il ait accès à d'autres machines locales.

11.10.2.2. Évaluer les dégâts

La première chose à faire est d'évaluer les dégâts. Qu'est-ce qui a été corrompu? Si vous utilisez un contrôleur d intégrité tel que Tripwire, vous pouvez le lancer pour exécuter une vérification d'intégrité, et cela devrait vous aider à dire ce qui a été corrompu. Sinon, vous devrez vérifier toutes vos données importantes.

Du fait que les systèmes GNU/Linux deviennent de plus en plus faciles à installer, vous devriez envisager de sauvegarder vos fichiers de configuration pour effacer vos disques puis réinstaller GNU/Linux, et restaurer les fichiers utilisateurs et fichiers de configuration des sauvegardes. Cela assurera que vous avez à nouveau un système propre. Si vous devez sauvegarder des données depuis le système corrompu, soyez particulièrement vigilant avec tous les binaires que vous restaurez, car ils pourraient contenir des chevaux de Troie, placés là par l'intrus.

La Réinstallation devrait être considérée obligatoire après qu'un intrus ait obtenu l'accès `root`. De plus, vous voudrez sans doute garder toutes les preuves, avoir un disque de rechange est donc recommandé.

Vous devez alors vous préoccuper de la date de l'intrusion, et si la sauvegarde contient alors du travail endommagé.

11.10.2.3. Sauvegardes, Sauvegardes, Sauvegardes!

Faire des sauvegardes régulières est une aubaine pour les problèmes de sécurité. Si votre système est compromis, vous pouvez restaurer les données dont vous avez besoin depuis les sauvegardes. Bien sûr, vos données intéressent aussi l'intrus, et il ne fera pas que les détruire, ils les volera et gardera sa propre copie; Mais au moins vous aurez encore vos données.

Vous devriez vérifier plusieurs sauvegardes en arrière avant de restaurer un fichier qui a été compromis. L'intrus pourrait avoir compromis vos fichiers il y a longtemps, et vous pourriez avoir fait plusieurs sauvegardes valides du fichier corrompu!

Bien sûr, il y a aussi une flopée de soucis avec les sauvegardes. Assurez-vous de les stocker dans un endroit sûr. Soyez informé de qui y accède. (Si un attaquant peut obtenir vos sauvegardes, il peut accéder à toutes vos données sans que vous vous en rendiez compte.)

11.10.2.4. Pister l'intrus.

OK, vous avez mis l'intrus hors de portée, et récupéré votre système, mais vous n'avez pas tout à fait fini encore. Bien qu'il soit improbable que la plupart des intrus soient jamais pris, vous devriez dénoncer l'attaque.

Vous devriez rendre compte de l'attaque au contact administratif du site depuis lequel l'attaquant s'en est pris à votre système. Vous pouvez rechercher ce contact avec `whois` ou la base de données Internic. Vous devriez leur envoyer un courrier électronique avec toutes les entrées de logs concernées, dates et heures. Si vous avez remarqué quoi que ce soit d'autre distinctif à propos de l'intrus, vous devriez le mentionner de même. Après avoir envoyé le courrier électronique, vous devriez (si vous y êtes disposé) le faire suivre d'un appel téléphonique. Si cet administrateur repère lui aussi l'attaquant, il pourrait être capable de contacter l'administrateur du site depuis lequel il vient, et ainsi de suite.

Les bons *crackers* utilisent souvent plusieurs systèmes intermédiaires, certains (ou plusieurs) pouvant même ne pas être au courant qu'ils ont été violés. Essayer de pister un cracker jusqu'à son système de base peut être difficile. Rester poli avec les administrateurs auxquels vous parlez peut être utile pour obtenir de l'aide de leur part.

Vous devriez aussi avertir toutes les organisations de sécurité dont vous faites partie, comme le CERT (`http://www.cert.org/`) ou autre.

11.11. Documents de base

Il y a **beaucoup** de bons sites sur la sécurité UNIX en général et GNU/Linux en particulier. Il est très important de s'abonner à une (ou plus) des listes de diffusion de sécurité et être informé des mises à jour de sécurité. La plupart de ces listes ont peu de trafic, et un contenu très informatif.

11.11.1. Références LinuxSecurity.com

Le site LinuxSecurity (`http://www.linuxsecurity.com`) contient de nombreuses références en matière de sécurité Linux et Open Source, lesquelles sont écrites par le personnel de LinuxSecurity ainsi que par des experts à travers le monde.

- Linux Advisory Watch (`http://www.linuxsecurity.com/vuln-newsletter.html`). Un bulletin d'information compréhensible qui souligne les vulnérabilités de sécurité qui ont été annoncées dans la semaine. Il inclut des astuces pour actualiser les paquetages, ainsi qu'une description de chacune des vulnérabilités ;
- Linux Security Week (`http://www.linuxsecurity.com/newsletter.html`). Le but de ce document est de fournir à ses lecteurs un résumé des annonces de sécurité les plus pertinentes du monde Linux au cours de la semaine ;
- Linux Security Discussion List (`http://www.linuxsecurity.com/general/mailinglists.html`) — cette liste de discussion s'adresse à ceux et celles qui voudraient poser des questions ou émettre des commentaires généraux relatifs à la sécurité ;
- Linux Security Newsletters (`http://www.linuxsecurity.com/general/mailinglists.html`) — information d'abonnement pour tous les bulletins de nouvelles ;
- comp.os.linux.security FAQ `http://www.linuxsecurity.com/docs/colsfaq.html`. Foire aux questions dotée de réponses provenant du groupe de nouvelles `comp.os.linux.security`.
- Linux Security Documentation (`http://www.linuxsecurity.com/docs/`). Un excellent point de départ pour obtenir de l'information relative à la sécurité dans les environnements Linux et Open Source.

11.11.2. Sites FTP

Le CERT (*Computer Emergency Response Team*) est l'équipe de réponses aux urgences informatiques. Ils émettent souvent des alertes sur les attaques actuelles et des solutions. Consultez ftp://ftp.cert.org (`ftp://ftp.cert.org`) pour plus d'informations.

ZEDZ (`http://www.zedz.net`) (anciennement Replay) possède des archives de plusieurs programmes de sécurité. Comme ils sont situés en dehors des États-Unis, ils n'ont pas à respecter les lois de restriction des États-Unis au sujet de la cryptographie.

Matt Blaze est l'auteur de CFS et un grand défenseur de la sécurité. Les archives de Matt sont disponibles sur att.com (`ftp://ftp.research.att.com/pub/mab`)

11.11.3. Sites Internet

- La FAQ des *hackers* : plethora.net (`http://www.plethora.net/~seebs/faqs/hacker.html`) ;
- L'archive COAST possède un grand nombre de programmes de sécurité pour UNIX et des informations : CERIAS (`http://www.cerias.purdue.edu/coast/`) ;
- Page sécurité de SuSE : SuSE (`http://www.suse.de/de/security/`) ;
- `BUGTRAQ` publie des conseils sur des problèmes de sécurité : securityfocus.com (`http://www.securityfocus.com/archive/1`) ;
- Le CERT (*Computer Emergency Response Team*), la célèbre équipe émet des avis sur des attaques courantes sur les plates-formes UNIX®: CERT (`http://www.cert.org/`) ;
- Dan Farmer est l'auteur de SATAN et beaucoup d'autres outils de sécurité. Sa page personnelle présente plusieurs études informatives de sécurité, ainsi que des outils de sécurité :trouble.org (`http://www.trouble.org/security/`) ;
- Le CIAC envoie des bulletins périodiques de sécurité sur les attaques courantes : CIAC (`http://ciac.llnl.gov/cgi-bin/index/bulletins`) ;
- Un bon point de départ pour les modules d'authentification additionnels GNU/Linux (PAM) peut être trouvé à kernel.org (`http://www.kernel.org/pub/linux/libs/pam/`).

- la FAQ « WWW Security », écrite par Lincoln Stein, est une bonne référence Web sur la sécurité. Elle peut être trouvée sur le site w3.org (`http://www.w3.org/Security/Faq/www-security-faq.html`)
- Mandriva Security Advisories (`http://www.mandriva.com/security`) est la page officielle pour les problèmes de sécurité de Mandriva Linux qui propose notamment les nouvelles alertes, la politique de maintenance des distributions, etc.

11.11.4. Listes de diffusion

Liste de sécurité Mandriva Linux : vous pouvez être informé de chaque correctif de sécurité en vous abonnant à notre liste : security (`http://www.mandrivalinux.com/fr/security.php3`).

`Bugtraq` : Pour vous abonner à `Bugtraq`, envoyer un message à listserv@netspace.org contenant dans le corps « subscribe bugtraq ». (voir le lien ci-dessus pour les archives).

CIAC : Envoyez un message à majordomo@tholia.llnl.gov. Dans le **corps** du message écrivez : « subscribe ciac-bulletin ».

11.11.5. Livres - Documents imprimés

Il y a un certain nombre de bons livres sur la sécurité. Cette section en cite quelques-uns. En plus des livres spécialement sur la sécurité, la sécurité est traitée par bon nombre d'autres livres sur l'administration système.

Références

D. Brent Chapman, Elizabeth D. Zwicky, *Building Internet Firewalls*, 1e Édition Septembre 1995, ISBN 1-56592-124-0.

Simson Garfinkel, Gene Spafford, *Practical UNIX & Internet Security*, 2e Édition Avril 1996, ISBN 1-56592-148-8.

Deborah Russell, G.T. Gangemi, Sr., *Computer Security Basics*, 1e Édition Juillet 1991, ISBN 0-937175-71-4.

Olaf Kirch, *Linux Network Administrator's Guide*, 1e Édition Janvier 1995, ISBN 1-56592-087-2.

Simson Garfinkel, *PGP: Pretty Good Privacy*, 1e Édition Décembre 1994, ISBN 1-56592-098-8.

David Icove, Karl Seger, William VonStorch, *Computer Crime A Crimefighter's Handbook*, 1ère édition août 1995, ISBN 1-56592-086-4.

John S. Flowers, *Linux Security*, New Riders, Mars 1999, ISBN 0735700354.

Anonymous, *Maximum Linux Security : A Hacker's Guide to Protecting Your Linux Server and Network*, Juillet 1999, ISBN 0672313413.

Terry Escamilla, *Intrusion Detection*, John Wiley and Sons, Septembre 1998, ISBN 0471290009.

Donn Parker, *Fighting Computer Crime*, John Wiley and Sons, Septembre 1998, ISBN 0471163783.

11.12. Foire aux questions

Q : Est-il plus sûr de compiler un gestionnaire de périphérique directement dans le noyau, plutôt que d'en faire un module ?

R : Certaines personnes pensent qu'il vaut mieux désactiver la possibilité de charger des gestionnaires de périphériques sous forme de modules, car un intrus pourrait charger un module cheval de Troie ou un module qui pourrait affecter la sécurité du système.

De toute façon, pour pouvoir charger des modules, vous devez être `root`. Les fichiers modules objets ne peuvent aussi qu'être écrits par `root`. Cela signifie qu'un intrus aurait besoin d'un accès `root` pour insérer un module. Si un intrus obtient l'accès `root`, il y a des choses plus sérieuses à propos desquelles se préoccuper que de savoir s'il voudra charger un module.

Les modules sont faits pour le chargement dynamique de gestionnaires de périphériques rarement utilisés. Sur des machines serveurs ou pare-feux, en l'occurrence, cela est très improbable. Pour cette raison, il devrait être plus logique de compiler les gestionnaires directement dans le noyau pour des machines agissant en tant que serveurs. Les modules sont aussi plus lents que les gestionnaires compilés directement dans le noyau.

Q : Pourquoi se connecter comme `root` d'une machine distante échoue ?

R : Lisez *Sécurité pour `root`*, page 98. Cela est fait à dessein pour empêcher des utilisateurs distants de se connecter via `telnet` à votre machine comme `root`, ce qui est une vulnérabilité sérieuse de sécurité, car alors le mot de passe de `root` serait transmis, en clair, à travers le réseau. N'oubliez pas : Les intrus potentiels ont du temps devant eux et peuvent lancer des programmes automatiques pour trouver votre mot de passe.

Q : Comment puis-je activer les extensions SSL d'Apache ?

R : Installez le paquetage `mod_ssl` et consultez la documentation sur le site Web de mod_ssl (`www.modssl.org`).

Vous pouvez aussi installer le module mod_sxnet, qui est un greffon pour mod_ssl et permet d'activer le *Thawte Secure Extranet*. mod_ssl chiffre les communications, mais mod_sxnet permet en plus d'authentifier de manière sûre les utilisateurs d'une page Web grâce à un certificat personnel. Vous pouvez consulter le site Web de Thawte (`http://www.thawte.com/certs/strongextranet/`) ou installer le paquetage du module `mod_xnet` à partir de votre distribution Mandriva Linux et lire la documentation incluse.

Vous devriez aussi essayer ZEDZ net (`http://www.zedz.net`) qui a plusieurs paquetages pré-compilés, et est situé en dehors des États-Unis.

Q : Comment puis-je manipuler les comptes des utilisateurs tout en assurant la sécurité ?

R : Votre distribution Mandriva Linux propose un grand nombre d'outils pour changer les propriétés des comptes utilisateurs.

- Les commandes `pwconv` et `unpwconv` peuvent être utilisées pour passer entre des mots de passe fantômes (shadow) ou non.
- Les commandes `pwck` et `grpck` peuvent être utilisées pour vérifier la cohérence des fichiers `passwd` et `group`.
- Les commandes `useradd`, `usermod`, et `userdel` peuvent être utilisées pour ajouter, supprimer, et modifier des comptes utilisateurs. Les commandes `groupadd`, `groupmod`, et `groupdel` feront de même pour les groupes.
- Des mots de passe de groupes peuvent être créés en utilisant `gpasswd`.

Tous ces programmes sont « compatibles shadow » -- c'est à dire, si vous activez les procédures *shadow*, ils utiliseront `/etc/shadow` pour l'information de mots de passes, sinon non.

Q : Comment puis-je protéger des documents HTML particuliers en utilisant Apache ?

R : Je parie que vous ne connaissiez pas Apache Week (`http://www.apacheweek.com`) ?

Vous pouvez trouver des informations sur l'authentification des utilisateurs sur le site Web de apacheweek (`http://www.apacheweek.com/features/userauth`) ainsi que d'autres conseils de sécurité pour serveurs Web sur le site de Apache (`http://www.apache.org/docs/misc/security_tips.html`).

11.13. Conclusion

En vous abonnant aux listes de diffusion d'alertes de sécurité, et en vous tenant au courant, vous pouvez faire beaucoup pour la sécurité de votre machine. Si vous gardez un œil sur vos fichiers de logs et lancez régulièrement quelque chose comme `tripwire`, Vous pouvez faire encore plus.

Un niveau raisonnable de sécurité informatique n'est pas difficile à maintenir sur une machine personnelle. Plus d'efforts sont nécessaires sur des machines de travail, mais GNU/Linux peut en fait être une plate-forme sûre. Du fait de la nature du développement de GNU/Linux, des correctifs de sécurité sortent souvent beaucoup plus rapidement qu'ils ne le font sur des systèmes d'exploitation commerciaux, faisant de GNU/Linux une plate-forme idéale lorsque la sécurité est une nécessité.

Vocabulaire relatif à la sécurité

Voici quelques-uns des termes les plus utilisés en sécurité informatique Un dictionnaire complet de termes de sécurité informatique est disponible sur le site de LinuxSecurity (`http://www.linuxsecurity.com/dictionary/`)

authentication (authentification)
: Le processus qui conduit à savoir que les données reçues sont bien les mêmes que celles qui ont été envoyées, et que celui qui prétend être l'expéditeur est l'expéditeur réel.

bastion Host (hôte bastion)
: Un système informatique qui doit être hautement sécurisé car il est vulnérable aux attaques, habituellement parce qu'il est exposé à Internet et est un point de contact principal pour les utilisateurs de réseaux internes. Il tire son nom des fortifications extérieures des châteaux médiévaux. Les bastions supervisent les régions critiques de défense, possédant généralement des murs plus épais, de la place pour plus de gens d'armes, et l'utile chaudron d'huile bouillante pour décourager les attaquants. Une définition raisonnable pour ce qui nous concerne.

buffer overflow (dépassement de tampon)
: Un style de programmation répandu est de ne jamais allouer des tampons suffisamment grands, et ne pas en vérifier les dépassements. Quand de tels tampons débordent, le programme l'exécutant (démon ou programme suid) peut être exploité pour faire autre chose. Cela fonctionne généralement en écrasant une adresse de retour de fonction sur la pile, de sorte qu'elle pointe vers un autre endroit.

denial of service (dénis de service)
: Une attaque qui consomme les ressources de votre ordinateur pour des tâches qu'il n'était pas supposé effectuer, empêchant de la sorte l'usage des ressources réseau ou autre pour des buts légitimes.

dual-homed Host (hôte à double patrie)
: Un ordinateur à usage général possédant au moins deux interfaces réseau.

firewall (pare-feu)
: Un composant ou ensemble de composants qui limite les transferts entre un réseau protégé et Internet, ou entre deux ensembles de réseaux.

host (hôte)
: Un système informatique relié à un réseau.

IP spoofing (Usurpation d'IP)
l'*IP Spoofing* est une technique d'attaque complexe composée de plusieurs composants. C'est une violation de sécurité qui trompe des ordinateurs sur des relations de confiance en leur faisant croire qu'ils sont quelqu'un qu'ils ne sont pas en fait. Il y a un article complet écrit par démon9, route, et infinity dans le volume Sept, numéro 48 du magazine `Phrack`.

non-répudiation
La caractéristique d'un destinataire capable de prouver que l'expéditeur de données est bien l'expéditeur réel, même s'il dément plus tard en être à l'origine.

packet (paquet)
L'unité de communication fondamentale sur Internet.

packet filtering (filtrage de paquets)
L'action qu'un périphérique réalise pour faire du contrôle sélectif sur le flot de données entrant et sortant d'un réseau. Le filtrage de paquets autorise ou bloque des paquets, généralement en les routant d'un réseau vers un autre (plus généralement d'Internet vers un réseau interne, et vice-versa). Pour accomplir le filtrage de paquets, vous définissez des règles qui spécifient quels types de paquets (ceux de ou vers une adresse IP particulière ou un port) doivent être autorisés, et quels autres doivent être bloqués.

perimeter network (réseau périmètre)
Un réseau ajouté entre un réseau protégé et un réseau externe , pour permettre un niveau de sécurité supplémentaire. Un réseau périmètre est parfois appelé un DMZ.

proxy server (serveur mandataire)
Un programme qui traite avec les serveurs externes au nom des clients internes. Les clients *Proxy* parlent au serveur *Proxy*, qui relaie les requêtes autorisées du client au serveur réel et relaie la réponse en retour au client.

superuser (super-utilisateur)
Un nom officieux de `root`.

Chapitre 12. Le réseau sous GNU/Linux

12.1. Copyright

Ce chapitre s'appuie sur un *HOWTO* de Joshua D. Drake {POET} dont l'original est hébergé sur le site The Linux Review (`http://www.thelinuxreview.com/`). La traduction française est basée sur l'adaptation française de Jacques Chion.

Les *HOWTO*s NET-3/4-HOWTO, NET-3, et Networking-HOWTO, renseignements au sujet de l'installation et la configuration de réseau prenant en charge Linux. Copyright (©) 1997 Terry Dawson, 1998 Alessandro Rubini, 1999 Joshua D. Drake {POET} —, CommandPrompt, Inc. est un document LIBRE. Vous pouvez le redistribuer sous les termes de la Licence Publique Générale GNU (GPL).

Les modifications depuis la version « v1.7.0, 2000 », sont sous (C)opyright 2000 - 2005 Mandriva.

12.2. Comment utiliser ce document ?

Ce document s'organise de haut en bas. La lecture des premières sections, qui fournissent des informations sur le matériel, est facultative ; par contre, il est conseillé d'avoir bien assimilé la section qui concerne les réseaux avant de poursuivre vers les suivantes qui s'avèreront plus pointues. Le reste du manuel est plus technologique. Il comporte trois grandes parties : Informations sur Ethernet et IP, Technologies pour matériel PC le plus courant, et Technologies moins répandues.

La démarche suggérée pour parcourir ce document est donc la suivante :

Lire les sections générales.

> Ces sections s'appliquent à quasiment toutes les technologies qui seront décrites plus loin. Il est donc important de les avoir bien saisies. La plupart d'entre vous connaissent sans doute déjà bien le sujet.

Réfléchissez à votre réseau.

> Il faudra savoir quelle est ou sera la conception de votre réseau, quels matériels et types de technologies seront utilisés.

Lisez la section *Informations sur IP et Ethernet*, page 134 si vous êtes connecté en direct sur un réseau local ou à Internet :

> Cette section traite de la configuration de base d'Ethernet et des différentes possibilités qu'offre Linux, concernant le réseau IP, telles que le pare-feu, le routage avancé, etc.

Lisez la suite si les réseaux locaux à bas coût ou les connexions par téléphone vous intéressent

> Cette section décrit PLIP, PPP, SLIP and RNIS, : les technologies utilisées habituellement sur les stations de travail personnelles.

Lisez les sections relatives à vos besoins technologiques spécifiques :

> Si vos besoins diffèrent de IP et/ou de matériel standard, *Autres technologies de réseau*, page 138 couvre des détails spécifiques aux protocoles non IP et au matériel de communication particulier.

Configurez votre réseau.

> Si vous avez la ferme intention de vous lancer dans la configuration de votre réseau, il serait prudent de prévenir tout problème éventuel en lisant attentivement cette partie.

Cherchez de l'aide si nécessaire.

> Si certains problèmes, non traités par notre documentation, apparaissent lors de votre installation, reportez-vous à notre section consacrée à la recherche de documentation ou celle des rapports de bogues.

Amusez-vous !

> On peut vraiment prendre son pied sur le réseau. Foncez ! N'hésitez pas !

12.2.1. Les conventions utilisées dans ce document.

Aucune convention spéciale n'est utilisée ici. Il faudra cependant prêter attention à la façon dont les commandes sont indiquées. Dans la documentation usuelle UNIX, toute commande à entrer est précédée d'une invite du shell. Ce chapitre utilisera « `user%` » comme invite pour les commandes ne nécessitant pas de privilèges de super utilisateur, et « `root#` » pour les commandes que l'on doit exécuter comme utilisateur root. Il nous a semblé préférable d'utiliser« `root#` » à la place du classique « # » pour éviter toute confusion avec les extraits de scripts shell, où le signe # (dièse) est utilisé pour définir les lignes de commentaires.

12.3. Informations générales concernant le réseau sous Linux.

12.3.1. Informations sur la couche réseau de Linux.

Bon nombre d'adresses existent pour dégoter des informations sur le réseau Linux.

Les spécialistes disponibles pullulent. Par exemple, voir la liste sur le site linuxports (`http://www.linuxports.com/`). Il existe également un groupe de discussion consacrée au réseau et à ce qui le concerne dans la hiérarchie Linux (`news:comp.os.linux.networking`).

Lorsque vous faites part d'un problème, n'omettez aucun détail. Plus spécifiquement, indiquez de quelles versions de logiciels vous vous servez - en particulier celle du noyau, des outils tels que `pppd` ou `dip`, et décrivez précisément la nature des problèmes rencontrés. Il faudra donc noter la syntaxe exacte des messages d'erreurs reçus, et les commandes que vous avez exécutées.

12.3.2. Où obtenir des informations sur le réseau, non spécifiques à Linux ?

Si vous désirez des informations générales sur les réseaux TCP/IP, lisez les documents suivants :

Introduction à TCP/IP

> ce document se trouve à la fois sur en version texte (`ftp://athos.rutgers.edu/runet/tcp-ip-intro.doc`) et en version postscript (`ftp://athos.rutgers.edu/runet/tcp-ip-intro.ps`).

Administration TCP/IP.

> ce document se trouve à la fois sur en version texte (`ftp://athos.rutgers.edu/runet/tcp-ip-admin.doc`) et en version postscript (`ftp://athos.rutgers.edu/runet/tcp-ip-admin.ps`).

Si vous recherchez des informations plus détaillées, alors : *Inter networking with TCP/IP, Volume 1: principles, protocols and architecture*, de Douglas E. Comer, `ISBN 0-13-227836-7`, Prentice Hall publications, 3ème est chaudement recommandé :

Si vous voulez apprendre comment écrire des applications réseau dans un environnement compatible avec UNIX, alors *Unix Network Programming*, de W. Richard Stevens, `ISBN 0-13-949876-1`, Prentice Hall publications, 2ème édition, est également recommandée. consultez le site Web de Prentice-Hall (`http://www.phptr.com/`) pour plus d'information.

Vous pouvez essayer aussi le groupe de discussions sur le protocole TCP-IP (`news:comp.protocols.tcp-ip`).

Une importante source d'informations techniques concernant Internet et la suite des protocoles TCP/IP sont les RFC. RFC est l'acronyme de « Request For Comment », c'est le moyen habituel de soumettre et de s'informer des normes de protocoles Internet. Il y a beaucoup d'endroits où sont stockées ces RFC, et certains vous permettent de lancer une recherche sur les bases de données RFC avec des mots-clés particuliers. Une source possible de RFC est :la base de données RFC de Nexor (`http://www.nexor.com/rfc_search.htm`).

12.4. Informations générales sur la configuration du réseau

Vous devez connaître et bien comprendre les sections suivantes avant d'essayer de configurer votre réseau. Ce sont des principes de base qui s'appliquent, indépendamment de la nature du réseau que vous voulez mettre en place.

12.4.1. De quoi ai-je besoin pour démarrer ?

Avant de commencer à construire ou configurer votre réseau, les éléments les plus importantes sont :

12.4.1.1. Support noyau pour le matériel et les protocoles réseau

Votre distribution Mandriva Linux est livrée avec l'option réseau activée, ainsi que la prise en charge de la plupart des périphériques réseau tels que les cartes 3COM, cartes NE2000 ou cartes Intel, ainsi que la plupart des protocoles. Reportez vous à la documentation accompagnant votre matériel pour plus d'information.

12.4.1.2. Une explication des adresses IP

Les adresses de protocole Internet (IP) sont composées de quatre octets.[1]. La convention d'écriture est appelée « notation décimale pointée ». Sous cette forme chaque octet est converti en un nombre décimal (0-255), les zéros de tête (à moins que ce nombre ne soit lui-même un zéro) étant omis et chaque octet séparé par le caractère « . ». Par convention, chaque interface d'un hôte ou routeur possède une adresse IP. Il est permis, dans certaines circonstances, d'utiliser la même adresse IP sur différentes interfaces d'une même machine, mais, en général, chaque interface possède sa propre adresse.

Les réseaux IP (protocole Internet) sont des séquences contiguës d'adresses IP. Toutes les adresses d'un même réseau ont des chiffres en commun. La partie de l'adresse commune à toutes les adresses d'un réseau s'appelle la « partie réseau ». Les chiffres restants s'appellent « partie hôte ». Le nombre de bits partagé par toutes les adresses d'un même réseau est appelé « masque de réseau » (*netmask*) et c'est le rôle du masque de réseau de déterminer quelles adresses appartiennent ou non à « son » réseau. Par exemple :

Adresse hôte (host address)	**`192.168.110.23`**
Masque de réseau (*network mask*)	`255.255.255.0`
Partie réseau (*network portion*)	`192.168.110.`
Partie hôte (*host portion*)	`.23`
Adresse réseau (*network address*)	`192.168.110.0`
Adresse de diffusion (*broadcast address*)	`192.168.110.255`

Si on effectue un ET logique sur une adresse avec son masque de réseau, on obtient l'adresse du réseau auquel elle appartient. L'adresse du réseau, par conséquent, sera l'adresse de plus petit nombre dans l'ensemble des adresses de la plage du réseau et aura toujours la partie hôte codée avec des zéros.

L'adresse de diffusion est une adresse spéciale que chaque hôte du réseau écoute en même temps que son adresse personnelle. Cette adresse est celle à laquelle les datagrammes sont envoyés si tous les hôtes du réseau sont en mesure de les recevoir. Certains types de données telles que les informations de routage et les messages d'alerte sont transmis vers l'adresse de diffusion. Il y a deux standards utilisés de manière courante pour définir ce que doit être l'adresse de diffusion. Ce qui est le plus courant est de prendre l'adresse la plus haute possible du réseau comme adresse de diffusion. Dans l'exemple ci-dessus ce serait `192.168.110.255`. Pour d'autres raisons, certains sites ont adopté la convention suivante: utiliser l'adresse de réseau comme adresse de diffusion. En pratique cela n'a guère d'importance. Cependant, il faudra s'assurer que tous les hôtes du réseau possèdent la même adresse de diffusion dans leur configuration.

Pour faciliter la gestion, il a été décidé, il y a quelque temps, lors du développement du protocole IP, que les ensembles d'adresses seraient organisés en réseaux et ces réseaux regroupés en "classes" qui fournissent un certain nombre de réseaux de tailles standards auxquels on peut assigner des adresses. Ces classes sont les suivantes :

1. Pour la version 4 de IP, soit IPv4

Classe de réseau	Masque de réseau	Adresses de réseau
A	255.0.0.0	0.0.0.0 – 127.255.255.255
B	255.255.0.0	128.0.0.0 – 191.255.255.255
C	255.255.255.0	192.0.0.0 – 223.255.255.255
Multicast	240.0.0.0	224.0.0.0 – 239.255.255.255

Le type d'adresse que vous devez utiliser dépend de ce que vous voulez faire exactement. On pourra combiner les actions suivantes pour obtenir l'ensemble des adresses dont on aura besoin :

Installer une machine Linux sur un réseau IP existant.

Il faudra alors contacter un des administrateurs du réseau pour lui demander les informations suivantes :

- Adresse hôte ;
- Adresse réseau ;
- Adresse de diffusion ;
- Masque de réseau ;
- Adresse de routage ;
- Adresse du serveur de noms de domaine (DNS).

Il vous faudra alors configurer votre réseau Linux à l'aide de ces données, qu'il est donc impossible d'inventer soi-même en espérant que la configuration fonctionnera.

Construire un réseau tout neuf non connecté à Internet.

Par contre, lors de la construction d'un réseau privé qui ne sera pas connecté à Internet, il est tout à fait possible de choisir son adresse. Cependant, pour des raisons de sécurité et de fiabilité, il existe quelques adresses de réseau IP réservées à cet usage. Elles sont spécifiées dans la RFC 1597 et sont les suivantes :

Classe réseau	Masque de réseau	Adresses de réseau
A	255.0.0.0	10.0.0.0 – 10.255.255.255
B	255.255.0.0	172.16.0.0 – 172.31.255.255
C	255.255.255.0	192.168.0.0 – 192.168.255.255

Tableau 12-1. Allocations pour réseaux privés

Il faudra dans un premier temps décider de la dimension du réseau requis avant de choisir les adresses nécessaires.

12.4.2. Routage

La question du routage est un large sujet. Mais il est fort probable que la plupart des lecteurs ne nécessitera qu'un routage simple, et les autres aucun ! Il ne sera donc question ici que des principes même du routage.

Commençons par proposer une définition du routage. Par exemple : « Le routage IP est le processus par lequel un hôte, ayant des connexions réseau multiples, décide du chemin par lequel délivrer les datagrammes IP qu'il a reçus. »

Donnons une petite illustration. Imaginons un routeur dans un bureau :il peut avoir un lien PPP sur Internet, un certain nombre de segments Ethernet alimentant les stations de travail et un second lien PPP vers un autre bureau. Lors de la réception par le routeur d'un datagramme de l'une de ses connexions, le routage est le mécanisme utilisé pour déterminer vers quelle interface, ce datagramme devra être renvoyé. De simples hôtes ont besoin aussi de routage, tous les hôtes Internet ayant deux périphériques réseau, l'un étant l'interface *loopback*, et l'autre celui qui est utilisé pour parler avec le reste du monde, soit un lien Ethernet, soit une interface série PPP ou SLIP.

Comment fonctionne le routage ? Chaque hôte possède une liste spéciale de règles de routage, appelée une table de routage. Cette table est composée de colonnes qui contiennent au moins trois champs : le premier étant une adresse de destination, le deuxième le nom de l'interface vers lequel le datagramme doit être routé et le troisième, qui est optionnel, l'adresse IP d'une autre machine qui transportera le datagramme vers sa prochaine destination sur le réseau passerelle. Cette table apparaît à la commande suivante :

```
user% cat /proc/net/route
```

ou avec l'une des commandes suivantes :

```
user% /sbin/route -n
user% /sbin/netstat -r
```

Le processus de routage est plutôt simple : un datagramme entrant est reçu, l'adresse de destination est examinée et comparée avec chaque entrée de la table. L'entrée qui correspond le mieux à cette adresse est choisie, et le datagramme est renvoyé vers l'interface spécifiée. Si le champ passerelle est rempli, alors le datagramme est renvoyé vers cet hôte via l'interface spécifiée, sinon l'adresse de destination est présupposée comme étant sur le réseau supporté par l'interface.

Pour manipuler cette table, la commande `route` est utilisée. Pour en savoir plus, référez-vous à la page `man` de route(8).

12.4.2.1. Que fait le programme routed ?

La configuration de routage décrite ci-dessus est bien adaptée aux réseaux simples où il n'existe que des chemins uniques pour parvenir à chaque destination. Plus le réseau est complexe, plus le reste se complique.

Le problème majeur est le suivant :dans le cas d'un « routage manuel » ou « routage statique », tel que décrit ci-dessus, si une machine ou un lien tombe en panne dans le réseau, la seule façon de diriger les datagrammes vers un autre chemin, s'il existe, sera d'intervenir manuellement en exécutant une série de commandes adéquate. Ceci est peu pratique et risqué, impliquant une lourdeur et une lenteur certaine. Dans le cas d'incidents sur un réseau où plusieurs routes coexistent, diverses techniques ont été mises au point pour que se règlent automatiquement les tables de routage – ces techniques étant regroupées sous le nom de « protocoles de routage dynamique ».

Les plus courants sont peut-être déjà connus du lecteur : RIP (*Routing Information Protocol*) et OSPF (*Open Shortest Path First Protocol*). RIP est très souvent utilisé sur réseaux d'entreprise petits et moyens. L'OSPF est plus moderne, plus apte à gérer de grands réseaux et mieux adapté lorsqu'un grand nombre de chemins sont possibles à travers le réseau. Les implantations usuelles de ces protocoles sont : **routed** - RIP, et **gated** - RIP, OSPF et autres. Le programme `routed` est fourni avec distribution Linux.

Un exemple d'utilisation d'un protocole de routage dynamique ressemblerait à la figure 12-1.

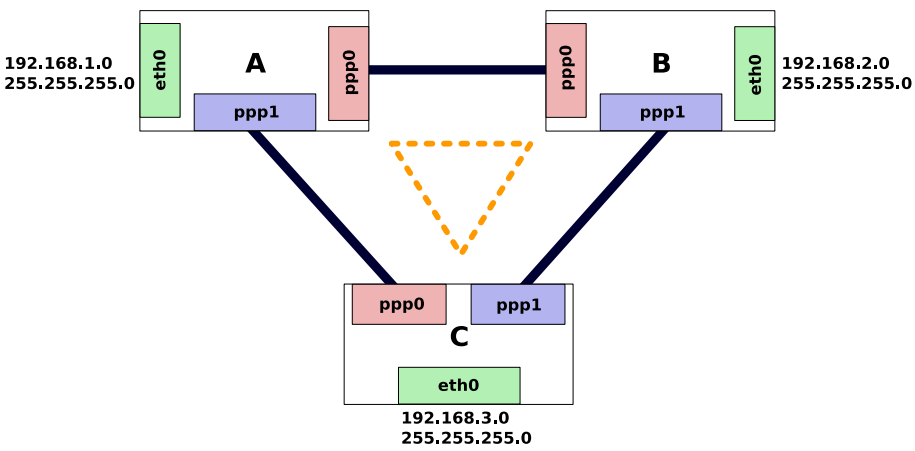


Figure 12-1. Un exemple de routage dynamique

Nous avons trois routeurs : A, B et C. Chacun supporte un segment Ethernet avec un réseau IP de classe C (masque de réseau 255.255.255.0). Chaque routeur a également une liaison PPP vers chacun des autres routeurs. Ce réseau forme un triangle.

La table de routage sur le routeur A ressemblera évidemment à ceci :

```
root# route add -net 192.168.1.0 netmask 255.255.255.0 eth0
root# route add -net 192.168.2.0 netmask 255.255.255.0 ppp0
root# route add -net 192.168.3.0 netmask 255.255.255.0 ppp1
```

Tout fonctionnera à merveille jusqu'à ce que le lien entre A et B tombe en panne. Si cette liaison défaille, alors l'entrée de routage montre que, sur le segment A, les hôtes ne peuvent en atteindre d'autres sur le segment B car leurs datagrammes seront dirigés sur le lien ppp0 du routeur A qui est rompu. Ils pourront continuer à communiquer avec les hôtes du segment C, et ces derniers avec ceux du segment B car la liaison restera intacte.

Mais, si A peut parler à C et si C peut toujours parler à B, pourquoi A ne routerait-il pas ses datagrammes pour B via C, et laisserait ensuite C les envoyer à B ? C'est exactement le type de problèmes que les protocoles de routage dynamique comme RIP sont en mesure de résoudre. Si chacun des routeurs A, B et C utilisent un Démon de routage, alors leurs tables de routage seront automatiquement réglées pour refléter le nouvel état du réseau même si l'une des liaisons est défectueuse. Configurer un tel réseau est simple, il s'agira d'accomplir deux choses sur chaque routeur. Pour le routeur A :

```
root# route add -net 192.168.1.0 netmask 255.255.255.0 eth0
root# /usr/sbin/routed
```

Le démon de routage **routed** trouve automatiquement tous les ports actifs vers le réseau quand il démarre et écoute tous les messages sur chacun des périphériques réseau. Ceci lui permet de déterminer et de mettre à jour sa table de routage.

Ce qui précède explique brièvement ce qu'est le routage dynamique et la façon de s'en servir. Pour de plus amples explications, on se reportera à la liste de références (*Informations générales concernant le réseau sous Linux.*, page 130).

Récapitulons les points importants relatifs au routage dynamique :

1. Un démon de routage dynamique n'est nécessaire que lorsque votre machine Linux est capable, de choisir entre plusieurs routes, pour une destination donnée, par exemple lorsque vous envisagez d'utiliser le masquage d'adresse IP.
2. Le démon de routage dynamique modifiera automatiquement votre table de routage pour tenir compte des changements survenus dans votre réseau.
3. RIP est adapté aux réseaux de petite et moyenne taille.

12.5. Informations sur IP et Ethernet

Cette section donnera des informations détaillées au sujet d'Ethernet et de la configuration des cartes Ethernet.

12.5.1. Cartes Ethernet prises en charge

GNU/Linux supporte la majorité des cartes réseau connues. Il serait donc inutile de toutes les décrire ici. Si vous rencontrez des problèmes lors de la configuration de votre carte réseau, consultez le manuel fourni (s'il existe) ou le site internet du fabricant. Vous pouvez aussi consulter la documentation du noyau spécifique à certaines cartes.

12.5.2. Information générales sur Ethernet

Les noms de périphériques Ethernet sont `eth0`, `eth1`, `eth2` etc. La première carte détectée par le noyau devient `eth0` et le reste est nommé selon l'ordre de détection.

La configuration d'une carte est très simple. En général, on fera ceci (ce que la plupart des distributions feront automatiquement pour vous, si vous les avez configurées pour reconnaître votre carte Ethernet) :

```
root# ifconfig eth0 192.168.0.1 netmask 255.255.255.0 up
root# route add -net 192.168.0.0 netmask 255.255.255.0 eth0
```

12.5.3. Utiliser plus d'une carte Ethernet dans la même machine

Si vous avez 3 cartes NE2000, une à `0x300`, une à `0x240` et une à `0x220`, il faudra ajouter les lignes suivantes à votre fichier `/etc/modprobe.conf` :

```
alias eth0 ne
alias eth1 ne
alias eth2 ne
options ne io = 0x220,0x240,0x300
```

Ceci indique au programme modprobe de rechercher trois cartes du type NE aux adresses en question. Les périphériques auxquels elles devraient être assignées sont également indiqués dans le même ordre.

La plupart des modules ISA peuvent prendre de multiples arguments I/O séparés par des virgules. Par exemple :

```
alias eth0 3c501
alias eth1 3c501
options eth0 -o 3c501-0 io = 0x280 irq = 5
options eth1 -o 3c501-1 io = 0x300 irq = 7
```

L'option `-o` permet à un nom unique d'être assigné à chaque module. La simple raison est qu'il est impossible de charger deux copies d'un même module.

L'option `irq=` est utilisée pour indiquer l'IRQ matériel et le `io=` pour les différents ports io.

Consultez le Ethernet-HOWTO (`http://www.tldp.org/HOWTO/Ethernet-HOWTO.html`) pour plus d'information à propos d'Ethernet.

12.6. Informations relative à IP

12.6.1. DNS

DNS signifie *Domain Name System*, système responsable de la production du nom d'une machine, tel que `www.mandriva.com` avec l'adresse IP de cet ordinateur, c'est-à-dire ici : `212.85.150.181` (à l'heure où nous mettons sous presse). Avec DNS, la résolution est disponible dans les deux sens, du nom vers le IP et vice-versa. (

Le DNS est constitué d'un grand nombre d'ordinateurs dans tout le réseau Internet ayant la charge d'un certain nombre de noms. A chaque machine correspond un serveur DNS auquel il peut se référer pour produire un nom en particulier avec son adresse. Si ce serveur ne possède pas la réponse, il en fait la demande à un autre, et ainsi de suite. Il est possible également d'avoir un DNS local qui aurait la charge de produire les adresses sur votre LAN.

Il est possible de diviser les DNS en deux grandes catégories: DNS antémémoire (*caching DNS*) et le serveur DNS maître (*master server*). Le premier se contente de « se souvenir » de requêtes précédentes auxquelles il pourra répondre sans reposer la question au serveur DNS maître. Ce dernier est un serveur à utiliser en dernier recours pour produire une adresse avec un nom — ou pour vérifier qu'un nom produit bien telle ou telle adresse.

12.6.2. DHCP

DHCP est l'acronyme de *Dynamic Host Configuration Protocol*. Sa création aura beaucoup simplifié la configuration d'un réseau à hôtes multiples. Nul besoin désormais de configurer chaque hôte séparément, il suffit d'assigner tous les paramètres utilisés couramment par les hôtes qui partagent un serveur DHCP.

Chaque fois qu'un hôte se connecte, un paquet sera émis au réseau. Ce paquet représente une demande de configuration par l'hôte à tout serveur DHCP localisé sur le même segment.

12.6.3. Alias IP

Il existe des applications pour lesquelles la configuration d'adresses IP multiples pour une seule interface réseau physique peut s'avérer utile. Les Fournisseurs d'Accès Internet utilisent souvent cette fonctionnalité pour offrir une « personnalisation » de leur offre Web et ftp pour leurs clients. Vous pouvez obtenir plus d'information en lisant IP-Alias mini-HOWTO (`http://www.tldp.org/HOWTO/IP-Alias/`).

12.6.4. Pare-feu IP

Les problèmes de Pare-feu IP et de configuration de pare-feu sont expliqués plus en détails dans le Firewall-HOWTO (`http://tldp.org/HOWTO/Firewall-HOWTO.html`). La configuration de pare-feu IP vous permet de sécuriser votre machine contre les accès réseau non-désirés en filtrant ou en acceptant des datagrammes venants ou à destination d'adresses IP que vous avez désignées. Il existe trois catégories différentes de règles ; filtrage des paquets entrants, filtrage des paquets sortants, et filtrage des paquets en transit. Les règles de filtrage des paquets entrants s'appliquent aux datagrammes reçus par une interface réseau. Les règles de filtrage de paquets sortants s'appliquent aux datagrammes qui sont transmis par une interface réseau. Quant aux règles de filtrage des paquets en transit, elle s'appliquent aux datagrammes qui sont reçus mais qui ne sont pas destinés à cette machine (c'est-à-dire les paquets qui seront routés).

12.6.5. Masquage et Translation d'adresses IP

Beaucoup de gens ont un accès Internet simple et une seule adresse IP leur est attribuée par leur Fournisseur d'Accès Internet. Cela est suffisant pour permettre l'accès d'un seul hôte au réseau. La translation d'adresses IP est une fonctionnalité qui vous permet d'utiliser une seule adresse IP pour plusieurs machines. Elle oblige les autres machines à se présenter comme la machine qui est réellement connectée. Et c'est pour cela qu'on applique les termes de « masquage » ou de « translation » d'adresses IP. Cependant, sachez que cette fonction de masquage IP ne fonctionne habituellement qu'à sens unique. Les hôtes masqués peuvent faire des requêtes vers l'extérieur, mais ils ne peuvent accepter de connections de l'extérieur. Cela signifie que certains services réseau ne fonctionnent pas (comme talk), et que d'autres (comme FTP) doivent être configuré en mode passif (`PASV`) afin de fonctionner. Heureusement, les services réseau les plus courants fonctionnent normalement.

12.6.6. IPv6

Alors que vous commenciez à comprendre comment fonctionne un réseau IP, le protocole IPv6 à changé les règles ! IPv6 est la dénomination du Protocole Internet version 6. Il a été développé afin de répondre aux préoccupations de la communauté Internet : les utilisateurs s'inquiétaient d'une pénurie potentielle d'adresses IP à allouer. Les adresses IPv6 sont composées de 16 octets (128 bits). Le protocole IPv6 inclut de nombreuses autres modifications, des simplifications pour la plupart, qui rendront les réseaux IPv6 plus faciles à administrer que les réseaux IPv4.

Visiter la page Linux IPv6 HOWTO (`http://www.tldp.org/HOWTO/Linux+IPv6-HOWTO/`) pour plus de renseignements.

12.6.7. Limitation du trafic

Le limiteur de trafic est utilisé pour limiter le trafic à certaines valeurs maximales. Le limiteur de trafic crée de nouveaux périphériques réseau qui reposent sur une interface réseau physique, et ils peuvent être employés pour router du trafic.

Visiter la page Traffic Control HOWTO (`http://www.tldp.org/HOWTO/Traffic-Control-HOWTO/`) pour de plus amples informations sur le contrôle de trafic en général, et sa limitation en particulier.

12.7. Utilisation du matériel courant pour PC

12.7.1. RNIS

Le Réseau Numérique à Intégration de Service (RNIS) (en anglais ISDN : *Integrated Services Digital Network*) est une série de normes attribuant les caractéristiques particulières d'un réseau de données numériques à usage général. Un « appel » RNIS permet de synchroniser des données point par point vers la destination. RNIS est généralement distribué sur une ligne à haut débit, divisée en un certain nombre de canaux discrets. Il existe deux types de canaux, les « canaux B » qui transportent de fait les données utilisateurs, et un canal unique appelé « canal D », utilisé pour envoyer les informations de contrôle pendant l'échange RNIS afin d'établir appels et autres fonctions. En Australie, par exemple, RNIS peut être fourni sur une liaison 2 Mbps qui est divisée en 30 canaux B discrets de 64 kbps et un canal D de 64 kbps. Le nombre de canaux utilisé en même temps importe peu, et ceci avec toutes les combinaisons possibles. Vous pouvez par exemple établir 30 appels différents de 64 kbps vers 30 destinations différentes, ou bien 15 appels de 128 kbps chacun vers 15 destinations différentes (2 canaux utilisés par appel), ou seulement un petit nombre d'appels, le reste restant inactif. Un canal peut être utilisé pour des appels entrants ou sortants. Le but initial de RNIS était de permettre aux sociétés de Télécommunications de fournir un seul service de données pouvant distribuer soit le téléphone (avec voix numérisée) ou bien des services de données vers le domicile ou le bureau sans que cela nécessite des modifications pour obtenir une configuration spéciale.

On pourra connecter son ordinateur à un service RNIS de différentes façons : en utilisant un dispositif appelé « adaptateur de terminal » qui se branche sur le terminal numérique de réseau que votre opérateur de télécommunications a installé au moment de l'obtention de votre service RNIS, et qui présente des interfaces séries - une de ces interfaces est utilisée pour entrer les commandes et établir les appels et la configuration; les autres sont reliées aux périphériques réseau qui utiliseront les circuits de données quand la connexion sera faite. Linux peut travailler avec ce type de configuration sans modification. Il suffira de traiter le port de l'adaptateur de terminal comme tout périphérique série. L'autre moyen, la raison d'être du support RNIS dans le noyau, vous permet d'installer une carte RNIS dans votre machine Linux et ce sera le logiciel Linux qui alors prendra en charge les protocoles et fera lui-même les appels.

L'implémentation Linux de RNIS reconnaît différents types de cartes internes RNIS, qu'elles soient passives ou actives. Nous n'en ferons pas la liste ici.

Certaines de ces cartes exigent certains logiciels téléchargeables pour être opérationnelles. Il existe pour cela différents utilitaires indépendants.

Tous les détails nécessaires à la configuration du support RNIS Linux se trouvent dans le site ISDN4Linux (`http://www.isdn4linux.de/faq/`).

Au sujet de PPP. L'ensemble des protocoles PPP fonctionne sur des lignes série synchrone ou asynchrone. Le démon PPP **pppd** couramment distribué pour Linux ne reconnaît que le mode asynchrone. Si vous désirez utiliser les protocoles PPP avec votre service RNIS, il vous faudra une version spéciale. Les détails pour la trouver se trouvent dans la documentation mentionnée ci-dessus.

12.7.2. PLIP

Le nouveau code pour PLIP fonctionne de la même façon (on utilise les mêmes commandes **ifconfig** et **route** comme dans le paragraphe précédent), mais l'initialisation du système est différente en raison de l'amélioration du support du port parallèle.

Le « premier » périphérique PLIP est toujours appelé `plip0` (premier signifiant ici « qui est détecté en premier par le système » comme pour les périphériques Ethernet). Le port parallèle utilisé de fait est l'un de ceux qui sont disponibles, comme indiqué dans `/proc/parport`. Par exemple, si vous n'avez qu'un seul port parallèle, vous n'aurez qu'un seul répertoire appelé `/proc/parport/0`.

Si votre noyau ne détecte pas l'IRQ utilisée par votre port parallèle, PLIP échouera. Dans ce cas, il vous suffit d'écrire le chiffre qui convient dans `/proc/parport/0/irq`, et chargez PLIP à nouveau.

Vous pouvez lire PLIP mini-HOWTO (`http://www.tldp.org/HOWTO/PLIP.html`) pour obtenir plus de renseignements sur le sujet.

12.7.3. PPP

De par la nature, la taille, la complexité et la flexibilité de PPP, il possède maintenant son propre *HOWTO*. Le PPP-HOWTO est toujours un document du Linux Documentation Project (`http://tldp.org/HOWTO/PPP-HOWTO/`), dont la page officielle se situe sur le site Web The Linux Review (`http://www.thelinuxreview.com`), dans la section PPP (`http://www.thelinuxreview.com/howto/ppp`).

12.8. Autres technologies de réseau

La prise en charge des réseaux par GNU/Linux ne se limite pas aux technologies Ethernet et IP. Pratiquement tous les matériels et protocoles réseaux existants sont pris en charge. Les section qui suivent listent les plus courants, sans ordre particulier.

12.8.1. Appletalk

Le support Appletalk permet à votre machine Linux d'interagir avec les réseaux Apple pour partager imprimantes ou disques durs entre les deux systèmes. Installez le paquetage `netatalk` puis consultez le site Networking Applet Macintosh through Open Source (`http://netatalk.sourceforge.net/`).

12.8.2. IPX

Le protocole IPX est le plus couramment utilisé dans des situations de réseau local Novell NetWare(tm). Linux reconnaît ce protocole et peut être configuré pour agir comme destinataire du réseau ou comme routeur pour IPX.

Le protocole IPX et le NCPFS (*Netware Core Protocol File System*) sont explicités plus en détail dans le Linux IPX-HOWTO (`http://www.tldp.org/HOWTO/IPX-HOWTO.html`).

12.8.3. NetBEUI, NetBios, CIFS

Samba est une implémentation du protocole de *Session Management Block* (SMB). Il permet à Windows® et à d'autres systèmes d'installer et d'utiliser vos disques et vos imprimantes.

Samba et ses configurations sont couvertes en détails dans SMB-HOWTO (`http://www.tldp.org/HOWTO/SMB-HOWTO.html`). Le site Samba - opening windows to a wider world (`http://www.samba.org`) contient aussi des informations à jour à propos de Samba.

12.8.4. Token Ring

Token Ring est un protocole IBM LAN standard qui évite les collisions grâce à un mécanisme qui ne permet qu'à une seule station à la fois de transmettre sur le LAN. Un « jeton » (*token*) est dispensé à une station à la fois, et celle qui le détient est la seule qui puisse transmettre. Une fois ses données transmises, elle passe son jeton à la suivante. Le jeton circule d'une station active à l'autre, d'où le nom de « Token Ring ».

La configuration de Token Ring est semblable à celle d'Ethernet à l'exception du nom du système réseau qui est à configurer. Les noms de périphériques Token Ring device sont `tr0`, `tr1` etc.

12.9. Câbles et câblages

Ceux qui sont habiles du fer à souder peuvent vouloir fabriquer leurs propres câbles pour relier deux machines Linux. Les schémas de câblage suivants pourront les y aider. La câble PLIP est composé de connecteurs D-25 mâles à ses deux bouts, alors que le câble série NULL-modem peut être fait en utilisant des connecteurs femelles D-25 ou DB-9.

12.9.1. Câble série NULL Modem

Tous les câbles NULL modem ne se ressemblent pas. Beaucoup se contentent de faire croire à votre ordinateur que tous les signaux appropriés sont présents et échangent les données de transmission et de réception. C'est bien, mais cela signifie que vous devez utiliser le contrôle de flux logiciel (XON/XOFF) qui est moins efficace que le contrôle de flux matériel (RTS/CTS). Le câble suivant donne la meilleure transmission de signal entre les deux machines et vous permet d'utiliser le contrôle de flux matériel.

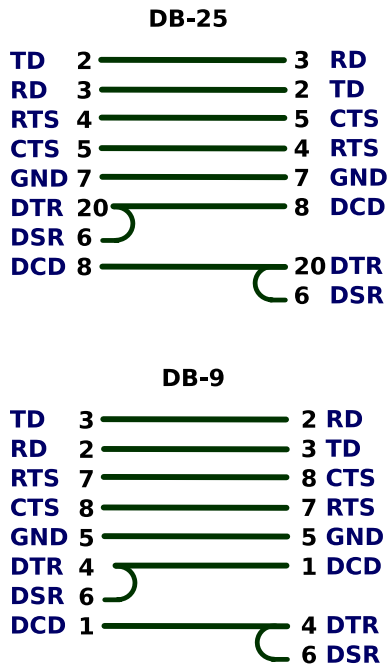


Figure 12-2. Le câblage « NULL-modem »

12.9.2. Câble port parallèle (câble PLIP)

Si vous avez l'intention d'utiliser le protocole PLIP entre deux machines alors ce câble (figure 12-3) vous conviendra indépendamment du type de port parallèle installé.

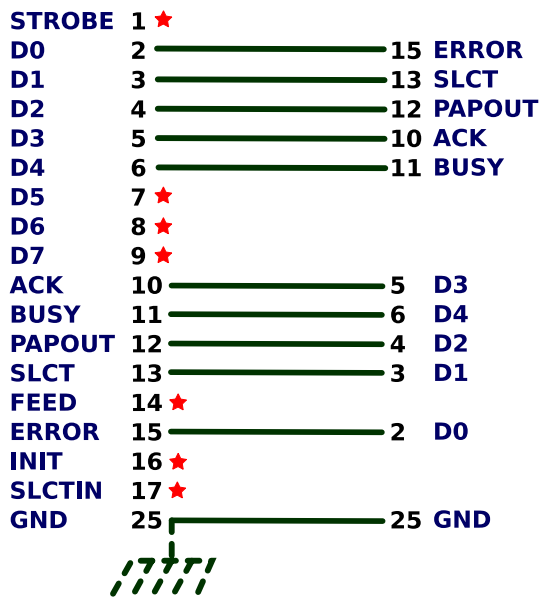


Figure 12-3. Câblage PLIP

- Ne pas connecter les broches marquées avec un astérisque (*).
- Les masses supplémentaires sont `18`, `19` ,`20`, `21` ,`22` ,`23` and `24`;
- Si le câble que vous utilisez possède un blindage, il doit être connecté à une des prises DB-25 et **une seule**.

un câble PLIP mal branché peut détruire votre port parallèle. Faites attention et vérifiez chaque connexion deux fois plutôt qu'une pour vous éviter de gros ennuis.

Bien que l'on puisse utiliser des câbles PLIP sur des longues distances, évitez de le faire si possible. Les spécifications du câble permettent d'avoir une longueur d'environ 1 mètre. Faites attention si vous utilisez de grandes longueurs, car les sources de champs magnétiques élevées comme la foudre, les lignes à haute tension et les émetteurs radio peuvent interférer et parfois endommager votre carte contrôleur. Si vous voulez vraiment connecter deux de vos ordinateurs sur une grande distance, utilisez plutôt des cartes Ethernet et un câble coaxial.

12.9.3. Câblage Ethernet 10base2 (coaxial fin)

10base2 est un standard de câblage Ethernet spécifiant l'utilisation d'un câble coaxial 52 ohms avec un diamètre d'environ 5 mm. Il faut se rappeler un nombre important de règles lorsqu'il s'agit de relier deux machines avec un câblage 10base2. La première :utilisez des terminaisons **à chaque extrémité** du câble. Un terminateur est une résistance de 50 ohm qui sert à s'assurer que le signal est absorbé et non réfléchi à l'extrémité du câble. Sans terminaison à chaque extrémité, vous pourriez trouver que l'Ethernet n'est pas fiable ou ne fonctionne pas du tout. Normalement vous utiliserez des « pièces en T » pour interconnecter les machines, de sorte que vous finirez avec quelque chose comme ceci :

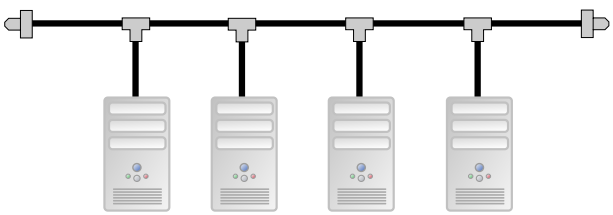


Figure 12-4. Câblage Ethernet 10base2

Chaque extrémité comporte une terminaison, les câbles coaxiaux ont des connecteurs BNC à chaque extrémité et les machines intermédiaires utilisent un connecteur en « T ». Gardez la longueur de câble entre les connecteurs en **T** et les cartes Ethernet aussi courte que possible, l'idéal étant que ces connecteurs soient branchés directement sur la carte Ethernet.

12.9.4. Câblage Ethernet à paires torsadées

Si vous n'avez que deux ordinateurs équipé de cartes Ethernet à paires torsadées et que vous voulez les relier, vous n'avez pas besoin de répartiteur (*hub*). Vous pouvez câbler les deux cartes directement ensemble (figure 12-5).

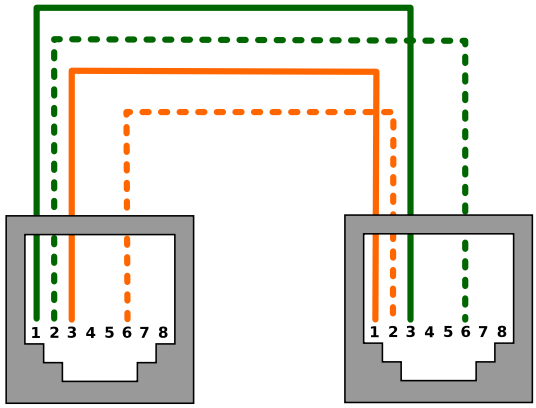


Figure 12-5. Câblage à paires torsadées « NULL-modem »

Chapitre 13. Faire face aux problèmes

Ce chapitre vous présentera quelques techniques de résolution de problèmes, c'est-à-dire : que faire quand tout va mal, ou mieux encore, que faire pour être **préparé** quand quelque chose va mal et comment le réparer.

13.1. Introduction

Faire des copies de sauvegarde, régler de petits problèmes, recompiler son noyau, installer de nouvelles applications ou bricoler ses fichiers de configuration sont des tâches que l'on est amené à effectuer un jour ou l'autre sous GNU/Linux. Toutes ces actions peuvent être maîtrisées sans histoire, si vous utilisez un peu de bon sens et que vous suivez quelques règles et techniques que nous allons vous présenter.

Presque tous les exemples et les outils présentés dans ce chapitre sont reliés à la ligne de commande. Bien souvent, la restauration d'un système endommagé ne peut se faire qu'avec elle. Donc, nous supposerons que vous maîtrisez la ligne de commande.

Donc, commençons par les bases nécessaires pour être prêt...

13.2. Disquette de démarrage

La première chose dont vous aurez besoin si votre système refuse de démarrer est une disquette de démarrage. Une telle disquette vous permettra de démarrer votre système et de corriger ce qui empêche votre système de démarrer normalement en quelques minutes.

13.2.1. Utilisation du mode Secours du CD Mandriva Linux

Un mode de secours est accessible à travers le premier CD-ROM Mandriva Linux. Pour y accéder, démarrez depuis le CD-ROM, et pressez la touche **F1**, puis tapez `rescue` et **Entrée**. Le système va démarrer en mode de secours (voir figure 13-1).

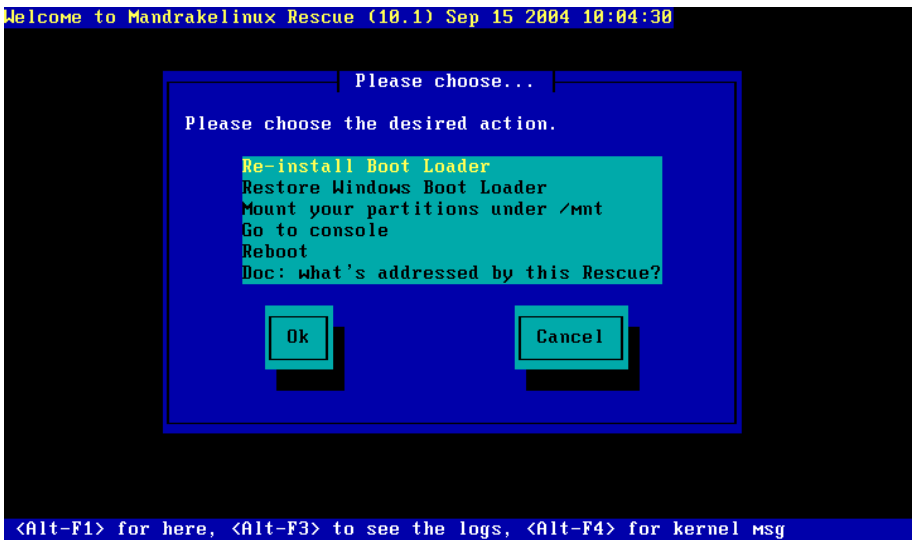


Figure 13-1. Actions disponibles en mode secours

Vous pouvez passer d'une option à l'autre grâce aux flèches du clavier et exécuter une action en pressant la touche **Entrée**. Les actions disponibles sont :

Re-install Bootloader (réinstaller le chargeur de démarrage)

Utilisez cette option pour restaurer le chargeur de démarrage Linux sur le MBR du disque dur. La configuration antérieure du chargeur de démarrage sera réactivée. Ceci peut être utile si, par exemple, un virus a infecté une éventuelle partition Windows® et a corrompu le MBR du disque, rendant le système inopérable.

Restore Windows Bootloader (restaurer le chargeur de démarrage Windows)

Utilisez cette option pour restaurer le chargeur de démarrage Windows Windows® sur le MBR du disque dur. Cela peut être utilisé pour supprimer l'information de démarrage de Linux pour ne garder que Windows® « comme si » Linux n'était pas installé. Pressez **Entrée** pour confirmer l'action ou **N** suivi de **Entrée** pour l'annuler.

Vous ne pourrez plus démarrer Linux après cela. Cependant, les partitions et le système Linux ne seront pas effacés.

Mount your partitions under /mnt (monter vos partitions sous /mnt)

Cette option permet de monter les partitions Linux dans le répertoire `/mnt`. Chaque partition sera montée dans son propre répertoire, avec le même nom que si la partition était montée dans le système original. Cette option est très utile lorsque vous avez besoin d'accéder aux données de votre disque dur, par exemple pour faire une sauvegarde. Vous aurez sans doute besoin de monter les partitions avant d'accéder à la console par exemple.

Go to Console (aller dans une console)

Ceci permet d'accéder à un *shell* pour exécuter d'autres opérations de maintenance, comme par exemple charger des gestionnaires de périphériques réseau, copier ou modifier des fichiers, formater des partitions, etc. Vous disposerez d'un système Linux simple avec quelques consoles virtuelles parmi lesquelles vous pourrez naviguer en pressant les touches **Alt-F<n>**.

Vous pouvez revenir au menu du mode secours en exécutant la commande `rescue-gui`.

Une fois que vous avez fini d'utiliser la console, vous pouvez également utiliser la commande `reboot` pour redémarrer le système.

Reboot (redémarrer)

Redémarre la machine. Enlevez le CD-ROM pour effectuer un démarrage normal. Aucune confirmation ne sera demandée.

Doc: What's addressed by this Rescue? (documentation : ce que cette tentative de secours couvre)

Affiche quelques pages d'aide (an anglais), expliquant brièvement à quoi sert le mode de secours. Naviguez à travers les pages en utilisant les flèches du clavier et pressez la touche **Q** puis **Entrée** pour retourner au menu.

13.3. Sauvegarde

13.3.1. Pourquoi sauvegarder ?

Sauvegarder votre système est le **seul** moyen de pouvoir le réparer s'il subit des dommages sérieux, si vous effacez accidentellement certains fichiers système importants, ou si quelqu'un infiltre votre ordinateur et efface certains fichiers intentionnellement. Vous devriez également sauvegarder votre travail quotidien (son, images, documents bureautique, courriers électroniques, carnet d'adresses, etc.) pour être en sécurité.

Vous devriez réaliser vos sauvegardes en utilisant un support approprié et les conserver dans un endroit sûr. Un tel endroit devrait, si possible, être en dehors du lieu où vous travaillez d'habitude. Vous pouvez même avoir deux sauvegardes, une sur place et une ailleurs. D'une manière générale, vous devriez vous assurer que vous serez capable de restaurer ces sauvegardes si vous voulez que tout cela soit réellement utile.

13.3.2. Préparation de votre système

Tout ce dont vous aurez besoin est probablement déjà installé sur votre système. Afin de parer à toute éventualité, vous devriez toujours avoir une disquette de démarrage sous la main (vous en avez créé une, n'est-ce pas ?). En fait, vous pouvez réaliser des sauvegardes en n'utilisant que `tar` et un utilitaire de compression tel que `gzip` ou `bzip2`. Voyez l'exemple dans *Exemple de sauvegarde avec tar*, page 146.

Vous pouvez également utiliser des logiciels spécialisés, tels que Taper, Time Navigator, Arkeia, ou Drakbackup, l'outil dédié de Mandriva Linux.

13.3.3. Que sauvegarder ?

Eh bien, voilà peut-être la question la plus difficile que tout administrateur système se pose lorsque vient le moment de sauvegarder. La réponse dépend de différents aspects : allez-vous sauvegarder seulement vos données personnelles, vos fichiers de configuration, ou tout le système ? Combien de temps, quel volume cela va-t-il occuper ? Allez-vous restaurer vos sauvegardes sur la même machine et le même système d'exploitation, ou bien sur d'autres ?

Comme il s'agit d'un guide de réparation, nous allons tenter de nous concentrer sur la réalisation d'une sauvegarde qui vous permettra de restaurer rapidement votre système dans l'état où il était, avant que ne survienne cette catastrophe qui l'a rendu inutilisable. Naturellement, vous devrez effectuer une sauvegarde de vos données personnelles si vous ne voulez pas les perdre.

Par principe, vous devriez sauvegarder les dossiers `/etc`, `/home`, `/root` et `/var`. Si vous effectuez une sauvegarde complète de ces dossiers, vous aurez sauvegardé non seulement vos configurations, mais vos données également. Gardez à l'esprit que cette sauvegarde peut prendre **beaucoup** de temps, mais c'est le moyen le plus sûr.

Un schéma plus sophistiqué consisterait à ne sauvegarder que les fichiers de configuration qui ont changé, laissant de côté ceux qui n'ont pas changé. Cela exige plus de préparation, mais les sauvegardes et les restaurations seront ensuite plus rapides à effectuer. De plus, ces sauvegardes sont plus « faciles » à transférer d'une machine ou d'un système d'exploitation à un autre.

Pour résumer, sauvegardez tous les fichiers de configuration des programmes que vous utilisez et tous les fichiers de configuration que vous avez modifiés. Sauvegardez aussi vos données personnelles et celles des utilisateurs du système. Vous ne le regretterez pas.

13.3.4. Où sauvegarder ?

L'autre grande question à laquelle répondre. Cela dépend de la quantité de données que vous voulez sauvegarder, du temps que vous pouvez y consacrer, de la facilité d'accès au support de sauvegarde, ainsi que de nombreux autres facteurs.

En général, vous avez besoin d'un support qui soit au moins aussi large que la quantité d'informations que vous voulez sauvegarder, et suffisamment rapide pour que le processus complet ne prenne pas une éternité.

Les supports de sauvegarde disponibles varient en capacité, fiabilité et vitesse. Vous pouvez combiner plusieurs supports différents suivant votre stratégie de sauvegarde, par exemple : bandes et CD-R/DVD+RW, disque dur et bande, disque dur et CD-R/DVD+RW, etc., mais assurez-vous que votre logiciel de sauvegarde accepte tous ces supports.

13.3.5. Quand sauvegarder ?

Il y a de nombreuses politiques de planification de sauvegarde. Nous allons vous en présenter quelques-unes. Conservez à l'esprit qu'elles ne sont pas obligatoires et que ce ne sont peut-être pas les meilleures, ni les seules. Ce ne sont que des lignes directrices que vous pouvez suivre pour établir votre propre programme de sauvegarde.

Les stratégies de sauvegarde dépendent du support que vous utilisez, de la fréquence à laquelle vos données changent et de l'importance de ces données pour vous ou votre organisation. Par exemple, une des stratégies veut que vous fassiez une sauvegarde complète chaque fin de semaine, et une sauvegarde incrémentale (seulement les changements) chaque jour ; ensuite il faudrait que vous fassiez une sauvegarde complète chaque mois et que vous la stockiez dans au moins deux endroits différents. Cette stratégie peut être adaptée à une entreprise, mais pas pour un ordinateur personnel. Pour vos sauvegardes personnelles, vous pourriez envisager une sauvegarde hebdomadaire de vos fichiers sur votre disque dur, et chaque mois, un transfert de ces sauvegardes sur un CD-R/DVD+RW ou une bande.

13.3.6. Exemple de sauvegarde avec tar

Nous allons maintenant vous présenter un petit script de sauvegarde qui utilise `tar` et `bzip2` pour réaliser une sauvegarde complète de votre dossier personnel. Lisez les commentaires du script pour obtenir des informations sur son utilisation.

Vous devez avoir les droits de lecture sur les fichiers et répertoires que vous allez sauvegarder, sinon la sauvegarde échouera.

```
#!/bin/bash

 # Crée une sauvegarde compressée de tous les répertoires spécifiés et stocke
 # le fichier en résultant dans un répertoire de votre choix.

 SAUVE_REP="$HOME /etc /var"
 NOM_SAUVEGARDE=`date '+%b%d%Y'`
 SAUVEGARDE_DEST_REP="/backups"

 # Décommentez la ligne suivante pour obtenir une sauvegarde GZippée,
 # commentez pour une sauvegarde BZippée

 #tar cvzf $SAUVEGARDE_DEST_REP/$NOM_SAUVEGARDE.tar.gz $SAUVE_REP

 # Nous créons une archive BZippée...
 # Commentez la ligne suivante pour une archive GZippée,
 # dé-commentez pour une archive BZippée

 tar cvjf $SAUVEGARDE_DEST_REP/$NOM_SAUVEGARDE.tar.bz2 $SAUVE_REP
```

Utilisez la variable `BACKUP_DIRS` pour déterminer les répertoires que vous voulez inclure dans votre sauvegarde et `BACKUP_DEST_DIR` pour le répertoire de destination du fichier de sauvegarde. Rendez le script exécutable en tapant `chmod 700 backup.sh` dans une console.

Naturellement, vous pouvez par la suite déplacer le fichier `.tar.bz2` ou `.tar.gz` sur n'importe quel support. Vous pouvez même sauvegarder directement sur le support de votre choix en le montant et en changeant la variable `SAUVEGARDE_DEST_REP` du script en fonction. N'hésitez pas à améliorer ce script et à le rendre aussi souple que vous le voulez.

Pour restaurer les sauvegardes réalisées de cette manière, voyez *Exemple de restauration avec TAR*, page 146.

13.4. Restauration

La restauration des sauvegardes dépend du programme, du support et de la planification que vous avez utilisés pour les réaliser. Nous n'allons pas couvrir ici toutes les situations. Assurez-vous de restaurer les fichiers ou répertoires aux mêmes endroits où ils étaient lorsque vous avez effectué la sauvegarde.

13.4.1. Exemple de restauration avec TAR

Nous allons maintenant voir un petit script qui restaure la sauvegarde que nous avons réalisée avec `tar` dans le script susmentionné dans *Exemple de sauvegarde avec tar*, page 146.

Vous devez avoir la permission d'écriture sur les fichiers et répertoires que vous allez restaurer, sinon l'opération de restauration échouera.

```
#!/bin/bash

 # Extrait une sauvegarde compressée de tous les répertoires spécifiés
 # et restaure les fichiers sauvegardés à leur endroit d'origine

 SAUVEGARDE_REP_SOURCE="/backups"
 NOM_SAUVEGARDE=$1

 # Décommentez la ligne suivante si vous restaurez une sauvegarde GZippée
 #tar xvzf $SAUVEGARDE_REP_SOURCE/$NOM_SAUVEGARDE

 # Restauration d'une sauvegarde BZippée
 tar xvyf $SAUVEGARDE_REP_SOURCE/$NOM_SAUVEGARDE
```

Comme vous pouvez le voir, ce script est très simple. Vous n'avez qu'à lui passer le nom du fichier que vous voulez restaurer en paramètre (juste le nom du fichier, pas le chemin complet), et il restaurera les fichiers sauvegardés à leur position initiale. N'oubliez pas de rendre le script exécutable en tapant `chmod 700 backup.sh` dans une console.

13.4.2. Création d'un CD-ROM de sauvetage

Il y a une manière d'être préparé dans le cas d'un « désastre total » : il s'agit de réaliser une sauvegarde **complète** de votre système. Des logiciels comme mkCDrec peuvent être très utiles pour mettre cela en place en quelques minutes. Vous pouvez l'obtenir avec sa documentation sur le site Web de mkCDrec (`http://mkcdrec.ota.be`).

mkCDrec vous permet de créer une sauvegarde sur plusieurs CD-ROM, de cloner un disque (copier le contenu d'un disque ou d'une partition vers un autre, pourvu qu'il soit suffisamment grand), et beaucoup d'autres choses.

Pour restaurer un système avec mkCDrec, il suffit de démarrer avec le premier CD-ROM (si la sauvegarde contient plusieurs CD-ROM) et de suivre les instructions à l'écran.

13.5. Problèmes au démarrage du système

Il peut arriver que votre système se bloque durant le démarrage. Si tel est le cas, ne paniquez pas, continuez à lire !

Les sections suivantes ne suivent pas d'ordre particulier.

13.5.1. Système qui se bloque dès le démarrage

Si votre système se bloque durant la `Reconstruction de la base de données RPM` ou la `Recherche des dépendances entre modules`, pressez simplement **Ctrl-C**. De cette façon, le système va passer cette étape et continuer à démarrer. Une fois démarré, exécutez `rpm --rebuilddb` en tant que `root` si le problème survient dans le premier cas. Si c'est le second cas qui se présente, vous avez probablement effectué une mise à jour du noyau, mais incorrectement. Vérifiez que les fichiers dans `/boot` et le répertoire `/lib/modules` correspondent à la version actuelle du noyau (c'est-à-dire, que les numéros de version suffixés soient corrects).

Si le processus de démarrage bloque à l'étape `RAMDISK: Compressed image found at block 0`, vous avez endommagé l'image `initrd`. Essayez de démarrer à l'aide d'une autre entrée du menu de démarrage

(`lilo.conf`) ou avec une disquette de secours, puis effacez ou corrigez la section `initrd=` dans `/etc/lilo.conf`.

13.5.2. Échec du contrôle des systèmes de fichiers

Les informations qui suivent ne s'appliquent qu'aux systèmes de fichiers ext2 et ext3. Si vous utilisez un autre système de fichiers, consultez sa documentation pour plus de renseignements.

Si, pour une raison quelconque, vous n'avez pas éteint votre machine correctement, le système exécutera un contrôle de routine des systèmes de fichiers au prochain démarrage. Parfois, cette commande échoue et le système demandera le mot de passe root pour vous transférer dans une console. Exécutez alors `e2fsck -py [périphérique]` où `[périphérique]` est le nom de la partition sur laquelle le test automatique a échoué. L'option `-p` demande à `e2fsck` d'effectuer toutes les réparations nécessaires sans rien demander tandis que l'option `-y` suppose que vous répondez `oui` à toutes les questions. Lorsque la phase de vérification et de réparation est terminée, pressez **Ctrl-D** pour quitter la console d'urgence. Le système redémarrera.

Si vous obtenez cette erreur régulièrement, il se peut qu'il y ait des secteurs défectueux sur votre disque. Exécutez `e2fsck -c [périphérique]` pour vérifier. Cette commande marquera automatiquement les secteurs défectueux et empêchera ainsi le système de fichiers de stocker des données dans ces blocs. `e2fsck` ne vérifiera le système de fichiers automatiquement que s'il n'a pas été proprement démonté lors du dernier arrêt, ou bien si le `nombre maximal de montages` a été atteint. Pour forcer une vérification, utilisez l'option `-f`.

La recherche des blocs défectueux sur un disque peut durer un temps considérable.

13.5.3. X ne démarre pas

Si vous démarrez **normalement** en mode graphique et avez réussi à casser la configuration de X au point où celui-ci ne démarre plus, vous pouvez vous connecter dans une console et utiliser XFdrake pour reconfigurer X. Vous pouvez aussi démarrer le système sur un autre niveau d'exécution (*runlevel*), réparer la configuration de X avec XFdrake puis redémarrer avec X.

13.5.3.1. Démarrage sur un autre niveau d'exécution

Le niveau par défaut est défini dans le fichier `/etc/inittab`. Cherchez une ligne telle que `id:5:initdefault:`. Si vous voulez démarrer dans le niveau d'exécution `3` (la console), vous devez le spécifier lors du démarrage. Sous LILO, pressez la touche **Échap**, puis tapez `linux init 3`. Si vous utilisez GRUB, pressez la touche **E** deux fois et ajoutez `init 3`, pressez alors la touche **Entrée** puis sur la touche **B** pour démarrer.

Pour une description plus détaillée des niveaux d'exécution, consultez le *Manuel de référence* de Mandriva Linux.

13.5.3.2. Configuration de X depuis la console

Pour reconfigurer X en utilisant XFdrake depuis une console, il suffit de taper `XFdrake`, en tant que `root`.

L'utilisation de XFdrake n'est pas différente d'une utilisation dans un environnement graphique, sauf que vous ne verrez peut-être pas de curseur ni de jolies icônes. Pour vous déplacer vers le bas, appuyez sur la flèche de droite ou du bas. Pour vous déplacer vers le haut, appuyez sur les flèches de gauche ou du haut. Vous pouvez aussi utiliser la touche **Tab** pour vous déplacer parmi les options/boutons. Le texte de l'option ou du bouton actuellement sélectionné sera en surbrillance et d'une couleur différente. Appuyez sur **Entrée** pour l'activer.

13.6. Problèmes de chargeur de démarrage

13.6.1. Réinstallation du chargeur de démarrage

Il est possible que, par erreur, vous écrasiez le MBR (*Master Boot Record*) de votre disque, que quelque programme défectueux engendre cette erreur ou encore, que vous démarriez sous Windows® et que vous attrapiez un virus qui l'écrase. Donc, vous pensez que vous ne pourrez plus démarrer votre système, n'est-ce pas ? Il y a en fait plusieurs façons de récupérer le chargeur de démarrage.

Pour récupérer votre chargeur de démarrage, vous **avez besoin** d'un disque de démarrage. Sans un disque de démarrage quelconque, vous pourriez bien être complètement perdu, à moins que vous n'ayez sauvegardé votre MBR : voir *Sauvegarde et récupération du MBR*, page 149.

Insérez simplement la disquette dans le lecteur et redémarrez votre ordinateur. Ce que vous devrez faire ensuite varie selon que vous utilisiez LILO ou GRUB. Quel que soit le chargeur de démarrage, toutes les commandes que vous devrez utiliser devront l'être en tant que `root`.

13.6.1.1. Avec LILO

Si vous utilisez LILO, il vous suffit d'exécuter ceci à l'invite : `/sbin/lilo`. Cela réinstallera LILO dans le secteur d'amorce de votre disque et corrigera le problème.

13.6.1.2. Avec GRUB

Si vous utilisez GRUB, les choses sont un peu différentes qu'avec LILO.

L'exemple suivant suppose que vous essayez d'installer GRUB dans le MBR de votre premier disque IDE et que le fichier `stage1` est dans le répertoire `/boot/grub/`.

D'abord, lancez le *shell* de GRUB en lançant la commande `grub`. Une fois que c'est fait, exécutez les commandes suivantes : `root (hd0,0)`. Ceci indiquera à GRUB que les fichiers nécessaires sont dans la première partition (`0`) de votre premier disque dur (`hd0`). Puis, exécutez `setup (hd0)`, ce qui installera GRUB dans le MBR de votre premier disque dur. C'est tout !

Vous pouvez aussi essayer d'utiliser `grub-install /dev/hda` pour installer GRUB sur le MBR de votre premier disque dur, mais la méthode décrite plus haut est préférable.

13.6.1.3. Quelques considérations concernant les systèmes à double amorçage (dual booting)

Mise à jour de Windows 9x, NT, 2000 et XP. Si vous utilisez un système à double démarrage (*dual-boot*), soyez prévoyant et ayez toujours un disque de démarrage GNU/Linux sous la main. Lors de la (ré)installation de Windows® (toutes les versions), il écrase le chargeur de démarrage **sans avertissement**, et si vous ne possédez pas de disque de démarrage, vous serez incapable de lancer GNU/Linux après avoir fait une mise à jour de Windows®.

13.6.2. Sauvegarde et récupération du MBR

Pour faire une copie du *Master Boot Record* (MBR), insérez une disquette vierge dans votre lecteur et tapez la commande suivante :

```
# dd if=/dev/hda of=/dev/fd0/mbr.bin bs=512 count=1
```

Si vous voulez restaurer une copie du MBR de votre disque dur, insérez une disquette le contenant dans votre lecteur et tapez la commande qui suit :

```
# dd if=/dev/fd0/mbr.bin of=/dev/hda bs=512
```

Les exemples susmentionnés supposent que le MBR de votre premier disque IDE (`/dev/hda`) soit sauvegardé dans un fichier nommé `mbr.bin`, lequel est sur une disquette dans le premier lecteur de votre ordinateur (`/dev/fd0`). Ces commandes doivent être lancées par l'utilisateur `root`.

13.7. Problèmes sur les systèmes de fichiers

13.7.1. Réparation d'un super-bloc endommagé

Les informations qui suivent ne s'appliquent qu'aux systèmes de fichiers ext2 et ext3. Si vous utilisez un autre système de fichiers, consultez sa documentation pour plus de renseignements.

Le super-bloc est le premier bloc de chaque partition ext2FS/ext3. Il contient des données importantes à propos du système de fichiers, comme sa taille, l'espace libre, etc. (c'est assez similaire sur les partitions FAT). Une partition comprenant un super-bloc endommagé ne peut être montée. Heureusement, ext2FS/ext3 conserve plusieurs sauvegardes du super-bloc disséminées sur la partition.

Démarrez votre système avec la disquette de démarrage créée plus tôt. La localisation des copies de sauvegarde dépend de la taille du bloc du système de fichiers. Pour les systèmes de fichiers dont la taille des blocs est de 1 Ko, vous la trouverez au début de chaque bloc de 8 Ko (8 192 octets). Pour les systèmes de fichiers avec des blocs de taille 2 Ko, c'est au début de chaque bloc de 16 Ko (16 384 octets), et ainsi de suite. Vous pouvez utiliser la commande `mke2fs -n [nom_de_votre_périphérique]` pour trouver à quel octet se trouvent les sauvegardes de super-bloc. En supposant que la taille du bloc soit de 1 Ko, la prochaine copie de sauvegarde commencera à l'octet 8 193. Pour restaurer le super-bloc à partir de cette copie, exécutez `e2fsck -b 8193 /dev/hda4` ; changez `hda4` pour désigner votre partition endommagée. Si ce bloc est également endommagé, essayez le suivant à l'octet numéro 16 385, et ainsi de suite jusqu'à ce que vous trouviez un super-bloc en bon état. Redémarrez votre système pour activer les changements.

13.7.2. Récupération de fichiers supprimés

Dans cette section, nous présentons diverses méthodes pour récupérer des fichiers et des répertoires effacés. Gardez à l'esprit que les outils de récupération ne sont pas magiques. Ils fonctionneront plus ou moins bien selon la durée écoulée depuis que vous avez effacé les fichiers que vous tentez de récupérer.

Vous vous demandez comment récupérer un fichier effacé accidentellement. Il existe quelques utilitaires prévus pour le système de fichiers ext2 de GNU/Linux qui vous permettent de récupérer des fichiers et des répertoires effacés. Cependant, ces outils ne pourront pas récupérer les fichiers que vous avez effacés il y a quelques mois : à cause de l'activité du système, l'espace marqué « libre » sera réécrit. Par conséquent, la **meilleure** méthode pour se prémunir des suppressions accidentelles est d'effectuer des sauvegardes.

Il n'existe pas pour l'instant d'outil pour récupérer les fichiers effacés sur un système de fichiers `reiserfs`. Gardez un oeil sur la page de ReiserFS (`http://www.namesys.com/`) pour rester au courant des dernières nouveautés.

Un des outils de récupération des fichiers effacés est Recover. Il est « interactif ». Si vous possédez une Mandriva Linux - Édition PowerPack, vous disposez déjà de cet outil dans le CD-ROM « contrib ». Sinon, vous pouvez le trouver sur le site RPMFind (`http://fr.rpmfind.net`). . Lorsque vous avez le RPM, installez-le. Puis, exécutez-le avec `recover` et répondez aux questions qui vous seront posées. Celles-ci permettent de définir l'intervalle de temps à l'intérieur duquel il faut chercher les répertoires et les fichiers effacés afin de limiter la durée de la recherche[1].

1. Vous pouvez chercher **tous** les fichiers effacés en ajoutant l'option `-a`, mais cela durera plus longtemps...

Lorsque l'outil a terminé sa recherche, il vous demandera où vous voulez sauvegarder les répertoires et fichiers récupérés. Choisissez un répertoire qui contiendra tous ces fichiers et répertoires récupérés. Notez que vous ne pourrez pas retrouver les noms des fichiers, seulement leur contenu, mais vous pouvez inspecter leur contenu ou tenter de les renommer avec différents noms jusqu'à ce que vous trouviez celui que vous cherchez. C'est mieux que rien !

Des mini-*HOWTO* consacrés à ce sujet existent également, dont Ext2fs-Undeletion (`http://www.freenix.fr/unix/linux/HOWTO/mini/Ext2fs-Undeletion.html`) et récupération d'une structure complète de répertoires (`http://www.tldp.org/HOWTO/mini/Ext2fs-Undeletion-Dir-Struct/index.html`) (en anglais).

13.8. Lorsque le système gèle

Lorsqu'il « gèle », votre ordinateur ne répond plus aux commandes et les périphériques d'entrée comme le clavier et la souris semblent bloqués. C'est le pire scénario et cela peut signifier qu'une erreur critique est survenue dans votre configuration logiciel ou matériel. Nous vous montrerons quoi faire face à cette situation pénible.

Dans le cas d'un gel du système, votre première priorité devrait être d'éteindre votre système correctement. En supposant que vous êtes sous X, essayez successivement ces étapes :

1. Essayez de tuer le serveur X en pressant **Alt-Ctrl-Backspace** simultanément.
2. Essayez de passer à une autre console avec **Alt-Ctrl-Fn** (où `n` équivaut au numéro de la console, soit de 1 à 6). Si vous y parvenez, connectez-vous en tant que `root` et exécutez la commande `kill -15 $(pidof X)`, ou la commande `kill -9 $(pidof X)` si la première n'a aucun effet (vérifiez avec la commande `top` pour vérifier si X fonctionne toujours).
3. Si vous êtes dans un réseau local, essayez de vous connecter par `ssh` sur votre machine à partir d'une autre. Il est recommandé de vous connecter en tant qu'utilisateur non privilégié, puis d'utiliser la commande `su` pour devenir `root`.
4. Si le système ne répond à aucune de ces tentatives, vous devez utiliser la séquence « SysRq » (*System Request*). Cette séquence implique de presser trois touches à la fois, la touche **Alt** de gauche, la touche **SysRq** (nommée **PrintScreen** ou **Impr écran** sur les vieux claviers) et une lettre.
   a. **Alt gauche-SysRq-R** place le clavier en mode « cru » (*raw mode*). Maintenant essayez de presser **Alt-Ctrl-Backspace** encore une fois pour tuer X. Si ça ne fonctionne pas, continuez.
   b. **Alt gauche-SysRq-S** tente d'écrire toutes les données non sauvegardées sur le disque (« synchronisation » du disque).
   c. **Alt gauche-SysRq-E** envoie un signal de terminaison à tous les processus, sauf à `init`.
   d. **Alt gauche-SysRq-I** envoie un signal de fin à tous les processus (terminaison beaucoup plus « ferme »), sauf à `init`.
   e. **Alt gauche-SysRq-U** tente de remonter tous les systèmes de fichiers montés en lecture seule. Ceci retire le marquage « dirty flag » et évitera ainsi une vérification du système de fichiers au redémarrage.
   f. **Alt gauche-SysRq-B** redémarre le système. Vous pouvez aussi presser le bouton « reset » sur votre machine.

Rappelez-vous qu'il s'agit d'une séquence, c'est-à-dire que vous devez presser une combinaison après l'autre dans le bon ordre : **R**aw, **S**ync, t**E**rm, k**I**ll, **U**mount, re**B**oot[2]. Lisez la documentation au sujet du noyau pour plus de renseignements.

5. Si rien de ce qui précède ne fonctionne, croisez les doigts et pressez le bouton « reset » de votre machine. Avec un peu de chance, GNU/Linux se contentera d'une vérification du disque au redémarrage.

Par tous les moyens, essayez de trouver ce qui a provoqué ce blocage car cela peut endommager sévèrement le système de fichiers. Vous pouvez aussi envisager d'utiliser un des systèmes de fichiers journalisés proposés par Mandriva Linux : ext3, `reiserfs`, etc., qui prennent en charge beaucoup mieux ce genre de problèmes. Cependant, remplacer ext2FS par `reiserfs` nécessite de reformater vos partitions. Vous pouvez utiliser `tune2fs -j /dev/hdaN` pour convertir le système de fichiers de la partition N du premier disque IDE de ext2FS à ext3FS

13.9. Arrêt des applications qui fonctionnent mal

Bien, ce n'est pas si difficile, et vous avez plusieurs possibilités pour y parvenir. Vous pouvez le faire en cherchant le PID du programme en cause, puis utiliser la commande `kill` pour le terminer, ou vous pouvez utiliser l'outil `xkill` ou tout autre outil graphique, tels que ceux qui montrent l'arborescence des processus.

13.9.1. Depuis la console

La première chose à faire pour terminer un programme récalcitrant est de trouver son PID, ou *Process ID* (son numéro identifiant système). Pour ce faire, tapez la commande qui suit dans une console : `ps aux | grep mozilla-firefox-bin`, en supposant que Firefox soit le programme incriminé. Vous allez obtenir quelque chose comme ce qui suit. Cela nous indique, entre autres, que Firefox a été démarré par l'utilisateur pierre et que son PID est `3505`.

```
pierre      3505  7.7 23.1 24816 15076 pts/2   Z    21:29   0:02 /usr/lib/mozilla
```

Maintenant que nous avons le PID du programme défectueux, nous pouvons poursuivre et exécuter la commande `kill` pour le terminer. Donc, nous exécutons ceci : `kill -9 3505`, et voilà ! Firefox est tué. Notez que cette méthode doit être utilisée **seulement** lorsque le programme ne répond plus à vos sollicitations. **Ne l'utilisez pas** comme méthode habituelle pour quitter une application.

En fait, nous avons envoyé le signal `KILL` au processus numéro `3505`. La commande `kill` accepte d'autres signaux que `KILL`, pour avoir un contrôle plus fin sur vos processus. Pour plus d'informations, voyez kill(1).

13.9.2. Utilisation d'autres outils de contrôle graphique

Vous pouvez également utiliser l'un des outils de surveillance de processus (tels que KPM, KSySGuard, ou GTOP, pour ne citer que ceux-là) qui vous permettent de trouver le nom du processus et, en un ou deux clics, leur envoyer un signal ou simplement les arrêter.

Si vous utilisez KDE, vous pouvez presser les touches **Ctrl**-**Alt**-**Esc** : le pointeur de la souris se change en tête de mort, et il suffit alors de cliquer sur la fenêtre de l'application malade pour la tuer.

13.10. Considérations diverses

Voici quelques considérations concernant du matériel nouveau tel que les systèmes « sans héritage » (*legacy-free*), les cartes d'accélération graphique nVidia® et ATI 3D®, les « winmodems » et d'autres choses qui n'entrent pas dans les sections précédentes.

13.10.1. Systèmes legacy-free

Les fabricants ont récemment introduit ce qu'ils appellent des systèmes « legacy free » (sans héritage), surtout sur les ordinateurs portables[3], mais aussi sur les ordinateurs de bureau. Ceci signifie que le BIOS a été significativement réduit pour vous permettre uniquement de choisir sur quel média vous voulez démarrer. Mandriva Linux sera apte à tout configurer correctement.

13.10.2. Cartes graphiques nVidia et ATI 3D

Les ordinateurs possédant des cartes graphiques nVidia ou ATI nécessitent un correctif noyau pour utiliser l'accélération matériel OpenGL 3D sur les applications compatibles avec OpenGL. Si vous possédez une Mandriva Linux - Édition PowerPack, le noyau devrait être installé par DrakX. Cependant, si ce n'est pas le cas, veuillez installer les paquetages relatifs, soit depuis les sites de nVidia (`http://www.nvidia.com`) ou ATI (`http://www.ati.com`), soit depuis le Mandriva Club (`http://club.mandriva.com`). Lancez le Centre de contrôle Mandriva Linux et reconfigurez X.

13.10.3. Winmodems

Les winmodems, sont nommés aussi modems sans contrôleur ou modems logiciel. La prise en charge de ces périphériques en est encore à ses balbutiements. Des pilotes existent, mais en mode binaire et ceci seulement pour certains d'entre eux.

Si vous possédez un modem PCI, regardez la sortie de `cat /proc/pci` en tant que `root`. Cela vous indiquera le port I/O ainsi que l'IRQ de ce périphérique. Puis, utilisez la commande `setserial` (dans notre exemple, l'adresse I/O est `0xb400`, l'IRQ est `10` et notre modem sera le quatrième périphérique série) comme suit :

```
setserial /dev/ttyS3 port 0xb400 irq 10 UART 16550A
```

Essayez alors d'interroger votre modem avec `minicom` ou `kppp`. Si cela ne fonctionne pas, il se peut que vous ayez un modem logiciel. Si cela fonctionne, créez le fichier `/etc/rc.d/rc.setserial` et placez-y la commande `setserial` appropriée.

Si vous possédez un modem interne, et que vous êtes membre du Mandriva Club, vous pouvez télécharger un paquetage pour le faire fonctionner sous Mandriva Linux (notamment `ltmodem`). Vous pouvez aussi consulter les sites du constructeur de votre modem, ainsi que linmodems (`http://linmodems.org`) et Winmodems are not modems (`http://start.at/modem`) (en anglais).

13.10.4. Mon ordinateur est ■ lent ■

Si vous remarquez que votre ordinateur est très lent, ou notablement plus lent qu'avec une autre version de GNU/Linux, vous pouvez essayer de contourner ce « problème » en désactivant l'ACPI. Pour ce faire, ajoutez la ligne suivante à votre fichier `/etc/lilo.conf` :

```
append="acpi=off"
```

S'il y a déjà une ligne `append=`, contentez-vous d'y ajouter `acpi=off` à la fin. Lancez alors `lilo -v` en tant que `root` et redémarrez la machine ce qui rendra actif le changement.

13.11. Outils Mandriva Linux pour faire face aux problèmes

Chaque outil d'administration (ceux que vous pouvez lancer depuis Centre de contrôle Mandriva Linux) peut vous aider à résoudre vos problèmes. Vous pouvez utiliser chacun d'eux pour annuler des changements de configuration, ajouter ou retirer des logiciels, mettre à jour votre système en utilisant les derniers correctifs de Mandriva, et ainsi de suite.

Si vous pensez avoir trouvé un bogue dans un des outils Mandriva Linux, vous pouvez le signaler en utilisant Drakbug, l'outil de signalement de bogues automatisé.

3. Reportez-vous à cet excellent site Web, Linux on Laptops (`http://www.linux-laptop.net`), pour plus de renseignements sur votre modèle d'ordinateur portable.

13.12. Comment résoudre un problème sous Mandriva Linux

Nous passerons maintenant en revue les différents moyens à votre disposition pour résoudre un problème particulier. Essayez d'abord la première proposition, si ça ne marche pas, la deuxième, et ainsi de suite.

13.12.1. Recherche sur Internet

Les nombreux sites Web susmentionnés sont d'excellents points de départ. Ils peuvent aborder de près comme de loin plusieurs aspects de votre problème. Finalement, essayez un moteur de recherche généraliste comme Google™ ou la version spéciale Linux de Google™. Et n'hésitez pas à utiliser l'option Recherche avancée (`http://www.google.fr/advanced_search`) avec des questions très détaillées, comme le message d'erreur que vous avez obtenu.

13.12.2. Archives de listes de diffusion et de forums

Les recherches sur Internet donnent des réponses générales qui cachent une réponse intéressante parmi de nombreuses autres. Pour affiner votre recherche, lisez ce qui suit.

Pour commencer, essayez de trouver une liste qui semble être directement liée à votre problème, puis cherchez dans ses archives.

Exemple

Vous avez remarqué un comportement étrange en utilisant GRUB avec une partition minix.

Une recherche en utilisant les mots clés « *grub mailing list* » sur Google™ donne dans ses premiers résultats le lien vers un message d'archive de la liste : *GRUB mailing list archive* (`http://mail.gnu.org/archive/html/bug-grub/`). Cette archive propose un moteur de recherche. En l'utilisant pour chercher « Minix », vous trouverez directement un correctif au problème.

Notez toutefois que peu d'archives proposent un moteur de recherche intégré. Il suffit alors d'utiliser le champ `domaine` du mode avancé de Google™ pour limiter vos recherches au site hébergeant les archives. Cette stratégie peut aussi être utilisée pour les sites qui renvoient régulièrement des réponses non pertinentes.

Pour une recherche sur les forums, Google Groups™ (`http://groups.google.com/`) contient les archives d'un nombre impressionnant de forums de discussion.

13.12.3. Contacter directement la personne responsable du projet

Utilisez cette option en tout dernier recours et en situation désespérée — à moins que vous ne vouliez offrir votre aide. Les programmeurs reçoivent généralement beaucoup de courrier électronique. Ainsi, votre question polémique sur l'utilisation de la commande `cd` sera probablement... ignorée !

Les adresses se trouvent soit sur la page du projet ou dans la documentation du logiciel.

Un dernier mot : ne sous-estimez pas les capacités de votre voisin ou de votre LUG (*Linux Users Group* ou Groupe d'Utilisateurs de Linux) local. Et, s'il vous plaît, ne jetez pas votre ordinateur par la fenêtre : si votre problème n'est pas résolu aujourd'hui, il le sera sûrement demain...

13.12.4. Services professionnels de Mandriva

Enfin, face à un défi complexe, les utilisateurs professionnels pourront faire appel à un consultant de Mandriva pour s'occuper de leurs besoins particuliers.

Voilà une des caractéristiques les plus significatives des produits libres : nous avons accès aux sources, nous possédons la connaissance ! Ainsi, tout problème, quelle que soit sa complexité, sa particularité et son niveau élevé, peut sans doute être résolu directement au cœur du logiciel.

Vous voudrez sûrement personnaliser votre environnement Linux pour atteindre des buts précis. Par exemple, vous pourriez vouloir utiliser Mandriva Linux comme application de routage spécialisée sur un périphérique particulier. Sachez alors que les services professionnels de Mandriva (`http://www.mandriva.com/enterprise/products`) peuvent vous y aider.

13.13. Derniers mots

Voilà, vous avez constaté qu'il existe de nombreuses façons de se sortir d'une situation critique, sans pour autant réinstaller tout le système[4] ! Bien sûr, vous devez avoir une certaine expertise pour utiliser certaines des techniques décrites dans ce chapitre, mais avec un peu de pratique, vous l'obtiendrez rapidement. Ceci étant dit, nous espérons que vous n'aurez jamais besoin de maîtriser ces techniques... bien qu'il soit toujours bon de les connaître. Nous espérons que les instructions et exemples donnés ici seront utiles en cas de besoin. Bonne chance dans vos résolutions de problèmes !

4. La façon habituelle de corriger les problèmes avec certains autres systèmes.

Annexe A. Glossaire

adresse IP
Adresse numérique composée de quatre séquences de un à trois chiffres qui identifient un ordinateur sur un réseau et notamment sur Internet. Les adresses IP sont structurées de manière hiérarchique, avec des domaines supérieurs et nationaux, domaines, sous-domaines, et adresses de chaque machine individuelle. Une adresse IP ressemble à `192.168.0.1`. L'adresse d'une machine personnelle peut être de deux types : statique ou dynamique. Les adresses IP statiques sont des adresses qui ne changent pas, alors que les adresses dynamiques sont réactualisées à chaque nouvelle connexion au réseau. Les utilisateurs de modem ou de câble ont généralement des adresses IP dynamiques, alors que certaines connexions DSL et d'autres à large bande fournissent des adresses IP statiques.

adresse matérielle
C'est un nombre encodé dans le matériel d'interface réseau. Il est unique à chaque interface réseau.

alias
Mécanisme utilisé dans un *shell* pour lui faire substituer une chaîne par une autre avant d'exécuter une commande. Vous pouvez voir tous les alias définis dans la session courante en tapant la commande `alias` à l'invite.

anneau tueur (kill ring)
Sous Emacs, c'est l'ensemble des zones de texte copiées ou coupées depuis le démarrage de l'éditeur, que l'on peut rappeler pour les insérer de nouveau, et qui est organisé sous forme d'anneau. On peut aussi l'appeler « cercle des morts ».

APM
Advanced Power Management (Gestion Avancée de l'Énergie) : fonctionnalité utilisée par quelques BIOS pour faire entrer la machine dans un état de latence après une période d'inactivité donnée. Sur les ordinateurs portables, l'APM est aussi chargé de reporter le statut de la batterie et, si l'ordinateur le permet, la « durée de vie » restante estimée.

arp
Address Resolution Protocol : Protocole de Résolution d'Adresses. Le protocole Internet utilisé pour faire automatiquement correspondre une adresse Internet et une adresse physique (matérielle) sur un réseau local. Cela est limité aux réseaux supportant la diffusion (*broadcasting*) matérielle.

arrière-plan
Dans le contexte du *shell*, un processus tourne en arrière-plan si vous pouvez envoyer des commandes pendant que ledit processus continue de fonctionner.
Voir aussi : job, premier plan.

ASCII
American Standard Code for Information Interchange : Code standard américain pour l'échange d'information. Le code standard utilisé pour stocker des caractères, y compris les caractères de contrôle, sur un ordinateur. Beaucoup de codes 8-bit (tels que ISO 8859-1, l'ensemble des caractères par défaut de GNU/Linux) contiennent ASCII sur leur moitié inférieure.
Voir aussi : ISO 8859.

ATAPI (AT Attachment Packet Interface)
Une extension des spécifications ATA (« Advanced Technology Attachment », plus connue sous le nom d'IDE, *Integrated Drive Electronics*) qui propose des commandes supplémentaires pour contrôler les lecteurs de CD-ROM et de bandes magnétiques. Les contrôleurs IDE proposant cette extension sont aussi appelés contrôleurs EIDE (*Enhanced IDE*).

ATM
C'est l'acronyme d'**Asynchronous Transfer Mode**, mode de transfert non synchrone. Un réseau ATM concentre des données en paquets de taille standard (53 octets : 48 pour les données et 5 pour l'en-tête) pour les transférer efficacement d'un point à un autre. ATM est une technologie de circuit commuté pour paquets réseau destinée aux réseaux optiques à haut débit (plusieurs mégabits).

atomique
Une série d'opérations est dite atomique si elle est exécutée en une seule fois, sans interruption.

batch
Mode de gestion pour lequel les travaux (*jobs*) sont soumis de façon séquentielle au processeur jusqu'au dernier, le processeur est alors libéré pour une autre liste de processus.

bêta test
Nom donné à la procédure visant à tester la version bêta (préliminaire) d'un programme. Ce dernier passe généralement par des phases dites « alpha » puis « bêta » de test avant de sortir officiellement (*release*).

bibliothèque
Ensemble de procédures et de fonctions au format binaire utilisé par les programmeurs dans leurs programmes (si la licence le leur permet). Le programme responsable du chargement des bibliothèques partagées au démarrage est appelé l'éditeur dynamique de liens (*dynamic linker*).

binaire
Format des fichiers exécutable par la machine. C'est généralement le résultat d'une compilation de fichiers sources

bip
Petit bruit aigu émis par l'ordinateur pour attirer votre attention sur une situation ambiguë ou une erreur. Il est utilisé en particulier lorsque le complètement automatique d'une commande propose plusieurs choix.

bit
Binary digIT (*Chiffre Binaire*). Un simple chiffre pouvant prendre les valeurs 0 ou 1, car le calcule s'effectue en base deux.

bitmap
Image en mode point, par opposition à une image en mode vectoriel.

block (fichier en mode)
Fichier dont le contenu est mis en tampon (*buffer*). Toutes les opérations d'entrée/sortie sur de tels fichiers passent par le tampon, ce qui permet des écritures asynchrones sur le matériel sous-jacent, et des lectures directes sur le tampon, donc plus rapides.
Voir aussi : tampon (*buffer*), cache mémoire, caractère (fichiers en mode).

bogue (bug)
Comportement illogique ou incohérent d'un programme dans un cas particulier, ou comportement qui n'est pas en accord avec sa documentation. Souvent, dans un programme, de nouvelles fonctionnalités introduisent de nouveaux bogues. Le mot « bogue » est une francisation du mot anglais *bug*. Historiquement, ce terme remonte au temps des cartes perforées : une punaise (l'insecte !) qui se serait glissée dans le trou d'une carte perforée et aurait engendré un dysfonctionnement du programme ; Ada Lovelace, voyant cela, déclara « C'est un bug » ; l'expression est restée depuis.

boot
Procédure qui s'enclenche au démarrage d'un ordinateur lorsque les périphériques sont reconnus un par un, et que le système d'exploitation est chargé en mémoire.

BSD
Berkeley Software Distribution Distribution Logicielle de Berkeley : variante d'Unix développée au département informatique de l'université de Berkeley. Cette version a toujours été considérée plus avancée technologiquement que les autres, et a apporté beaucoup d'innovations au monde de l'informatique en général et à Unix en particulier.

bureau
Si vous utilisez l'environnement graphique X, le bureau est l'endroit de l'écran avec lequel vous travaillez et sur lequel sont placées les icônes et les fenêtres. Il peut aussi être appelé le fond d'écran, et est généralement rempli par une simple couleur, un gradient de couleur ou même une image.
Voir aussi : bureau virtuel.

bureau virtuel
Dans le système de fenêtres X, le gestionnaire de fenêtres peut vous proposer plusieurs bureaux. Cette fonctionnalité pratique vous permet d'organiser vos fenêtres en limitant le nombre de fenêtres se superposant l'une à l'autre. Cela fonctionne de la même manière que si vous possédiez plusieurs écrans. Vous

pouvez passer d'un bureau virtuel à un autre par le clavier ou la souris, selon le gestionnaire de fenêtres que vous utilisez.
Voir aussi : gestionnaire de fenêtres, bureau.

cache mémoire
Élément crucial du noyau d'un système d'exploitation, il a pour rôle de maintenir les tampons à jour, de les effacer lorsqu'ils sont inutiles, de réduire la taille de l'antémémoire si nécessaire, etc.
Voir aussi : tampon (*buffer*).

caché (fichier)
Fichier qui n'apparaît pas lorsque l'on exécute la commande `ls` sans option. Les noms de fichiers cachés commencent par un `.` et sont notamment utilisés pour enregistrer les préférences et configurations propres à chaque utilisateur. Par exemple, l'historique des commandes de bash est enregistré dans le fichier caché `.bash_history`.

canaux IRC
« Points de rencontre » à l'intérieur des serveurs IRC où vous pouvez converser avec d'autres utilisateurs. Les canaux sont créés dans les serveurs IRC et les utilisateurs se connectent à ces canaux afin de pouvoir communiquer entre eux. Les messages écrits sur un canal ne sont visibles que par les personnes connectées à ce canal. Deux ou plusieurs utilisateurs peuvent aussi créer des canaux « privés » afin de ne pas être dérangés par les autres utilisateurs. Les noms de canaux commencent par un `#`.

caractère (fichiers en mode)
Fichiers dont le contenu n'est pas mis en tampon (*buffer*). Lorsqu'associé à un périphérique physique, toutes les entrées/sorties sont immédiatement effectuées. Certains périphériques caractères spéciaux sont créés par le système (`/dev/zero`, `/dev/null` et d'autres). Ils correspondent aux flux de données.
Voir aussi : block (fichier en mode).

casse
Dans le contexte de chaînes de caractères, la casse est la différenciation entre lettres minuscules et majuscules (ou capitales).

CHAP
Challenge-Handshake Authentication Protocol (Protocole d'Authentification par Poignée de main-défi) : protocole utilisé par les FAI pour authentifier leurs clients. Dans ce schéma, une valeur est envoyée au client (la machine qui se connecte), le client calcule un hash à partir de cette valeur qu'il envoie au serveur, et le serveur compare le hash avec celui qu'il a calculé.
Voir aussi : PAP.

Chargeur de démarrage (bootloader)
Programme responsable du chargement du système d'exploitation. De nombreux chargeurs de démarrage vous donnent la possibilité de charger plus d'un système en vous proposant un menu. Les chargeurs tels que grub sont disponibles avec cette fonctionnalité et sont très utiles sur les machines multi-systèmes.

chemin
Affectation d'un fichier ou d'un répertoire au système de fichiers. Les différents niveaux d'un chemin sont séparés par le *slash* soit la barre oblique (« / »). Il y a deux types de chemins sous GNU/Linux. Le chemin **relatif** est la position d'un fichier ou un répertoire par rapport au répertoire courant. Le chemin **absolu** est la position d'un fichier ou un répertoire par rapport au répertoire racine.

cible (target)
Objet d'une compilation, généralement le fichier binaire devant être généré par le compilateur.

CIFS
Common Internet FileSystem (Système de Fichiers Internet Commun) : prédécesseur du système de fichiers de SMB, utilisé sur les systèmes DOS.

client
Programme ou ordinateur qui se connecte de façon épisodique et temporaire à un autre programme ou ordinateur pour lui donner des ordres ou lui demander des renseignements. C'est l'une des composantes d'un système **client/serveur**.

code objet
Code généré par le processus de compilation devant être lié avec les autres codes objets et bibliothèques pour former un fichier exécutable. Le code objet est lisible par la machine.
Voir aussi : binaire, compilation, liaison.

compilation
Une des étapes de la traduction du code source (en langage compréhensible avec un peu d'entraînement) écrit en un langage de programmation (C, par exemple) en un fichier binaire lisible par la machine.

complètement
Néologisme (substantif masculin) désignant la capacité du *shell* à étendre une sous-chaîne en un nom de fichier, nom d'utilisateur ou autre, de façon automatique, si la sous-chaîne n'est pas ambiguë.

compression
Moyen de diminuer la taille des fichiers ou le nombre de caractères transmis lors d'une connexion. Certains programmes de compression de fichiers sont compress, `zip`, `gzip`, et `bzip2`.

compte
Sur un système Unix, un nom de connexion, un répertoire personnel, un mot de passe et un *shell* qui autorisent une personne à se connecter sur ce système.

console
Nom donné à ce que l'on appelait autrefois « terminal ». Les terminaux constituaient les postes utilisateurs des gros ordinateurs centraux (*mainframe*). Sur les postes de travail, le terminal physique est le clavier plus l'écran.
Voir aussi : consoles virtuelles.

consoles virtuelles
Sur les systèmes GNU/Linux, les consoles virtuelles sont utilisées pour vous permettre de lancer plusieurs sessions sur un seul écran. Vous disposez par défaut de six consoles virtuelles qui peuvent être activées en pressant les combinaisons de touches : **ALT-F1** à **ALT-F6**. Il y a une septième console virtuelle par défaut, **ALT-F7**, qui vous permet de lancer le serveur X (interface graphique) Depuis X, vous pourrez activer les consoles virtuelles en pressant **CTRL-ALT-F1** à **CTRL-ALT-F6**.
Voir aussi : console.

continu (périphérique en)
Périphérique qui traite des « flots » (non interrompus ou divisés en blocs) de caractère en entrée. Un périphérique en continu typique est le lecteur de bandes.

cookies
Fichiers temporaires écrits sur le disque dur local par un site Web distant. Cela permet au serveur d'être prévenu des préférences de l'utilisateur quand celui-ci se connecte à nouveau.

courrier électronique
Aussi appelé « mail », « e-mail », « mèl » ou encore « courriel », il désigne un message que l'on fait parvenir à un autre utilisateur d'un même réseau informatique par voie électronique. Similaire au courrier traditionnel (dit courrier « escargot »), le courrier électronique a besoin des adresses de l'expéditeur et du destinataire pour être envoyé correctement. L'expéditeur doit avoir une adresse du type « moi@chez.moi » et le destinataire une adresse « lui@chez.lui ». Le courrier électronique est un moyen de communication très rapide (généralement quelques minutes quelle que soit la destination). Afin de pouvoir écrire un courrier électronique, vous avez besoin d'un client de courrier du type de pine ou `mutt` qui sont en mode texte, ou des clients en mode graphique comme K Mail.

datagramme
Un datagramme est un petit paquet de données et d'en-têtes qui contient des adresses. C'est l'unité basique de transmission d'un réseau IP. Vous pouvez aussi le rencontrer sous le nom de « paquet »

dépendances
Étapes de la compilation nécessaires pour passer à l'étape suivante dans la compilation finale d'un programme.

DHCP
Dynamic Host Configuration Protocol (Protocole Dynamique de Configuration d'Hôtes). Protocole conçu pour que les machines sur un réseau local puissent se voir allouer une adresse IP dynamiquement.

disquette de démarrage
Disquette de démarrage (*bootable* en anglais) contenant le code nécessaire pour démarrer le système d'exploitation présent sur le disque dur (parfois, elle se suffit à elle-même).

distribution
Terme utilisé pour distinguer les différents produits proposés par les fournisseurs GNU/Linux. Une distribution est constituée du noyau Linux, et d'utilitaires, ainsi que de programmes d'installation, programmes de tiers, et parfois même des programmes propriétaires.

DLCI
(*Data Link Connection Identifier* ou Identifiant de Connexion de Liaison de Données. Il est utilisé pour identifier une connexion point à point unique et virtuelle via un réseau à relais de trames. Le DLCI est normalement assigné par le fournisseur du réseau à relais de trames.

DMA
(*Direct Memory Access* ou Accès Direct à la Mémoire) : fonctionnalité utilisée sur l'architecture PC qui permet à un périphérique de lire ou d'écrire dans la mémoire principale sans l'aide du processeur. Les périphériques PCI utilisent le *bus mastering* (ou maîtrise de bus, soit le contrôle du bus par un périphérique en lieu et place du processeur) et n'ont pas besoin de DMA.

DNS
Domain Name System : système de nom de domaine. Le mécanisme de correspondance nom/adresse utilisé sur Internet. C'est ce mécanisme qui permet de mettre en correspondance un nom de domaine et une adresse IP, qui vous laisse rentrer un nom de domaine sans connaître l'adresse IP du site. DNS permet aussi d'effectuer une recherche inversée, de sorte que vous pouvez obtenir l'adresse IP d'une machine à partir de son nom.

doux (lien)
Voir : symboliques, liens

DPMS
Display Power Management System (Système de Gestion de l'Alimentation de l'Affichage). Protocole utilisé par tous les écrans modernes pour gérer les fonctionnalités de gestion d'énergie. Les moniteurs disposant de ces fonctionnalités sont souvent appelés des moniteurs « verts ».

drapeau
Indicateur (généralement un seul bit) utilisé pour signaler une condition particulière à un programme Par exemple, un système de fichier a, entre autre, un drapeau indiquant s'il doit être inclus dans une sauvegarde ; lorsque le drapeau est levé le système de fichier est sauvegardé, il ne l'est pas si le drapeau est désactivé.

échappement
Dans le contexte du *shell*, désigne l'action d'encadrer une chaîne entre guillemets pour empêcher son interprétation. Par exemple, pour utiliser des espaces sur une ligne de commande, puis rediriger le résultat à une autre commande, il faudra mettre la première commande entre guillemets (« échapper » la commande) sinon le *shell* l'interprétera mal, ce qui empêchera le bon fonctionnement.
Action d'encadrer une chaîne entre guillemets pour empêcher son interprétation, dans le contexte du *shell* Par exemple, pour utiliser des espaces sur une ligne de commande, puis rediriger le résultat à une autre commande, il faudra mettre la première commande entre guillemets (« échapper » la commande) sinon le *shell* l'interprétera mal, ce qui empêchera le bon fonctionnement.

écho
Voir un écho signifie voir à l'écran les caractères qui sont frappés au clavier. Par exemple, lorsque l'on tape un mot de passe, on n'a généralement pas d'écho mais de simple étoiles « * » pour chaque caractère tapé.

éditeur
Programme spécialisé dans la modification des fichiers texte. Les éditeurs les plus connus sous GNU/Linux sont GNU Emacs (Emacs) et l'éditeur Unix : Vi.

ELF
Executable and Linking Format (Format d'Exécutable et de Liaison). C'est le format binaire utilisé par la plupart des distributions GNU/Linux de nos jours.

englobement
Capacité de regrouper dans le *shell*, un certain ensemble de noms de fichiers avec un motif d'englobement.
Voir aussi : motif d'englobement.

entrée standard
Descripteur de fichier numéro 0, ouvert par tous les processus, utilisé par convention comme le descripteur de fichier par lequel le processus reçoit ses données.
Voir aussi : erreur standard, canal d', sortie standard.

environnement
Contexte d'exécution d'un processus. Cela inclut toute l'information dont le système d'exploitation a besoin pour gérer le processus, et ce dont le processeur a besoin pour exécuter correctement ce processus.
Voir aussi : processus.

erreur standard, canal d'
Descripteur de fichier numéro 2, ouvert par tous les processus, utilisé par convention pour les messages d'erreur et, par défaut, l'écran du terminal.
Voir aussi : entrée standard, sortie standard.

expression rationnelle
Outil théorique très puissant utilisé pour la recherche et la correspondance de chaînes de texte. Il permet de spécifier des motifs auxquels les chaînes recherchées doivent se conformer. Beaucoup d'utilitaires Unix l'utilisent : `sed`, awk, `grep` et perl, entre autres.

ext2
Abréviation de *Second Extended Filesystem* : système de fichiers étendu 2. ext2 est le système de fichiers natif de GNU/Linux et possède toutes les caractéristiques d'un système de fichiers Unix : support des fichiers spéciaux (périphériques caractères, liens symboliques...), permissions sur les fichiers et propriétaires, etc.

FAI
Fournisseur d'Accès Internet. Société qui revend un accès Internet à ses clients, que l'accès soit par ligne téléphonique ou par ligne dédiée.

FAQ
Frequently Asked Questions (Foire Aux Questions). Document contenant une série de questions/réponses sur un domaine spécifique. Historiquement, les FAQ sont apparues dans les groupes de discussion, mais cette sorte de document est maintenant disponible sur des sites Web divers. Même des produits commerciaux ont leur FAQ. Généralement, ce sont de très bonnes sources d'informations.

FAT
File Allocation Table. (Table d'Allocation des Fichiers). Système de fichiers utilisé par DOS / Windows.

FDDI
Fiber Distributed Digital Interface (Interface Numérique Distribuée par Fibre) : couche réseau matérielle à haut débit, qui utilise des fibres optiques pour la communication. Seulement utilisée sur les gros réseaux surtout à cause de son prix.

FHS
Filesystem Hierarchy Standard (Standard pour la Hiérarchie des Systèmes de fichier) : document contenant des lignes de conduite pour une arborescence des fichiers cohérente sur les systèmes Unix. Mandriva Linux se conforme à ce standard.

FIFO
First In, First Out (Premier Entré, Premier Sorti) : structure de données ou tampon matériel depuis lequel les éléments sont enlevés dans l'ordre de leur insertion. Les tubes Unix sont l'exemple le plus courant de FIFO.

focus
Fait qu'une fenêtre reçoive les événements clavier (tels que les pressions ou les relâches des touches) et les clics de la souris, à moins que ces derniers ne soient interceptés par le gestionnaire de fenêtres.

forum de discussions (newsgroup)
Zones de discussion et de nouvelles auxquelles on peut accéder par l'intermédiaire d'un client de nouvelles ou un client USENET pour écrire et lire des messages spécifiques au sujet du forum de discussion.

Par exemple, le forum `alt.os.linux.mandrake` est un forum de discussion alternatif (alt) qui traite des systèmes d'exploitation *Operating Systems* (os) GNU/Linux, et en particulier, Mandriva Linux (mandrake). Les noms des forums de discussion sont déclinés de cette façon afin de rendre plus aisée la recherche d'un sujet en particulier.

framebuffer
Projection de la RAM d'une carte graphique dans la mémoire principale. Cela autorise les applications à accéder à la mémoire vidéo en évitant les complications liées à la communication directe avec la carte. Toutes les stations graphiques de haut niveau utilisent des framebuffers.

FTP
File Transfer Protocol (Protocole de Transfert de Fichiers). C'est le protocole Internet standard pour transférer des fichiers d'une machine à une autre.

gestionnaire de fenêtres
Programme responsable de l'allure générale d'un environnement graphique et qui s'occupe des barres et cadres des fenêtres, des boutons, des menus issus de l'image de fond, et de certains raccourcis clavier. Sans lui, il serait difficile ou impossible d'avoir des bureaux virtuels, de changer la taille des fenêtres à la volée, de déplacer ces dernières, etc.

GFDL
*GNU Free Documentation License*ou Licence de Documentation GNU Libre. Licence appliquée à toute la documentation Mandriva Linux

GIF
Graphics Interchange Format (soit Format Graphique d'échange). Format de fichier image, très utilisé sur le Web. Les images GIF sont compressées, et elles peuvent même être animées. Pour des questions de droits d'auteur, il est conseillé de remplacer ce format d'image par un format plus récent : le format PNG.

GNU
GNU is Not Unix (GNU N'est pas Unix). Le projet GNU a été initié par Richard Stallman au début des années 80. Son but est de concevoir un système d'exploitation libre et complet. Aujourd'hui, la plupart des outils sont disponibles, sauf... le noyau. Le noyau du projet GNU, Hurd, n'est pas encore prêt à sortir du laboratoire. Linux emprunte, entre autres, deux choses au projet GNU : son compilateur C, `gcc`, et sa licence, la GPL.
Voir aussi : GPL.

gourou
Expert, nom utilisé pour désigner une personne particulièrement qualifiée dans un domaine particulier, mais qui est aussi d'une grande utilité à ceux qui sollicitent son aide.

GPL
General Public License (Licence Publique Générale). Licence de nombreux programmes libres, notamment du noyau Linux. Elle va à l'encontre de toutes les licences propriétaires puisqu'elle ne donne aucune restriction en ce qui concerne la copie, la modification et la redistribution du logiciel, aussi longtemps que le code source est disponible. La seule restriction, si on peut l'appeler ainsi, est que les personnes à qui vous le redistribuez doivent aussi bénéficier des mêmes droits.

hôte
Relatif à un ordinateur qui est généralement utilisé pour des ordinateurs reliés à un réseau.

HTML
HyperText Markup Language (Langage de Balisage HyperTexte). Langage utilisé pour créer les documents Web.

HTTP
HyperText Transfer Protocol (Protocole de Transfert HyperTexte). Protocole utilisé pour se connecter à des sites Web et retirer des documents HTML ou des fichiers.

i-nSud
Point d'entrée menant au contenu d'un fichier sur un système de fichiers Unix. Un i-nœud est identifié de façon spécifique par un numéro, et contient des méta-informations sur le fichier auquel il se réfère, tels que ses temps d'accès, son type, sa taille, **mais pas son nom!**

icône
Petit dessin (généralement en 16 x 16, 32 x 32, 48 x 48, et parfois 64 x 64 pixels) qui représente, sous un environnement graphique, un document, un fichier ou un programme.

IDE
Integrated Drive Electronics (Électronique Intégrée au Disque). Le plus utilisé des bus sur les PC d'aujourd'hui pour les disques durs. Un bus IDE peut contenir jusqu'à deux périphériques. Sa vitesse est limitée par le périphérique au bus qui a la file de commandes la plus lente (et pas la vitesse de transfert la plus lente !).
Voir aussi : ATAPI (« AT Attachment Packet Interface ») .

Interface graphique : GUI
Graphical User Interface. Interface d'un ordinateur constituée de menus, boutons, icônes, et autres éléments graphiques. La plupart des utilisateurs préfèrent une interface graphique plutôt qu'une interface en ligne de commande ou CLI (*Command Line Interface*) pour sa facilité d'utilisation, même si cette dernière est plus polyvalente.

Internet
Immmense réseau qui connecte des ordinateurs tout autour du monde.

invite
Prompt dans un *shell*, c'est la chaîne de caractères avant le curseur. Lorsqu'elle est visible, il est possible de taper vos commandes.

IRC
Internet Relay Chat (Conversation Relayée par Internet) : une des rares normes sur Internet pour la conversation en direct. Elle autorise la création de canaux, de conversations privées et aussi l'échange de fichiers. Elle est aussi conçue pour être capable de faire se connecter les serveurs entre eux, et c'est pourquoi plusieurs réseaux IRC existent aujourd'hui : *Undernet*, *DALnet*, *EFnet* pour n'en citer que quelques-uns.

ISA
Industry Standard Architecture (Architecture Standard pour l'Industrie). Premier bus utilisé sur les cartes mère, il est lentement abandonné au profit du bus PCI. Cependant, quelques fabricants de matériel l'utilisent toujours. Il est encore très courant que les cartes SCSI fournies avec des scanneurs, graveurs, etc. soient des ISA.

ISDN
Integrated Services Digital Network ou RNIS : Réseau Numérique à Intégration de Services. Ensemble de standards de communication permettant à un câble unique ou une fibre optique de transporter de la voix, des services de réseau numérique et de la vidéo. Il a été conçu afin de remplacer le système téléphonique actuel, connu sous l'acronyme RTC (*Réseau Téléphonique Commuté*).

ISO
International Standards Organisation (*Organisation Internationale de Standards*) : groupement d'entreprises, de consultants, d'universités et autres sources qui élaborent des standards dans divers domaines, y compris l'informatique. Les documents décrivant les standards sont numérotés. Le standard numéro 9660, par exemple, décrit le système de fichiers utilisé par les CD-ROM.

ISO 8859
Le standard ISO 8859 inclut plusieurs extensions 8-bit à l'ensemble de caractères ASCII. Il y a notamment ISO 8859-1, l' « Alphabet Latin No. 1 », largement utilisé, qui peut en fait être considéré comme le remplaçant de facto du standard ASCII.
ISO 8859-1 reconnaît les langues suivantes : afrikaans, allemand, anglais, basque, catalan, danois, hollandais, écossais, espagnol, féroais, finlandais, français, gallois, islandais, irlandais, italien, norvégien, portugais, et suédois.
Notez bien que les caractères ISO 8859-1 sont aussi les 256 premiers caractères de ISO 10646 (Unicode). Néanmoins, il lui manque le symbole EURO et ne reconnaît pas complètement le finlandais ni le français. L'ISO 8859-15 est une modification de ISO 8859-1 qui couvre ces besoins.
Voir aussi : ASCII.

job
Processus fonctionnant en arrière-plan dans le contexte du *shell*. Vous pouvez avoir plusieurs *jobs* dans un même *shell*, et contrôler ces *jobs*.
Voir aussi : premier plan, arrière-plan.

joker (wildcard)
Les caractères « * » et « ? » sont utilisés comme caractères dit jokers car ils peuvent représenter n'importe quoi. Le « * » représente un nombre quelconque de caractères, alors que le « ? » représente exactement un caractère. Les jokers sont utilisés fréquemment dans les expressions ordinaires.

JPEG
Joint Photographic Experts Group (*Regroupement d'Experts de la Photographie*) : autre format de fichier image très connu. JPEG est surtout habilité à compresser des scènes réelles, et ne fonctionne pas très bien avec les images non réalistes.

lancer
Action d'invoquer, ou de démarrer un programme.

langage assembleur
Langage de programmation le plus proche de l'ordinateur, d'où son nom de langage de programmation de « bas niveau ». L'assembleur a l'avantage de la vitesse puisque les programmes sont écrits directement sous la forme d'instructions pour le processeur, de sorte qu'aucune ou peu de traduction ne soit nécessaire pour en faire un programme exécutable. Son inconvénient majeur est qu'il est fondamentalement dépendant du processeur (ou de l'architecture). Écrire des programmes complexes est donc très long. Ainsi l'assembleur est le langage de programmation le plus rapide, mais il n'est pas transportable entre architectures.

TLDP
The Linux Documentation Project (*Project de Documentation pour Linux*) : organisation à but non lucratif qui maintient de la documentation sur GNU/Linux. Ses documents les plus connus sont les *HOWTO*, mais elle produit aussi des FAQ, et même quelques livres.

lecture seule (read-only mode)
Relatif à un fichier qui ne peut pas être modifié. On pourra en lire le contenu, mais pas le modifier.
Voir aussi : lecture-écriture (read-write mode).

lecture-écriture (read-write mode)
Relatif à un fichier qui peut être modifié. Ce type d'autorisation permet à la fois de lire et de modifier un fichier.
Voir aussi : lecture seule (read-only mode).

liaison
Dernière étape du processus de compilation, consistant à lier ensemble les différents fichiers objet de façon à produire un fichier exécutable, et à résoudre les symboles manquants avec les librairies dynamiques (à moins qu'une liaison statique ait été demandée, auquel cas le code de ces symboles sera inclus dans l'exécutable).

libre (logiciel) open source
Nom donné au code source libre d'un programme qui est rendu disponible à la communauté de développement, et au public en général. La théorie sous-jacente est qu'en autorisant à ce que le code source soit utilisé et modifié par un groupe plus large de programmeurs, cela produira un produit plus utile pour davantage de personnes. On peut citer parmi les programmes libres les plus célèbres Apache, sendmail et GNU/Linux.

lien
I-nœud dans un répertoire, donnant par là un nom (de fichier) à cet i-nœud. Des exemples d'i-nœuds n'ayant pas de lien (et donc aucun nom) sont : les tubes anonymes (utilisés par le *shell*), les sockets (connexions réseau), périphériques réseau, etc.

ligne de commande
Ce que fournit un *shell* et permet à l'utilisateur de taper des commandes directement. C'est également le sujet d'une bataille éternelle entre ses adeptes et ses détracteurs **:-)**

Linux
Système d'exploitation du type Unix adapté à une grande variété d'architectures; il est utilisable et modifiable à volonté. Linux (le noyau) a été écrit par Linus Torvalds.

login
Nom de connexion de l'utilisateur sur un système Unix, et l'action même de se connecter.

loopback
Interface réseau virtuelle d'une machine avec elle-même, qui permet aux programmes en fonctionnement de ne pas devoir prendre en compte le cas particulier où deux entités réseau correspondent à la même machine.

majeur
Numéro caractéristique de la classe de périphériques considérée.

mandataire
(*proxy*) Machine qui se situe entre un réseau et l'Internet, dont le rôle est d'accélérer les transferts de données pour les protocoles les plus utilisés (HTTP et FTP par exemple). Il maintient un tampon des demandes précédentes, ce qui évite le coût impliqué par une nouvelle demande de fichier alors qu'une autre machine a fait cette requête récemment. Les serveurs mandataires sont très utiles sur les réseaux à petite vitesse (comprenez : connexions modems RTC). Quelquefois, le mandataire est la seule machine capable d'atteindre l'extérieur.

masquage IP
Technique utilisée lorsque vous utilisez un pare-feu pour cacher la véritable adresse IP de votre ordinateur depuis l'extérieur. Généralement, les connexions faites en dehors du réseau hériteront de l'adresse IP du pare-feu lui-même. Cela est utile dans les cas où vous avez une connexion Internet rapide avec une seule adresse IP officielle, mais souhaitez partager cette connexion avec d'autres ordinateurs d'un réseau local ayant des adresses IP privées.

MBR
Master Boot Record (*Secteur de Démarrage Maître*). Nom donné au premier secteur d'un disque dur amorçable. Le MBR contient le code utilisé pour charger le système d'exploitation en mémoire ou un chargeur de démarrage (tel que LILO), et la table des partitions de ce disque dur.

menu déroulant
Menu qui peut s' « enrouler » et se « dérouler » à volonté à l'aide d'un bouton situé à l'une de ses extrémités. Il sert généralement à choisir une des valeurs proposées dans ce menu.

MIME
Multipurpose Internet Mail Extensions (*Extensions de Courrier pour Internet à Usages Multiples*) : chaîne de la forme `type/sous-type` décrivant le contenu d'un fichier attaché dans un courrier électronique. Cela autorise les lecteurs de courrier reconnaissant le MIME à effectuer des actions dépendantes du type du fichier.

mineur
Numéro précisant le périphérique dont il est question.

mode commande
Sous Vi ou l'un de ses clones, c'est l'état du programme dans lequel la pression sur une touche (ceci concerne surtout les lettres) n'aura pas pour effet d'insérer le caractère correspondant dans le fichier en cours d'édition, mais d'effectuer une action propre à la touche enfoncée (à moins que le clone que vous utilisez ne permette de personnaliser la correspondance entre touches et actions, et que vous ayez choisi cette fonctionnalité). On en sort en enfonçant l'une des touches ramenant au mode *insert*, comme **i**, **I**, **a**, **A**, **s**, **S**, **o**, **O**, **c**, **C**, etc.

mode insertion
Sous Vi ou l'un de ses clones, c'est l'état du programme dans lequel la pression sur une touche aura pour effet d'insérer le caractère correspondant dans le fichier en cours d'édition (sauf dans certains cas comme le complètement d'une abréviation, le calibrage à droite en fin de ligne,...). On en sort par une pression sur la touche **échap** (ou **Ctrl-[**).

mode multitâche
la capacité d'un système d'exploitation à partager le temps d'utilisation du processeur entre plusieurs applications. A bas niveau, on parle aussi de multiprogrammation. Passer d'une application à une autre necessite de sauvegarder tout le contexte du processus courant et de le charger lorsque cette application reprend son exécution. Cette opération est appelée changement de contexte, et un processeur Intel le fait 100 fois par seconde, opérant de manière tellement rapide qu'un utilisateur aura l'illusion que le système d'exploitation exécute plusieurs applications en même temps. Il existe deux types de mode multitâche: en mode multitâche préemptif, le système d'exploitation est responsable for taking away the CPU and passing it à une autre application; en mode multitâche coopératif, c'est l'application elle-même

qui cède le contrôle des ressources du système. La premiere option est evidemment la meilleure car aucun programme ne peut utiliser en permanence le temps d'utilisation du processeur et ainsi bloquer les autres applications. GNU/Linux fonctionne sous le mode multitâche préemptif. La règle de sélection de l'application qui doit ou non s'exécuter, et qui dépend de plusieurs paramètres, est appelée « planification »

montage (point de)
Répertoire où une partition (ou un périphérique en général) va se rattacher au système de fichiers de GNU/Linux. Par exemple, votre lecteur de CD-ROM est monté dans le répertoire `/mnt/cdrom`, d'où vous pouvez avoir accès au contenu du CD.

monté
Un périphérique est monté lorsqu'il rattaché au système de fichiers de GNU/Linux. Quand vous montez un périphérique, vous pouvez en explorer le contenu. Ce terme est en partie obsolète dû à la fonctionnalité « supermount », et ainsi les utilisateurs n'ont pas à monter manuellement un périphérique amovible. *Voir aussi :* montage (point de).

mot de passe
Mot secret ou combinaison de lettres, de chiffres et de symboles, utilisé pour protéger quelque chose. Les mots de passe sont utilisés de concert avec les noms d'utilisateur (*login*) pour les systèmes multi-utilisateurs, sites Web, FTP, etc. Les mots de passe devraient être des phrases difficiles à deviner, ou des combinaisons alphanumériques, et ne doivent en aucun cas être basées sur des mots du dictionnaire. Les mots de passe empêchent que d'autres personnes puissent se connecter sur un ordinateur ou un site en utilisant votre compte.

motif d'englobement
Chaîne de caractères composée de caractères normaux et de caractères spéciaux. Les caractères spéciaux sont interprétés et étendus par le *shell*.

MPEG
Moving Pictures Experts Group (*Groupe d'Experts en Images Animées*) : comité ISO qui génère des normes de compression audio et vidéo. MPEG est aussi le nom de leurs algorithmes. Malheureusement, la licence de ce format est très restrictive, par conséquent il n'existe aucun visualisateur MPEG sous licence libre...

MSS
La MSS (*Maximum Segment Size*, « Taille Maximale d'un Segment ») est la plus grande quantité de données pouvant être transmise en une fois. Si vous souhaitez éviter la fragmentation locale, la MSS devrait être égale à l'entête MTU-IP.

MTU
La MTU (*Maximum Transmission Unit*, « Unité Maximale de Transmission ») est le paramètre qui détermine le datagramme de plus grande taille pouvant être transmis par une interface IP sans devoir être découpé en unités plus petites. La MTU devrait être plus grande que la taille du plus grand datagramme que vous souhaitez transmettre entier. Il est à noter que cela ne concerne que la fragmentation locale, d'autres liens sur le chemin peuvent avoir une MTU plus petite et engendrer une fragmentation du datagramme à ce niveau. Les valeurs standards peuvent être de 1500 octets pour une interface ethernet, ou 576 octets pour une interface SLIP.

multi-utilisateur
Caractéristique d'un système d'exploitation qui permet à plusieurs utilisateurs de se connecter et d'utiliser une même machine au même moment, chacun d'entre eux pouvant effectuer ses tâches indépendamment des autres utilisateurs. GNU/Linux est à la fois un système multi-tâches et multi-utilisateur, de même que tout système UNIX®.

NCP
NetWare Core Protocol (*Protocole de Base de NetWare*) : protocole défini par **Novell** pour accéder aux services de fichiers et d'impression de Novell Netware.

NFS
Network FileSystem (*Système de Fichiers Réseau*) : système de fichiers réseau créé par **Sun Microsystems** pour partager des fichiers le long d'un réseau en toute transparence.

NIC
Network Interface Controller (*Contrôleur d'Interface Réseau*) : adaptateur installé dans un ordinateur qui fournit une connexion physique à un réseau, comme une carte Ethernet.

NIS
Network Information System (*Système d'Informations par Réseau*). NIS était aussi connu sous le nom de « Yellow Pages » (*Pages Jaunes*), mais **British Telecom** possède un copyright sur ce nom. NIS est un protocole conçu par **Sun Microsystems** pour partager des informations communes le long d'un **domaine** NIS, qui peut regrouper un réseau local complet, quelques machines de ce réseau ou plusieurs réseaux locaux. Il peut exporter des bases de données de mots de passe, de services, d'informations de groupe, etc.

niveau d'exécution (runlevel)
Configuration d'un système logiciel, qui ne permet que certains processus. Les processus autorisés sont définis pour chaque niveau dans le fichier `/etc/inittab`. Il y a huit niveaux prédéfinis : 0, 1, 2, 3, 4, 5, 6, S et passer de l'un à l'autre ne peut se faire que par l'administrateur en exécutant les commandes `init` et `telinit`.

nom d'utilisateur (username)
Appelé aussi *login*, nom (ou plus généralement un mot) qui identifie un utilisateur dans un système. Chaque nom d'utilisateur est associé à un unique UID (*user ID* : IDentificateur d'Utilisateur)
Voir aussi : login.

nommage
Néologisme couramment employé dans le milieu de l'informatique pour nommer une méthode de désignation de certains objets. On parle souvent de « convention de nommage » pour des fichiers, des fonctions dans un programme, etc.

noyau
Largement connu sous son nom anglais *kernel*, il est le coeur du système d'exploitation. Le noyau est chargé de l'allocation des ressources et de la gestion des processus. Il prend en charge toutes les opérations de bas-niveau qui permettent aux programmes de communiquer directement avec le matériel de l'ordinateur.

nul (caractère)
Caractère ou octet de numéro 0, il est utilisé pour marquer la fin d'une chaîne de caractères.

octet
Huit bits consécutifs. Il est interprété comme un nombre, en base deux, compris entre 0 et 255.
Voir aussi : bit.

page de manuel
Petit document contenant la définition d'une commande et son utilisation, à consulter avec la commande `man`. La première chose à (savoir) lire lorsqu'on entend parler d'une commande inconnue **:-)**

PAP
Password Authentication Protocol (*Protocole d'Authentification par Mot de Passe*) : protocole utilisé par les FAI pour authentifier leurs clients. Dans ce schéma, le client (c'est vous) envoie une paire identifiant/mot de passe au serveur, non cryptée.
Voir aussi : CHAP.

pare-feu
(*firewall*) Machine qui est l'unique point d'entrée et de sortie avec le réseau extérieur dans la topologie d'un réseau local, et qui filtre ou contrôle l'activité sur certains ports, ou les réserve à des interfaces IP précises.

passerelle
Equipement d'interconnexion entre deux réseaux IP

patch, patcher
Correctif, fichier contenant une liste de modifications à apporter à un code source dans le but d'y ajouter des fonctionnalités, d'en ôter des bogues, ou d'y apporter toute autre modification souhaitée. L'action d'appliquer ce fichier à l'archive du code source.

PCI
Peripheral Components Interconnect (*Interconnexion de Composants Périphériques*) : bus créé par **Intel** et qui est aujourd'hui le bus standard pour les architectures, mais d'autres architectures l'utilisent également. C'est

le successeur de l' ISA, et il offre de nombreux services : identification du périphérique, informations de configuration, partage des IRQ, bus mastering, etc.

PCMCIA
Personal Computer Memory Card International Association (Association Internationale des Cartes Mémoires pour Ordinateurs Personnels) : de plus en plus souvent appelé « PC Card » pour des raisons de simplicité ; c'est la norme pour les cartes externes attachées aux ordinateurs portables : modems, disques durs, cartes mémoire, cartes Ethernet, etc. L'acronyme est quelquefois étendu avec humour en *People Cannot Memorize Computer Industry Acronyms* (Les gens ne peuvent pas mémoriser les acronymes de l'industrie informatique)...

plein-écran
Terme utilisé pour désigner les applications qui prennent toute la place disponible de votre affichage.

plugin
Programme d'appoint utilisé pour afficher ou enclencher un contenu multimédia proposé sur un document web. Il est généralement facile à télécharger lorsque le navigateur est encore incapable d'afficher ce type d'information.

PNG
Portable Network Graphics (*Graphiques Réseau Portables*) : format de fichier image créé principalement pour l'utilisation sur le Web, il a été conçu comme un remplacement de GIF (sans les problèmes de brevets et avec des fonctionnalités supplémentaires).

PNP
Plug'N'Play (*Brancher Et Utiliser*). Conçu en premier lieu pour l' ISA pour ajouter des informations de configuration pour les périphériques, c'est devenu un terme plus générique qui regroupe tous les périphériques capables de rapporter leurs paramètres de configuration. Tous les périphériques PCI sont Plug'n'Play.

précédence
Action de dicter l'ordre d'évaluation des opérations d'une expression. Par exemple : Si vous évaluez l'opération `4 + 3 * 2` vous obtenez 10 comme résultat, du fait que la multiplication a une précédence plus élevée que l'addition. Si vous souhaitez évaluer l'addition d'abord, vous devrez utiliser des parenthèses : `(4 + 3) * 2`. Vous obtiendrez alors 14 comme résultat, du fait que les parenthèses ont une précédence supérieure à la multiplication, l'opération entre parenthèses est donc évaluée en premier.

premier plan
Dans le contexte du *shell*, le processus au premier plan est celui qui est en train d'être exécuté. Vous devez attendre qu'un tel processus ait fini pour pouvoir entrer à nouveau des commandes.
Voir aussi : job, arrière-plan.

processus
Dans un contexte Unix, un processus est l' instance d'un programme en cours d'exécution, avec son environnement.

propriétaire
Dans le contexte des utilisateurs et de leurs fichiers, le propriétaire d'un fichier est celui qui a créé ce fichier.
Dans le contexte des groupes, le groupe propriétaire d'un fichier est le groupe auquel appartient le créateur de ce fichier.

propriétaire (groupe)
Dans le contexte des groupes et de leurs fichiers, le groupe propriétaire d'une fichier est le groupe auquel appartient l'utilisateur qui a créé ce fichier.

racine (système de fichier)
Système de fichiers de plus haut niveau, sur lequel GNU/Linux monte son arborescence de répertoires racine. Il est indispensable que le système de fichier racine réside sur une partition séparée, car il s'agit de la base de tout le système. Il héberge le répertoire racine.

RAID
Redundant Array of Independent Disks (*Ensemble Redondant de Disques Indépendants*) : projet initié par le département informatique de l'université de Berkeley, et dans lequel le stockage des données est réparti sur un ensemble de disques.

RAM
Random Access Memory (*Mémoire à Accès Aléatoire*). Terme utilisé pour identifier la mémoire principale d'un ordinateur.

Relai de trames
(*frame relay*) Le relai de trames est une technologie réseau qui convient parfaitement à des transferts sporadiques ou en rafale. Les coûts du réseau sont réduits par la multitude de clients de relais de trames qui partagent la même bande passante. Cette réduction de coût repose aussi sur une utilisation du réseau qui peut diffèrer en besoin de bande passante en fonction du moment .

répertoire
Partie de la structure du système de fichiers. Un répertoire est un contenant pour les fichiers et éventuellement d'autres répertoires. Ces derniers sont alors appelés sous-répertoires (ou branches) du premier répertoire. On y fait souvent référence sous le terme d'arborescence. Si vous souhaitez voir le contenu d'un répertoire, vous pouvez soit le lister, soit y pénétrer. Les fichiers d'un répertoire sont appelés « feuilles » et les sous-répertoires « branches ». Les répertoires suivent les même restrictions que les fichiers, bien que la signification des autorisations y soit parfois différente. Les répertoires spéciaux « . » et « .. » font respectivement référence au répertoire même et à son parent.

répertoire personnel
Très souvent abrégé par « *home* », même en français, c'est le nom donné au répertoire d'un utilisateur donné.
Voir aussi : compte.

réseau local
Aussi appelé LAN *Local Area Network*. Nom générique donné à un réseau de machines physiquement connectées au même câble.

RFC
Request For Comments (*Appel à Commentaires*). Les RFC sont les documents officiels des standards de l' Internet. Ils décrivent tous les protocoles, leur utilisations, les pré-requis imposés, etc. Pour comprendre le fonctionnement d'un protocole, allez chercher le RFC correspondant.

root (utilisateur)
Super-utilisateur sur tout système UNIX®. En particulier root (c'est à dire l'administrateur du système) est la personne responsable de la maintenance et de la supervision du système. Cette personne a aussi un accès illimité à tout le système.

route
Chemin que prennent vos données à travers le réseau pour atteindre leur destination. Chemin entre une machine et une autre sur le réseau.

RPM
Redhat Package Manager (*Gestionnaire de Paquetages de* ***Red Hat***). Format d'empaquetage développé par **Red Hat** pour créer des paquetages logiciels, et utilisé par beaucoup de distributions GNU/Linux, y compris Mandriva Linux.

sauvegarde
Moyen visant à protéger vos données importantes en les conservant sur un support et un endroit fiables. Les sauvegardes devraient être faites régulièrement, tout particulièrement pour les informations critiques et les fichiers de configuration (les premiers répertoires à sauvegarder sont `/etc`, `/home`, et `/usr/local`). Généralement, on utilise `tar` avec `gzip` ou `bzip2` pour sauvegarder des répertoires et des fichiers. Il existe d'autres outils ou programmes tels que `dump` et `restore`, ainsi qu'une quantité d'autres solutions libres ou commerciales pour la sauvegarde des documents.

SCSI
Small Computers System Interface (*Interface Système pour Petits Ordinateurs*) : bus avec une grande bande passante mis au point pour autoriser plusieurs types de périphériques. Contrairement à l' IDE, un bus SCSI n'est pas limité par la vitesse à laquelle les périphériques acceptent les commandes. Seules les machines de haut niveau intègrent un bus SCSI directement sur la carte mère; une carte additionnelle est donc nécessaire pour les PC.

sélecteur d'espace de travail
Une appliquette permettant de se déplacer d'un bureau virtuel à un autre.
Voir aussi : bureau virtuel.

serveur
Programme ou ordinateur qui propose une fonctionnalité ou service et attend les connexions des **clients** pour répondre à leurs ordres ou leur fournir les renseignements qu'ils demandent. C'est l'une des composantes d'un système **client/serveur**.

shadow, mots de passe
Système de gestion des mots de passe dans lequel le fichier contenant les mots de passe chiffrés n'est plus lisible par tout le monde, alors qu'il l'est quand on utilise le système normal de mots de passe.

SMB
Server Message Block (*Serveur de Messages par Blocs*). Protocole utilisé par les machines windows (9x or NT) pour le partage de fichiers le long d'un réseau.

socket
Type de fichier correspondant à tout ce qui est connexion réseau.

sortie standard
Descripteur de fichier numéro 1, ouvert par tous les processus, utilisé par convention comme le descripteur de fichier dans lequel le processus écrit les données qu'il produit.
Voir aussi : erreur standard, canal d', entrée standard.

SVGA
Super Video Graphics Array (*Super Affichage Graphique Vidéo*) : norme d'affichage vidéo définie par VESA pour l'architecture PC. La résolution est de 800 x 600 x 16 couleurs.

switch (options)
Les switches sont utilisés pour modifier le comportement des programmes, et sont aussi appelés : options de ligne de commande ou arguments. Pour déterminer si un programme propose des switches en option, lisez sa page de `man` pages ou essayez de lui passer l'option `--help` (ie. `program --help`).

symboliques, liens
Fichiers particuliers, ne contenant qu'une chaîne de caractères. Tout accès à ces fichiers est équivalent à un accès au fichier dont le nom est donné par cette chaîne de caractères, qui peut ou non exister, et qui peut être précisé par un chemin relatif ou absolu.

système client/serveur
Système ou protocole composé d'un **serveur** et d'un ou plusieurs **clients**.

système d'exploitation
Interface entre les applications et le matériel sous-jacent. La tâche de tout système d'exploitation est en premier lieu de gérer toutes les ressources spécifiques à une machine. Sur un système GNU/Linux, cela est fait pas le noyau et les modules chargeables. D'autres systèmes d'exploitation connus sont AmigaOS, MacOS, FreeBSD, OS/2, Unix, Windows NT et Windows 9x.

système de fichiers
Schéma utilisé pour stocker des fichiers sur un support physique (disque dur, disquette) d'une manière consistante. Des exemples de systèmes de fichiers sont la FAT, ext2fs de Linux, iso9660 (utilisé par les CD-ROM), etc.

table de conversion
C'est un tableau qui référence des corresponding codes (ou tags) et leurs significations.C'est souvent un fichier de données utilisé par un programme pour obtenir plus d'information sur un sujet particulier.
Par exemple, HardDrake utilise un tableau similaire pour identifier le code d'un produit d'un constructeur. Voici une ligne de ce tableau, nous renseignant sur l'article `CTL0001`

```
CTL0001 sound   sb      Creative Labs   SB16 HAS_OPL3|HAS_MPU401|HAS_DMA16|HAS_JOYSTICK
```

tampon (buffer)
Zone de mémoire de taille fixe, pouvant être associée à un fichier en mode bloc, une table du système, un processus etc. La cohérence de tous les tampons est assurée par le cache mémoire.

thémable
Pour une application graphique, cela indique qu'elle peut changer son apparence en temps réel. Beaucoup de gestionnaires de fenêtres sont également thémables.

traverser
Pour un répertoire sur un système Unix, cela signifie que l'utilisateur est autorisé à passer à travers ce répertoire et, si possible, de se rendre dans ses sous-répertoires. Cela requiert que l'utilisateur ait le droit d'exécution sur ce répertoire.

tube
Type de fichiers spécial d'Unix. Un programme écrit des données dans le tube, et un autre programme lit les données à l'autre bout. Les tubes Unix sont FIFO, donc les données sont lues à l'autre bout dans l'ordre où elles ont été envoyées. Très utilisés dans le *shell*. Voir aussi **tube nommé**.

tube nommé
Tube Unix qui est lié, contrairement aux tubes utilisés dans le *shell*.
Voir aussi : tube, lien.

URL
Uniform Resource Locator (*Localisateur Uniforme de Ressources*) : ligne avec un format spécial utilisée pour identifier une ressource sur l' Internet d'une façon univoque. La ressource peut être un fichier, un serveur etc. La syntaxe d'un URL est
`protocole://nom.du.serveur[:port]/chemin/vers/ressource`.
Quand est donné seulement un nom de machine et que le protocole est `http://`, cela équivaut à retirer l'éventuel fichier intitulé `index.html` du serveur par défaut.

utilisateur unique (single user)
État du système d'exploitation, ou même un système d'exploitation en soi, qui n'autorise qu'à un seul utilisateur à la fois de se connecter et d'utiliser le système.

valeurs discrètes
Valeurs non continues ou qui ne se suivent pas, comme s'il existait une sorte d' « espace » entre deux valeurs consécutives.

variables
Chaînes utilisées dans les fichiers `Makefile` pour être remplacées par leur valeur chaque fois qu'elles apparaissent. Elles sont généralement définies au début du fichier `Makefile` et sont utilisées pour simplifier le `Makefile` et la gestion de l'arborescence des fichiers source.
De manière plus générale, en programmation, les variables sont des mots qui font référence à d'autres entités (nombres, chaînes, tableaux de valeurs, etc.) qui sont susceptibles de varier au cours de l'exécution du programme.

variables d'environnement
Partie de l'environnement d'un processus. Les variables d'environnement sont directement visibles depuis le *shell*.
Voir aussi : processus.

verbeux
Pour les commandes, le mode verbeux fait que la commande va afficher sur la sortie standard (ou erreur) toutes les actions engagées et les résultats de ces actions. Les commandes offrent parfois un « niveau de volubilité », ce qui signifie que la quantité d'information fournie peut être contrôlée.

VESA
Video Electronics Standards Association (*Association pour les Standards des matériels Vidéo électroniques*) : association de normes de l'industrie orientée vers l'architecture. Elle est l'auteur de la norme SVGA, par exemple.

visionneuse (pager)
Programme présentant un fichier texte page écran par page écran, et proposant des facilités de déplacement et de recherche dans ce fichier. Nous vous conseillons `less`.

volée (à la)
On dit qu'une action est réalisée « à la volée » lorsqu'elle est faite en même temps qu'une autre sans que l'on s'en rende compte ou sans qu'on l'ait explicitement demandé.

WAN : réseau étendu
Wide Area Network : réseau à large portée. Ce réseau, bien que similaire au réseau local (LAN), connecte des ordinateurs sur un réseau qui n'est pas relié physiquement aux mêmes brins, et sont séparés par une large distance.

Index