Guide pour serveurs Ubuntu

Projet de Documentation d'Ubuntu <*ubuntu-doc@lists.ubuntu.com*>

Guide pour serveurs Ubuntu

par Projet de Documentation d'Ubuntu <*ubuntu-doc@lists.ubuntu.com*>

Résumé

Une introduction à l'installation et à la configuration d'applications pour serveurs sur Ubuntu.

Remerciements et licence

Les auteurs suivants de l'équipe de documentation d'Ubuntu tiennent ce document à jour :

- Bhuvaneswaran Arumugam

Le Guide serveur d'Ubuntu est aussi basé sur les contributions de :

- Robert Stoffers
- Brian Shumate
- Rocco Stanzione

Mise en garde

Tous les efforts possibles ont été faits afin que toutes les informations contenues dans ce document soient précises et correctes. Malgré tout, ceci ne garantit pas une précision parfaite. Ni Canonical Ltd., ni les auteurs, ni les traducteurs ne peuvent être tenus responsables des erreurs possibles ou des conséquences de celles-ci.

Certains matériels et logiciels cités dans cette publication peuvent être des marques enregistrées et par conséquent tomber sous le coup de restrictions de droit de copie (copyright) et de lois de protection de commerce. En aucun cas les auteurs ne prétendent posséder ces noms. (N.B. : en cas de litige, seule la version anglaise fait foi)

CETTE DOCUMENTATION EST FOURNIE PAR SES AUTEURS « EN L"ÉTAT » ET SANS AUCUNE GARANTIE DE QUELQUE NATURE QUE CE SOIT, EXPRESSE OU IMPLICITE, Y COMPRIS, MAIS SANS Y ÊTRE LIMITÉ, LES GARANTIES D"APTITUDE À LA VENTE OU À UN BUT PARTICULIER. EN AUCUN CAS, LES AUTEURS NE PEUVENT ÊTRE TENUS RESPONSABLES POUR DES DOMMAGES GÉNÉRIQUES, SPÉCIFIQUES, SECONDAIRES, OU CONSÉCUTIFS (Y COMPRIS, MAIS SANS Y ÊTRE LIMITÉ, LA FOURNITURE DE BIENS OU SERVICES DE SUBSTITUTION ; LES INTERRUPTIONS D"UTILISATION ; LES PERTES DE DONNÉES OU MANQUES À GAGNER ; OU LES INTERRUPTIONS D"AFFAIRES COMMERCIALES) MÊME PROVOQUÉS ET FONDÉS SUR QUELQUE THÉORIE DE RESPONSABILITÉ QUE CE SOIT, QU"IL S"AGISSE D"UNE RESPONSABILITÉ CONTRACTUELLE, RELATIVE À DES VICES CACHÉS, OU À UN DÉLIT (Y COMPRIS, MAIS SANS Y ÊTRE LIMITÉ, LES NÉGLIGENCES) SURVENANT DE QUELQUE FAÇON QUE CE SOIT DE L"UTILISATION DE CE PROGRAMME, MÊME AVISÉS DE L"ÉVENTUALITÉ DE TELS DOMMAGES. (N.B. : en cas de litige, seule la version anglaise fait foi)

Table des matières

Liste des tableaux

À propos de ce guide

1. Conventions

Vous trouverez la signalitique suivante tout au long de cet ouvrage :

Une note met en relief un élément d'information intéressant, parfois technique, en rapport avec le thème abordé.

Une astuce présente un conseil ou une méthode plus simple.

Un avertissement signale au lecteur les problèmes potentiels et l'aide à les éviter.

Une alerte avertit le lecteur d'un risque lié à la réalisation d'un scénario donné.

Les conventions d'affichage des références croisées seront les suivantes :

- Les liens vers d'autres documents ou sites web auront cet aspect :

Les versions PDF, HTML et XHTML de ce document utiliseront les hyperliens pour gérer les références croisées.

Les conventions typographiques seront les suivantes :

- Les noms de fichiers ou les chemins d'accès aux répertoires seront affichés avec la police de caractères `monospace`.
- Les commandes à saisir dans l'invite de commande d'un terminal seront affichées ainsi :

```
commande à saisir
```

- Les options à cliquer, à sélectionner ou à choisir dans une interface utilisateur seront affichées avec la police de caractères `monospace`.

Sélections de menu, actions de la souris et raccourcis clavier :

- Une séquence de sélection de menu sera affichée comme suit : Fichier → Ouvrir
- Dans la suite de ce document, nous supposerons que la souris est configurée pour les droitiers. Les termes « cliquez » et « double-cliquez » renvoient à l'utilisation du bouton gauche de la souris. Le terme « clic-droit » renvoit à l'utilisation du bouton droit de la souris. Le terme « clic-molette » renvoit à l'utilisation du bouton central de la souris qui s'obtient, selon le modèle de votre souris, par pression sur la molette centrale ou par pression simultanée des boutons de droite et de gauche.
- Les raccourcis clavier seront présentés comme suit : **Ctrl-N**. Par convention, les touches « Contrôle », « Majuscule » et « Alternative » seront respectivement abrégées en **Ctrl**, **Maj** et **Alt**. En outre, cette représentation des raccourcis signifiera que la première touche devra être maintenue tout en enfonçant la seconde.

2. Contribution et retour d'expérience

Ce guide est développé par l'

Si vous trouvez une anomalie dans ce document ou souhaitez faire une suggestion, vous pouvez tout simplement envoyer un rapport de bogue au

Mille mercis,

Votre équipe de documentation d'Ubuntu

Chapitre 1. Introduction

Bienvenue dans le *Guide serveur d'Ubuntu* !

Le *Guide serveur d'Ubuntu* contient des informations sur la manière d'installer et de configurer selon vos besoins différentes applications serveur sur votre système Ubuntu. C'est un guide pas à pas, organisé selon les tâches de configuration et de personnalisation du système. Ce manuel aborde beaucoup de sujets intermédiaires comme :

- Configuration du réseau
- Configuration Apache2
- Bases de données
- Réseaux Windows

Ce manuel est divisé en catégories principales que voici :

- Installation
- Gestion des paquets
- Réseau
- Réseaux Windows

Ce guide présume que vous avez une connaisance suffisante de votre système Ubuntu. Si vous avez besoin d'une aide plus détaillée pour l'installation, référez-vous au guide d'installation d'Ubuntu.

Les versions HTML et PDF de ce manuel sont disponibles en ligne sur *le site web de la Documentation d'Ubuntu* [http://help.ubuntu.com].

You can buy this guide in book form from *our Lulu store* [http://www.lulu.com/ubuntu-doc]. You will only pay for the price of printing and postage.

Chapitre 2. Installation

Ce chapitre présente un survol rapide de l'installation de Ubuntu 6.06 LTS édition serveur. Pour des instructions plus détaillées, référez-vous au guide d'installation d'Ubuntu.

1. Préparer l'installation

Cette section détaille différents aspects à considérer avant de commencer l'installation.

1.1. Exigences du système

L'édition serveur de Ubuntu 6.06 LTS supporte trois architectures importantes : Intel x86, AMD64, et PowerPC. Le tableau ci-dessous présente les exigences matérielles recommandées. Selon vos besoins, il serait possible de se débrouiller avec des ressources plus faibles. Cependant, la pluspart des utilisateurs risquent de se sentir frustrés s'ils ignorent ces suggestions.

Tableau 2.1. Exigences minimales recommandées

Type d'installation	**RAM**	**Capacité Disqu**
Serveur	64 Megaoctects	500 Megaoctect

Vous trouverez ci-dessous le profil par défaut pour l'édition serveur de Ubuntu 6.06 LTS. Il est clair que la taille de l'installation dépendra grandement des services sélectionnés durant l'installation. Pour la plupart des administrateurs, les services par défaut conviendront pour une utilisation généraliste d'un serveur.

Serveur

Ce profil correspond à un petit serveur, constituant une base commune pour toutes sortes de serveurs d'applications. C'est une configuration minimale, sur laquelle il est prévu d'ajouter des services supplémentaires comme le service de fichiers ou d'impression, l'hébergement Web, l'hébergement de messagerie, etc. Pour ces services, 500 Mo d'espace disque devraient suffire, mais il s'agit de prévoir l'ajout d'espace supplémentaire selon les services que vous souhaitez ajouter au serveur.

Souvenez-vous que ces quantités n'incluent pas tous les autres types objets qu'on trouve généralement, comme les fichiers personnels des utilisateurs, les courriels, les journaux et les données. Il convient toujours d'être généreux quand on prévoit l'espace destiné à ses propres fichiers et données.

1.2. Sauvegarde

- Avant de commencer, assurez-vous de sauvegarder chaque fichier présent sur votre système. Si c'est la première fois que vous installez un autre système d'exploitation, autre que celui préinstallé, il est vraisemblable que vous ayez à repartitioner votre disque, pour faire de la place pour Ubuntu. Chaque fois, que vous partitionez votre disque, vous devez être prêt à perdre toutes les données qu'il contient, suite à une erreur de votre part, ou un problème autre, comme une coupure de l'alimentation. Les programmes utilisés lors de l'installation sont très fiables et sont utilisés depuis des années, mais ils peuvent réaliser des actions destructives, et une erreur dans leur emploi, peut provoquer la perte de données importantes.

If you are creating a multi-boot system, make sure that you have the distribution media of any other present operating systems on hand. Especially if you repartition your boot drive, you might find that you have to reinstall your operating system's boot loader, or in many cases the whole operating system itself and all files on the affected partitions.

2. Installation à partir du CD

Insérez votre CD d'installation dans le lecteur puis redémarrez l'ordinateur. La procédure d'installation démarre immédiatement après l'insertion du CD. Après l'initialisation, votre premier écran apparaîtra.

At this point, read the text on the screen. You may want to read the help screen provided by the installation system. To do this, press F1.

To perform a default server installation, select « Install to the hard disk » and press **Enter**. The installation process will be started. Simply follow the on-screen instructions, and your Ubuntu system will be installed.

Alternatively, to install a LAMP server (Linux, Apache, MySQL, PHP/Perl/Python), select « Install a LAMP server », and follow the instructions.

Chapitre 3. Gestion des paquets

Ubuntu dispose d'un système complet de gestion de paquets pour l'installation, la configuration et la suppression de programmes. Ce système permet non seulement d'accéder à une base de données contenant plus de 17 000 paquets de programmes pour votre ordinateur Ubuntu, mais aussi de gérer les résolutions de dépendances ainsi que les vérifications de mises à jour.

Divers outils pour interagir avec le système de gestion de paquets d'Ubuntu sont disponibles, des utilitaires en simple ligne de commande qui peuvent aisément être automatisés par les administrateurs système, à une interface graphique simple à utiliser pour les débutants sur Ubuntu.

1. Introduction

Le système de gestion des paquets d'Ubuntu est dérivé du même système utilisé par la distribution GNU/Linux Debian. Les paquets contiennent tous les fichiers nécessaires, ainsi que les méta-données et les instructions permettant d'implémenter une fonctionnalité particulière ou une application logicielle dans votre ordinateur Ubuntu.

Les paquets Debian portent généralement l'extension ".deb", et sont situés dans des *dépôts* qui sont des collections de paquets existants sur divers médias, tels que les CD-ROM ou Internet. Les paquets sont généralement au format binaire précompilé, ce qui rend leur installation rapide et ne requiert aucune compilation de logiciel.

Un grand nombre de paquets évolués utilisent le concept de *dépendances*. Les dépendances sont des paquets additionnels requis par le principal pour fonctionner correctement. Par exemple, l'application de synthèse vocale Festival nécessite festvox-kalpc16k, qui est un paquet fournissant une des voix utilisées par le logiciel. Pour que Festival fonctionne, toutes ses dépendances devront être installées en même temps que le paquet principal. Les outils de gestion d'applications d'Ubuntu le feront automatiquement.

2. Apt-Get

La commande apt-get est un puissant outil en ligne de commande travaillant avec l'*Advanced Packaging Tool* (APT) d'Ubuntu, offrant des fonctionnalités telles que l'installation de nouveaux logiciels, la mise à jour de ceux déjà existants, le rafraîchissement des index de paquets et même la mise à niveau complète de votre système Ubuntu.

Etant un simple outil en ligne de commande, apt-get a de nombreux avantages par rapport aux autres outils de gestion de paquets disponibles dans Ubuntu pour les administrateurs de serveurs. Ces avantages incluent la simplicité d'utilisation à travers de simples connections terminal (SSH) et la possibilité d'être utilisé dans des scripts d'administration système, qui peuvent à leur tour être automatisés par l'utilitaire de planification cron.

Quelques exemples d'utilisation habituelle de l'utilitaire apt-get :

- **Installation d'un paquet** : L'installation de paquets en utilisant l'outil apt-get est relativement simple. Par exemple, pour installer le scanner réseau *nmap*, entrez la commande suivante :

  ```
  sudo apt-get install nmap
  ```

- **Suppression d'un paquet** : La suppression d'un paquet ou de paquets est également un processus simple et direct. Pour supprimer le paquet nmap installé dans l'exemple précédent, entrez la commande suivante :

  ```
  sudo apt-get remove nmap
  ```

  Paquets multiples : Vous pouvez spécifier plusieurs paquets à installer ou à supprimer en les séparant par des espaces.

- **Mettre à jour l'index des paquets** : L'index des paquets de APT est principalement une base de données des paquets disponibles dans les dépôts listés dans le fichier `/etc/apt/sources.list`. Pour synchroniser l'index local avec les derniers changements effectués sur les dépôts, tapez cette ligne de commande :

  ```
  sudo apt-get update
  ```

- **Mettre à jour les paquets** : Avec le temps, des versions mises à jour des paquets installés sur votre ordinateur peuvent être mise en ligne dans les dépots (des mises à jour de sécurité par exemple). Pour mettre à jour votre système, mettez d'abord à jour l'index des paquet comme expliqué ci-dessus, puis tapez :

  ```
  sudo apt-get upgrade
  ```

Si un paquet a besoin d'installer ou de supprimer de nouvelles dépendances lorsqu'il est mis à jour, il ne sera pas mis à jour par la commande *upgrade*. Pour une mise à jour de ce type, il est nécessaire d'utiliser la commande *dist-upgrade*.

Vous pouvez également mettre à jour votre système Ubuntu entièrement d'une version à une autre avec dist-upgrade. Par exemple pour mettre à jour Ubuntu de la version 5.10 à 6.06, vous devez d'abord remplacer les dépots 5.10 par les 6.06 dans `/etc/apt/sources.list`, puis exécuter apt-get update come expliqué ci-dessus, et enfin faire la mise à jour en tapant :

```
sudo apt-get dist-upgrade
```

Après un certain temps, votre ordinateur sera à jour. En général, des étape supplémentaires sont nécessaires et sont expliquées dans les notes de mise à jour de la version vers laquelle vous avez fait la mise à jour.

Les actions de la commande apt-get, tel que l'ajout ou la suppression de paquets, sont inscrites dans le fichier /var/log/dpkg.log.

Pour plus d'information sur l'utilisation de APT, consultez la documentation détaillée sur *Debian APT User Manual* [http://www.debian.org/doc/user-manuals#apt-howto] ou tapez

```
apt-get help
```

3. Aptitude

Aptitude est une application texte utilisant des menus, et servant d'interface à *Advanced Packaging Tool* (APT). Beaucoup des fonctions communes de gestion des paquets, comme l'installation, la désinstallation, et la mise à jour, sont effectuées dans Aptitude avec une simple commande ayant une seule option, qui sont généralement des lettres minuscules.

Aptitude est mieux indiquée pour être utilisée dans un environnement présentant un terminal non graphique pour s'assurer un bon fonctionnement des touches de commandes. Vous pouvez démarrer Aptitude en tant qu'utilisateur normal avec la commande suivante dans un terminal:

```
sudo aptitude
```

Au démarrage d'Aptitude, vous verrez une barre de menu en haut de l'écran et deux panneaux sous cette barre. Le panneau du haut contient les catégories des paquets, telles que *Nouveaux Paquets* et *Paquets Non Installés*. Le panneau du bas contient les informations relatives aux paquets et catégories de paquets.

Utiliser Aptitude pour la maintenance des paquets est relativement direct, et l'interface utilisateur simplifie les tâches communes. Les exemples suivants sont des opération de maintenance des paquets habituelles effectuées à la manière d'Aptitude :

- **Installer des paquets**: Pour installer un paquet, localisez le avec la catégories "Paquets non installés", par example, en utilisant les touches fléchées du clavier et en appuyant sur **Entrée**, puis sélectionnez le paquet que vous voulez installer. Appuyez ensuite sur la touche **+**, et la couleur du paquet changera en *vert*, indiquant qu'il est sélectionné pour être installé. Appuyez maintenant sur la touche **g** pour avoir un liste des actions possibles. Appuyez à nouveau sur **g**, et on vous demandera de devenir super-utilisateur pour continuer. Appuyez sur **Entrée** pour avoir une invite et tapez le mot de passe pour vous identifier en tant que super-utilisateur. Enfin, appuyez sur **g** une fois de plus et il vous sera demandé de télécharger le logiciel. Appuyez sur **Entrée** à l'invite *Continuer* pour que le téléchargement et l'installation commencent.
- **Désinstaller des paquets**: Pour désinstaller un paquet, localisez le avec la catégories "Paquets installés", par example, en utilisant les touches fléchées du clavier et en appuyant sur **Entrée**, puis sélectionnez le paquet que vous voulez déinstaller. Appuyez ensuite sur la touche **-**, et la couleur du paquet changera en *rose*, indiquant qu'il est sélectionné pour être désinstallé. Appuyez maintenant sur la touche **g** pour avoir un liste des actions possibles. Appuyez à nouveau sur **g**, et on vous demandera de devenir super-utilisateur pour continuer. Appuyez sur **Entrée** pour avoir une invite et tapez le mot de passe pour vous identifier en tant que super-utilisateur. Appuyez sur **Entrée** à l'invite *Continuer* pour que la désinstallation commencent.
- **Mettre à jour l'index des paquets**: Pour mettre à jour l'index des paquets, appuyez sur la touche **u**, et on vous demandera de devenir super-utilisateur pour continuer. Appuyez

sur **Entrée** pour avoir une invite et tapez le mot de passe pour vous identifier en tant que super-utilisateur. La mise à jour de l'index va commencer. Appuyez sur keycap>Entrée

- **Mettre à jour des paquets**: Pour mettre à jour des paquets, suivez la procédure ci-dessus pour mettre à jour l'index, puis appuyez sur la touche **U** pour marquer tous les paquets que vous pouvez mettre à jour. Appuyez maintenant sur la touche **g** pour avoir un liste des actions possibles. Appuyez à nouveau sur **g**, et on vous demandera de devenir super-utilisateur pour continuer. Appuyez sur **Entrée** pour avoir une invite et tapez le mot de passe pour vous identifier en tant que super-utilisateur. Enfin, appuyez sur **g** une fois de plus et il vous sera demandé de télécharger le logiciel. Appuyez sur **Entrée** à l'invite *Continuer* pour que le téléchargement et la mise à jour des paquets commencent.

La première colonne d'information affichée dans la liste des paquets dans le panneau du haut, lorsqu'on examine réellement des paquets, liste l'état actuel du paquet et utilise la syntaxe suivante pour décrire l'état du paquet:

- **i** : Paquet installé.
- **c**: Le paquet n'est plus installé, mais sa configuration est conservée sur le système
- **p**: Purgé du système
- **v** : Paquet virtuel
- **B** : Paquet cassé
- **u**: Fichiers décompressés, mais paquet pas encore configuré.
- **C**: Mal configuré- La configuration a échouée et nécessite une correction
- **H**: Demi-installé- La Suppression a échoué et nécessite une correction

Pour quitter Aptitude, appuyez simplement sur la touche **q** et confirmez que vous désirez fermer le logiciel. Beaucoup d'autres fonctions sont disponibles à partir du menu d'Aptitude, en appuyant sur la touche **F10**.

4. Configuration

La liste des dépôts utilisée par *Advanced Packaging Tool* (APT) est enregistrée dans le fichier de configuration /etc/apt/sources.list. Un exemple de ce fichier est présenté ici, de même que les informations pour ajouter ou supprimer des liens vers des dépôts dans ce fichier.

Ceci [../sample/sources.list] est un exemple simple d'un fichier `/etc/apt/sources.list` typique.

Vous pouvez éditer le fichier pour activer ou désactiver certains dépôts. Par exemple, pour désactiver la nécessité d'insérer le CD-ROM Ubuntu à chaque fois que vous faites une opération sur les paquets, mettez simplement en commentaire la ligne appropriée qui se trouve au début du fichier :

```
# no more prompting for CD-ROM please
# deb cdrom:[Ubuntu 6.06 _Dapper Drake_ - Release i386 (20060329.1)]/ dapper main restrict
```

5. Dépôts supplémentaires

En plus des dépôts officiellement supportés par Ubuntu, il en existe des supplémentaires maintenus par la communauté qui offrent un grand nombre de paquets supplémentaires. Deux de ces dépôts les plus populaires sont *Universe* et *Multiverse*. Bien qu'ils ne soient pas officiellement supportés par Ubuntu, ce pourquoi ils ne sont pas activés par défaut, ils proposent généralement des paquets sûrs et ne présentant aucun risque pour votre ordinateur.

Les paquets situés dans le dépôt Multiverse ont souvent des licences particulières qui les empêchent d'être distribués avec un système d'exploitation libre, et ils peuvent être illégaux dans votre pays.

Soyez prévenus que ni le dépôt *Universe* ni le dépôt *Multiverse* ne contiennent des paquets officiellement supportés. Il peut donc ne pas y avoir de mises à jour de sécurité pour ces paquets.

De nombreux autres sources de paquets sont disponibles, et offrent même souvent un seul paquet, comme par exemple dans le cas des sources venant de développeurs d'une seule application. Vous devriez cependant toujours faire très attention quand vous utilisez des sources exotiques. Recherchez des sources et des paquets fiables avant d'effectuer une installation. Certains paquets provenant de sources non fiables peuvent rendre votre système instable ou inutilisable.

Pour activer les dépôts *Universe* et *Multiverse*, éditez le fichier `/etc/apt/sources.list` et supprimez les commentaires des lignes appropriées.

```
# Nous désirons les dépôts Multiverse et Universe

deb http://archive.ubuntu.com/ubuntu dapper universe multiverse
deb-src http://archive.ubuntu.com/ubuntu dapper universe multiverse
```

5.1. Références

Méthode pour ajouter des Dépôts (Wiki Ubuntu) [https://wiki.ubuntu.com/AddingRepositoriesHowto]

Chapitre 4. Réseau

Les réseaux sont formés de 2 ou plusieurs appareils, comme des ordinateurs ou des imprimantes par exemple, qui sont reliés entre eux par un lien physique ou sans fil dans le but d'échanger des informations.

Cette partie du Guide du serveur Ubuntu offre des informations générales et spécifiques aux réseaux, y compris un aperçu des concepts des réseaux et des détails sur les principaux protocoles réseau et applications pour serveurs.

1. Configuration du réseau

Ubuntu est fourni avec de nombreux utilitaires graphiques pour la configuration des périphériques réseau. Ce document s'adresse aux administrateurs de serveurs et se focalisera sur la gestion de votre réseau par la ligne de commande.

1.1. Ethernet

La plus grande partie de la configuration d'ethernet est dans un seul fichier : `/etc/network/interfaces`. Si vous n'avez pas de périphérique ethernet, seule l'interface de boucle locale sera dans ce fichier, qui ressemblera à ceci :

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback
address 127.0.0.1
netmask 255.0.0.0
```

Si vous n'avez qu'un périphérique, eth0, qu'il obtient sa configuration depuis un serveur DHCP et qu'il doit être activé au démarrage, seulement 2 lignes supplémentaires sont nécessaires :

```
auto eth0
iface eth0 inet dhcp
```

La première ligne précise que le périphérique doit être automatiquement activé au démarrage. La deuxième ligne précise que cette interface (« iface ») eth0 doit avoir un adressage IPv4 (remplacer « inet » par « inet6 » pour un périphérique IPv6) et qu'elle doit être configurée automatiquement par DHCP. En supposant que votre réseau et votre serveur DHCP sont correctement configurés, vous ne devriez pas avoir besoin de configuration supplémentaire. Le serveur DHCP fournira la passerelle par défaut (via la comande route), l'adresse IP du périphérique (via la commande ifconfig), et les serveurs DNS (dans le fichier `/etc/resolv.conf`).

Pour configurer votre périphérique ethernet avec une adresse IP statique et des paramètres personnalisés, plus d'informations sont nécessaires. Supposez que vous voulez assigner l'adresse 192.168.0.2 au périphérique eth1, avec le masque 255.255.255.0 et une passerelle par défaut sera 192.168.0.1. Le fichier `/etc/network/interfaces` ressemblera à ceci :

```
iface eth1 inet static
 address 192.168.0.2
 netmask 255.255.255.0
 gateway 192.168.0.1
```

Dans ce cas vous devez préciser les serveurs DNS vous même dans `/etc/resolv.conf`, qui ressemblera à ça :

```
search mydomain.com
nameserver 192.168.0.1
nameserver 4.2.2.2
```

La directive *search* ajoutera mydomain.com aux requêtes de nom d'hôte dans le but de résoudre les noms dans votre réseau. Par exemple, si le domaine de votre réseau est mydomain.com et que vous tentez de pinger l'hôte « mybox », la requête DNS sera modifiée pour chercher « mybox.mydomain.com ». La directive *nameserver* précise les serveurs qui seront utilisés pour la résolution de noms. Si vous utilisez votre propre serveur, entrez-le ici. Sinon demandez à votre fournisseur d'accès les adresses des serveurs DNS primaires et secondaires et entrez-les dans `/etc/resolv.conf` comme expliqué ci-dessus.

De nombreuses autres configurations sont possible, y compris pour les interfaces de modem PPP, les réseaux IPv6, des VPN, etc. Lisez man 5 interfaces pour plus d'informations et les options supportées. Souvenez-vous que `/etc/network/interfaces` est utilisé par les scripts ifup/ifdown à un niveau plus haut que dans beaucoup d'autres distribution Linux, et que les utilitaires de bas niveau comme ifconfig, route, et dhclient sont toujours disponibles pour configurer votre réseau comme vous le souhaitez.

1.2. Gérer les entrées DNS

Cette section explique la configuration du serveur de noms dans le cas d'une résolution d'adresses IP en noms d'hôtes et vice-versa. Elle ne concerne pas la configuration du système en tant que serveur de noms.

Pour gérer les entrées DNS, vous pouvez ajouter, modifier, ou enlever les noms des DNS du fichier `/etc/resolv.conf`. Un *fichier d'exemple* [../sample/resolv.conf] est donné ci-dessous :

```
search com
nameserver 204.11.126.131
nameserver 64.125.134.133
nameserver 64.125.134.132
nameserver 208.185.179.218
```

La clé search spécifie la chaîne de caractères qui sera ajoutée à un nom d'hôte incomplet. Ici, nous avons choisi com. Donc quand vous exécuterez **ping ubuntu**, ça sera interprété comme **ping ubuntu.com**.

La clé nameserver précise l'adresse IP du serveur de noms. Elle sera utilisée pour résoudre l'adresse IP ou le nom de domaine donné. Ce fichier peut avoir plusieurs entrées de serveurs de nom. Ils seront utilisés par les requêtes dans l'ordre où ils sont écrits dans le fichier.

Si les serveurs DNS sont récupérés automatiquement par DHCP ou PPOE (depuis votre fournisseur d'accès), n'ajoutez rien à ce fichier. Il sera mis à jour automatiquement.

1.3. Gérer les hôtes

Pour gérer les hôtes, vous pouvez ajouter, éditer ou retirer des hôtes du fichier `/etc/hosts`. Ce fichier contient les adresses IP et leur nom d'hôte correspondant. Quand votre système essaye de résoudre un nom de domaine vers une IP ou une IP vers un nom de domaine, il regarde d'abord dans le fichier `/etc/hosts` avant de faire appel aux serveurs DNS. Si l'adresse IP est listée dans `/etc/hosts`, les serveurs DNS ne seront pas utilisés. Ce comportement peut être modifié en éditant `/etc/nsswitch.conf` à vos risques et périls.

Si votre réseau contient des ordinateurs dont les adresses IP ne sont pas listées par les DNS, il est recommandé de les ajouter dans le fichier `/etc/hosts`.

2. TCP/IP

Transmission Control Protocol et Internet Protocol (TCP/IP) sont les protocoles standards développés à la fin des années 1970 par la Defense Advanced Research Projects Agency (DARPA) pour servir de moyen de communication entre les différents types d'ordinateurs et de réseaux. TCP/IP est le moteur d'Internet, et est donc l'ensemble de protocoles le plus populaire au monde.

2.1. Introduction à TCP/IP

Les deux protocoles de TCP/IP traitent différentes parties des réseau. *Internet Protocol*, le "IP" de TCP/IP, est un protocole non-connecté qui ne traite que le routage de paquets en utilisant le *datagramme IP* comme unité de base de l'information passant sur le réseau. Un datagramme IP consiste en un en-tête suivi d'un message. Le *Transmission Control Protocol* est le "TCP" of TCP/IP. Il permet aux hôtes d'établir des connexions qui serviront à échanger des flux de données. TCP assure que les données arriveront à destinationdans le même ordre que lorsqu'elles ont été envoyées.

2.2. Configuration TCP/IP

La configuration du protocole TCP/IP consiste en plusieurs éléments qui doivent être configurés en éditant le fichier de configuration adapté, ou en déployant des solutions telles qu'un serveur Dynamic Host Configuration Protocol (DHCP) qui pourra fournir automatiquement la bonne configuration IP aux clients. Ces données de configuration doivent être définies correctement pour assurer un bon fonctionnement du réseau avec Ubuntu.

Les paramètres de configuration TCP/IP et leurs buts sont les suivants:

- **adresse IP** L'adresse IP est un identifiant unique composé de 4 nombres entre 0 et 255., séparés par des point. Chaque nombre représente 8 bits des l'adresse qui fait au total 32 bits. Ce format est appelé *notation décimale*.
- **Masque de sous-réseau** Le masque de sous-réseau est un masque de bits, ou ensemble de marqueurs, qui séparent les parties de l'adresse IP correspondantes au réseau, et celles qui correspondent au *sous-réseau*. Par exemple dans un réseau de classe C, le masque standard qui est 255.255.255.0 cache les 3 premiers octets de l'adresse et permet d'utiliser le dernier octet pour adresser les hôtes du réseau.
- **Adresse du réseau** L'adresse du réseau représente les octets qui forment la partie réseau de l'adresse IP. par exemple, l'hôte 12.128.1.2 dans un réseau de classe A utilisera 12.0.0.0 comme adresse du réseau. 12 représente la partie réseau, et les 0 représentent la partie hôte. Les hôtes qui utilisent les adresses privées non routables telles que 192.168.1.100 utiliseront 192.168.1.0 comme adresse du réseau. Elle est constituée des 3 premiers octets de l'adresse de classe C 19.168.1 et d'un 0 pour la partie hôtes.

- **Adresse de diffusion** L'adresse de diffusion est une adresse IP qui permet d'envoyer des données simultanément à tous les hôtes d'un sous-réseau au lieu d'un hôte particulier. L'adresse standard de diffusion des réseaux IP est 255.255.255.255, mais cette adresse ne peut pas envoyer de message à tous les hôtes d'Internet car les routeurs la bloquent. Une adresse mieux appropriée sera adaptée à un sous-réseau spécifique. Par exemple, dans un réseau de classe C, 192.168.1.0, l'adresse de diffusion sera 192.168.1.255. Les messages diffusés sont généralement envoyés par les protocoles comme Address Resolution Protocol (ARP) et Routing Information Protocol (RIP).
- emphasis role="bold">Adresse de la passerelle Adresse de la passerelle est l'adresse IP passerelle. En g Adresse DNS L'adresse DNS reprprimaires, les secondaires, et les tertiaires. Pour que votre syst Les adresses IP, masques, adresses de r/etc/network/interfaces. L'adresse de serveur de nom est spnameserver dans le fichier /etc/resolv.conf. Pour plus d'informations, lisez la page de manuel pour interfaces ou resolv.conf respectivement, avec les commande suivantes en console : Accinterfaces avec la commande suivante : man interfaces Accresolv.conf avec la commande suivante :resolv.conf avec la commande suivante : man resolv.conf

2.3. Routage IP

Le routage IP est un moyen de choisir des chemins à travers différents réseaux pour envoyer les données dans un réseau TCP/IP. Le routage utilise des *tables de routage* pour diriger les paquets de la source vers la destination, souvent en passant à travers plusieurs noeuds intermédiaires appelés *routeurs*. Le routage IP est le mode de choix de chemins le plus utilisé sur internet. Il existe 2 modes de routage IP : le *routage statique* et la *routage dynamique*.

Le routage statique implique l'ajout manuel des routes dans la table de routage, ce qui est généralement fait grâce à la commande route. Le routage statique a des nombreux avantages sur le routage dynamique, comme la simplicité d'implémentation dans un petit réseau, le fait que les routes soient prévisibles (la table de routage est générée à l'avance et donc la route est la même à chaque fois qu'elle est utilisée), et une faible utilisation du réseau due à l'absence de protocole de routage dynamique. Cependant le routage statique a également des inconvénients. Il est par exemple limité aux petits réseaux et s'étend avec difficultés. Il est également incapable de s'adapter à des pannes sur le réseau à cause de la nature fixe des routes.

Le routage dynamique dépends de larges réseaux où de multiples routes sont possibles entre la source et la destination, et utilise des protocoles spécialisés comme Router Information Protocol (RIP), qui prend en charge l'adaptation des tables de routage qui rend le routage dynamique possible. Le routage dynamique a de nombreux avantages sur le routage statique, comme une plus grande adaptabilité à la taille des réseaux et la possibilité de faire face à des pannes dans le réseau. De plus il nécessite moins de configuration manuelle des tables de routage puisque le routeur apprend tout seul les routes disponibles et la présence d'autres routeurs. Cela empêche également de faire des erreurs humaines dans les tables de routage. Le routage dynamique a cependant des inconvénients comme une plus grande complexité, ainsi qu'une utilisation plus intensive du réseau à cause de la communication entre routeurs, qui ne bénéficie pas directement à l'utilisateur.

2.4. TCP et UDP

TCP est un protocole dit "connecté", qui permet la correction d'erreurs, et garantie que les données arriveront à destination grâce à un *contrôle de flux*. Le contrôle de flux détermine quand le flux de données doit être stoppé, et les précédents paquets doivent être envoyés à nouveau à cause de problèmes comme des *collisions* par exemple, pour assurer un transport fiable des données. TCP est généralement utilisé dans l'échange de données importantes comme les transactions de bases de données par exemple.

User Datagram Protocol (UDP), à l'inverse, est un protocole dit *"non-connecté"* qui est peu utilisé pour l'échange de données importantes puisqu'il ne gère pas le contrôle de flux ou d'autres méthodes pour fiabiliser le transport des données. UDP est souvent utilisé dans des applications de diffusion audio ou vidéo car il est plus rapide que TCP grâce à l'absence de correction d'erreur et de contrôle de flux, et également parce-que la perte de quelques paquets n'est généralement pas importante pour ces applications.

2.5. ICMP

Internet Control Messaging Protocol (ICMP) est une extension de Internet Protocol (IP) comme défini dans la Request For Comments (RFC) #792 et qui supporte les paquets de réseau incluant des messages de contrôle, d'erreur, et d'informations. ICMP est utilisé par des application comme ping, qui peut déterminer si un hôte ou un périphérique est en ligne ou non. *Destination Unreachable* et *Time Exceeded* sont des exemples de messages retournés par ICMP et qui sont utiles pour des hôtes comme pour des routeurs par exemple.

2.6. Services

Les services sont des applications particulières qui s'exécutent généralement en permanence et en tâche de fond, et qui attendent des requêtes venant d'autres applications pour la fonctions qu'ils exercent. De nombreux services sont liés au réseau, et donc beaucoup de services dans un système Ubuntu offrent des fonctionnalités pour les réseaux. Les services possibles sont par exemple *Hyper Text Transport Protocol Daemon* (httpd), qui propose des fonctions de serveur web, *Secure SHell Daemon* (sshd), qui permet un accès distant sécurisé au système et le transfert de fichiers sécurisé, ou *Internet Message Access Protocol Daemon* (imapd), qui offre des services de messagerie électronique.

3. Configuration du pare-feu

Le noyau Linux intègre le sous-système *Netfilter*, qui est utilisé pour manipuler ou décider ce qui arrivera lorsque du traffic réseau passe par votre serveur. Tous les pare-feu modernes pour Linux utilisent ce système pour le filtrage des paquets.

3.1. Introduction au pare-feu

Le filtrage de paquets du noyau serait d'une utilité relative aux administrateurs sans une interface utilisateur pour le gérer. C'est le but d'iptables. Quand un paquet atteint votre serveur, Netfilter décidera si il sera accepté, manipulé, ou rejeté en suivant les règles fournies grâce à iptables. Iptables suffit donc à gérer votre firewall, mais de nombreuses interfaces existent pour vous simplifier la tâche.

3.2. Translation d'IP

The purpose of IP Masquerading is to allow machines with private, non-routable IP addresses on your network to access the Internet through the machine doing the masquerading. Traffic from your private network destined for the Internet must be manipulated for replies to be routable back to the machine that made the request. To do this, the kernel must modify the *source* IP address of each packet so that replies will be routed back to it, rather than to the private IP address that made the request, which is impossible over the Internet. Linux uses *Connection Tracking* (conntrack) to keep track of which connections belong to which machines and reroute each return packet accordingly. Traffic leaving your private network is thus "masqueraded" as having originated from your Ubuntu gateway machine. This process is referred to in Microsoft documentation as Internet Connection Sharing.

Cela peut être effectué à l'aide d'une simple règle iptables, qui pourra éventuellement changer suivant la configuration de votre réseau :

```
sudo iptables -t nat -A POSTROUTING -s 192.168.0.0/16 -o ppp0 -j MASQUERADE
```

La commande ci-dessus considère que votre adresse de réseau privé est 192.168.0.0/16 et que votre interface reliée à Internet est ppp0. La syntaxe est construite comme ceci :

- -t nat -- la règle ira dans la table NAT
- -A POSTROUTING -- la règle sera ajoutée (-A) à la chaîne POSTROUTING
- -s 192.168.0.0/16 -- la règle s'applique au trafic provenant de plage d'adresse précisée
- -o ppp0 -- la règle s'applique au trafic devant être routé à travers l'interface réseau précisée
- -j MASQUERADE -- traffic matching this rule is to "jump" (-j) to the MASQUERADE target to be manipulated as described above

Each chain in the filter table (the default table, and where most or all packet filtering occurs) has a default *policy* of ACCEPT, but if you are creating a firewall in addition to a gateway device, you may have set the policies to DROP or REJECT, in which case your masqueraded traffic needs to be allowed through the FORWARD chain for the above rule to work:

```
sudo iptables -A FORWARD -s 192.168.0.0/16 -o ppp0 -j ACCEPT
sudo iptables -A FORWARD -d 192.168.0.0/16 -m state --state ESTABLISHED,RELATED -i ppp0 -j
```

The above commands will allow all connections from your local network to the Internet and all traffic related to those connections to return to the machine that initiated them.

3.3. Outils

There are many tools available to help you construct a complete firewall without intimate knowledge of iptables. For the GUI-inclined, Firestarter is quite popular and easy to use, and fwbuilder is very powerful and will look familiar to an administrator who has used a commercial firewall utility such as Checkpoint FireWall-1. If you prefer a command-line tool with plain-text configuration files, Shorewall is a very powerful solution to help you configure an advanced firewall for any network. If your network is relatively simple, or if you don't have a network, ipkungfu should give you a working firewall "out of the box" with zero configuration, and will allow you to easily set up a more advanced firewall by editing simple, well-documented configuration files. Another interesting tool is fireflier, which is designed to be a desktop firewall application. It is made up of a server (fireflier-server) and your choice of GUI clients (GTK or QT), and behaves like many popular interactive firewall applications for Windows.

3.4. Journaux

Firewall logs are essential for recognizing attacks, troubleshooting your firewall rules, and noticing unusual activity on your network. You must include logging rules in your firewall for them to be generated, though, and logging rules must come before any applicable terminating rule (a rule with a target that decides the fate of the packet, such as ACCEPT, DROP, or REJECT). For example:

```
sudo iptables -A INPUT -m state --state NEW -p tcp --dport 80 -j LOG --log-prefix "NEW_HTT
```

A request on port 80 from the local machine, then, would generate a log in dmesg that looks like this:

```
[4304885.870000] NEW_HTTP_CONN: IN=lo OUT= MAC=00:00:00:00:00:00:00:00:00:00:00:00:08:00 S
```

The above log will also appear in `/var/log/messages`, `/var/log/syslog`, and `/var/log/kern.log`. This behavior can be modified by editing `/etc/syslog.conf` appropriately or by installing and configuring ulogd and using the ULOG target instead of LOG. The ulogd daemon is a userspace server that listens for logging instructions from the kernel specifically for firewalls, and can log to any file you like, or even to a PostgreSQL or MySQL database. Making sense of your firewall logs can be simplified by using a log analyzing tool such as fwanalog, fwlogwatch, or lire.

4. Serveur OpenSSH

4.1. Introduction

Cette partie du Guide du serveur Ubuntu parle du puissant ensemble d'outils pour le contrôle à distance d'ordinateurs connectés et le transfert de fichiers entre ordinateurs connectés, appelé *OpenSSH*. Vous apprendrez également certains paramètres de configuration possibles avec le serveur OpenSSH et comment les modifier sur votre système Ubuntu.

OpenSSH est une version libre du protocole Secure Shell (SSH), comme d'autres logiciels utilisés pour le contrôle d'ordinateurs à distance, ou le transfert de fichiers entre ordinateurs. Les outils traditionnels pour effectuer ces tâches, comme telnet ou rcp, ne sont pas sécurisés et font transiter le mot de passe de l'utilisateur en clair. OpenSSH fournit un serveur et des outils clients pour faciliter le contrôle à distance et le tranfert de fichiers de façon sécurisée grâce au chiffrement des données, et donc remplace efficacement les anciens outils.

Le serveur OpenSSH, sshd, attends en permanence des connexions depuis des clients. Quand une connexion a lieu, sshd établit la connexion correcte en fonction du type de client. Par exemple, si un client se conencte avec le client ssh, le serveur OpenSSH va établir une connexion sécurisée après une authentification. Si un client se conencte avec scp, le serveur OpenSSH va commencer un transfert de fichier sécurisé entre le serveur et le client après une authentification. OpenSSH peut utiliser de nombreuses méthodes d'authentification, par exemple un mot de passe, une clé publique, ou un ticket Kerberos.

4.2. Installation

L'installation des applications client et serveur d'OpenSSH est simple. Pour installer les applications clientes d'OpenSSH sur votre système Ubuntu, tapez cette commande dans un terminal :

```
sudo apt-get install openssh-client
```

Pour installer le serveur OpenSSH et les fichiers nécessaires, utilisez cette commande dans un terminal :

```
sudo apt-get install openssh-server
```

4.3. Configuration

You may configure the default behavior of the OpenSSH server application, sshd, by editing the file `/etc/ssh/sshd_config`. For information about the configuration directives used in this file, you may view the appropriate manual page with the following command, issued at a terminal prompt:

```
man sshd_config
```

There are many directives in the sshd configuration file controlling such things as communications settings and authentication modes. The following are examples of configuration directives that can be changed by editing the `/etc/ssh/ssh_config` file.

Avant d'éditer le fichier de configuration, vous devriez faire une copie du fichier original et le protéger en écriture de façon à conserver les paramètres d'origine en référence et à pouvoir les réutiliser en cas de besoin.

Copy the `/etc/ssh/sshd_config` file and protect it from writing with the following commands, issued at a terminal prompt:

```
sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.original
sudo chmod a-w /etc/ssh/sshd_config.original
```

Voici des exemples de directives de configuration que vous pourriez changer :

- To set your OpenSSH to listen on TCP port 2222 instead of the default TCP port 22, change the Port directive as such:

  Port 2222

- To have sshd allow public key-based login credentials, simply add or modify the line:

  PubkeyAuthentication yes

  in the `/etc/ssh/sshd_config` file, or if already present, ensure the line is not commented out.

- To make your OpenSSH server display the contents of the `/etc/issue.net` file as a pre-login banner, simply add or modify the line:

  Banner /etc/issue.net

  dans le fichier `/etc/ssh/sshd_config`.

After making changes to the `/etc/ssh/sshd_config` file, save the file, and restart the sshd server application to effect the changes using the following command at a terminal prompt:

```
sudo /etc/init.d/ssh restart
```

Many other configuration directives for sshd are available for changing the server application's behavior to fit your needs. Be advised, however, if your only method of access to a server is ssh, and you make a mistake in configuring sshd via the `/etc/ssh/sshd_config` file, you may find you are locked out of the server upon restarting it, or that the sshd server refuses to start due to an incorrect configuration directive, so be extra careful when editing this file on a remote server.

4.4. Références

Site Internet de OpenSSH [http://www.openssh.org/]

Advanced OpenSSH Wiki Page [https://wiki.ubuntu.com/AdvancedOpenSSH]

5. Serveur FTP

File Transfer Protocol (FTP) is a TCP protocol for uploading and downloading files between computers. FTP works on a client/server model. The server component is called an *FTP daemon*. It continuously listens for FTP requests from remote clients. When a request is received, it manages the the login and sets up the connection. For the duration of the session it executes any of commands sent by the FTP client.

L'accès à un serveur FTP peut être réalisé de deux façons:

- Anonyme
- Authentifié

In the Anonymous mode, remote clients can access the FTP server by using the default user account called 'anonymous" or "ftp" and sending an email address as the password.
In the Authenticated mode a user must have an account and a password. User access to the FTP server directories and files is dependent on the permissions defined for the account used at login. As a general rule, the FTP daemon will hide the root directory of the FTP server and change it to the FTP Home directory. This hides the rest of the file system from remote sessions.

5.1. vsftpd - Installation du serveur FTP

vsftpd is an FTP daemon available in Ubuntu. It is easy to install, set up, and maintain. To install vsftpd you can run the following command:

```
sudo apt-get install vsftpd
```

5.2. vsftpd - Configuration du serveur FTP

You can edit the vsftpd configuration file, `/etc/vsftpd.conf`, to change the default settings. By default only anonymous FTP is allowed. If you wish to disable this option, you should change the following line:

```
anonymous_enable=YES
```

to

```
anonymous_enable=NO
```

By default, local system users are not allowed to login to FTP server. To change this setting, you should uncomment the following line:

```
#local_enable=YES
```

By default, users are allowed to download files from FTP server. They are not allowed to upload files to FTP server. To change this setting, you should uncomment the following line:

```
#write_enable=YES
```

Similarly, by default, the anonymous users are not allowed to upload files to FTP server. To change this setting, you should uncomment the following line:

```
#anon_upload_enable=YES
```

The configuration file consists of many configuration parameters. The information about each parameter is available in the configuration file. Alternatively, you can refer to the man page, **man 5 vsftpd.conf** for details of each parameter.

Une fois vsftpd configuré, vous pouvez démarrer le démon. La commande suivante permet de démarrer le démon vsftpd :

```
sudo /etc/init.d/vsftpd start
```

Veuillez noter que les réglages par défaut du fichier de configuration sont tels qu'ils sont pour des raisons de sécurité. Chacun des changements cités ci-dessus diminue la sécurité du système, par conséquent ne les appliquez qu'en cas de nécessité.

6. Network File System (NFS)

NFS permet à un système de partager des répertoires et des fichiers à travers un réseau. En utilisant NFS, utilisateurs et programmes peuvent accéder aux fichiers de systèmes distants comme s'ils étaient des fichiers locaux.

Quelques uns des plus remarquables avantages que NFS peut apporter sont :

- Local workstations use less disk space because commonly used data can be stored on a single machine and still remain accessible to others over the network.
- There is no need for users to have separate home directories on every network machine. Home directories could be set up on the NFS server and made available throughout the network.
- Storage devices such as floppy disks, CDROM drives, and USB Thumb drives can be used by other machines on the network. This may reduce the number of removable media drives throughout the network.

6.1. Installation

Dans un terminal, entrez la commande suivante pour installer le serveur NFS :

```
sudo apt-get install nfs-kernel-server
```

6.2. Configuration

Vous pouvez choisir les répertoires à exporter en les ajoutant au fichier `/etc/exports`. Par exemple :

```
/ubuntu *(ro,sync,no_root_squash)
/home *(rw,sync,no_root_squash)
```

You can replace * with one of the hostname formats. Make the hostname declaration as specific as possible so unwanted systems cannot access the NFS mount.

Pour démarrer le serveur NFS, vous pouvez taper la commande suivante dans un terminal :

```
sudo /etc/init.d/nfs-kernel-server start
```

6.3. Configuration du client NFS

Utilisez la commande mount pour monter un répertoire NFS partagé à partir d'une autre machine, en tapant dans un terminal une commande telle que :

```
sudo mount exemple.nomhote.com:/ubuntu /local/ubuntu
```

Le répertoire `/local/ubuntu` du point de montage doit exister. Il ne devrait y avoir ni fichiers ni sous-répertoires dans le répertoire `/local/ubuntu`

An alternate way to mount an NFS share from another machine is to add a line to the `/etc/fstab` file. The line must state the hostname of the NFS server, the directory on the server being exported, and the directory on the local machine where the NFS share is to be mounted.

La syntaxe générale des lignes dans le fichier `/etc/fstab` est celle-ci :

```
exemple.nomhote.com:/ubuntu /local/ubuntu nfs rsize=8192,wsize=8192,timeo=14,intr#
```

6.4. Références

FAQ Linux NFS [http://nfs.sourceforge.net/]

7. Dynamic Host Configuration Protocol (DHCP)

The Dynamic Host Configuration Protocol (DHCP) is a network service that enables host computers to be automatically assigned settings from a server as opposed to manually configuring each network host. Computers configured to be DHCP clients have no control over the settings they receive from the DHCP server, and the configuration is transparent to the computer's user.

The most common settings provided by a DHCP server to DHCP clients include:

- Adresse IP et masque réseau
- DNS
- WINS

However, a DHCP server can also supply configuration properties such as:

- Nom d'hôte
- Nom de domaine
- Passerelle par défaut
- Serveur de temps
- Serveur d'impression

The advantage of using DHCP is that changes to the network, for example a change in the address of the DNS server, need only be changed at the DHCP server, and all network hosts will be reconfigured the next time their DHCP clients poll the DHCP server. As an added advantage, it is also easier to integrate new computers into the network, as there is no need to check for the availability of an IP address. Conflicts in IP address allocation are also reduced.

A DHCP server can provide configuration settings using two methods:

Adresse MAC

> This method entails using DHCP to identify the unique hardware address of each network card connected to the network and then continually supplying a constant configuration each time the DHCP client makes a request to the DHCP server using that network device.

Address Pool

> This method entails defining a pool (sometimes also called a range or scope) of IP addresses from which DHCP clients are supplied their configuration properties dynamically and on a fist come first serve basis. When a DHCP client is no longer on the network for a specified period, the configuration is expired and released back to the address pool for use by other DHCP Clients.

Ubuntu is shipped with both DHCP server and client. The server is dhcpd (dynamic host configuration protocol daemon). The client provided with Ubuntu is dhclient and should be installed on all computers required to be automatically configured. Both programs are easy to install and configure and will be automatically started at system boot.

7.1. Installation

At a terminal prompt, enter the following command to install dhcpd:

```
sudo apt-get install dhcpd
```

You will see the following output, which explains what to do next:

```
Please note that if you are installing the DHCP server for the first
time you need to configure. Please stop (/etc/init.d/dhcp
stop) the DHCP server daemon, edit /etc/dhcpd.conf to suit your needs
and particular configuration, and restart the DHCP server daemon
(/etc/init.d/dhcp start).

You also need to edit /etc/default/dhcp to specify the interfaces dhcpd
should listen to. By default it listens to eth0.

NOTE: dhcpd's messages are being sent to syslog. Look there for
diagnostics messages.

Starting DHCP server: dhcpd failed to start - check syslog for diagnostics.
```

7.2. Configuration

The error message the installation ends with might be a little confusing, but the following steps will help you configure the service:

Most commonly, what you want to do is assign an IP address randomly. This can be done with settings as follows:

```
# Sample /etc/dhcpd.conf
# (add your comments here)
default-lease-time 600;
max-lease-time 7200;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.1.255;
option routers 192.168.1.254;
option domain-name-servers 192.168.1.1, 192.168.1.2;
option domain-name "mydomain.org";

subnet 192.168.1.0 netmask 255.255.255.0 {
range 192.168.1.10 192.168.1.100;
range 192.168.1.150 192.168.1.200;
}
```

This will result in the DHCP server giving a client an IP address from the range 192.168.1.10-192.168.1.100 or 192.168.1.150-192.168.1.200. It will lease an IP address for 600 seconds if the client doesn't ask for a specific time frame. Otherwise the maximum (allowed) lease will be 7200 seconds. The server will also "advise" the client that it should use 255.255.255.0 as its subnet mask, 192.168.1.255 as its broadcast address, 192.168.1.254 as the router/gateway and 192.168.1.1 and 192.168.1.2 as its DNS servers.

If you need to specify a WINS server for your Windows clients, you will need to include the netbios-name-servers option, e.g.

```
option netbios-name-servers 192.168.1.1;
```

Dhcpd configuration settings are taken from the DHCP mini-HOWTO, which can be found *here* [http://www.tldp.org/HOWTO/DHCP/index.html].

7.3. Références

FAQ DHCP [http://www.dhcp-handbook.com/dhcp_faq.html]

8. Domain Name Service (DNS)

Domain Name Service (DNS) is an Internet service that maps IP addresses and fully qualified domain names (FQDN) to one another. In this way, DNS alleviates the need to remember IP addresses. Computers that run DNS are called *name servers*. Ubuntu ships with BIND (Berkley Internet Naming Daemon), the most common program used for maintaining a name server on GNU/Linux.

8.1. Installation

At a terminal prompt, enter the following command to install dns:

```
sudo apt-get install bind
```

8.2. Configuration

The DNS configuration files are stored in the `/etc/bind` directory. The primary configuration file is `/etc/bind/named.conf`. The content of the default configuration file is shown below:

```
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind/README.Debian for information on the
// structure of BIND configuration files in Debian for BIND versions 8.2.1
// and later, *BEFORE* you customize this configuration file.
//

include "/etc/bind/named.conf.options";

// reduce log verbosity on issues outside our control
logging {
 category lame-servers { null; };
 category cname { null; };
};

// prime the server with knowledge of the root servers
zone "." {
        type hint;
        file "/etc/bind/db.root";
};

// be authoritative for the localhost forward and reverse zones, and for
// broadcast zones as per RFC 1912

zone "localhost" {
        type master;
        file "/etc/bind/db.local";
};
```

```
zone "127.in-addr.arpa" {
        type master;
        file "/etc/bind/db.127";
};

zone "0.in-addr.arpa" {
        type master;
        file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
        type master;
        file "/etc/bind/db.255";
};

// add local zone definitions here
include "/etc/bind/named.conf.local";
```

The include line specifies the filename which contains the DNS options. The directory line in the options file tells DNS where to look for files. All files BIND uses will be relative to this directory.

The file named `/etc/bind/db.root` describes the root name servers in the world. The servers change over time and must be maintained now and then.

The zone section defines a master server, and it is stored in a file mentioned against file tag. Every zone file contains 3 resource records (RRs): an SOA RR, an NS RR and a PTR RR. SOA is short of Start of Authority. The "@" is a special notation meaning the origin. NS is the Name Server RR. PTR is Domain Name Pointer. To start the DNS server, run the following command from a terminal prompt:

```
sudo /etc/init.d/bind start
```

You can refer to the documentation mentioned in the references section for details.

8.3. Références

DNS HOWTO [http://www.tldp.org/HOWTO/DNS-HOWTO.html]

9. CUPS - Serveur d'impression

The primary mechanism for Ubuntu printing and print services is the **Common UNIX Printing System** (CUPS). This printing system is a freely available, portable printing layer which has become the new standard for printing in most GNU/Linux distributions.

CUPS manages print jobs and queues and provides network printing using the standard Internet Printing Protocol (IPP), while offering support for a very large range of printers, from dot-matrix to laser and many in between. CUPS also supports PostScript Printer Description (PPD) and auto-detection of network printers, and features a simple web-based configuration and administration tool.

9.1. Installation

To install CUPS on your Ubuntu computer, simply use sudo with the the apt-get command and give the packages to install as the first parameter. A complete CUPS install has many package dependencies, but they may all be specified on the same command line. Enter the following at a terminal prompt to install CUPS:

```
sudo apt-get install cupsys cupsys-client
```

Upon authenticating with your user password, the packages should be downloaded and installed without error. Upon the conclusion of installation, the CUPS server will be started automatically. For troubleshooting purposes, you can access CUPS server errors via the error log file at: `/var/log/cups/error_log`. If the error log does not show enough information to troubleshoot any problems you encounter, the verbosity of the CUPS log can be increased by changing the **LogLevel** directive in the configuration file (discussed below) to "debug" or even "debug2", which logs everything, from the default of "info". If you make this change, remember to change it back once you've solved your problem, to prevent the log file from becoming overly large.

9.2. Configuration

The Common UNIX Printing System server's behavior is configured through the directives contained in the file `/etc/cups/cupsd.conf`. The CUPS configuration file follows the same syntax as the primary configuration file for the Apache HTTP server, so users familiar with editing Apache's configuration file should feel at ease when editing the CUPS configuration file. Some examples of settings you may wish to change initially will be presented here.

Prior to editing the configuration file, you should make a copy of the original file and protect it from writing, so you will have the original settings as a reference, and to reuse as necessary.

Copy the `/etc/cups/cupsd.conf` file and protect it from writing with the following commands, issued at a terminal prompt:

```
sudo cp /etc/cups/cupsd.conf /etc/cups/cupsd.conf.original
sudo chmod a-w /etc/cups/cupsd.conf.original
```

- **ServerAdmin**: To configure the email address of the designated administrator of the CUPS server, simply edit the `/etc/cups/cupsd.conf` configuration file with your preferred text editor, and modify the *ServerAdmin* line accordingly. For example, if you are the Administrator for the CUPS server, and your e-mail address is 'bjoy@somebigco.com', then you would modify the ServerAdmin line to appear as such:

  ```
  ServerAdmin bjoy@somebigco.com
  ```

For more examples of configuration directives in the CUPS server configuration file, view the associated system manual page by entering the following command at a terminal prompt:

```
man cupsd.conf
```

Whenever you make changes to the `/etc/cups/cupsd.conf` configuration file, you'll need to restart the CUPS server by typing the following command at a terminal prompt:

```
sudo /etc/init.d/cupsys restart
```

Some other configuration for the CUPS server is done in the file `/etc/cups/cups.d/ports.conf`:

- **Listen**: By default on Ubuntu, the CUPS server installation listens only on the loopback interface at IP address *127.0.0.1*. In order to instruct the CUPS server to listen on an actual network adapter's IP address, you must specify either a hostname, the IP address, or optionally, an IP address/port pairing via the addition of a Listen directive. For example, if your CUPS server resides on a local network at the IP address *192.168.10.250* and you'd like to make it accessible to the other systems on this subnetwork, you would edit the `/etc/cups/cups.d/ports.conf` and add a Listen directive, as such:

  ```
  Listen 127.0.0.1:631           # existing loopback Listen
  Listen /var/run/cups/cups.sock # existing socket Listen
  Listen 192.168.10.250:631      # Listen on the LAN interface, Port 631 (IPP)
  ```

  In the example above, you may comment out or remove the reference to the Loopback address (127.0.0.1) if you do not wish cupsd to listen on that interface, but would rather have it only listen on the Ethernet interfaces of the Local Area Network (LAN). To enable listening for all network interfaces for which a certain hostname is bound, including the Loopback, you could create a Listen entry for the hostname *socrates* as such:

```
Listen socrates:631  # Listen on all interfaces for the hostname 'socrates'
```

or by omitting the Listen directive and using *Port* instead, as in:

```
Port 631  # Listen on port 631 on all interfaces
```

9.3. Références

Site Internet de CUPS [http://www.cups.org/]

10. HTTPD - serveur Internet Apache2

Apache is the most commonly used Web Server on GNU/Linux systems. Web Servers are used to serve Web Pages requested by client computers. Clients typically request and view Web Pages using Web Browser applications such as Firefox, Opera, or Mozilla.

Users enter a Uniform Resource Locator (URL) to point to a Web server by means of its Fully Qualified Domain Name (FQDN) and a path to the required resource. For example, to view the home page of the *Ubuntu Web site* [http://www.ubuntu.com] a user will enter only the FQDN. To request specific information about *paid support* [http://www.ubuntu.com/support/supportoptions/paidsupport], a user will enter the FQDN followed by a path.

The most common protocol used to transfer Web pages is the Hyper Text Transfer Protocol (HTTP). Protocols such as Hyper Text Transfer Protocol over Secure Sockets Layer (HTTPS), and File Transfer Protocol (FTP), a protocol for uploading and downloading files, are also supported.

Apache Web Servers are often used in combination with the MySQL database engine, the HyperText Preprocessor (PHP) scripting language, and other popular scripting languages such as Python and Perl. This configuration is termed LAMP (Linux, Apache, MySQL and Perl/Python/PHP) and forms a powerful and robust platform for the development and deployment of Web-based applications.

10.1. Installation

The Apache2 web server is available in Ubuntu Linux. To install Apache2:

- At a terminal prompt enter the following command:

```
sudo apt-get install apache2
```

10.2. Configuration

Apache is configured by placing *directives* in plain text configuration files. The main configuration file is called `apache2.conf`. In addition, other configuration files may be added using the *Include* directive, and wildcards can be used to include many configuration files. Any directive may be placed in any of these configuration files. Changes to the main configuration files are only recognized by Apache2 when it is started or restarted.

The server also reads a file containing mime document types; the filename is set by the *TypesConfig* directive, and is `mime.types` by default.

The default Apache2 configuration file is `/etc/apache2/apache2.conf` . You can edit this file to configure the Apache2 server. You can configure the port number, document root, modules, log files, virtual hosts, etc.

10.2.1. Réglages de base

This section explains Apache2 server essential configuration parameters. Refer to the *Apache2 Documentation* [http://httpd.apache.org/docs/2.0/] for more details.

- Apache2 ships with a virtual-host-friendly default configuration. That is, it is configured with a single default virtual host (using the *VirtualHost* directive) which can modified or used as-is if you have a single site, or used as a template for additional virtual hosts if you have multiple sites. If left alone, the default virtual host will serve as your default site, or the site users will see if the URL they enter does not match the *ServerName* directive of any of your custom sites. To modify the default virtual host, edit the file `/etc/apache2/sites-available/default`. If you wish to configure a new virtual host or site, copy that file into the same directory with a name you choose. For example, **sudo cp /etc/apache2/sites-available/default /etc/apache2/sites-available/mynewsite** Edit the new file to configure the new site using some of the directives described below.
- The *ServerAdmin* directive specifies the email address to be advertised for the server's administrator. The default value is webmaster@localhost. This should be changed to an email address that is delivered to you (if you are the server's administrator). If your website has a problem, Apache2 will display an error message containing this email address to report the problem to. Find this directive in your site's configuration file in /etc/apache2/sites-available.
- The *Listen* directive specifies the port, and optionally the IP address, Apache2 should listen on. If the IP address is not specified, Apache2 will listen on all IP addresses assigned to the machine it runs on. The default value for the Listen directive is 80. Change this to 127.0.0.1:80 to cause Apache2 to listen only on your loopback interface so that it will not be available to the Internet, to (for example) 81 to change the port that it listens on, or leave it as is for normal operation. This directive can be found and changed in its own file, `/etc/apache2/ports.conf`
- The *ServerName* directive is optional and specifies what FQDN your site should answer to. The default virtual host has no ServerName directive specified, so it will respond to all requests that do not match a ServerName directive in another virtual host. If you have just acquired the domain name ubunturocks.com and wish to host it on your Ubuntu server, the value of the ServerName directive in your virtual host configuration file should be ubunturocks.com. Add this directive to the new virtual host file you created earlier (`/etc/apache2/sites-available/mynewsite`).

  > You may also want your site to respond to www.ubunturocks.com, since many users will assume the www prefix is appropriate. Use the *ServerAlias* directive for this. You may also use wildcards in the ServerAlias directive. For example, **ServerAlias *.ubunturocks.com** will cause your site to respond to any domain request ending in .ubunturocks.com.

- The *DocumentRoot* directive specifies where Apache should look for the files that make up the site. The default value is /var/www. No site is configured there, but if you uncomment the *RedirectMatch* directive in `/etc/apache2/apache2.conf` requests will be redirected to /var/www/apache2-default where the default Apache2 site awaits. Change this value in your site's virtual host file, and remember to create that directory if necessary!

The /etc/apache2/sites-available directory is **not** parsed by Apache2. Symbolic links in /etc/apache2/sites-enabled point to "available" sites. Use the a2ensite (Apache2 Enable Site) utility to create those symbolic links, like so: **sudo a2ensite mynewsite** where your site's configuration file is `/etc/apache2/sites-available/mynewsite`. Similarly, the a2dissite utility should be used to disable sites.

10.2.2. Réglages par défaut

This section explains configuration of the Apache2 server default settings. For example, if you add a virtual host, the settings you configure for the virtual host take precedence for that virtual host. For a directive not defined within the virtual host settings, the default value is used.

- The *DirectoryIndex* is the default page served by the server when a user requests an index of a directory by specifying a forward slash (/) at the end of the directory name.

  For example, when a user requests the page http://www.example.com/this_directory/, he or she will get either the DirectoryIndex page if it exists, a server-generated directory list if it does not and the Indexes option is specified, or a Permission Denied page if neither is true. The server will try to find one of the files listed in the DirectoryIndex directive and will return the first one it finds. If it does not find any of these files and if Options Indexes is set for that directory, the server will generate and return a list, in HTML format, of the subdirectories and files in the directory. The default value, found in `/etc/apache2/apache2.conf` is " index.html index.cgi index.pl index.php index.xhtml". Thus, if Apache2 finds a file in a requested directory matching any of these names, the first will be displayed.
- The *ErrorDocument* directive allows you to specify a file for Apache to use for specific error events. For example, if a user requests a resource that does not exist, a 404 error will occur, and per Apache2's default configuration, the file `/usr/share/apache2/error/HTTP_NOT_FOUND.html.var` will be displayed. That file is not in the server's DocumentRoot, but there is an Alias directive in `/etc/apache2/apache2.conf` that redirects requests to the /error directory to /usr/share/apache2/error/. To see a list of the default ErrorDocument directives, use this command: **grep ErrorDocument /etc/apache2/apache2.conf**
- By default, the server writes the transfer log to the file /var/log/apache2/access.log. You can change this on a per-site basis in your virtual host configuration files with the *CustomLog* directive, or omit it to accept the default, specified in `/etc/apache2/apache2.conf`. You may also specify the file to which errors are logged,

via the *ErrorLog* directive, whose default is `/var/log/apache2/error.log`. These are kept separate from the transfer logs to aid in troubleshooting problems with your Apache2 server. You may also specify the *LogLevel* (the default value is "warn") and the *LogFormat* (see `/etc/apache2/apache2.conf` for the default value).

- Some options are specified on a per-directory basis rather than per-server. Option is one of these directives. A Directory stanza is enclosed in XML-like tags, like so:

  ```
  <Directory /var/www/mynewsite>
      ...
     </Directory>
  ```

  The Options directive within a Directory stanza accepts one or more of the following values (among others), separated by spaces:

  - **ExecCGI -** Allow execution of CGI scripts. CGI scripts are not executed if this option is not chosen.

    💡 Most files should not be executed as CGI scripts. This would be very dangerous. CGI scripts should kept in a directory separate from and outside your DocumentRoot, and only this directory should have the ExecCGI option set. This is the default, and the default location for CGI scripts is /usr/lib/cgi-bin.

  - **Includes** - Allow server-side includes. Server-side includes allow an HTML file to *include* other files. This is not a common option. See *the Apache2 SSI Howto* [http://httpd.apache.org/docs/2.0/howto/ssi.html] for mor information.
  - **IncludesNOEXEC -** Allow server-side includes, but disable the #exec and #include commands in CGI scripts.
  - **Indexes -** Display a formatted list of the directory's contents, if no DirectoryIndex (such as index.html) exists in the requested directory.

    ⚠ For security reasons, this should usually not be set, and certainly should not be set on your DocumentRoot directory. Enable this option carefully on a per-directory basis only if you are certain you want users to see the entire contents of the directory.

  - **Multiview -** Support content-negotiated multiviews; this option is disabled by default for security reasons. See the *Apache2 documentation on this option* [http://httpd.apache.org/docs/2.0/mod/mod_negotiation.html#multiviews].
  - **SymLinksIfOwnerMatch -** Only follow symbolic links if the target file or directory has the same owner as the link.

10.2.3. Virtual Hosts Settings

Virtual hosts allow you to run different servers for different IP addresses, different host names, or different ports on the same machine. For example, you can run the website for http://www.example.com and http://www.anotherexample.com on the same Web server using virtual hosts. This option corresponds to the <VirtualHost> directive for the default virtual host and IP-based virtual hosts. It corresponds to the <NameVirtualHost> directive for a name-based virtual host.

The directives set for a virtual host only apply to that particular virtual host. If a directive is set server-wide and not defined within the virtual host settings, the default setting is used. For example, you can define a Webmaster email address and not define individual email addresses for each virtual host.

Set the DocumentRoot directive to the directory that contains the root document (such as index.html) for the virtual host. The default DocumentRoot is `/var/www`.

The ServerAdmin directive within the VirtualHost stanza is email the address used in the footer of error pages if you choose to show a footer with an email address on the error pages.

10.2.4. Paramètres du serveur

This section explains how to configure basic server settings.

LockFile - The LockFile directive sets the path to the lockfile used when the server is compiled with either USE_FCNTL_SERIALIZED_ACCEPT or USE_FLOCK_SERIALIZED_ACCEPT. It must be stored on the local disk. It should be left to the default value unless the logs directory is located on an NFS share. If this is the case, the default value should be changed to a location on the local disk and to a directory that is readable only by root.

PidFile - The PidFile directive sets the file in which the server records its process ID (pid). This file should only be readable by root. In most cases, it should be left to the default value.

User - The User directive sets the userid used by the server to answer requests. This setting determines the server's access. Any files inaccessible to this user will also be inaccessible to your website's visitors. The default value for User is www-data.

⛒ Unless you know exactly what you are doing, do not set the User directive to root. Using root as the User will create large security holes for your Web server.

The Group directive is similar to the User directive. Group sets the group under which the server will answer requests. The default group is also www-data.

10.2.5. Modules d'Apache

Apache is a modular server. This implies that only the most basic functionality is included in the core server. Extended features are available through modules which can be loaded into Apache. By default, a base set of modules is included in the server at compile-time. If the server is compiled to use dynamically loaded modules, then modules can be compiled separately, and added at any time using the LoadModule directive. Otherwise, Apache must be recompiled to add or remove modules. Ubuntu compiles Apache2 to allow the dynamic loading of modules. Configuration directives may be conditionally included on the presence of a particular module by enclosing them in an <IfModule> block. You can install additional Apache2 modules and use them with your Web server. You can install Apache2 modules using the apt-get command. For example, to install the Apache2 module for MYSQL authentication, you can run the following command from a terminal prompt:

```
sudo apt-get install libapache2-mod-auth-mysql
```

Once you install the module, the module will be available in the `/etc/apache2/mods-available` directory. You can use the a2enmod command to enable a module. You can use the a2dismod command to disable a module. Once you enable the module, the module will be available in the the `/etc/apache2/mods-enabled` directory.

10.3. HTTPS Configuration

The mod_ssl module adds an important feature to the Apache2 server - the ability to encrypt communications. Thus, when your browser is communicating using SSL encryption, the https:// prefix is used at the beginning of the Uniform Resource Locator (URL) in the browser navigation bar.

The mod_ssl module is available in apache2-common package. If you have installed this package, you can run the following command from a terminal prompt to enable the mod_ssl module:

```
sudo a2enmod ssl
```

10.3.1. Certificats et sécurité

To set up your secure server, use public key cryptography to create a public and private key pair. In most cases, you send your certificate request (including your public key), proof of your company's identity, and payment to a Certificate Authority (CA). The CA verifies the certificate request and your identity, and then sends back a certificate for your secure server.

Alternatively, you can create your own self-signed certificate. Note, however, that self-signed certificates should not be used in most production environments. Self-signed certificates are not automatically accepted by a user's browser. Users are prompted by the browser to accept the certificate and create the secure connection.

Once you have a self-signed certificate or a signed certificate from the CA of your choice, you need to install it on your secure server.

10.3.2. Types de certificats

You need a key and a certificate to operate your secure server, which means that you can either generate a self-signed certificate or purchase a CA-signed certificate. A CA-signed certificate provides two important capabilities for your server:

- Browsers (usually) automatically recognize the certificate and allow a secure connection to be made without prompting the user.
- When a CA issues a signed certificate, it is guaranteeing the identity of the organization that is providing the web pages to the browser.

Most Web browsers that support SSL have a list of CAs whose certificates they automatically accept. If a browser encounters a certificate whose authorizing CA is not in the list, the browser asks the user to either accept or decline the connection.

You can generate a self-signed certificate for your secure server, but be aware that a self-signed certificate does not provide the same functionality as a CA-signed certificate. A self-signed certificate is not automatically recognized by most Web browsers, and a self-signed certificate does not provide any guarantee concerning the identity of the organization that is providing the website. A CA-signed certificate provides both of these important capabilities for a secure server. The process of getting a certificate from a CA is fairly easy. A quick overview is as follows:

1. Create a private and public encryption key pair.
2. Create a certificate request based on the public key. The certificate request contains information about your server and the company hosting it.
3. Send the certificate request, along with documents proving your identity, to a CA. We cannot tell you which certificate authority to choose. Your decision may be based on your past experiences, or on the experiences of your friends or colleagues, or purely on monetary factors.

   Once you have decided upon a CA, you need to follow the instructions they provide on how to obtain a certificate from them.
4. When the CA is satisfied that you are indeed who you claim to be, they send you a digital certificate.
5. Install this certificate on your secure server, and begin handling secure transactions.

Whether you are getting a certificate from a CA or generating your own self-signed certificate, the first step is to generate a key.

10.3.3. Generating a Certificate Signing Request (CSR)

To generate the Certificate Signing Request (CSR), you should create your own key. You can run the following command from a terminal prompt to create the key:

```
openssl genrsa -des3 -out server.key 1024
```

```
Generating RSA private key, 1024 bit long modulus
.....................++++++
.................++++++
unable to write 'random state'
e is 65537 (0x10001)
Enter pass phrase for server.key:
```

You can now enter your passphrase. For best security, it should at least contain eight characters. The minimum length when specifying -des3 is four characters. It should include numbers and/or punctuation and not be a word in a dictionary. Also remember that your passphrase is case-sensitive.

Re-type the passphrase to verify. Once you have re-typed it correctly, the server key is generated and stored in `server.key` file.

You can also run your secure web server without a passphrase. This is convenient because you will not need to enter the passphrase every time you start your secure web server. But it is highly insecure and a compromise of the key means a compromise of the server as well.

In any case, you can choose to run your secure web server without a passphrase by leaving out the -des3 switch in the generation phase or by issuing the following command at a terminal prompt:

```
openssl rsa -in server.key -out server.key.insecure
```

Once you run the above command, the insecure key will be stored in the `server.key.insecure` file. You can use this file to generate the CSR without passphrase.

To create the CSR, run the following command at a terminal prompt:

```
openssl req -new -key server.key -out server.csr
```

It will prompt you enter the passphrase. If you enter the correct passphrase, it will prompt you to enter Company Name, Site Name, Email Id, etc. Once you enter all these details, your CSR will be created and it will be stored in the `server.csr` file. You can submit this CSR file to a CA for processing. The CAN will use this CSR file and issue the certificate. On the other hand, you can create self-signed certificate using this CSR.

10.3.4. Creating a Self-Signed Certificate

To create the self-signed certificate, run the following command at a terminal prompt:

```
openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
```

The above command will prompt you to enter the passphrase. Once you enter the correct passphrase, your certificate will be created and it will be stored in the `server.crt` file.

> If your secure server is to be used in a production environment, you probably need a CA-signed certificate. It is not recommended to use self-signed certificate.

10.3.5. Installing the Certificate

You can install the key file `server.key` and certificate file `server.crt` or the certificate file issued by your CA by running following commands at a terminal prompt:

```
sudo cp server.crt /etc/ssl/certs
sudo cp server.key /etc/ssl/private
```

You should add the following four lines to the `/etc/apache2/sites-available/default` file or the configuration file for your secure virtual host. You should place them in the *VirtualHost* section. They should be placed under the *DocumentRoot* line:

```
SSLEngine on

SSLOptions +FakeBasicAuth +ExportCertData +CompatEnvVars +StrictRequire

SSLCertificateFile /etc/ssl/certs/server.crt
SSLCertificateKeyFile /etc/ssl/private/server.key
```

HTTPS should listen on port number 443. You should add the following line to the `/etc/apache2/ports.conf` file:

```
Listen 443
```

10.3.6. Accéder au serveur

Once you install your certificate, you should restart your web server. You can run the following command at a terminal prompt to restart your web server:

```
sudo /etc/init.d/apache2 restart
```

> You should remember and enter the passphrase every time you start your secure web server.

You will be prompted to enter the passphrase. Once you enter the correct passphrase, the secure web server will be started. You can access the secure server pages by typing https://your_hostname/url/ in your browser address bar.

10.4. Références

Documentation d'Apache2 [http://httpd.apache.org/docs/2.0/]

Mod SSL Documentation [http://www.modssl.org/docs/]

11. Squid - Proxy Server

Squid is a full-featured web proxy cache server application which provides proxy and cache services for Hyper Text Transport Protocol (HTTP), File Transfer Protocol (FTP), and other popular network protocols. Squid can implement caching and proxying of Secure Sockets Layer (SSL) requests and caching of Domain Name Server (DNS) lookups, and perform transparent caching. Squid also supports a wide variety of caching protocols, such as Internet Cache Protocol, (ICP) the Hyper Text Caching Protocol, (HTCP) the Cache Array Routing Protocol (CARP), and the Web Cache Coordination Protocol. (WCCP)

The Squid proxy cache server is an excellent solution to a variety of proxy and caching server needs, and scales from the branch office to enterprise level networks while providing extensive, granular access control mechanisms and monitoring of critical parameters via the Simple Network Management Protocol (SNMP). When selecting a computer system for use as a dedicated Squid proxy, or caching servers, ensure your system is configured with a large amount of physical memory, as Squid maintains an in-memory cache for increased performance.

11.1. Installation

At a terminal prompt, enter the following command to install the Squid server:

```
sudo apt-get install squid squid-common
```

11.2. Configuration

Squid is configured by editing the directives contained within the `/etc/squid/squid.conf` configuration file. The following examples illustrate some of the directives which may be modified to affect the behavior of the Squid server. For more in-depth configuration of Squid, see the References section.

Prior to editing the configuration file, you should make a copy of the original file and protect it from writing so you will have the original settings as a reference, and to re-use as necessary.

Copy the `/etc/squid/squid.conf` file and protect it from writing with the following commands entered at a terminal prompt:

```
sudo cp /etc/squid/squid.conf /etc/squid/squid.conf.original
sudo chmod a-w /etc/squid/squid.conf.original
```

- To set your Squid server to listen on TCP port 8888 instead of the default TCP port 3128, change the http_port directive as such:

  http_port 8888

- Change the visible_hostname directive in order to give the Squid server a specific hostname. This hostname does not necessarily need to be the computer's hostname. In this example it is set to *weezie*

  visible_hostname weezie

- Again, Using Squid's access control, you may configure use of Internet services proxied by Squid to be available only users with certain Internet Protocol (IP) addresses. For example, we willll illustrate access by users of the 192.168.42.0/24 subnetwork only:

  Add the following to the **bottom** of the ACL section of your `/etc/squid/squid.conf` file:

  acl fortytwo_network src 192.168.42.0/24

  Then, add the following to the **top** of the http_access section of your `/etc/squid/squid.conf` file:

  http_access allow fortytwo_network

- Using the excellent access control features of Squid, you may configure use of Internet services proxied by Squid to be available only during normal business hours. For example, we'll illustrate access by employees of a business which is operating between 9:00AM and 5:00PM, Monday through Friday, and which uses the 10.1.42.0/42 subnetwork:

  Add the following to the **bottom** of the ACL section of your `/etc/squid/squid.conf` file:

  acl biz_network src 10.1.42.0/24 acl biz_hours time M T W T F 9:00-17:00

  Then, add the following to the **top** of the http_access section of your `/etc/squid/squid.conf` file:

  http_access allow biz_network biz_hours

After making changes to the `/etc/squid/squid.conf` file, save the file and restart the squid server application to effect the changes using the following command entered at a terminal prompt:

```
sudo /etc/init.d/squid restart
```

11.3. Références

Squid Website [http://www.squid-cache.org/]

12. Version Control System

Version control is the art of managing changes to information. It has long been a critical tool for programmers, who typically spend their time making small changes to software and then undoing those changes the next day. But the usefulness of version control software extends far beyond the bounds of the software development world. Anywhere you can find people using computers to manage information that changes often, there is room for version control.

12.1. Subversion

Subversion is an open source version control system. Using Subversion, you can record the history of source files and documents. It manages files and directories over time. A tree of files is placed into a central repository. The repository is much like an ordinary file server, except that it remembers every change ever made to files and directories.

12.1.1. Installation

To access Subversion repository using the HTTP protocol, you must install and configure a web server. Apache2 is proven to work with Subversion. Please refer to the HTTP subsection in the Apache2 section to install and configure Apache2. To access the Subversion repository using the HTTPS protocol, you must install and configure a digital certificate in your Apache 2 web server. Please refer to the HTTPS subsection in the Apache2 section to install and configure the digital certificate.

To install Subversion, run the following command from a terminal prompt:

```
sudo apt-get install subversion libapache2-svn
```

12.1.2. Server Configuration

This step assumes you have installed above mentioned packages on your system. This section explains how to create a Subversion repository and access the project.

12.1.2.1. Create Subversion Repository

The Subversion repository can be created using the following command from a terminal prompt:

```
svnadmin create /path/to/repos/project
```

12.1.3. Access Methods

Subversion repositories can be accessed (checked out) through many different methods --on local disk, or through various network protocols. A repository location, however, is always a URL. The table describes how different URL schemas map to the available access methods.

Tableau 4.1. Access Methods

Schema	**Access Method**
file://	direct repository access (on local disk)
http://	Access via WebDAV protocol to Subversion-aware Apache2 web server
https://	Same as http://, but with SSL encryption
svn://	Access via custom protocol to an svnserve server
svn+ssh://	Same as svn://, but through an SSH tunnel

In this section, we will see how to configure Subversion for all these access methods. Here, we cover the basics. For more advanced usage details, refer to the *svn book* [http://svnbook.red-bean.com/].

12.1.3.1. Direct repository access (file://)

This is the simplest of all access methods. It does not require any Subversion server process to be running. This access method is used to access Subversion from the same machine. The syntax of the command, entered at a terminal prompt, is as follows:

```
svn co file:///chemin/vers/depot/nomduprojet
```

ou

```
svn co file://localhost/chemin/vers/depot/nomduprojet
```

> If you do not specify the hostname, there are three forward slashes (///) -- two for the protocol (file, in this case) plus the leading slash in the path. If you specify the hostname, you must use two forward slashes (//).

The repository permissions depend on filesystem permissions. If the user has read/write permission, he can checkout from and commit to the repository.

12.1.3.2. Access via WebDAV protocol (http://)

To access the Subversion repository via WebDAV protocol, you must configure your Apache 2 web server. You must add the following snippet in your `/etc/apache2/apache2.conf` file:

```
 <Location /svn>
```

```
  DAV svn
  SVNPath /path/to/repos
  AuthType Basic
  AuthName "Your repository name"
  AuthUserFile /etc/subversion/passwd
  <LimitExcept GET PROPFIND OPTIONS REPORT>
  Require valid-user
  </LimitExcept>
  </Location>
```

Next, you must create the `/etc/subversion/passwd` file. This file contains user authentication details. To add an entry, i.e. to add a user, you can run the following command from a terminal prompt:

```
htpasswd2 /etc/subversion/passwd nom_utilisateur
```

This command will prompt you to enter the password. Once you enter the password, the user is added. Now, to access the repository you can run the following command:

```
svn co http://nomduserveur/svn
```

The password is transmitted as plain text. If you are worried about password snooping, you are advised to use SSL encryption. For details, please refer next section.

12.1.3.3. Access via WebDAV protocol with SSL encryption (https://)

Accessing Subversion repository via WebDAV protocol with SSL encryption (https://) is similar to http:// except that you must install and configure the digital certificate in your Apache2 web server.

You can install a digital certificate issued by a signing authority like Verisign. Alternatively, you can install your own self-signed certificate.

This step assumes you have installed and configured a digital certificate in your Apache 2 web server. Now, to access the Subversion repository, please refer to the above section! The access methods are exactly the same, except the protocol. You must use https:// to access the Subversion repository.

12.1.3.4. Access via custom protocol (svn://)

Once the Subversion repository is created, you can configure the access control. You can edit the `/path/to/repos/project/conf/svnserve.conf` file to configure the access control. For example, to set up authentication, you can uncomment the following lines in the configuration file:

```
# [general]
# password-db = passwd
```

After uncommenting the above lines, you can maintain the user list in the passwd file. So, edit the file `passwd` in the same directory and add the new user. The syntax is as follows:

```
username = password
```

For more details, please refer to the file.

Now, to access Subversion via the svn:// custom protocol, either from the same machine or a different machine, you can run svnserver using svnserve command. The syntax is as follows:

```
$ svnserve -d --foreground -r /path/to/repos
# -d -- daemon mode
# --foreground -- run in foreground (useful for debugging)
# -r -- root of directory to serve

For more usage details, please refer to:
$ svnserve --help
```

Once you run this command, Subversion starts listening on default port (3690). To access the project repository, you must run the following command from a terminal prompt:

```
svn co svn://nom_hote/projet project --username nom_utilisateur
```

Based on server configuration, it prompts for password. Once you are authenticated, it checks out the code from Subversion repository. To synchronize the project repository with the local copy, you can run the **update** sub-command. The syntax of the command, entered at a terminal prompt, is as follows:

```
cd repertoire_du_projet ; svn update
```

For more details about using each Subversion sub-command, you can refer to the manual. For example, to learn more about the co (checkout) command, please run the following command from a terminal prompt:

```
svn co help
```

12.1.3.5. Access via custom protocol with SSL encryption (svn+ssh://)

The configuration and server process is same as in the svn:// method. For details, please refer to the above section. This step assumes you have followed the above step and started the#Subversion server using svnserve command.

It is also assumed that the ssh server is running on that machine and that it is allowing incoming connections. To confirm, please try to login to that machine using ssh. If you can login, everything is perfect. If you cannot login, please address it before continuing further.

The svn+ssh:// protocol is used to access the Subversion repository using SSL encryption. The data transfer is encrypted using this method. To access the project repository (for example with a checkout), you must use the following command syntax:

```
svn co svn+ssh://hostname/var/svn/repos/project
```

? You must use the full path (/path/to/repos/project) to access the Subversion repository using this access method.

Based on server configuration, it prompts for password. You must enter the password you use to login via ssh. Once you are authenticated, it checks out the code from the Subversion repository.

12.2. Serveur CVS

CVS is a version control system. You can use it to record the history of source files.

12.2.1. Installation

At a terminal prompt, enter the following command to install cvs:

```
sudo apt-get install cvs
```

After you install cvs, you should install xinetd to start/stop the cvs server. At the prompt, enter the following command to install xinetd:

```
sudo apt-get install xinetd
```

12.2.2. Configuration

Once you install cvs, the repository will be automatically initialized. By default, the repository resides under the /var/lib/cvs directory. You can change this path by running following command:

```
cvs -d /your/new/cvs/repo init
```

Once the initial repository is set up, you can configure xinetd to start the CVS server. You can copy the following lines to the `/etc/xinetd/cvspserver` file.

```
service cvspserver
{
     port = 2401
     socket_type = stream
     protocol = tcp
     user = root
     wait = no
     type = UNLISTED
     server = /usr/bin/cvs
     server_args = -f --allow-root /var/lib/cvs pserver
     disable = no
}
```

Be sure to edit the repository if you have changed the default repository (/var/lib/cvs) directory.

Once you have configured xinetd you can start the cvs server by running following command:

```
sudo /etc/init.d/xinetd start
```

You can confirm that the CVS server is running by issuing the following command:

```
sudo netstat -tap | grep cvs
```

When you run this command, you should see the following line or something similar:

```
tcp 0 0 *:cvspserver *:* LISTEN
```

From here you can continue to add users, add new projects, and manage the CVS server.

CVS allows the user to add users independently of the underlying OS installation. Probably the easiest way is to use the Linux Users for CVS, although it has potential security issues. Please refer to the CVS manual for details.

12.2.3. Add Projects

This section explains how to add new project to the CVS repository. Create the directory and add necessary document and source files to the directory. Now, run the following command to add this project to CVS repository:

```
cd your/project
cvs import -d :pserver:username@hostname.com:/var/lib/cvs -m "Importing my project to CVS
```

You can use the CVSROOT environment variable to store the CVS root directory. Once you export the CVSROOT environment variable, you can avoid using -d option to above cvs command.

The string *new_project* is a vendor tag, and *start* is a release tag. They serve no purpose in this context, but since CVS requires them, they must be present.

When you add a new project, the CVS user you use must have write access to the CVS repository (/var/lib/cvs). By default, the src group has write access to the

CVS repository. So, you can add the user to this group, and he can then add and manage projects in the CVS repository.

12.3. Références

Subversion Home Page [http://subversion.tigris.org/]

Subversion Book [http://svnbook.red-bean.com/]

CVS Manual [http://ximbiot.com/cvs/manual/cvs-1.11.21/cvs_toc.html]

13. Bases de données

Ubuntu provides two Database servers. They are:

- MySQL™
- PostgreSQL

They are available in the main repository. This section explains how to install and configure these database servers.

13.1. MySQL

MySQL is a fast, multi-threaded, multi-user, and robust SQL database server. It is intended for mission-critical, heavy-load production systems as well as for embedding into mass-deployed software.

13.1.1. Installation

To install MySQL, run the following command from a terminal prompt:

```
sudo apt-get install mysql-server mysql-client
```

Once the installation is complete, the MySQL server should be started automatically. You can run the following command from a terminal prompt to check whether the MySQL server is running:

```
sudo netstat -tap | grep mysql
```

When you run this command, you should see the following line or something similar:

```
tcp 0 0 localhost.localdomain:mysql *:* LISTEN -
```

If the server is not running correctly, you can type the following command to start it:

```
sudo /etc/init.d/mysql restart
```

13.1.2. Configuration

By default, the administrator password is not set. Once you install MySQL, the first thing you must do is to configure the MySQL administrator password. To do this, run the following commands:

```
sudo mysqladmin -u root password nouveau_mot_de_passe_sql
sudo mysqladmin -u root -h localhost password nouveau_mot_de_passe_sql
```

You can edit the `/etc/mysql/my.cnf` file to configure the basic settings -- log file, port number, etc. Refer to `/etc/mysql/my.cnf` file for more details.

13.2. PostgreSQL

PostgreSQL is an object-relational database system that has the features of traditional commercial database systems with enhancements to be found in next-generation DBMS systems.

13.2.1. Installation

To install PostgreSQL, run the following command in the command prompt:

```
sudo apt-get install postgresql
```

Once the installation is complete, you should configure the PostgreSQL server based on your needs, although the default configuration is viable.

13.2.2. Configuration

By default, connection via TCP/IP is disabled. PostgreSQL supports multiple client authentication methods. By default, IDENT authentication method is used. Please refer *the PostgreSQL Administrator's Guide* [http://www.postgresql.org/docs/8.1/static/admin.html].

The following discussion assumes that you wish to enable TCP/IP connections and use the MD5 method for client authentication. PostgreSQL configuration files are stored in the `/etc/postgresql/<version>/main` directory. For example, if you install PostgreSQL 7.4, the configuration files are stored in the `/etc/postgresql/7.4/main` directory.

To configure ident authentication, add entries to the `/etc/postgresql/7.4/main/pg_ident.conf` file.

To enable TCP/IP connections, edit the file `/etc/postgresql/7.4/main/postgresql.conf`

Locate the line *#tcpip_socket = false* and change it to *tcpip_socket = true*. You may also edit all other parameters, if you know what you are doing! For details, refer to the configuration file or to the PostgreSQL documentation.

By default, the user credentials are not set for *MD5* client authentication. So, first it is necessary to configure the PostgreSQL server to use *trust* client authentication, connect to the database, configure the password, and revert the configuration back to use *MD5* client authentication. To enable *trust* client authentication, edit the file `/etc/postgresql/7.4/main/pg_hba.conf`

Comment out all the existing lines which use *ident* and *MD5* client authentication and add the following line:

```
local all postgres trust sameuser
```

Then, run the following command to start the PostgreSQL server:

```
sudo /etc/init.d/postgresql start
```

Once the PostgreSQL server is successfully started, run the following command at a terminal prompt to connect to the default PostgreSQL template database

```
psql -U postgres -d template1
```

The above command connects to PostgreSQL database *template1* as user *postgres*. Once you connect to the PostgreSQL server, you will be at a SQL prompt. You can run the following SQL command at the psql prompt to configure the password for the user *postgres*.

```
template1=# ALTER USER postgres with encrypted password 'your_password';
```

After configuring the password, edit the file `/etc/postgresql/7.4/main/pg_hba.conf` to use *MD5* authentication:

Comment the recently added *trust* line and add the following line:

```
local all postgres md5 sameuser
```

The above configuration is not complete by any means.
Please refer *the PostgreSQL Administrator's Guide* [http://www.postgresql.org/docs/8.1/static/admin.html] to configure more parameters.

14. Email Services

The process of getting an email from one person to another over a network or the Internet involves many systems working together. Each of these systems must be correctly configured for the process to work. The sender uses a *Mail User Agent* (MUA), or email client, to send the message through one or more *Mail Transfer Agents* (MTA), the last of which will hand it off to a *Mail Delivery Agent* (MDA) for delivery to the recipient's mailbox, from which it will be retrieved by the recipient's email client, usually via a POP3 or IMAP server.

14.1. Postfix

Postfix is the default Mail Transfer Agent (MTA) in Ubuntu. It attempts to be fast and easy to administer and secure. It is compatible with the MTA sendmail. This section explains how to install and configure postfix. It also explains how to set it up as an SMTP server using a secure connection (for sending emails securely).

14.1.1. Installation

To install postfix with SMTP-AUTH and Transport Layer Security (TLS), run the following command:

```
sudo apt-get install postfix
```

Simply press return when the installation process asks questions, the configuration will be done in greater detail in the next stage.

14.1.2. Configuration de base

To configure postfix, run the following command:

```
sudo dpkg-reconfigure postfix
```

The user interface will be displayed. On each screen, select the following values:

- OK
- Site Internet
- NONE
- mail.example.com
- mail.example.com, localhost.localdomain, localhost
- Non
- 127.0.0.0/8
- Oui
- 0
- +

- AUCUN(E)

Replace mail.example.com with your mail server hostname.

14.1.3. Authentification SMTP

The next steps are to configure postfix to use SASL for SMTP AUTH. Rather than editing the configuration file directly, you can use the **postconf** command to configure all postfix parameters. The configuration parameters will be stored in `/etc/postfix/main.cf` file. Later if you wish to re-configure a particular parameter, you can either run the command or change it manually in the file.

1. Configure Postfix to do SMTP AUTH using SASL (saslauthd):

```
postconf -e 'smtpd_sasl_local_domain ='
postconf -e 'smtpd_sasl_auth_enable = yes'
postconf -e 'smtpd_sasl_security_options = noanonymous'
postconf -e 'broken_sasl_auth_clients = yes'
postconf -e 'smtpd_recipient_restrictions = permit_sasl_authenticated,permit_mynetwork
postconf -e 'inet_interfaces = all'
echo 'pwcheck_method: saslauthd' >> /etc/postfix/sasl/smtpd.conf
echo 'mech_list: plain login' >> /etc/postfix/sasl/smtpd.conf
```

2. Next, configure the digital certificate for TLS. When asked questions, follow the instructions and answer appropriately.

```
openssl genrsa -des3 -rand /etc/hosts -out smtpd.key 1024
chmod 600 smtpd.key
openssl req -new -key smtpd.key -out smtpd.csr
openssl x509 -req -days 3650 -in smtpd.csr -signkey smtpd.key -out smtpd.crt
openssl rsa -in smtpd.key -out smtpd.key.unencrypted
mv -f smtpd.key.unencrypted smtpd.key
openssl req -new -x509 -extensions v3_ca -keyout cakey.pem -out cacert.pem -days 3650
mv smtpd.key /etc/ssl/private/
mv smtpd.crt /etc/ssl/certs/
mv cakey.pem /etc/ssl/private/
mv cacert.pem /etc/ssl/certs/
```

   You can get the digital certificate from a certificate authority. Alternatively, you can create the certificate yourself. Refer to *Section 10.3.4, « Creating a Self-Signed Certificate » [53]* for more details.

3. Configure Postfix to do TLS encryption for both incoming and outgoing mail:

```
postconf -e 'smtpd_tls_auth_only = no'
postconf -e 'smtp_use_tls = yes'
postconf -e 'smtpd_use_tls = yes'
postconf -e 'smtp_tls_note_starttls_offer = yes'
postconf -e 'smtpd_tls_key_file = /etc/ssl/private/smtpd.key'
postconf -e 'smtpd_tls_cert_file = /etc/ssl/certs/smtpd.crt'
postconf -e 'smtpd_tls_CAfile = /etc/ssl/certs/cacert.pem'
postconf -e 'smtpd_tls_loglevel = 1'
postconf -e 'smtpd_tls_received_header = yes'
postconf -e 'smtpd_tls_session_cache_timeout = 3600s'
postconf -e 'tls_random_source = dev:/dev/urandom'
postconf -e 'myhostname = mail.example.com'
```

After you run all the commands, the SMTP AUTH is configured with postfix. The self-signed cerficiate is created for TLS and it is configured with postfix.

Now, the file `/etc/postfix/main.cf` should look like *this* [../sample/postfix_configuration].

The postfix initial configuration is complete. Run the following command to start postfix daemon:

```
sudo /etc/init.d/postfix start
```

Now the postfix daemon is installed, configured and run successfully. Postfix supports SMTP AUTH as defined in *RFC2554* [ftp://ftp.isi.edu/in-notes/rfc2554.txt]. It is based on *SASL* [ftp://ftp.isi.edu/in-notes/rfc2222.txt]. However it is still necessary to set up SASL authentication before you can use SMTP.

14.1.4. Configuring SASL

The libsasl2, sasl2-bin and libsasl2-modules are necessary to enable SMTP AUTH using SASL. You can install these applications if you have not installed them already.

```
apt-get install libsasl2 sasl2-bin
```

A few changes are necessary to make it work properly. Because Postfix runs chrooted in `/var/spool/postfix`, SASL needs to be configured to run in the false root (`/var/run/saslauthd` becomes `/var/spool/postfix/var/run/saslauthd`):

```
mkdir -p /var/spool/postfix/var/run/saslauthd
rm -rf /var/run/saslauthd
```

To activate saslauthd, edit the file `/etc/default/saslauthd`, and change or add the START variable. In order to configure saslauthd to run in the false root, add the PWDIR, PIDFILE and PARAMS variables. Finally, configure the MECHANISMS variable to your liking. The file should look like this:

```
# This needs to be uncommented before saslauthd will be run
# automatically
START=yes
```

```
PWDIR="/var/spool/postfix/var/run/saslauthd"
PARAMS="-m ${PWDIR}"
PIDFILE="${PWDIR}/saslauthd.pid"

# You must specify the authentication mechanisms you wish to use.
# This defaults to "pam" for PAM support, but may also include
# "shadow" or "sasldb", like this:
# MECHANISMS="pam shadow"

MECHANISMS="pam"
```

If you prefer, you can use **shadow** instead of **pam**. This will use MD5 hashed password transfer and is perfectly secure. The username and password needed to authenticate will be those of the users on the system you are using on the server.

Next, update the dpkg "state" of `/var/spool/portfix/var/run/saslauthd`. The saslauthd init script uses this setting to create the missing directory with the appropriate permissions and ownership:

```
dpkg-statoverride --force --update --add root sasl 755 /var/spool/postfix/var/run/saslauth
```

14.1.5. Testing

SMTP AUTH configuration is complete. Now it is time to start and test the setup. You can run the following command to start the SASL daemon:

```
sudo /etc/init.d/saslauthd start
```

To see if SMTP-AUTH and TLS work properly, run the following command:

```
telnet mail.example.com 25
```

After you have established the connection to the postfix mail server, type:

```
ehlo mail.example.com
```

If you see the following lines among others, then everything is working perfectly. Type **quit** to exit.

```
250-STARTTLS
250-AUTH LOGIN PLAIN
250-AUTH=LOGIN PLAIN
250 8BITMIME
```

14.2. Exim4

Exim4 is is another Message Transfer Agent (MTA) developed at the University of Cambridge for use on Unix systems connected to the internet. Exim can be installed in place of sendmail, although the configuration of exim is quite different to that of sendmail.

14.2.1. Installation

To install exim4, run the following command:

```
sudo apt-get install exim4 exim4-base exim4-config
```

14.2.2. Configuration

To configure exim4, run the following command:

```
sudo dpkg-reconfigure exim4-config
```

The user interface will be displayed. The user interface lets you configure many parameters. For example, In exim4 the configuration files are split among multiple files. If you wish to have them in one file you can configure accordingly in this user interface.

All the parameters you configure in the user interface are stored in `/etc/exim4/update-exim4.conf.conf` file. If you wish to re-configure, either you re-run the configuration wizard or manually edit this file using your favourite editor. Once you configure, you can run the following command to generate the master configuration file:

```
sudo update-exim4.conf
```

The master configuration file, is generated and it is stored in `/var/lib/exim4/config.autogenerated`.

⛒ At any time, you should not edit the master configuration file, `/var/lib/exim4/config.autogenerated` manually. It is updated automatically every time you run **update-exim4.conf**

You can run the following command to start exim4 daemon.

```
sudo /etc/init.d/exim4 start
```

TODO: This section should cover configuring SMTP AUTH with exim4.

14.3. Serveur Dovecot

Dovecot is a Mail Delivery Agent, written with security primarily in mind. It supports the major mailbox formats: mbox or Maildir. This section explain how to set it up as an imap or pop3 server.

14.3.1. Installation

To install dovecot, run the following command in the command prompt:

```
sudo apt-get install dovecot-common dovecot-imapd dovecot-pop3d
```

14.3.2. Configuration

To configure dovecot, you can edit the file `/etc/dovecot/dovecot.conf`. You can choose the protocol you use. It could be pop3, pop3s (pop3 secure), imap and imaps (imap secure). A description of these protocols is beyond the scope of this guide. For further information, refer to the wikipedia articles on *POP3* [http://en.wikipedia.org/wiki/POP3] and *IMAP* [http://en.wikipedia.org/wiki/Internet_Message_Access_Protocol].

IMAPS and POP3S are more secure that the simple IMAP and POP3 because they use SSL encryption to connect. Once you have chosen the protocol, amend the following line in the file `/etc/dovecot/dovecot.conf`:

```
protocols = pop3 pop3s imap imaps
```

It enables the protocols when dovecot is started. Next, add the following line in pop3 section in the file `/etc/dovecot/dovecot.conf`:

```
pop3_uidl_format = %08Xu%08Xv
```

Next, choose the mailbox you use. Dovecot supports **maildir** and **mbox** formats. These are the most commonly used mailbox formats. They both have their own benefits and they are discussed on *the dovecot website* [http://dovecot.org/doc/configuration.txt].

Once you have chosen your mailbox type, edit the file `/etc/dovecot/dovecot.conf` and change the following line:

```
default_mail_env = maildir:~/Maildir # (pour maildir)
ou
default_mail_env = mbox:~/mail:INBOX=/var/spool/mail/%u # (pour mbox)
```

You should configure your Mail Trasport Agent (MTA) to transfer the incoming mail to this type of mailbox if it is different from the one you have configured.

Once you have configured dovecot, start the dovecot daemon in order to test your setup:

```
sudo /etc/init.d/dovecot start
```

If you have enabled imap, or pop3, you can also try to log in with the commands **telnet localhost pop3** or **telnet localhost** imap2. If you see something like the following, the installation has been successful:

```
bhuvan@rainbow:~$ telnet localhost pop3
Trying 127.0.0.1...
```

```
Connected to localhost.localdomain.
Escape character is '^]'.
+OK Dovecot ready.
```

14.3.3. Dovecot SSL Configuration

To configure dovecot to use SSL, you can edit the file `/etc/dovecot/dovecot.conf` and amend following lines:

```
ssl_cert_file = /etc/ssl/certs/dovecot.pem
ssl_key_file = /etc/ssl/private/dovecot.pem
ssl_disable = no
disable_plaintext_auth = no
```

The **cert** and **key** files are created automatically by dovecot when you install it. Please note that these keys are not signed and will give "bad signature" errors when connecting from a client. To avoid this, you can use commercial certificates, or even better, you can use your own SSL certificates.

14.3.4. Firewall Configuration for an Email Server

To access your mail server from another computer, you must configure your firewall to allow connections to the server on the necessary ports.

- IMAP - 143
- IMAPS - 993
- POP3 - 110
- POP3S - 995

14.4. Mailman

Mailman is an open source program for managing electronic mail discussions and e-newsletter lists. Many open source mailing lists (including all the *Ubuntu mailing lists* [http://lists.ubuntu.com]) use Mailman as their mailing list software. It is powerful and easy to install and maintain.

14.4.1. Installation

Mailman provides a web interface for the administrators and users. So, it requires apache with mod_perl support. Mailman uses an external mail server to send and receive emails. It works perfectly with the following mail servers:

- Postfix
- Exim
- Sendmail

- Qmail

We will see how to install mailman, the apache web server and the Exim mail server. If you wish to install mailman with a different mail server, please refer to the references section.

14.4.1.1. Apache2

To install apache2 you refer to *Section 10.1, « Installation » [46]*.

14.4.1.2. Exim4

To install Exim4 you run the following commands at a terminal prompt:

```
sudo apt-get install exim4
sudo apt-get install exim4-base
sudo apt-get install exim4-config
```

Once exim4 is installed, the configuration files are stored in the `/etc/exim4` directory. In ubuntu, by default, the exim4 configuration files are split across different files. You can change this behavior by changing the following variable in the `/etc/exim4/update-exim4.conf` file:

- dc_use_split_config='true'

14.4.1.3. Mailman

To install Mailman, run following command at a terminal prompt:

```
sudo apt-get install mailman
```

It copies the installation files in /var/lib/mailman directory. It installs the CGI scripts in /usr/lib/cgi-bin/mailman directory. It creates *list* linux user. It creates the *list* linux group. The mailman process will be owned by this user.

14.4.2. Configuration

This section assumes you have successfully installed mailman, apache2, and exim4. Now you just need to configure them.

14.4.2.1. Apache2

Once apache2 is installed, you can add the following lines in the `/etc/apache2/apache2.conf` file:

```
Alias /images/mailman/ "/usr/share/images/mailman/"
Alias /pipermail/ "/var/lib/mailman/archives/public/"
```

Mailman uses apache2 to render its CGI scripts. The mailman CGI scripts are installed in the /usr/lib/cgi-bin/mailman directory. So, the mailman url will be http://hostname/cgi-bin/mailman/. You can make changes to the `/etc/apache2/apache2.conf` file if you wish to change this behavior.

14.4.2.2. Exim4

Once Exim4 is installed, you can start the Exim server using the following command from a terminal prompt:

```
sudo apt-get /etc/init.d/exim4 start
```

In order to make mailman work with exim4, you need to configure exim4. As mentioned earlier, by default, exim4 uses multiple configuration files of different types. For details, please refer to the *Exim* [http://www.exim.org] website. To run mailman, we should add new a configuration file to the following configuration types:

- Main
- Transport
- Router

Exim creates a master configuration file by sorting all these mini configuration files. So, the order of these configuration files is very important.

14.4.2.3. Main

All the configuration files belonging to the main type are stored in the `/etc/exim4/conf.d/main/` directory. You can add the following content to a new file, named `04_exim4-config_mailman`:

```
# start
# Home dir for your Mailman installation -- aka Mailman's prefix
# directory.
# On Ubuntu this should be "/var/lib/mailman"
# This is normally the same as ~mailman
MM_HOME=/var/lib/mailman
#
# User and group for Mailman, should match your --with-mail-gid
# switch to Mailman's configure script. Value is normally "mailman"
MM_UID=list
MM_GID=list
#
# Domains that your lists are in - colon separated list
# you may wish to add these into local_domains as well
domainlist mm_domains=hostname.com
#
# -=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
#
```

```
# These values are derived from the ones above and should not need
# editing unless you have munged your mailman installation
#
# The path of the Mailman mail wrapper script
MM_WRAP=MM_HOME/mail/mailman
#
# The path of the list config file (used as a required file when
# verifying list addresses)
MM_LISTCHK=MM_HOME/lists/${lc::$local_part}/config.pck
# end
```

14.4.2.4. Transport

All the configuration files belonging to transport type are stored in the `/etc/exim4/conf.d/transport/` directory. You can add the following content to a new file named `40_exim4-config_mailman`:

```
  mailman_transport:
   driver = pipe
   command = MM_WRAP \
               '${if def:local_part_suffix \
                     {${sg{$local_part_suffix}{-(\\w+)(\\+.*)?}{\$1}}} \
                     {post}}' \
               $local_part
    current_directory = MM_HOME
    home_directory = MM_HOME
    user = MM_UID
    group = MM_GID
```

14.4.2.5. Router

All the configuration files belonging to router type are stored in the `/etc/exim4/conf.d/router/` directory. You can add the following content in to a new file named `101_exim4-config_mailman`:

```
  mailman_router:
   driver = accept
   require_files = MM_HOME/lists/$local_part/config.pck
   local_part_suffix_optional
   local_part_suffix = -bounces : -bounces+* : \
                    -confirm+* : -join : -leave : \
                    -owner : -request : -admin
   transport = mailman_transport
```

The order of main and transport configuration files can be in any order. But, the order of router configuration files must be the same. This particular file must appear before the 200_exim4-config_primary file. These two configuration files contain same type of information. The first file takes the precedence. For more details, please refer to the references section.

14.4.2.6. Mailman

Once mailman is installed, you can run it using the following command:

```
sudo /etc/init.d/mailman start
```

Once mailman is installed, you should create the default mailing list. Run the following command to create the mailing list:

```
sudo /usr/sbin/newlist mailman
```

```
  Enter the email address of the person running the list: bhuvan at ubuntu.com
  Initial mailman password:
  To finish creating your mailing list, you must edit your /etc/aliases (or
  equivalent) file by adding the following lines, and possibly running the
  `newaliases' program:

  ## mailman mailing list
  mailman: "|/var/lib/mailman/mail/mailman post mailman"
  mailman-admin: "|/var/lib/mailman/mail/mailman admin mailman"
  mailman-bounces: "|/var/lib/mailman/mail/mailman bounces mailman"
  mailman-confirm: "|/var/lib/mailman/mail/mailman confirm mailman"
  mailman-join: "|/var/lib/mailman/mail/mailman join mailman"
  mailman-leave: "|/var/lib/mailman/mail/mailman leave mailman"
  mailman-owner: "|/var/lib/mailman/mail/mailman owner mailman"
  mailman-request: "|/var/lib/mailman/mail/mailman request mailman"
  mailman-subscribe: "|/var/lib/mailman/mail/mailman subscribe mailman"
  mailman-unsubscribe: "|/var/lib/mailman/mail/mailman unsubscribe mailman"

  Hit enter to notify mailman owner...

  #
```

We have configured exim to recognize all emails from mailman. So, it is not mandatory to make any new entries in `/etc/aliases`. If you have made any changes to the configuration files, please ensure that you restart those services before continuing to next section.

14.4.3. Administration

We assume you have a default installation. The mailman cgi scripts are still in /usr/lib/cgi-bin/mailman/ directory. Mailman provides a web based administration facility. To access this page, point your browser to the following url:

http://hostname/cgi-bin/mailman/admin

The default mailing list, *mailman*, will appear in this screen. If you click the mailing list name, it will ask for your authentication password. If you enter the correct password, you will be able to change administrative settings of this mailing list. You can create a new mailing list using command line utility (**/usr/sbin/newlist**). Alternatively, you can create a new mailing list using web interface.

14.4.4. Utilisateurs

Mailman provides a web based interface for users. To access this page, point your browser to the following url:

http://hostname/cgi-bin/mailman/listinfo

The default mailing list, *mailman*, will appear in this screen. If you click the mailing list name, it will display the subscription form. You can enter your email address, name (optional), and password to subscribe. An email invitation will be sent to you. You can follow the instructions in the email to subscribe.

14.4.5. Références

GNU Mailman - Manuel d'installation [http://www.list.org/mailman-install/index.html]

Guide partique - Utiliser Exim4 avec Mailman 2.1
[http://www.exim.org/howto/mailman21.html]

Chapitre 5. Réseaux Windows

Les réseaux d'ordinateurs sont souvent composés de systèmes divers et, même si opérer un réseau constitué entièrement de serveurs et de postes d'utilisateur Ubuntu serait plaisant, certains environnements réseau doivent comprendre à la fois des systèmes Ubuntu et Microsoft®Windows® travaillant ensemble en harmonie. Cette section du Guide du Serveur Ubuntu présente les principes et les outils utilisés afin de configurer votre serveur Ubuntu pour le partage des ressources réseau avec des ordinateurs Windows.

1. Introduction

Pour établir avec succès un réseau entre votre système Ubuntu et des clients Windows, il faut fournir et intégrer les services utilisés courament dans les environnements Windows. Ces services assistent aux transfert de données et d'information sur les ordinateurs et utilisateurs existant dans le réseau. Ils peuvent être classifiés en trois catégories principales selon leur fonctionalité.

- **Services de partage de fichiers et d'imprimantes**. Utiliser le protocole Server Message Block (SMB) pour faciliter le partage de fichiers, de dossiers, de volumes et d'imprimantes à travers le réseau.
- **Services d'annuaire**. Partager l'information vitale sur les ordinateurs et utilisateurs du réseau avec des technologies telles que le Lightweight Directory Access Protocol (LDAP) et le Microsoft Active Directory®.
- **Authentification et accès**. Établir l'identité d'un ordinateur ou d'un utilisateur et déterminer l'information à laquelle l'ordinateur ou l'utilisateur a l'autorisation d'accéder en utilisant des principes et technologies telles les permissions sur les fichiers, les politiques de groupes, et le service d'authentification Kerberos.

Heureusement, votre système Ubuntu peut fournir tous ces services aux clients Windows et partager les ressources réseau avec eux. Un des principaux composants de votre système Ubuntu pour la réseautique Windows est la suite SAMBA d'outils et d'applications pour serveur SMB. Cette section du Guide serveur d'Ubuntu présentera brièvement l'installation et la configuration de base de la suite SAMBA. La documentation et l'information additionnelle et détaillée sur SAMBA dépassent le but du présent document mais peuvent être trouvées sur le *site web SAMBA* [http://www.samba.org].

2. Installer SAMBA

A l'invite système, entrez la commande suivante pour installer les applications serveur SAMBA :

```
sudo apt-get install samba
```

3. Configurer SAMBA

Vous pouvez configurer le serveur SAMBA en éditant le fichier `/etc/samba/smb.conf` pour modifier les paramètres par défaut ou en ajouter des nouveaux. De l'information supplémentaire sur chaque paramètre est disponible dans les commentaires du fichier `/etc/samba/smb.conf` ou en regardant la page manuel du fichier `/etc/samba/smb.conf` en entrant la commande suivante dans un terminal :

```
man smb.conf
```

Avant de modifier le fichier de configuration, vous devriez faire une copie du fichier original et le protéger contre l'écriture pour avoir les paramètres originaux comme référence et ainsi le réutiliser si nécessaire.

Sauvegardez le fichier `/etc/samba/smb.conf` :

```
sudo cp /etc/samba/smb.conf /etc/samba/smb.conf.original
```

Maintenant, éditez le fichier `/etc/samba/smb.conf` et faites vos modifications.

3.1. Serveur

En supplément de la suite d'applications serveur SAMBA de partage de fichiers et d'imprimantes, Ubuntu inclus aussi d'autres applications serveur puissantes destinées à fournir des fonctionnalités réseau supplémentaires et similaires à celles fournies par les serveurs Windows aux clients Windows. Par exemple, Ubuntu offre une gestion centralisée des ressources réseau telles que les ordinateurs ou les utilisateurs grâce à Directory Services, et facilite l'identification et la gestion des permissions des ordinateurs et des utilisateurs grâce à Authentication Services.

Les sections suivantes évoqueront plus en détails SAMBA et les technologies associées, telles que le serveur Lightweight Directory Access Protocol (LDAP) ou le serveur d'authentification Kerberos. Vous apprendrez aussi quelques directives de configuration disponibles pour SAMBA qui facilitent l'intégration dans un réseau comportant des clients et des serveurs Windows.

3.1.1. Active Directory

Active Directory est une implémentation propriétaire de Microsoft des services d'annuaire et est utilisé pour partager l'information sur les ressources réseau et utilisateurs. En plus de fournir une source centralisée de cette information, Active Directory agit aussi comme autorité centralisée de l'authentification sécuritaire pour le réseau. Active Directory, qui combine des capacités traditionnellement trouvées dans des systèmes d'annuaire distincts et spécialisés, simplifie l'intégration, la gestion et la sécurité des ressources réseau. Le paquet

SAMBA peut être configuré pour utiliser les services Active Directory d'un contrôleur de domaine Windows.

3.1.1.1. LDAP

L'application serveur LDAP fournit les fonctionalités Directory Services aux ordinateurs Windows d'une manière très similaire aux services Microsoft Active Directory. Ces services comprennent la gestion des identités et des relations entre ordinateurs, utilisateurs ainsi que des groupes d'ordinateurs et d'utilisateurs qui font partie du réseau et fournissent une manière cohérente de décrire, localiser et gérer ces ressources. L'implémentation de LDAP librement disponible pour votre système Ubuntu se nomme *OpenLDAP*. Le processus serveur responsable de traiter les requêtes OpenLDAP et de propager les données d'un seveur LDAP à l'autre sur Ubuntu sont slapd et slurpd. OpenLDAP peut être utilisé conjointement avec SAMBA pour fournir les services de partage des fichiers, d'imprimerie et de directoire tout comme le ferait un Windows Domain Controller pour autant que SAMBA soit compilé avec le support LDAP.

3.1.1.2. Kerberos

Le système de sécurisation des authentifications Kerberos est un service standardisé qui fournit une authentification aux ordinateurs et aux utilisateurs grâce à un serveur centralisé qui accorde des tickets d'autorisation cryptés acceptés comme authentification par tout autre ordinateur utilisant Kerberos. Parmi les avantages de l'authentification avec Kerberos, on peut citer l'authentification réciproque, l'authentification par procuration, l'interopérabilité et une gestion simplifiée de la confiance. Les démons serveurs principaux qui gèrent l'authentification Kerberos et l'administration de la base de données Kerberos sous Ubuntu sont krb5kdc et kadmin. Il se peut que SAMBA utilise Kerberos comme mécanisme pour authentifier des ordinateurs et des utilisateurs au moyen d'un contrôleur de domaine Windows. À cette fin, il faut que Kerberos soit installé sur le système Ubuntu, et le fichier `/etc/samba/smb.conf` doit être modifié pour choisir le mode convenable de *realm* et *security*. Par exemple, modifiez le fichier `/etc/samba/smb.conf` et ajoutez les valeurs:

realm = NOM_DOMAINE

security = ADS

dans le fichier, et enregistrez-le.

Assurez-vous de remplacer l'expression NOM_DOMAINE de l'exemple ci-dessus par le nom réel de votre propre domaine Windows.

Vous devrez redémarrer les démons SAMBA pour appliquer ces changements. Redémarrez les démons SAMBA en entrant la commande suivante lors de l'invite du terminal :

```
sudo /etc/init.d/samba restart
```

3.1.2. Comptes d'ordinateurs

Les comptes d'ordinateur sont utilisés dans Directory Services pour identifier de manière unique les ordinateurs d'un réseau, et sont traités de la même manière que les utilisateurs en terme de sécurité. Les comptes d'ordinateurs peuvent avoir des mots de passe commes les comptes utilisateurs, et font l'objet d'autorisation pour accéder aux ressources du réseau. Par exemple, si un utilisateur du réseau avec un compte valide pour un réseau en particuler essaye de s'authentifier à partir d'un ordinateur qui n'a pas de compte d'ordinateur valide, par rapport à la politique mise en oeuvre sur le réseau, il peut lui être refusé l'accès si cet ordinateur ne fait pas partie des ordinateurs autorisés.

Un compte d'ordinateur peut être ajouté au fichier de mots de passe SAMBA, pourvu que le nom de l'ordinateur à ajouter existe déjà comme un nom de compte d'utilisateur valide dans la base de données locale. Pour ajouter un compte d'ordinateur ou de machine au fichier de mots de passe SAMBA, il faut utiliser la commande smbpasswd dans une console comme ceci :

```
sudo smbpasswd -a -m NOM_ORDINATEUR
```

Assurez-vous de remplacer la chaîne COMPUTER_NAME dans l'exemple ci-dessus avec le nom de l'ordinateur pour lequel vous voulez ajouter un compte de machine.

3.1.3. Permissions de fichier

Les Permissions de fichiers définissent les droits explicites qu'un ordinateur ou un utilisateur a sur un dossier, fichier ou groupe de fichiers particulier. De telles permissions peuvent être définies en éditant le fichier `/etc/samba/smb.conf` et en définissant explicitement les permissions d'un partage de fichiers défini. Par exemple, si vous avez défini un partage SAMBA intitulé *sourcedocs* et souhaitez donner les droits de *lecture seule* au groupe d'utilisateurs appelé *planning*, mais souhaitez autoriser l'accès au partage en écriture par le groupe appelé *authors* et à l'utilisateur nommé *richard*, alors vous pouvez éditer le fichier `/etc/samba/smb.conf`, et ajouter les lignes suivantes sous l'entrée *[sourcedocs]* :

read list = @planning

write list = @authors, richard

Sauvegardez `/etc/samba/smb.conf` pour que les changements prennent effet.

Une autre possibilité de permission est de déclarer des permissions *administratives* pour une ressource partagée particulière. Les utilisateurs ayant des permissions administratives peuvent lire, écrire, ou modifier toutes information contenue dans la ressource dont l'utilisateur a explicitement donné des permissions administratives. Par exemple, si vous voulez donner à l'utilisateur *melissa* des permissions administratives sur le partage *sourcedocs* de l'exemple, vous devez éditer le fichier `/etc/samba/smb.conf` et ajouter la ligne suivante sous l'entrée *[sourcedocs]* :

admin users = melissa

Sauvegardez `/etc/samba/smb.conf` pour que les changements prennent effet.

3.2. Clients

Ubuntu fournit des applications clientes et des capacités pour accéder aux ressources partagées grâce au protocole SMB. Par exemple, l'utilitaire nommé smbclientpermet d'accdocuments, proposbill, en utilisant smbclient, on entrera la commande suivante

```
smbclient //bill/documents -U <nomutilisateur>
```

Il vous sera alors demandé le mot de passe de l'utilisateur spécifié après le paramètre -U, et après la réussite de l'authentification, vous obtiendrez une invite vous permettant de manipuler ou transférer des fichiers avec une syntaxe semblable au client FTP en mode texte. Pour plus d'informations sur l'utilitaire smbclient, consultez la page du manuel avec la commande :

```
man smbclient
```

Le montage d'une ressource réseau fournie par le protocole SMB est aussi possible grâce à la commande mount. Par exemple, pour monter un répertoire nommé *code-projet* disponible sur un serveur Windows *developpement* pour l'utilisateur *toto* sur votre système Ubuntu dans le répertoire /mnt/pcode, vous devrez entrer la commande suivante à l'invite :

```
mount -t smbfs -o username=toto //developpement/code-projet- /mnt/pcode
```

Il vous sera alors demandé d'entrer le mot de passe utilisateur, et après vous être authentifié, le contenu de la ressource partagée sera accessible localement via le point de montage spécifié par le dernier argument de la commande mount. Pour déconnecter la ressource partagée, utilisez simplement la commande umount comme vous le feriez avec n'importe quel autre système de fichiers monté. Par exemple :

```
umount /mnt/pcode
```

3.2.1. Comptes d'utilisateurs

Les comptes d'utilisateurs définissent des personnes avec un certain niveau d'autorisation pour utiliser un certain ordinateur et des ressources réseau. Typiquement, dans un environnement réseau, un compte d'utilisateur est fourni à chaque personne autorisée à accéder à un ordinateur ou à un réseau, où des politiques de sécurité et des permissions définissent alors de quels droits explicites ce compte d'utilisateur dispose. Pour définir des utilisateurs réseau SAMBA sur votre système Ubuntu, vous pouvez utiliser la commande smbpasswd. Par exemple, pour ajouter un utilisateur SAMBA à votre système Ubuntu avec le nom d'utilisateur *toto*, vous pourriez entrer ceci à l'invite de commande :

```
smbpasswd -a toto
```

L'application smbpasswd vous demandera alors d'entrer un mot de passe pour l'utilisateur :

```
Nouveau mot de passe SMB :
```

Entrez le mot de passe que vous désirez fixer pour l'utilisateur, et l'application smbpasswd vous demandera de confirmer le mot de passe:

```
Retapez le nouveau mot de passe SMB :
```

Confirmez le mot de passe et smbpasswd ajoutera une entrée pour l'utilisateur au fichier de mots de passe SAMBA.

3.2.2. Groupes

Les Groupes définissent un ensemble d'ordinateurs ou d'utilisateurs qui ont un niveau d'accès commun à des ressources réseau particulières, et offrent une certaine granularité dans le contrôle d'accès à de telles ressources. Par exemple, si un groupe *qa* est défini et contient les utilisateurs *freda*, *danika*, et *rob*, et un second groupe *support* est défini et contient les utilisateurs *danika*, *jeremy* et *vincent*, alors certaines ressources réseau configurées pour autoriser l'accès au groupe *qa* autoriseraient par conséquent l'accès à freda, danika et rob, mais pas à jeremy ou à vincent. Comme l'utilisateur *danika* appartient aux deux groupes *qa* et *support*, elle sera capable d'accéder aux ressources configurées comme accessibles par les deux groupes, tandis que tous les autres utilisateurs n'auront accès qu'aux ressources autorisant explicitement le groupe dont ils font partie.

Lors de la définition de groupes dans le fichier de configuration de SAMBA, `/etc/samba/smb.conf`, la syntaxe reconnue est le préfixage du nom de groupe par le symbole "@". Par exemple, si vous souhaitez définir un groupe nommé *sysadmin* dans une certaine section du fichier `/etc/samba/smb.conf, vous devez entrer le nom de groupe @sysadmin.`

3.2.3. Stratégie de groupe

Les stratégies de groupes définissent certains réglages de configuration SAMBA en rapport avec le domaine ou le groupe de travail auquel appartient le compte d'ordinateur, ainsi que d'autres réglages globaux du serveur SAMBA. Par exemple, si le serveur

SAMBA appartient au groupe de travail Windows appelé *NIVEAU1*, le fichier `/etc/samba/smb.conf` pourrait alors être modifié de la manière suivante :

workgroup = NIVEAU1

Enregistrez le fichier et redémarrez les démons SAMBA pour appliquer le changement.

D'autres réglages de stratégie globaux importants comprennent la *chaîne server* qui définit le nom serveur NETBIOS qui sera annoncé aux autres machines du réseau Windows par votre système Ubuntu. C'est le nom par lequel votre système Ubuntu sera reconnu par les clients Windows et d'autres ordinateurs capables de parcourir le réseau avec le protocole SMB. De plus, vous pouvez indiquer le nom et l'emplacement du fichier journal du serveur SAMBA en utilisant la directive *log file* dans le fichier `/etc/samba/smb.conf`.

Quelques directives supplémentaires influençant la stratégie de groupe globale concernent la spécification de la nature globale des ressources partagées. Par exemple, l'emplacement de certaines directives sous la section *[global]* du fichier `/etc/samba/smb.conf` concernera toutes les ressources partagées, sauf si une directive identique remplace celle-ci sous la section d'une ressource partagée précise. Vous indiquez que tous les partages peuvent être parcourus par tous les clients du réseau en plaçant la directive *browseable*, qui prend une valeur booléenne, sous la section *[global]* du fichier `/etc/samba/smb.conf`. C'est-à-dire que si vous modificez le fichier en ajoutant la ligne :

browseable = true

sous la section *[global]* de `/etc/samba/smb.conf`, tous les partages offerts par votre système Ubuntu par SAMBA pourront être parcourus par tous les clients autorisés, sauf si un partage précis contient une directive *browseable = false* qui remplacera la directive globale.

Les directives *public* et *writeable* sont d'autres exemples qui fonctionnent de la même manière. La directive *public* prend une valeur booléenne et détermine si une ressource partagée particulière est visible par tous les clients, autorisés ou non. La directive *writeable* prend également une valeur booléenne et détermine si une ressource partagée particulière est accessible en écriture par n'importe quel client du réseau.

Annexe A. Creative Commons by Attribution-ShareAlike 2.0

CREATIVE COMMONS CORPORATION IS NOT A LAW FIRM AND DOES NOT PROVIDE LEGAL SERVICES. DISTRIBUTION OF THIS LICENSE DOES NOT CREATE AN ATTORNEY-CLIENT RELATIONSHIP. CREATIVE COMMONS PROVIDES THIS INFORMATION ON AN "AS-IS" BASIS. CREATIVE COMMONS MAKES NO WARRANTIES REGARDING THE INFORMATION PROVIDED, AND DISCLAIMS LIABILITY FOR DAMAGES RESULTING FROM ITS USE.

License

THE WORK (AS DEFINED BELOW) IS PROVIDED UNDER THE TERMS OF THIS CREATIVE COMMONS PUBLIC LICENSE ("CCPL" OR "LICENSE"). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK OTHER THAN AS AUTHORIZED UNDER THIS LICENSE OR COPYRIGHT LAW IS PROHIBITED.

BY EXERCISING ANY RIGHTS TO THE WORK PROVIDED HERE, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE. THE LICENSOR GRANTS YOU THE RIGHTS CONTAINED HERE IN CONSIDERATION OF YOUR ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

1. **Definitions.**

   a. **"Collective Work"** means a work, such as a periodical issue, anthology or encyclopedia, in which the Work in its entirety in unmodified form, along with a number of other contributions, constituting separate and independent works in themselves, are assembled into a collective whole. A work that constitutes a Collective Work will not be considered a Derivative Work (as defined below) for the purposes of this License.

   b. **"Derivative Work"** means a work based upon the Work or upon the Work and other pre-existing works, such as a translation, musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which the Work may be recast, transformed, or adapted, except that a work that constitutes a Collective Work will not be considered a Derivative Work for the purpose of this License. For the avoidance of doubt, where the Work is a musical composition or sound recording, the synchronization of the Work in timed-relation with a moving image ("synching") will be considered a Derivative Work for the purpose of this License.

   c. **"Licensor"** means the individual or entity that offers the Work under the terms of this License.

d. **"Original Author"** means the individual or entity who created the Work.

e. **"Work"** means the copyrightable work of authorship offered under the terms of this License.

f. **"You"** means an individual or entity exercising rights under this License who has not previously violated the terms of this License with respect to the Work, or who has received express permission from the Licensor to exercise rights under this License despite a previous violation.

g. **"License Elements"** means the following high-level license attributes as selected by Licensor and indicated in the title of this License: Attribution, ShareAlike.

2. **Fair Use Rights.** Nothing in this license is intended to reduce, limit, or restrict any rights arising from fair use, first sale or other limitations on the exclusive rights of the copyright owner under copyright law or other applicable laws.

3. **License Grant.** Subject to the terms and conditions of this License, Licensor hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) license to exercise the rights in the Work as stated below:

a. to reproduce the Work, to incorporate the Work into one or more Collective Works, and to reproduce the Work as incorporated in the Collective Works;

b. to create and reproduce Derivative Works;

c. to distribute copies or phonorecords of, display publicly, perform publicly, and perform publicly by means of a digital audio transmission the Work including as incorporated in Collective Works;

d. to distribute copies or phonorecords of, display publicly, perform publicly, and perform publicly by means of a digital audio transmission Derivative Works.

e. For the avoidance of doubt, where the work is a musical composition:

i. **"Performance Royalties Under Blanket Licenses."** Licensor waives the exclusive right to collect, whether individually or via a performance rights society (e.g. ASCAP, BMI, SESAC), royalties for the public performance or public digital performance (e.g. webcast) of the Work.

ii. **"Mechanical Rights and Statutory Royalties."** Licensor waives the exclusive right to collect, whether individually or via a music rights society or designated agent (e.g. Harry Fox Agency), royalties for any phonorecord You create from the Work ("cover version") and distribute, subject to the compulsory license created by 17 USC Section 115 of the US Copyright Act (or the equivalent in other jurisdictions).

f. **"Webcasting Rights and Statutory Royalties."** For the avoidance of doubt, where the Work is a sound recording, Licensor waives the exclusive right to collect, whether individually or via a performance-rights society (e.g. SoundExchange), royalties for the public digital performance (e.g. webcast) of the Work, subject to the compulsory license created by 17 USC Section 114 of the US Copyright Act (or the equivalent in other jurisdictions).

The above rights may be exercised in all media and formats whether now known or hereafter devised. The above rights include the right to make such modifications as are technically necessary to exercise the rights in other media and formats. All rights not expressly granted by Licensor are hereby reserved.

4. **Restrictions.** The license granted in Section 3 above is expressly made subject to and limited by the following restrictions:

   a. You may distribute, publicly display, publicly perform, or publicly digitally perform the Work only under the terms of this License, and You must include a copy of, or the Uniform Resource Identifier for, this License with every copy or phonorecord of the Work You distribute, publicly display, publicly perform, or publicly digitally perform. You may not offer or impose any terms on the Work that alter or restrict the terms of this License or the recipients' exercise of the rights granted hereunder. You may not sublicense the Work. You must keep intact all notices that refer to this License and to the disclaimer of warranties. You may not distribute, publicly display, publicly perform, or publicly digitally perform the Work with any technological measures that control access or use of the Work in a manner inconsistent with the terms of this License Agreement. The above applies to the Work as incorporated in a Collective Work, but this does not require the Collective Work apart from the Work itself to be made subject to the terms of this License. If You create a Collective Work, upon notice from any Licensor You must, to the extent practicable, remove from the Collective Work any reference to such Licensor or the Original Author, as requested. If You create a Derivative Work, upon notice from any Licensor You must, to the extent practicable, remove from the Derivative Work any reference to such Licensor or the Original Author, as requested.

   b. You may distribute, publicly display, publicly perform, or publicly digitally perform a Derivative Work only under the terms of this License, a later version of this License with the same License Elements as this License, or a Creative Commons iCommons license that contains the same License Elements as this License (e.g. Attribution-ShareAlike 2.0 Japan). You must include a copy of, or the Uniform Resource Identifier for, this License or other license specified in the previous sentence with every copy or phonorecord of each Derivative Work You distribute, publicly display, publicly perform, or publicly digitally perform. You may not offer or impose any terms on the Derivative Works that alter or restrict the terms of this License or the recipients' exercise of the rights granted hereunder, and You must keep intact all notices that refer to this License and to the disclaimer of warranties. You may not distribute, publicly display, publicly perform, or publicly digitally perform the Derivative Work with any technological measures that control access or use of the Work in a manner inconsistent with the terms of this License Agreement. The above applies to the Derivative Work as incorporated in a Collective Work, but this does not require the Collective Work apart from the Derivative Work itself to be made subject to the terms of this License.

c. If you distribute, publicly display, publicly perform, or publicly digitally perform the Work or any Derivative Works or Collective Works, You must keep intact all copyright notices for the Work and give the Original Author credit reasonable to the medium or means You are utilizing by conveying the name (or pseudonym if applicable) of the Original Author if supplied; the title of the Work if supplied; to the extent reasonably practicable, the Uniform Resource Identifier, if any, that Licensor specifies to be associated with the Work, unless such URI does not refer to the copyright notice or licensing information for the Work; and in the case of a Derivative Work, a credit identifying the use of the Work in the Derivative Work (e.g., "French translation of the Work by Original Author," or "Screenplay based on original Work by Original Author"). Such credit may be implemented in any reasonable manner; provided, however, that in the case of a Derivative Work or Collective Work, at a minimum such credit will appear where any other comparable authorship credit appears and in a manner at least as prominent as such other comparable authorship credit.

5. **Representations, Warranties and Disclaimer**

   UNLESS OTHERWISE AGREED TO BY THE PARTIES IN WRITING, LICENSOR OFFERS THE WORK AS-IS AND MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND CONCERNING THE MATERIALS, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF TITLE, MERCHANTIBILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR THE ABSENCE OF LATENT OR OTHER DEFECTS, ACCURACY, OR THE PRESENCE OF ABSENCE OF ERRORS, WHETHER OR NOT DISCOVERABLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO SUCH EXCLUSION MAY NOT APPLY TO YOU.

6. **Limitation on Liability.** EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW, IN NO EVENT WILL LICENSOR BE LIABLE TO YOU ON ANY LEGAL THEORY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES ARISING OUT OF THIS LICENSE OR THE USE OF THE WORK, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. **Termination**

   a. This License and the rights granted hereunder will terminate automatically upon any breach by You of the terms of this License. Individuals or entities who have received Derivative Works or Collective Works from You under this License, however, will not have their licenses terminated provided such individuals or entities remain in full compliance with those licenses. Sections 1, 2, 5, 6, 7, and 8 will survive any termination of this License.

b. Subject to the above terms and conditions, the license granted here is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, Licensor reserves the right to release the Work under different license terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this License (or any other license that has been, or is required to be, granted under the terms of this License), and this License will continue in full force and effect unless terminated as stated above.

8. **Miscellaneous**

   a. Each time You distribute or publicly digitally perform the Work or a Collective Work, the Licensor offers to the recipient a license to the Work on the same terms and conditions as the license granted to You under this License.

   b. Each time You distribute or publicly digitally perform a Derivative Work, Licensor offers to the recipient a license to the original Work on the same terms and conditions as the license granted to You under this License.

   c. If any provision of this License is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this License, and without further action by the parties to this agreement, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

   d. No term or provision of this License shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.

   e. This License constitutes the entire agreement between the parties with respect to the Work licensed here. There are no understandings, agreements or representations with respect to the Work not specified here. Licensor shall not be bound by any additional provisions that may appear in any communication from You. This License may not be modified without the mutual written agreement of the Licensor and You.

Creative Commons is not a party to this License, and makes no warranty whatsoever in connection with the Work. Creative Commons will not be liable to You or any party on any legal theory for any damages whatsoever, including without limitation any general, special, incidental or consequential damages arising in connection to this license. Notwithstanding the foregoing two (2) sentences, if Creative Commons has expressly identified itself as the Licensor hereunder, it shall have all rights and obligations of Licensor.

Except for the limited purpose of indicating to the public that the Work is licensed under the CCPL, neither party will use the trademark "Creative Commons" or any related trademark or logo of Creative Commons without the prior written consent of Creative

Commons. Any permitted use will be in compliance with Creative Commons' then-current trademark usage guidelines, as may be published on its website or otherwise made available upon request from time to time.

Creative Commons may be contacted at *http://creativecommons.org/*.

Annexe B. GNU Free Documentation License

Version 1.2, November 2002
Copyright © 2000,2001,2002 Free Software Foundation, Inc.

Free Software Foundation, Inc.
51 Franklin St, Fifth Floor,
Boston,
MA
02110-1301
USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.
Version 1.2, November 2002

PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

GNU FDL Modification Conditions

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the *Addendum [1]02* below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified

Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in *section 4 [98]* above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

Sample Invariant Sections list

> Copyright (c) YEAR YOUR NAME. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with...Texts." line with this:

Sample Invariant Sections list

> with the Invariant Sections being LIST THEIR TITLES, with the Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.