Guide du serveur Ubuntu

TABLE DES MATIÈRES

Bienvenue dans le **Guide du Serveur Ubuntu** ! Vous trouverez ici des informations concernant l'installation et la configuration de plusieurs applications serveur sur votre système Ubuntu afin de satisfaire vos besoins. Il s'agit d'un guide pratique, procédant étape par étape, pour configurer et personnaliser votre système.

Remerciements et licence

Ce document est rédigé par l'équipe de documentation d'Ubuntu **pour la majeure partie** : https://wiki.ubuntu.com/DocumentationTeam . Une liste de contributeurs se trouve ci-dessous.

La traduction finale a été réalisée par Pascal Baudry, voir l'**Avertissement** ci-dessous.

Ont contribué à ce document :

Les membres du **Projet de Documentation Ubuntu** : https://launchpad.net/~ubuntu-core-doc

Les membres de l'**équipe Ubuntu Serveur** : https://launchpad.net/~ubuntu-server

Contributeurs à la **Communauté d'aide Wiki** : https://help.ubuntu.com/community/

D'autres contributeurs peuvent être trouvés dans l'histoire de la révision du Guide du serveur : https://bazaar.launchpad.net/~ubuntu-core-doc/serverguide/trunk/changes

et de la documentation Ubuntu : https://bazaar.launchpad.net/~ubuntu-core-doc/ubuntu-docs/trunk/changes qui sont les branches bzr disponibles sur Launchpad.

Avertissement

Pour la version française de ce guide, la majeure partie de la traduction est issue du site Launchpad consacrée à la version française du Guide du Serveur Ubuntu.

Seules les traductions antérieures au 30 mai 2017 sont intégrées.

J'ai constaté une carence de validation de certaines traductions, tout à fait correctes, qui dorment sur le site de Launchpad depuis leur naissance.

Afin de généré une traduction complète, j'ai pris la décision de collecter ces traductions, les corriger pour certaines, terminer la traduction pour les parties non traduites et générer ce document.

En ce sens, cette traduction **n'a pas reçu** la validation du groupe de traduction de Launchpad, et vous pouvez rencontrer quelques erreurs de traduction ou de compréhension du fonctionnement du serveur Ubuntu.

Veuillez m'en excuser par avance, et n'hésitez pas à relever toute erreur et à me la transmettre pour correction.

Bonne lecture.

Pascal Baudry

TABLE DES MATIÈRES

TABLE DES MATIÈRES

TABLE DES MATIÈRES

TABLE DES MATIÈRES

TABLE DES MATIÈRES

TABLE DES MATIÈRES

TABLE DES MATIÈRES

TABLE DES MATIÈRES

TABLE DES MATIÈRES

TABLE DES MATIÈRES

TABLE DES MATIÈRES

TABLE DES MATIÈRES

TABLE DES MATIÈRES

Chapitre 1. Introduction

Bienvenue dans **le guide du serveur Ubuntu** !

Vous trouverez ici des informations sur l'installation et la configuration de diverses applications serveur. C'est un guide décrivant les actions pas-à-pas pour configurer et personnaliser votre système.

Ce guide suppose que vous ayez des connaissances de base du système ubuntu. Les informations d'installation sont présentées au *Chapitre 2. Installation*, mais si vous recherchez des informations d'installation d'Ubuntu, alors référez-vous au **Guide d'Installation d'Ubuntu :** https://help.ubuntu.com/16.04/installation-guide .

Une version HTML du manuel est disponible en ligne sur le site de la documentation Ubuntu : https://help.ubuntu.com .

1.1. Assistance

L’édition Ubuntu Serveur est maintenue de deux manières : une maintenance à but commercial et une maintenance de la communauté. La principale maintenance commerciale (et l’investissement en développement) vient de Canonical. Cette entreprise propose des contrats de maintenance à un prix raisonnable, par ordinateur ou par serveur. Pour plus d’informations voir Ubuntu Advantage : http://www.ubuntu.com/management .

La maintenance par la communauté est aussi proposée par des individus et des entreprises consciencieuses dans l’espoir de voir devenir Ubuntu la meilleure distribution existante. La maintenance est fournie par le biais de plusieurs listes de courriels, canaux IRC, forums, pages personnelles, tutoriels, etc... Le montant astronomique d’informations disponibles peut être écrasante, bien qu’un bon moteur de recherche peut vous fournir une réponse à votre question. Voir la page de maintenance d’Ubuntu : http://www.ubuntu.com/support .

Chapitre 2. Installation

Ce chapitre propose un survol de l’installation de Ubuntu 16.04 LTS Server Edition. Pour obtenir plus d’informations détaillées, référez-vous au Guide d’Installation d’Ubuntu : https://help.ubuntu.com/16.04/installation-guide .

2.1. Préparation de l'installation

Ce chapitre expose les différents aspects à prendre en considération avant de commencer l'installation.

2.1.1. Exigences du système

L'édition serveur Ubuntu 16.04 LTS est compatible avec trois architectures principales : Intel x86, AMD64 et ARM. Le tableau ci-dessous donne la liste des spécifications matériel recommandées. Selon vos besoins, vous n'utiliserez pas toutes ces données. Cependant, la plupart des utilisateurs prennent le risque d'être frustrés s'ils ignorent ces suggestions.

Tableau 2.1 Exigences minimales recommandées

Type d'installation	Processeur	RAM	Capacité du disque dur	
			Système de base	Toutes les tâches installées
Serveur (Standard)	1 gigahertz	512 megaoctets	1 gigaoctet	1,75 gigaoctets
Serveur (Minimal)	300 mégahertz	192 mégaoctets	700 mégaoctets	1,4 gigaoctets

L'édition serveur fournit une base commune à toutes sortes de programmes serveurs. Sa conception minimaliste offre une plate-forme pour de multiples services, tels que serveur de fichier ou d'impression, hébergement Web, serveur de courriel, etc.

2.1.2. Différences entre la version serveur et la version Desktop

Il y a quelques différences entre **Ubuntu Édition Serveur** et **Ubuntu Édition Desktop**. Il convient de noter que les deux éditions utilisent les mêmes dépôts **apt**, ce qui rend l'installation d'une application ***serveur*** aussi facile sur l'Édition Desktop que sur l'Édition Serveur.

Les différences entre les deux éditions sont l'absence d'environnement graphique dans l'Édition Serveur et le processus d'installation.

2.1.2.1. Différences concernant le noyau :

Ubuntu 10.10 et les versions précédentes, avaient en fait des noyaux différents pour les éditions serveur et de bureau. Ubuntu n'a plus ces variantes du noyau distinctes -server et -generic. Celles-ci ont été fusionnées en une seule variante du noyau -generic pour aider à réduire la charge pour la maintenance sur la durée de support de la version.

> Quand vous exécutez une version 64-bit d'Ubuntu sur un processeur 64-bit vous n'êtes pas limité par l'espace d'adressage mémoire.

Pour connaître toutes les options de configurations du noyau, vous pouvez regarder dans le

fichier **/boot/config-4.4.0-server**. Également, Linux Kernel in a Nutshell : http://www.kroah.com/lkn/ est une ressource importante sur les options disponibles.

2.1.3. Sauvegarde

Avant d'installer **Ubuntu édition serveur** vous devez être certain que toutes les données de votre système sont sauvegardées. Voir *Chapitre 19. Sauvegardes* pour les options de sauvegarde.

Si ce n'est pas le premier système d'exploitation installé sur votre ordinateur, il se pourrait que vous ayez à partitionner à nouveau votre disque dur afin de faire de la place pour Ubuntu.

A chaque fois que vous partitionnez votre disque dur, vous devez être conscient que vous pouvez effacer toutes les données de votre disque dur, faire une erreur ou que quelque chose se passe mal durant le partitionnement. Les programmes utilisés dans l'installation sont fiables, la plupart sont utilisés depuis de nombreuses années, mais ils sont capables d'effectuer des actions destructrices.

2.2. Installation à partir du CD

Les étapes de base pour installer l'Edition Ubuntu Serveur à partir du CD sont les mêmes que celles pour l'installation de tout système d'exploitation à partir d'un CD. Contrairement à l'**Édition Desktop**, l'**Édition Serveur** n'inclut pas de programme d'installation graphique. L'Édition Serveur utilise, à la place, un procédé basé sur des menus dans une console.

- Téléchargez et gravez le fichier ISO approprié depuis le **site internet Ubuntu** : http://www.ubuntu.com/download/server/download .
- Démarrer le système depuis le lecteur CD.
- À l'invite de démarrage, il vous sera demandé de sélectionner une langue.
- Dans le menu de démarrage principal il ya quelques options supplémentaires à installer l'Édition Ubuntu Serveur. Vous pouvez installer un serveur de base Ubuntu, consulter le CD-ROM pour les défaillances, vérifier la RAM du système, démarrer à partir du disque dur, ou récupérer un système cassé. Le reste de ce chapitre traite de l'installation de base du serveur Ubuntu.
- L'installation demandera quel langage devra être utiliser. Ensuite, votre localisation vous sera demandée.
- Ensuite, le processus d'installation commence par demander la disposition de votre clavier. Vous pouvez demander à l'installateur de tenter l'auto-détection, ou vous pouvez le sélectionner manuellement dans une liste.
- L'installateur découvre alors votre configuration matérielle, et configure les paramètres de réseau en utilisant le protocole DHCP. Si vous ne souhaitez pas utiliser DHCP, choisissez « Retour » à l'écran suivant, et apparaît alors l'option « Configurer le réseau manuellement ».
- Ensuite, l'installateur demande le nom du système.
- Un nouvel utilisateur est créé, il aura l'accès **root** via l'utilitaire **sudo**.
- Après que les données utilisateur aient été renseignées, il vous sera demandé si vous souhaitez chiffrer votre répertoire home.
- Ensuite, l'installeur demande fuseau horaire du système.
- Vous pouvez choisir maintenant, selon plusieurs options, de configurer l'arrangement du disque dur. Ensuite, il vous sera demandé sur quel disque vous voulez procéder à l'installation. Vous recevrez peut-être des messages de confirmation afin de redéfinir la table de partitionnement ou la configuration de LVM, selon l'arrangement du disque, puis il vous sera demandé la dimension de la partition logique racine. Pour les options avancées de disque voir le *Chapitre 2, paragraphe 4. Installation avancée*.
- Le système Ubuntu de base est maintenant installée.
- La prochaine étape vous proposera de mettre à jour le système. Trois options sont possibles :
    - **Pas de mises à jour automatiques** : un administrateur devra se connecter à la machine et effectuer les mises à jour manuellement.
    - **Installez les mises à jour de sécurité automatiquement** : ceci installera le paquet **unattended-upgrades**, qui installera les mises à jour de sécurité sans l'aide d'un administrateur. Pour plus de détails, voir le *Chapitre 3, paragraphe 5. Mises à jour automatiques*.
    - **Gérer les mises à jour avec Landscape** : Landscape est un service payant fourni par Canonical pour aider à la maintenance des machines Ubuntu. Voir le site Landscape :

http://landscape.canonical.com pour de plus amples informations.

- Vous avez maintenant la possibilité d'installer ou de ne pas installer plusieurs paquets de tâches. Voir *2.1. Paquet de fonctionnalités* pour plus de détails. Il existe aussi une option pour lancer **aptitude** afin de choisir les paquets à installer. Pour de plus amples informations, voir le C*hapitre 3, paragraphe 4. Aptitude*.
- Finalement, la dernière étape avant de redémarrer le système est d'initialiser l'horloge sur UTC.

Si à un moment quelconque de l'installation vous n'êtes pas satisfait de la configuration par défaut, vous pouvez utiliser la fonction « Précédent » qui vous présentera un menu d'installation plus détaillé permettant de modifier les options par défaut.

A n'importe quel moment durant le processus d'installation vous pouvez avoir envie d'accéder à l'écran d'aide fourni par le système d'installation. Pour ce faire, appuyez sur F1.

Pour obtenir plus d'informations détaillées, référez-vous au Guide d'Installation d'Ubuntu : https://help.ubuntu.com/16.04/installation-guide

2.2.1 Paquet de fonctionnalités

Pendant l'installation de l'édition serveur vous avez la possibilité d'installer des paquets supplémentaires à partir du CD. Ces paquets sont regroupés en fonction du type de service qu'ils fournissent.

Serveur DNS : Sélectionne le serveur DNS BIND et sa documentation.

Serveur LAMP : Sélectionne un serveur Linux/Apache/MySQL/PHP prêt à utiliser.

Serveur de messagerie : Cette tâche choisit une variété de paquets utiles pour un système de serveur de messagerie d'usage général.

Serveur OpenSSH : Sélectionne les paquets nécessaires pour un serveur OpenSSH.

Base de données PostgreSQL : cette tâche sélectionne les paquets client et serveur pour la base de données PostgreSQL.

Serveur d'impression : cette tâche configure votre système pour qu'il devienne un serveur d'impression.

Serveur de fichiers Samba : cette tâche installe un serveur de fichiers Samba, qui est particulièrement adapté aux réseaux hétérogènes Windows et Linux.

Serveur Java Tomcat : Installe Apache Tomcat et les dépendances requises.

Hôte de machine virtuelle : Comprend les paquets nécessaires à l'exécution des machines virtuelles KVM.

Sélectionnez manuellement des paquets : Exécute **aptitude** vous permettant de sélectionner individuellement des paquets.

Installation des groupes de paquetages est réalisée en utilisant l'utilitaire **tasksel** . L'une des différences importantes entre Ubuntu (ou Debian) et d'autres distribution GNU/Linux est que, une fois installé, un paquet est également configuré les paramètres par défaut raisonnables, éventuellement vous demander des informations complémentaires requises. De même, lors de l'installation d'une tâche, les paquets ne sont pas installés uniquement, mais également configuré pour fournir un service entièrement intégré.

Une fois le processus d'installation terminé vous pouvez obtenir une liste des tâches disponibles en saisissant la commande suivante depuis un terminal :

```
tasksel --list-tasks
```

Le résultat de cette commande listera les tâches des autres distributions basées sur Ubuntu comme Kubuntu et Edubuntu. Remarquez que vous pouvez aussi appeler la commande tasksel seule afin d'obtenir un menu des différentes tâches disponibles.

Vous pouvez voir une liste des paquets qui sont installés pour chaque tâche en utilisant l'option --task-packages. Par exemple, pour lister les paquets installés avec la tâche du serveur DNS saisissez ce qui suit :

```
tasksel --task-packages dns-server
```

Le résultat de cette commande doit lister :

```
bind9-doc
bind9utils
Bind9
```

Si vous n'avez pas installé l'une des tâches pendant le processus d'installation, mais par exemple, vous décidez de faire de votre nouveau serveur LAMP un serveur DNS également, il suffit d'insérer le CD d'installation et depuis un terminal :

```
sudo tasksel install dns-server
```

2.3. Mise à niveau

Il y a plusieurs façons de migrer d'une version d'Ubuntu vers une autre. ce chapitre donne un aperçu des méthodes de mises à niveau recommandées.

2.3.1. do-release-upgrade

La manière recommandée pour mettre à jour une installation d'une édition serveur est l'utilisation de **do-release-upgrade**. C'est un composant du paquet **update-manager-core**, qui ne dépend d'aucun gestionnaire graphique et qui est installé par défaut.

Les systèmes basés sur Debian peuvent être également mis à niveau en utilisant la commande **apt dist-upgrade**. Cependant, l'utilisation de la commande **do-release-upgrade** est recommandée car cette dernière a la capacité de gérer les modifications de configuration du système, quelques fois nécessaires entre les mises à jours.

Pour mettre à jour vers une nouvelle version, saisissez dans un terminal :

```
do-release-upgrade
```

Il est également possible d'utiliser **do-release-upgrade** pour mettre à jour vers une version d'Ubuntu en cours de développement. Pour ce faire utilisez l'option **-d** :

```
do-release-upgrade -d
```

Mettre à jour vers une version en cours de développement **n'est pas** recommandé pour les environnements de production.

Pour une meilleure stabilité d'une version LTS (Long Term Support), il y a un léger changement dans le comportement si vous utilisez actuellement une version LTS. Les systèmes LTS sont uniquement gérés automatiquement pour une mise à jour vers la version LTS suivante avec la commande **do-release-upgrade** sur le premier point de mise à jour. Donc, par exemple, une version 14.04 sera uniquement mise à jour lorsque la version 16.04.1 sera proposée. Si vous voulez mettre à jour votre installation plus tôt, par exemple sur une partie de vos machines pour évaluer une mise à jour LTS, selon votre configuration, l'argument -d doit être utilisé, comme un changement pour une version en développement.

2.4. Installation avancée

2.4.1. RAID logiciel

Le regroupement redondant de disques indépendants « RAID » est une méthode utilisant plusieurs disques pour permettre la fiabilité des données et/ou avoir des performances accrues, dépendant du niveau de RAID utilisé. Le RAID est mis en œuvre dans n'importe quel logiciel (où le système d'exploitation connaît tous les disques et entretient ceux-ci activement) ou matériel (où un contrôleur spécial fait croire au système d'exploitation qu'il n'y a qu'un seul disque et qu'il entretient celui-ci de façon « invisible »).

Le logiciel RAID inclut dans les versions actuelles de Linux (dont Ubuntu) est basé sur le pilote **'mdadm'** et fonctionne très bien, et même mieux que la plupart des soi-disant « contrôleurs matériels RAID ». ce chapitre vous aidera à installer l'Édition Serveur d'Ubuntu en utilisant deux partitions RAID1 avec deux disques durs, une partition pour **/**, une autre pour **swap**.

2.4.1.1 Partitionnement

Suivez les étapes d'installation jusqu'à l'étape de Partitionnement des disques, puis :

1. Sélectionnez **Manuel** comme méthode de partitionnement.
2. Sélectionnez le disque racine, et acceptez de **« Créer une nouvelle table de partition sur ce périphérique ? »**.

   Répétez cette étape pour chaque disque que vous souhaitez inclure dans la matrice RAID.
3. Sélectionner l'**« Espace libre »** du premier disque, appuyez sur entrée puis choisissez **« Créer une nouvelle partition »**.
4. Fixez ensuite la **Taille** de la partition. Elle sera utilisée pour le **swap**. Il est généralement recommandé de fixer la taille du fichier d'échange (swap) comme étant égale à deux fois celle de votre mémoire vive (RAM). Saisissez le nombre désiré, appuyez sur entrée, choisissez **Primaire** puis **Début**.

   Une partition d'échange de deux fois la taille de la RAM n'est pas forcement souhaitable, spécialement sur les systèmes dotés d'une grande quantité de RAM. Le calcul de la taille de la partition d'échange pour les serveurs dépend de la façon dont le système sera utilisé.
5. Sélectionnez la ligne située en haut, **« Utiliser en tant que : »**. Par défaut, **« système de fichiers journalisé Ext4 »** est sélectionné, changez ceci en **« volume physique pour RAID »**, puis **« fin du paramétrage de la partition »**.
6. Agissez de manière similaire pour la partition **/**. Sélectionnez l'**« Espace libre »** du premier disque, appuyez sur entrée puis choisissez **« Créer une nouvelle partition »**.
7. Utilisez l'espace libre restant et choisissez **Continuer**, puis **Primaire**.
8. Comme avec la partition de swap, sélectionnez le **"Utiliser comme: "** ligne en haut, de le changer pour **"volume physique pour RAID "**. Également sélectionner le **"drapeau de démarrage: "** ligne pour modifier la valeur de **"sur "**. Ensuite, choisissez **"Terminer le paramétrage de la partition "**.
9. Répétez les étapes trois à huit pour les autres disques et partitions que vous souhaitez créer.

2.4.1.2. Configuration du RAID

Une fois les partitions configurées, les matrices sont prêtes à être paramétrées :

1. Retournez à la page principale de « Partitionner les disques » et sélectionnez en haut **« Configurer le RAID logiciel »**.
2. Sélectionnez **« Oui »** pour appliquer les changements au disque.
3. Choisissez **« Créer un périphérique MD »**.
4. Pour cet exemple, choisissez **« RAID1 »**, mais si vous utilisez une autre configuration, choisissez un autre type (RAID0 RAID1 RAID5).

   A u moins **trois** disques sont nécessaires pour utiliser le **RAID5**. Deux suffisent pour le **RAID0** ou le **RAID1**.

5. Saisissez le nombre de périphériques actifs **« 2 »**, ou le nombre de disques dur que vous possédez pour la matrice. Ensuite, sélectionnez **« Continuer »**.
6. Ensuite, saisissez le nombre de périphériques restants **« 0 »** par défaut, puis, choisissez **« Continuer »**.
7. Choisissez les partitions à utiliser (généralement sda1, sdb1, sdc1, etc.). Habituellement, les chiffres se correspondent et les différentes lettres correspondent à des disques différents.

   Pour la partition **swap** choisissez **sda1** et **sdb1**. Sélectionnez ensuite **« Continuer »** pour vous rendre à l'étape suivante.
8. Répétez les étapes **trois** à **sept** pour la partition **/** en choisissant cette fois **sda2** et **sdb2**.
9. Une fois fait, sélectionnez **« Terminer »**.

2.4.1.3. Formatage

Vous avez maintenant une liste des disques durs ainsi que celle des périphériques RAID. Il faut alors les formater et leur assigner le(s) point(s) de montage. Considérez les ensembles RAID comme des partitions normales en ce qui concerne le formatage et le montage.

1. Sélectionnez **« #1 »** sous la partition **« RAID1 périphérique #0 »**.
2. Choisissez **« Utiliser comme : »** suivi de **« espace d'échange (swap) »** puis **« Fin de paramétrage de cette partition »**.
3. Ensuite, sélectionnez **« #1 »** sous la partition **« RAID1 périphérique #1 »**.
4. Choisissez **« Utiliser en tant que : »**, puis sélectionnez **« système de fichiers journalisé Ext4 »**.
5. Choisissez **« Point de montage »** suivi de **« / - système de fichiers racine »**. Sélectionnez **« Fin de paramétrage de cette partition »**.
6. Pour finir sélectionnez **« Fin de paramétrage de cette partition et appliquer les changements »** puis répondez **« Oui »**.

Si vous choisissez de placer la partition racine sur une matrice RAID, l'installateur vous demandera alors si vous voulez démarrer dans un état RAID **dégradé**. Consultez le *Chapitre 2, paragraphe 4. Installation avancée.1.4. RAID dégradé* pour plus de renseignements.

Le processus d'installation continuera ensuite normalement.

2.4.1.4. RAID dégradé

Au cours de la vie d'un ordinateur, une panne de disque dur peut survenir. Lorsque ceci arrive avec du RAID logiciel, les système d'exploitation placera la matrice RAID dans un état que l'on appelle **dégradé**.

Si la matrice est endommagée, en raison de la possibilité de corruption de données, l'Edition Serveur d'Ubuntu démarrera par défaut vers **initramfs** au bout de trente secondes. Une fois que initramfs aura démarré, une invite sera affichée pendant quinze secondes vous donnant la possibilité de continuer et d'amorcer le système, ou de tenter de faire une récupération manuelle. Démarrer sur initramfs peut être ou non le comportement désiré, surtout si la machine est située dans un endroit éloigné. Le lancement d'une matrice endommagée peut être configuré de plusieurs manières :

- L'outil **dpkg-reconfigure** peut être utilisé pour paramétrer le comportement par défaut. Durant ce processus, vous aurez à choisir de nouvelles options (surveillance, alertes par courriel etc.) concernant la matrice. Pour configurer à nouveau **mdadm**, saisissez :
  ```
  sudo dpkg-reconfigure mdadm
  ```

- Le processus **dpkg-reconfigure mdadm** changera le contenu du fichier de configuration /etc/initramfs-tools/conf.d/mdadm. Ce fichier a l'avantage de pouvoir pré-configurer le comportement de votre système et il peut également être modifié manuellement :

  ```
  BOOT_DEGRADED=true
  ```

  L e fichier de configuration peut être outrepassé en utilisant un argument de noyau.

- Donner un argument au noyau autorisera également le système à démarrer sur une matrice RAID endommagée :
  - Lorsque le serveur démarre, pressez **Maj** pour ouvrir le menu **Grub**.
  - Appuyez sur **e** pour modifier vos options de commande noyau.
  - Appuyez sur la flèche **bas** pour mettre en surbrillance la ligne du noyau.
  - Ajoutez **"bootdegraded=true"** (sans les guillemets) en fin de ligne.
  - Appuyez sur **Ctrl+x** pour démarrer le système.

Une fois le système démarré, vous pouvez réparer la matrice voir le *Chapitre 2, paragraphe 4. Installation avancée.1.5. Maintenance RAID* pour de plus amples informations ou transférez les données importantes vers un autre machine en cas de panne matérielle majeure.

2.4.1.5. Maintenance RAID

L'utilitaire **mdadm** peut être utilisé pour afficher l'état d'une matrice, ajouter des disques à une matrice, en supprimer etc... :

- Pour afficher l'état d'une matrice, depuis un terminal entrez :

  ```
  sudo mdadm -D /dev/md0
  ```

  L'option **-D** ordonne à **mdadm** d'afficher les informations **détaillées** du périphérique /dev/md0. Remplacez /dev/md0 par le périphérique RAID souhaité.

- Pour afficher l'état d'un disque d'une matrice, écrivez :

```
sudo mdadm -E /dev/sda1
```

Le résultat est très similaire à celui de la commande **mdadm -D**, modifiez /dev/sda1 à votre convenance pour chaque disque.

- Si un disque devient défectueux et doit être retiré d'une matrice, entrez :

```
sudo mdadm --remove /dev/md0 /dev/sda1
```

Changez /dev/md0 et /dev/sda1 par les périphériques et les disques RAID appropriés.

- De la même manière, pour ajouter un disque :

```
sudo mdadm --add /dev/md0 /dev/sda1
```

Il peut arriver qu'un disque change d'état et soit décrit comme **défectueux** bien qu'il n'y ait aucun problème physique. Dans ce cas, il est généralement utile de le retirer de la matrice et de l'ajouter à nouveau. Cela forcera une synchronisation de la matrice. Si le disque ne se synchronise pas, alors il y a de fortes chances pour qu'il s'agisse d'une panne matérielle.

Le fichier /proc/mdstat contient également des informations utiles concernant les périphériques RAID du système :

```
cat /proc/mdstat
```

```
Personalities : [linear] [multipath] [raid0] [raid1] [raid6] [raid5] [raid4] [raid10]
md0 : active raid1 sda1[0] sdb1[1]
      10016384 blocks [2/2] [UU]

unused devices: &lt;none&gt;
```

La commande suivante est très utile pour surveiller l'état d'avancement d'une synchronisation de disque :

```
watch -n1 cat /proc/mdstat
```

Appuyez sur **Ctrl+c** pour arrêter la commande **watch**.

Une fois qu'un disque défectueux a été remplacé par un disque en bon état et que celui-ci a été synchronisé, vous devez installer **grub**. Pour l'installer sur le nouveau disque, saisissez :

```
sudo grub-install /dev/md0
```

Remplacez /dev/md0 par le nom du périphérique approprié.

2.4.1.6. Ressources

Les matrices RAID sont un sujet complexe en raison de la multitude de façons de paramétrer le RAID. Consultez les liens suivants pour plus d'informations :

Les Articles du Wiki Ubuntu sur RAID (en anglais) : https://help.ubuntu.com/community/Installation#raid .

Guide pratique du RAID logiciel : http://www.faqs.org/docs/Linux-HOWTO/Software-RAID-HOWTO.html

Gérer le RAID sous Linux : http://oreilly.com/catalog/9781565927308/

2.4.2. Gestionnaire de volumes logiques (Logical Volume Manager, LVM)

Le gestionnaire de volumes logiques, ou **LVM**, permet aux administrateurs de créer des volumes **logiques** à partir d'un ou plusieurs espaces de stockage. Les volumes LVM peuvent être créés sur des partitions RAID logicielles ou sur des partitions normales résidant sur un unique disque. Les volumes peuvent être dimensionnés après-coup, donnant ainsi une plus grande flexibilité au système.

2.4.2.1. Vue d'ensemble

Un effet secondaire de la puissance et de la flexibilité de LVM est un degré accru de complexité. Avant de se plonger dans le processus d'installation de LVM, il est préférable de se familiariser avec quelques termes techniques.

- **Volume physique (PV)** : disque dur physique, partition de disque ou partition RAID logicielle au format LVM PV.
- **Groupe de volumes (VG)** : il est fait à partir d'un ou plusieurs volumes physiques. Un VG peut être étendu en ajoutant plus de volumes physiques (PV). Un VG est comme un disque dur virtuel, à partir duquel un ou plusieurs volumes logiques sont découpés.
- **Volume logique (LV)** : est similaire à une partition dans un système sans LVM. Un LV est formaté avec le système de fichier de votre choix (EXT3, XFS, JFS, etc), il est alors disponible pour le montage et le stockage des données.

2.4.2.2. Installation

À titre d'exemple, ce chapitre décrit l'installation d'Ubuntu édition serveur en montant /srv sur un volume LVM. Lors de l'installation initiale, un seul volume physique (PV) fera partie du groupe de volumes (VG). Un autre PV lui sera affecté plus tard pour montrer comment un VG peut être agrandi.

Plusieurs méthodes d'installation sont disponibles pour LVM : **Assistée - utiliser tout un disque avec LVM**, **Assistée - utiliser tout un disque avec LVM chiffré** et **Manuelle**. Pour l'instant l'approche manuelle est la seule option nous permettant de paramétrer des partitions usuelles et LVM.

1. Suivez les étapes de l'installation jusqu'à ce que vous arriviez à l'étape de Partitionnement des disques, alors :
2. Choisissez **Manuel** à l'étape **Partitionner les disques**.
3. Sélectionnez votre disque et répondez **oui** à la question **Faut-il créer une nouvelle table de partitions sur ce disque** de l'écran suivant.
4. Créez ensuite trois partitions usuelles **/boot**, **swap** et **/** avec le système de fichiers de votre choix.
5. Pour le répertoire /srv de LVM, créez une nouvelle partition **logique** puis sélectionner **« volume physique pour LVM »** dans l'option **« utiliser comme »** et enfin **« fin de paramétrage de cette partition »**.
6. Sélectionnez ensuite **« Configurez le gestionnaire de volumes logiques (LVM) »** et répondez **« Oui »** pour appliquer les changements au disque.
7. À l'écran suivant (**Action de configuration de LVM**), choisissez **« Créer un groupe de volumes »**. Saisissez un nom de volume (**vg01** dans notre exemple) puis sélectionnez **Continuer** (appuyez sur entrée).
8. De retour à l'écran **Action de configuration de LVM**, sélectionnez **« Créer un volume logique »**.

Sélectionnez le nouveau groupe de volumes et saisissez un nom pour le nouveau volume logique, **srv** dans notre exemple. Utilisez la partition entière ou non, de toute façon cette taille peut être changée par la suite grâce aux outils LVM. Choisissez **Terminer** pour revenir à l'écran principal **Partitionner les disques**.

9. Sélectionnez le disque sous **Groupe de volume vg01**, volume logique srv et affectez lui les informations habituelles (type de système de fichier, point de montage - prenez /srv !) puis sélectionnez **Continuer** (appuyez sur entrée).
10. Pour finir, sélectionnez **« Terminer le partitionnement et appliquer les changements »**. Puis confirmez les modifications et continuez avec le reste de l'installation.

Il existe des outils pratiques pour afficher des informations sur LVM :

- **pvdisplay** : affiche des nformations sur les Volumes Physiques.
- **vgdisplay** : affiche les informations des groupes de volumes.
- **lvdisplay** : affiche des informations sur les Volumes Logiques.

2.4.2.3. Agrandir des groupes de volumes

Poursuivant **srv** comme un exemple de volumes LVM, ce chapitre couvre l'ajout d'un deuxième disque dur, la création d'un volume physique (PV), de l'ajouter au groupe de volumes (VG), l'extension du volume logique <nom de fichier rôle ="répertoire ">srv et enfin l'extension du système de fichiers. Cet exemple suppose un second disque dur a été ajouté au système. Dans cet exemple, le disque dur sera nommé <nom/dev/sdb et nous allons utiliser l'intégralité du disque en tant que volume physique (vous pouvez choisir de créer des partitions et de les utiliser comme des volumes physiques différents)

> ! Soyez sur que vous n'avez pas déjà un /dev/sdb existant avant d'exécuter les commandes ci-dessous. Vous pourriez perdre des données si vous exécutez ces commandes sur un disque qui n'est pas vide.

1. Commencez par créer le volume physique. Depuis un terminal, lancez :

```
sudo pvcreate /dev/sdb
```

2. Agrandissez maintenant le groupe de volumes (VG) :

```
sudo vgextend vg01 /dev/sdb
```

3. Servez-vous de **vgdisplay** pour afficher les extensions physiques libres (Free PE - Size). Prenons pour exemple un espace libre de 511 PE (équivalent à 2 Go pour une taille de PE égale à 4 Mo) et nous utiliserons entièrement cet espace.

   Le volume logique (LV) peut désormais être agrandi par des méthodes différentes. Nous ne verrons que l'utilisation de PE pour étendre le volume logique (LV) :

```
sudo lvextend /dev/vg01/srv -l +511
```

   L'option **-l** permet d'agrandir le volume logique LV en se servant de PE. L'option **-L** utilise la taille en octets (Mo, Go, To ...).

4. Même si vous êtes censé être en mesure de **développer** un système de fichiers ext3 ou ext4 sans le démonter d'abord, il peut être une bonne pratique de le démonter et vérifier de toute façon le système de fichiers, de sorte que vous n'avez pas gâcher le jour où vous voulez réduire un volume logique (dans ce cas, le démontage première est obligatoire).

Les commandes suivantes sont pour un système de fichiers **EXT3** ou **EXT4**. Si vous utilisez un autre système de fichiers, il peut exister d'autres utilitaires disponibles.

```
sudo umount /srv
sudo e2fsck -f /dev/vg01/srv
```

L'option **-f** de **e2fsck** force le contrôle, même si le système semble propre.

5. Enfin, redimensionnez le système de fichiers :

```
sudo resize2fs /dev/vg01/srv
```

6. Montez ensuite la partition et vérifiez sa taille.

```
mount /dev/vg01/srv /srv &amp;&amp; df -h /srv
```

2.4.2.4. Ressources

Voir les articles du Wiki Ubuntu sur LVM : https://help.ubuntu.com/community/Installation#lvm

Consultez le guide pratique LVM (en anglais) pour plus d'informations : http://tldp.org/HOWTO/LVM-HOWTO/index.html

Un autre bon article Managing Disk Space with LVM (en anglais) sur le site linuxdevcenter.com de O'Reilly : http://www.linuxdevcenter.com/pub/a/linux/2006/04/27/managing-disk-space-with-lvm.html

Pour de plus amples informations sur la commande **fdisk** consultez la page de man de fdisk : http://manpages.ubuntu.com/manpages/xenial/en/man8/fdisk.8.html .

2.4.3. iSCSI

Le protocole iSCSI peut être utilisé pour installer Ubuntu sur un système avec des disques durs dédiés ou non.

2.4.3.1. Installation sur un système sans disque dur

Les premiers pas d'une 'installation iSCSI sans disque dur sont identiques au *Chapitre 2, paragraphe 2. Installation à partir du CD*, jusqu'à la ligne « arrangement du disque dur ».

1. L'installation affichera une alerte avec le message suivant :
   `Aucun disque n'a été détecté. Si vous connaissez le nom du pilote nécessaire à votre unité de disque, vous pouvez le sélectionner dans la liste.`
2. Sélectionnez la proposition **Se connecter aux cibles iSCSI**.
3. Il vous sera proposé de saisir une adresse IP pour rechercher les cibles iSCSI, avec une description du format de l'adresse. Saisissez l'adresse IP de votre cible iSCSI et progressez jusqu'à <**continuer**> puis validez par **Entrée**.
4. Si une authentification est demandée, dans le but d'accéder au périphérique iSCSI, fournissez l'i**dentifiant** dans le champ suivant. Sinon, laissez-le vide.
5. Si votre système est capable de se connecter au fournisseur iSCSI, vous devriez voir une liste de

cibles iSCSI disponibles où le système d'exploitation peut être installé. La liste devrait ressembler à ceci :

```
Select the iSCSI targets you wish to use.

iSCSI targets on 192.168.1.29:3260:

[ ] iqn.2016-03.TrustyS-iscsitarget:storage.sys0

<Go Back>              <Continue>
```

6. Sélectionnez la cible iSCSI que vous voulez utiliser avec la barre Espace. Utilisez les flèches pour se positionner sur la cible que vous voulez utiliser.
7. Allez jusqu'à <**Continuer**> puis validez par **Entrée**.

Si la connexion avec la cible iSCSI est réussie, il vous sera proposé le menu d'installation **[!!] Partition des Disques**. Le reste de la procédure est identique à toute installation sur un disque dédié à un système. Lorsque l'installation est terminée, il vous sera demandé de redémarrer.

2.4.3.2. Installation d'un système avec un disque dédié

Comme précédemment, l'installation iSCSI d'un serveur courant sur un ou plusieurs disques dédiés est identique à l'installation présentée au *Chapitre 2, paragraphe 2. Installation à partir du CD* jusqu'à la partie consacrée à la partition du disque dur. Plutôt que d'utiliser une sélection guidée, vous devez suivre ces étapes :

1. Allez jusqu'à la ligne « Manuel » du menu
2. Sélectionnez la ligne« Configurez les volumes iSCSI »
3. Choisissez la cible « Se connecter à la cible iSCSI »
4. Il vous sera proposé de saisir une adresse IP pour rechercher les cibles iSCSI, avec une description du format de l'adresse. Saisissez l'adresse IP de votre cible iSCSI et progressez jusqu'à <**continuer**> puis validez par **Entrée**.
5. Si une authentification est demandée, dans le but d'accéder au périphérique iSCSI, fournissez l' **identifiant** dans le champ suivant. Sinon, laissez-le vide.
6. Si votre système est capable de se connecter au fournisseur iSCSI, vous devriez voir une liste de cibles iSCSI disponibles où le système d'opération peut être installé. La liste devrait ressembler à ceci :

```
Select the iSCSI targets you wish to use.

iSCSI targets on 192.168.1.29:3260:

[ ] iqn.2016-03.TrustyS-iscsitarget:storage.sys0

<Go Back>              <Continue>
```

7. Sélectionnez la cible iSCSI que vous voulez utiliser avec la barre Espace. Utilisez les flèches pour se positionner sur la cible que vous voulez utiliser.
8. Allez jusqu 'à <**Continuer>** et validez par **Entrée**.

9. Si vous avez réussi, vous reviendrez au menu vous proposant de vous connecter aux cibles iSCSI. Allez jusqu'à « **Terminer** » et validez par **Entrée**.

Le disque iSCSI récemment connecté apparaîtra dans la section de présentation comme un périphérique avec un préfixe SCSI. C'est ce disque que vous devez choisir comme disque d'installation. Une fois identifié, vous pouvez choisir n'importe quelle méthode de partitionnement.

> ! Selon la configuration de votre système, il peut y avoir d'autres disques SCSI dédiés à votre système. Faîtes très attention à bien identifier le bon périphérique avant l'installation. Sinon, une perte de données irréversible risque de se produire en cas d'installation sur le mauvais disque.

2.4.3.3. Redémarrer sur une cible iSCSI

La procédure est spécifique à votre plateforme matérielle. Pour exemple, voici comment redémarrer sur votre cible iSCSI en utilisant iPXE :

```
iPXE> dhcp

Configuring (net0 52:54:00:a4:f2:a9)....... ok

iPXE> sanboot iscsi:192.168.1.29::::iqn.2016-03.TrustyS-iscsitarget:storage.sys0
```

Si la procédure est réussie, vous devriez voir le menu Grub apparaître à l'écran.

2.5. Décharge de la mémoire vive

2.5.1. Introduction

La décharge de la mémoire vive signifie qu'une partie du contenu de la mémoire vive (RAM) est copiée sur disque lorsque l'exécution du noyau est perturbée. Les événements suivants peuvent causer la perturbation du noyau :

- Kernel Panic
- Interruptions non masquables (NMI)
- Erreur processeur (MCE)
- Problème matériel
- Intervention manuelle

Pour certains de ces événements (panique, NMI), le noyau réagit automatiquement et déclenche le mécanisme de décharge de la mémoire vive avec **kexec**. Dans d'autres situations, une intervention manuelle est nécessaire afin de capter la mémoire. Chaque fois que l'un des événements ci-dessus survient, il est important de trouver la cause originelle afin de l'empêcher de se reproduire. La cause peut être déterminé en examinant le contenu de la mémoire copiée.

2.5.2. Mécanisme de décharge de la mémoire vive kdump

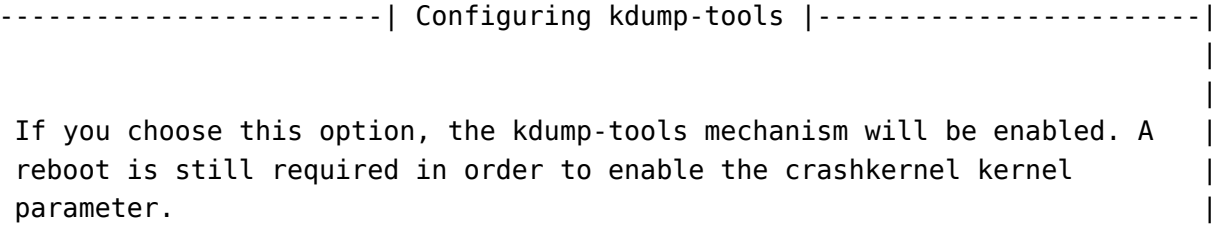
Quand survient une panique du noyau, le noyau s'appuie sur le mécanisme **kexec** pour redémarrer rapidement une nouvelle instance du noyau dans une partie de la mémoire pré-réservée, qui a été allouée lorsque le système a démarré (voir ci-dessous). Cela permet à la mémoire existante de rester inchangée, dans le but de sauvegarder en toute sécurité ses données en mémoire.

2.5.3. Installation

Le mécanisme de décharge de la mémoire vive est installé avec la commande suivante :

```
sudo apt install linux-crashdump
```

A partir de la version 16.04, le mécanisme de décharge de la mémoire vive est actif par défaut. Pendant l'installation, vous serez invité par le dialogue ci-dessous. Même non sélectionné, le mécanisme sera actif.



```
 |                                                                          |
 | Should kdump-tools be enabled by default?                                |
 |                                                                          |
 |                <Yes>                              <No>                   |
 |                                                                          |
 |--------------------------------------------------------------------------|
```

Si éventuellement vous voulez activer manuellement cette fonctionnalité, vous pouvez utiliser la commande **dpkg-reconfigure kdump-tools** et répondre Oui à la question posée. Vous pouvez aussi éditer le fichier /etc/default/kdump-tools en y incluant la ligne suivante :

```
USE_KDUMP=1
```

S'il n'y a pas eu de redémarrage depuis l'installation du paquet linux-crashdump, il doit être effectué pour activer le paramètre crashkernel= boot. Au redémarrage, kdump-tools sera activé et fonctionnel.

Si vous activez kdump-tools après un redémarrage, vous devez lancer la commande **kdump-config load** pour activer le mécanisme kdump.

2.5.4. Configuration

En plus de la décharge de la mémoire vive en local, il est maintenant possible d'utiliser la fonctionnalité d'une décharge distante, pour enregistrer les données de la mémoire vive sur un serveur distant, en utilisant l'un ou l'autre des protocoles SSH ou NFS.

2.5.4.1. Décharge de la mémoire vive en local

Les décharges locales sont configurées automatiquement et resteront en utilisation à moins qu'un protocole de décharge distante ne soit choisie. Une multitude d'options de configuration existent et sont soigneusement documentées dans le fichier /etc/default/kdump-tools.

2.5.4.2. Décharge distante de la mémoire vive avec le protocole SSH

Pour activer les décharges distantes en utilisant le protocole **SSH**, le fichier /etc/default/kdump-tools doit être modifié ainsi :

```
# ------------------------------------------------------------------------
# Remote dump facilities:
# SSH - username and hostname of the remote server that will receive the dump
#       and dmesg files.
# SSH_KEY - Full path of the ssh private key to be used to login to the remote
#           server. use kdump-config propagate to send the public key to the
#           remote server
# HOSTTAG - Select if hostname of IP address will be used as a prefix to the
#           timestamped directory when sending files to the remote server.
#           'ip' is the default.
SSH="ubuntu@kdump-netcrash"
```

La seule variable obligatoire à définir est la variable SSH. Elle doit contenir l'identifiant et le nom d'hôte du serveur distant utilisant la forme {identifiant}@{serveur distant}.

La variable SSH_KEY sera utilisée pour fournir une clé privée qui doit être utilisée. Sinon, la commande **kdump-config propagate** créera une nouvelle paire de clé. La variable HOSTTAG sera utilisée pour inclure le nom d'hôte du système, en tant que préfixe, dans le nom du répertoire distant qui sera créer, en lieu et place de l'adresse IP.

L'exemple suivant montre comment la commande **kdump-config propagate** est utilisée pour créer et propager une nouvelle pair de clés au serveur distant :

```
sudo kdump-config propagate
Need to generate a new ssh key...
The authenticity of host 'kdump-netcrash (192.168.1.74)' can't be established.
ECDSA key fingerprint is SHA256:iMp+5Y28qhbd+tevFCWrEXykDd4dI3yN4OVlu3CBBQ4.
Are you sure you want to continue connecting (yes/no)? yes
ubuntu@kdump-netcrash's password:
propagated ssh key /root/.ssh/kdump_id_rsa to server ubuntu@kdump-netcrash
```

Le mot de passe du compte utilisé sur le serveur distant sera requis dans le but d'envoyer, avec succès, la clé publique au serveur.

La commande **kdump-config** show peut être utilisée pour confirmer que kdump est correctement configuré pour utiliser le protocole SSH :

```
kdump-config show
DUMP_MODE:
kdump
USE_KDUMP:
KDUMP_SYSCTL:
1
kernel.panic_on_oops=1
KDUMP_COREDIR:
/var/crash
crashkernel addr: 0x2c000000
/var/lib/kdump/vmlinuz: symbolic link to /boot/vmlinuz-4.4.0-10-generic
kdump initrd:
/var/lib/kdump/initrd.img: symbolic link to /var/lib/kdump/initrd.img-4.4.0-10-generic
SSH:            ubuntu@kdump-netcrash
SSH_KEY:        /root/.ssh/kdump_id_rsa
HOSTTAG:        ip
current state:  ready to kdump
```

2.5.4.3. Décharge distante de la mémoire vive avec le protocole NFS

Pour activer les décharges distantes en utilisant le protocole **NFS**, le fichier /etc/default/kdump-tools doit être modifié ainsi :

```
# NFS - Hostname and mount point of the NFS server configured to receive
# the crash dump. The syntax must be {HOSTNAME}:{MOUNTPOINT}
# (e.g. remote:/var/crash)
#
NFS="kdump-netcrash:/var/crash"
```

Comme pour le protocole SSH, la variable HOSTTAG peut être utilisée pour remplacer l'adresse IP par le nom d'hôte comme préfixe du répertoire distant.

La commande **kdump-config show** peut être utilisée pour confirmer que kdump est correctement configuré pour utiliser le protocole SSH :

```
kdump-config show
DUMP_MODE:
USE_KDUMP: kdump
1
KDUMP_SYSCTL: kernel.panic_on_oops=1
KDUMP_COREDIR: /var/crash
crashkernel addr: 0x2c000000
/var/lib/kdump/vmlinuz: symbolic link to /boot/vmlinuz-4.4.0-10-generic
kdump initrd:
/var/lib/kdump/initrd.img: symbolic link to /var/lib/kdump/initrd.img-4.4.0-10-generic
NFS:              kdump-netcrash:/var/crash
HOSTTAG:          hostname
current state:    ready to kdump
```

2.5.5. Vérification

Pour confirmer que le mécanisme de décharge est activé, il y a quelques petites choses à vérifier. Tout d'abord, vérifiez que le paramètre de démarrage de **crashkernel** est présent (note: La ligne suivante a été scindé en deux pour s'adapter au format de ce document :

```
    cat /proc/cmdline
```

```
BOOT_IMAGE=/vmlinuz-3.2.0-17-server root=/dev/mapper/PreciseS-root ro
 crashkernel=384M-2G:64M,2G-:128M
```

Le paramètre **crashkernel** a la syntaxe suivante :

```
crashkernel=<range1>:<size1>[,<range2>:<size2>,...][@offset]
    range=start-[end] 'start' is inclusive and 'end' is exclusive.
```

Donc, pour le paramètre crashkernel trouvé dans /proc/cmdline, nous devrions avoir :

```
crashkernel=384M-2G:64M,2G-:128M
```

La valeur ci-dessus signifie :

- si le volume de la RAM est inférieure à 384 Mo, alors ne prévoyez pas de réserve (appelez au secours !)
- si la quantité de RAM se situe entre 386 Mo et 2 Go (exclusif), alors réservez 64 Mo
- si la quantité de RAM est supérieure à 2 Go, alors réservez 128 Mo

Deuxièmement, vérifiez que le noyau a réservé la zone de mémoire requise pour le noyau kdump en faisant :

```
dmesg | grep -i crash
```

```
...
[ 0.000000] Reserving 64MB of memory at 800MB for crashkernel (System RAM: 1023MB)
```

Enfin, comme vu précédemment, la commande **kdump-config show** montre les statuts courants de la configuration de kdump-tools :

```
        kdump-config show
DUMP_MODE: kdump
USE_KDUMP: 1
KDUMP_SYSCTL: kernel.panic_on_oops=1
KDUMP_COREDIR: /var/crash
crashkernel addr: 0x2c000000
   /var/lib/kdump/vmlinuz: symbolic link to /boot/vmlinuz-4.4.0-10-generic
kdump initrd:
      /var/lib/kdump/initrd.img: symbolic link to /var/lib/kdump/initrd.img-4.4.0-10-
generic
current state: ready to kdump

kexec command:
      /sbin/kexec -p --command-line="BOOT_IMAGE=/vmlinuz-4.4.0-10-generic
root=/dev/mapper/VividS--vg-root ro debug break=init console=ttyS0,115200 irqpoll
maxcpus=1 nousb systemd.unit=kdump-tools.service" --initrd=/var/lib/kdump/initrd.img
/var/lib/kdump/vmlinuz
```

2.5.6. Test du mécanisme de décharge sur incident

> ! Tester le mécanisme de décharge sur incident causera **un redémarrage du système**. Dans certains cas, cela peut entraîner une perte de données si le système est sous une charge lourde. Si vous voulez tester le mécanisme, assurez-vous que le système est au repos ou en charge très légère.

Vérifiez que le mécanisme **SysRq** est activé en regardant la valeur du paramètre noyau /proc/sys/kernel/sysrq :

```
cat /proc/sys/kernel/sysrq
```

Si une valeur de **0** est renvoyée, la fonction est désactivée. Activez-la avec la commande suivante :

```
sudo sysctl -w kernel.sysrq=1
```

Une fois cela fait, vous devez devenir root, comme nous venons utilisant **sudo** ne sera pas suffisant. Comme la racine d'utilisateur, vous devez exécuter la commande **echo c>/proc/sysrq-trigger** . Si vous utilisez une connexion réseau, vous perdrez le contact avec le système. C'est pourquoi il est préférable de faire le test tout en étant connecté à la console système. Ceci a l'avantage de rendre visible le processus de décharge sur incident de la mémoire vive.

Une sortie de test typique devrait ressembler à ce qui suit :

```
sudo -s
[sudo] password for ubuntu:
# echo c > /proc/sysrq-trigger
[ 31.659002] SysRq : Trigger a crash
[ 31.659749] BUG: unable to handle kernel NULL pointer dereference at (null)
[ 31.662668] IP: [<ffffffff8139f166>] sysrq_handle_crash+0x16/0x20
[ 31.662668] PGD 3bfb9067 PUD 368a7067 PMD 0
[ 31.662668] Oops: 0002 [#1] SMP
[ 31.662668] CPU 1
....
```

Le reste de la production est tronquée, mais vous devriez voir le système de redémarrer et quelque part dans le journal, vous verrez la ligne suivante:

```
Début: Enregistrement vmcore de crash du noyau ...
```

Une fois terminé, le système redémarre à son mode de fonctionnement normal. Vous trouverez alors le fichier de décharge sur incident dans le répertoire /var/crash :

```
ls /var/crash
```

```
linux-image-3.0.0-12-server.0.crash
```

2.5.7. Ressources

La décharge de la mémoire vive est un vaste sujet qui nécessite une bonne connaissance du noyau Linux. Vous pouvez trouver plus d'informations sur le sujet ici :

- Documentation de Kdump kernel : http://www.kernel.org/doc/Documentation/kdump/kdump.txt
- L'outil accident : http://people.redhat.com/~anderson/
- Analyse La décharge de la mémoire vive Linux (Basé sur Fedora, il donne toujours une bonne procédure pas à pas de l'analyse de décharge de la mémoire vive) : http://www.dedoimedo.com/computers/crash-analyze.html

Chapitre 3. Gestionnaire de paquets

Ubuntu a les caractéristiques d'un système de gestion exhaustive de paquets pour installer, mettre à jour, configurer et supprimer des logiciels. En plus de fournir un accès à une base de plus de 45000 paquets de logiciels pour votre installation Ubuntu, l'outil de gestion des paquets a des capacités de résolution des dépendances et de contrôle des mises à jour.

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

3.1. Introduction

Le système de gestion des paquets d'Ubuntu est dérivé de celui 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 fichiers de paquets Debian ont généralement une extension « .deb », et existent habituellement dans les **dépôts** qui sont une collecte de paquets trouvés sur différents supports comme les CD-ROM ou en ligne. Les paquets sont normalement dans un format binaire pré-compilé, donc l'installation est rapide et ne nécessite pas de compilation de logiciels.

Plusieurs paquets complexes utilisent des **dépendances**. Les dépendances sont des paquets additionnels nécessaires au paquet principal dans le but de fonctionner correctement. Par exemple, le paquet synthèse de la parole **festival** dépend du paquet **libasound2**, qui est un paquet qui fourni la bibliothèque de son **ALSA** nécessaire pour la réécoute auditive. Pour que l'application **festival** fonctionne, elle doit être installée ainsi que toutes ses dépendances. L'outil de gestion de logiciels d'Ubuntu exécutera cela automatiquement.

3.2. dpkg

dpkg est un gestionnaire de paquets pour les systèmes basés sur **Debian**. Il peut installer, supprimer et créer des paquets, mais, contrairement à d'autres systèmes de gestion de paquets, il ne peut pas télécharger automatiquement et installer des paquets avec leurs dépendances. Cette section traite de l'utilisation de **dpkg** pour gérer les logiciels installés localement :

- Pour lister tous les paquets installés sur le système, saisissez dans un terminal :

```
dpkg -l
```

- Selon le nombre de paquets installés sur votre système, ceci peut générer un nombre important d'information sur la sortie standard. Filtrez le résultat à l'aide de **grep** pour trouver un paquet particulier :

```
dpkg -l | grep apache2
```

- Remplacez **apache2** par un nom de paquet, par une partie du nom d'un paquet ou par une expression régulière.
- Pour lister les fichiers installés par un paquet, ici **ufw**, saisissez :

```
dpkg -L ufw
```

- Si vous n'êtes pas certain qu'un paquet est installé, **dpkg -S** peut vous aider. Par exemple :

```
dpkg -S /etc/host.conf
```

```
base-files : /etc/host.conf
```

- Le résultat montre que /etc/host.conf appartient au paquet **base-files**

Beaucoup de fichiers sont générés automatiquement lors de l'installation d'un paquet, et même si ils sont sur le système de fichiers, dpkg-S peut ignorer à quel paquet ils appartiennent.

- Vous pouvez installer un fichier local **.deb** en saisissant :

```
sudo dpkg -i zip_3.0-4_i386.deb
```

- Remplacez zip_3.0-4_i386.deb par le nom du fichier .deb que vous souhaitez installer.
- Vous pouvez désinstaller un paquet en saisissant :

```
sudo dpkg -r zip
```

Dans la plupart des cas, la désinstallation de paquets avec **dpkg** n'est **PAS** recommandée. Il est préférable d'utiliser un gestionnaire de paquets qui traite les dépendances pour être sûr que le système reste dans un état cohérent. Par exemple, la commande **dpkg -r zip** supprimera le paquet **zip**, mais tous les autres paquets dont il dépend resteront installés et ne fonctionneront plus correctement.

Pour lister les options de **dpkg**, consultez la page de manuel : **man dpkg**.

3.3. Apt

La commande **apt** est un outil en lignes de commandes puissant, qui fonctionne avec l'**outil avancé de gestion des paquets** (Advanced Packaging Tool ou APT) d'Ubuntu et exécute des fonctions telles que l'installation de nouveaux paquets logiciels, la mise à jour de paquets existants, la mise à jour de l'index de la liste des paquets, et même la mise à niveau du système Ubuntu dans son ensemble.

S'agissant d'un simple outil en lignes de commandes, **apt** présente un grand nombre d'avantage pour les administrateurs de serveurs, comparé à d'autres outils de gestion des paquets disponibles sous Ubuntu. Ces avantages incluent la simplicité d'utilisation à travers une simple connexion de terminal (SSH), et la possibilité de l'utiliser dans des scripts d'administration système, qui peuvent ensuite être automatisés par l'utilitaire de planification **cron**.

- **Installer un paquet** : L'installation de paquets avec l'outil **apt** est relativement simple. Par exemple, pour installer l'analyseur de réseau application>nmap, saisissez :

  ```
  sudo apt install nmap
  ```

- **Supprimer un paquet** : La suppression d'un ou plusieurs paquet(s) est également simple. Pour supprimer le paquet installé dans l'exemple précédent, saisissez :

  ```
  sudo apt remove nmap
  ```

  P **aquets multiples** : vous pouvez spécifier plusieurs paquets à installer ou à supprimer en les séparant par des espaces.

  L'option **--purge**, quand elle est ajoutée à **apt remove**, supprime aussi le fichier de configuration du paquet. Utilisez cette option avec prudence, selon l'effet désiré.

- **Mettre à jour l'index de paquets** : L'index de paquets APT est une base de données des paquets disponibles depuis les dépôts définis dans le fichier /etc/apt/sources.list et dans le répertoire /etc/apt/sources.list.d. Pour mettre à jour l'index local de paquets avec les dernières modifications opérées sur les dépôts, saisissez :

  ```
  sudo apt update
  ```

- **Mettre à jour les paquets** : Avec le temps, des versions plus récentes des paquets installés sur votre ordinateur peuvent être mises à disposition dans les dépôts de paquets (par exemple, des mises à jour de sécurité). Pour mettre à jour votre système, il faut d'abord mettre à jour votre index de paquets comme indiqué ci-dessus, avant de saisir :

  ```
  sudo apt upgrade
  ```

  Pour plus d'informations sur la mise à niveau vers une nouvelle version d'Ubuntu consultez le *Chapitre 2, paragraphe 3. Mise à niveau*.

Voici quelques exemples courants d'utilisation de l'utilitaire apt :

Les actions de la commande **apt**, comme l'installation et la désinstallation de paquets, sont enregistrées dans le fichier journal /var/log/dpkg.log.

Pour de plus amples informations à propos de l'utilisation de commande APT, veuillez lire le manuel

d’utilisation APT Debian exhaustif http://www.debian.org/doc/user-manuals#apt-howto ou tapez :

```
apt help
```

3.4. Aptitude

Le lancement d'**Aptitude** avec aucune option de ligne de commande, vous donnera une interface pilotée par des menus, basée sur du texte, de l'**Outil d'Empaquetage Avancé**(APT : Advanced Packaging Tool) . La plupart des fonctions communes de gestion de paquets, tels que l'installation, l'enlèvement et la mise à niveau, peut être effectuée dans **Aptitude** avec des commandes d'une touche, qui sont généralement des lettres minuscules.

Aptitude est le mieux adapté pour l'utilisation dans un environnement de terminal non graphique pour assurer le bon fonctionnement des touches de commande. Vous pouvez démarrer l'interface de menus de **Aptitude** en tant qu'utilisateur normal en tapant la commande suivante dans un terminal :

```
sudo aptitude
```

Lorsque **Aptitude** démarre, vous verrez une barre de menu en haut de l'écran et deux panneaux en dessous de cette barre. Le volet supérieur contient les catégories de paquets, comme **Nouveaux paquets** et **Paquets non installés**. Le volet inférieur contient des informations concernant les paquets et leurs catégories.

L'utilisation de **Aptitude** pour gérer des paquets est assez immédiate, et l'interface utilisateur facilite l'exécution des tâches usuelles. Voici des exemples de fonctions fréquentes de gestions de paquets dans **Aptitude** :

- **Installer des paquets** : Pour installer un paquet, localisez le via la catégorie des **paquets non installés** en utilisant les flèches du clavier et la touche **ENTRÉE**. Mettez le paquet désiré en surbrillance et appuyez sur la touche **+**. L'entrée du paquet devrait devenir **verte**, indiquant le marquage pour l'installation. Maintenant, appuyez sur **g** pour que les actions du paquet soient présentées. Appuyez encore sur **g**, le téléchargement et l'installation du paquet commenceront. Ceci terminé, appuyez sur **ENTRÉE** pour retourner au menu.
- **Supprimer des paquets** : pour supprimer un paquet, localisez le via la catégorie des **paquets installés** en utilisant les flèches du clavier et la touche **ENTRÉE**. Mettez en surbrillance le paquet que vous souhaitez supprimer et appuyez sur **-**. L'entrée du paquet devrait devenir **rose**, indiquant le marquage pour la suppression. Maintenant appuyez sur **g** pour que les actions du paquet soient présentées. Appuyez encore sur **g**, la suppression du paquet commencera. Ceci terminé, appuyez sur **ENTRÉE** pour retourner au menu.
- **Mise à jour de l'index des paquets** : Pour mettre à jour l'index des paquets, appuyez simplement sur la touche **u**. La mise à jour des paquets commencera.
- **Mise à niveau des paquets** : pour mettre à niveau les paquets, effectuez la mise à jour de l'index des paquets comme détaillé ci-dessus et appuyez sur **u** pour marquer les paquets ayant des mises à jour. Maintenant, appuyer sur la touche **g** au moyen de laquelle un résumé de l'action des paquets sera présenté. Appuyez de nouveau sur **g**, le téléchargement et l'installation commenceront. Ceci terminé, appuyez sur **ENTRÉE** pour retourner au menu.

La première colonne d'information affichée dans la liste des paquets du 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 : paquets installés

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 : à moitié configuré - la configuration a échoué et nécessite d'être réparée

H : à moitié installé - la suppression a échoué et nécessite d'être réparée

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**.

3.4.1. Ligne de commande Aptitude

Vous pouvez utiliser également la commande **Aptitude** comme un outil en ligne de commande, similaire à la commande **apt**. Pour installer le paquet **nmap** avec l'ensemble des dépendances nécessaires, comme dans l'exemple de la commande **apt**, vous pouvez utiliser la commande :

```
sudo aptitude install nmap
```

Pour enlever le même paquet, vous devez utiliser la commande :

```
sudo aptitude remove nmap
```

Consultez la page de **man** pour plus de détail sur les options de ligne de commande d'**Aptitude**.

3.5. Mises à jour automatiques

Le paquet **unattended-upgrades** peut être utilisé pour installer automatiquement les mises à jour de paquets. Il peut être configuré pour mettre à jour tous les paquets ou uniquement les mises à jour de sécurité. Installez d'abord le paquet en saisissant dans un terminal :

```
sudo apt install unattended-upgrades
```

Pour paramétrer **unattended-upgrades**, ouvrez /etc/apt/apt.conf.d/50unattended-upgrades et modifiez ce fichier à votre convenance :

```
Unattended-Upgrade::Allowed-Origins {
        "Ubuntu xenial-security";
// "Ubuntu xenial-updates";
};
```

Certains paquets peuvent être mis en **liste noire** et ne seront donc pas mis à jour automatiquement. Pour mettre un paquet en liste noire, ajoutez le à la liste :

```
Unattended-Upgrade::Package-Blacklist {
// "vim";
// "libc6";
// "libc6-dev";
// "libc6-i686";
};
```

Le double « *//* » sert à commenter, donc tout ce qui suit « *//* » ne sera pas pris en compte.

Pour activer la mise à jour automatique, modifiez le fichier /etc/apt/apt.conf.d/10periodic et configurez **apt** comme suit :

```
APT::Periodic::Update-Package-Lists "1";
APT::Periodic::Download-Upgradeable-Packages "1";
APT::Periodic::AutocleanInterval "7";
APT::Periodic::Unattended-Upgrade "1";
```

Cette configuration fera en sorte qu'à tous les jours, la liste des paquets sera actualisée et les mises à jour disponibles seront téléchargées puis installées. Les archives locales de téléchargement seront nettoyées à chaque semaine.

> Vous pouvez obtenir plus d'informations à propos des options de configuration de la périodicité de l'application **apt** dans l'en-tête du script /etc/cron.daily/apt.

Le résultat des **mises à jour automatiques** sera journalisé dans /var/log/unattended-upgrades.

3.5.1. Notifications

Le paramétrage de **Unattended-Upgrade::Mail** dans /etc/apt/apt.conf.d/50unattended-upgrades permettra l'envoi d'un courriel à l'administrateur détaillant tous les paquets pouvant être mis à jour ou ayant un problème.

Un autre paquet très utile est le paquet **apticron**. **apticron** permet de configurer une tâche **cron** pour envoyer un courriel à un administrateur sur n'importe quel paquet ayant des mises à jour disponibles, ou pour afficher un résumé des modifications de chaque paquet.

Pour installer **apticron**, saisissez dans un terminal :

```
sudo apt install apticron
```

Une fois que le paquet est installé, vous pouvez modifier l'adresse de courriel et d'autres options en modifiant /etc/apticron/apticron.conf :

```
EMAIL="root@example.com"
```

3.6. Configuration

La configuration du système de dépôt de l'**Outil d'Empaquetage Avancé** (APT) est stockée dans le fichier /etc/apt/sources.list et dans le repertoire /etc/apt/sources.list.d. Un exemple de ce fichier y est référencé, ainsi que des informations sur l'ajout ou la suppression de références de dépôt.

Vous pouvez modifier 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 16.04 _Xenial Xerus_ - Release i386 (20111013.1)]/ xenial main
restricted
```

3.6.1. Dépôts supplémentaires

En plus des dépôts de paquets officiellement supportés disponibles pour Ubuntu, il existe d'autres dépôts entretenus par la communauté qui mettent à votre disposition des milliers d'autres paquets. Deux des dépôts les plus populaires sont **Universe** et **Multiverse**. Ces derniers ne sont pas officiellement supportés par Ubuntu, mais du fait qu'ils sont entretenus par la communauté, ils fournissent en général des paquets qui sont sûrs pour votre ordinateur Ubuntu.

Les paquets du dépôt **Multiverse** posent souvent des problèmes de licence qui empêchent de les distribuer avec un système d'exploitation libre. Ils peuvent de plus être interdits par la législation de certains pays.

Soyez attentifs au fait que ni le dépôt **Universe** ni le dépôt **Multiverse** ne contiennent des paquets officiellement pris en charge. Il peut donc ne pas y avoir de mises à jour de sécurité pour ces paquets.

De nombreuses autres sources de paquets sont disponibles, et ne proposent parfois qu'un seul paquet, c'est le cas des sources proposés par les développeurs d'une application unique. Vous devriez cependant toujours faire très attention quand vous utilisez des sources exotiques. Recherchez des sources et des paquets avec prudence avant d'effectuer une installation. Certains paquets provenant de sources non fiables peuvent rendre votre système instable ou inutilisable à certains égards.

Les dépôts **Universe** et **Multiverse** sont activés par défaut, mais si vous voulez les désactiver, modifiez le fichier /etc/apt/sources.list et mettez en commentaire les lignes suivantes :

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

deb http://us.archive.ubuntu.com/ubuntu/ xenial universe
deb-src http://us.archive.ubuntu.com/ubuntu/ xenial universe
deb http://us.archive.ubuntu.com/ubuntu/ xenial-updates universe
deb-src http://us.archive.ubuntu.com/ubuntu/ xenial-updates universe

deb http://us.archive.ubuntu.com/ubuntu/ xenial multiverse
deb-src http://us.archive.ubuntu.com/ubuntu/ xenial multiverse
deb http://us.archive.ubuntu.com/ubuntu/ xenial-updates multiverse
deb-src http://us.archive.ubuntu.com/ubuntu/ xenial-updates multiverse

deb http://security.ubuntu.com/ubuntu xenial-security universe
deb-src http://security.ubuntu.com/ubuntu xenial-security universe
deb http://security.ubuntu.com/ubuntu xenial-security multiverse
deb-src http://security.ubuntu.com/ubuntu xenial-security multiverse
```

3.7. Références

La plupart des informations traités dans ce chapitre sont disponibles dans les pages de manuel **man**. Beaucoup de ces pages sont disponibles en ligne.

- La page du Wiki Ubuntu, consacrée à l'installation d'applications, comporte quelques informations complémentaires : https://help.ubuntu.com/community/InstallingSoftware
- Pour plus de détails sur la commande **dpkg** voir la page de man dpkg : http://manpages.ubuntu.com/manpages/xenial/en/man1/dpkg.1.html .
- Le guide APT : http://www.debian.org/doc/manuals/apt-howto/ et la page de man apt http://manpages.ubuntu.com/manpages/xenial/en/man8/apt.8.html contiennent des informations utiles sur l'utilisation d'**apt**.
- Voir la page de man aptitude http://manpages.ubuntu.com/manpages/xenial/man8/aptitude.8.html pour plus d'options **aptitude**.
- La page du Wiki Ubuntu francophone consacrée aux dépôts APT contient des renseignements supplémentaires sur l'ajout de dépôts : http://doc.ubuntu-fr.org/depots .

Chapitre 4. Utilisation du réseau

Les réseaux sont constitués d’au moins deux dispositifs, tels que des ordinateurs, des imprimantes ou des équipements similaires, connectés soit par câble soit par connexion sans-fil, dans le but de partager et de distribuer de l’information entre les dispositifs connectés.

Cette section fournit des informations générales, mais aussi spécifiques, relatives aux réseaux, comprenant une introduction aux concepts de base et une présentation détaillée des protocoles réseaux les plus connus.

4.1. Configuration du réseau

Ubuntu est fournie 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 en ligne de commande.

4.1.1. Interfaces Ethernet

Le système identifie les interfaces Ethernet à l'aide de la convention **ethX**, la valeur **X** étant un chiffre. La première interface Ethernet porte le nom **eth0**, la deuxième porte le nom **eth1**, et ainsi de suite.

4.1.1.1. Repérer les interfaces Ethernet

Pour repérer rapidement toutes les interfaces Ethernet disponibles, vous pouvez utilisez la commande **ifconfig** comme indiqué ci-après.

```
ifconfig -a | grep eth
```

```
eth0 Link encap:Ethernet HWaddr 00:15:c5:4a:16:5a
```

Une autre application capable d'identifier toutes les interfaces réseau disponibles sur votre système est la commande **lshw**. Dans l'exemple ci-dessous, **lshw** affiche une seule interface Ethernet avec le nom logique **eth0** suivi de plusieurs détails sur le bus, le pilote et les fonctionnalités prises en charge.

```
sudo lshw -class network
```

```
  *-network
       description: Ethernet interface
       product: BCM4401-B0 100Base-TX
       vendor: Broadcom Corporation
       physical id: 0
       bus info: pci@0000:03:00.0
       logical name: eth0
       version: 02
       serial: 00:15:c5:4a:16:5a
       size: 10MB/s
       capacity: 100MB/s
       width: 32 bits
       clock: 33MHz
       capabilities: (snipped for brevity)
       configuration: (snipped for brevity)
       resources: irq:17 memory:ef9fe000-ef9fffff
```

4.1.1.2. Noms logiques de l'interface Ethernet

La configuration des noms logiques des interfaces s'effectue à l'aide du fichier /etc/udev/rules.d/70-persistent-net.rules. Si vous voulez attribuer un nom logique particulier à une certaine interface, trouvez la ligne correspondant à son adresse MAC physique et modifiez la valeur de **NAME=ethX** afin de lui donner le nom

logique désiré. Redémarrez le système pour appliquer les changements.

4.1.1.3. Paramètres de l'interface Ethernet

ethtool est une application qui permet d'afficher et de changer les paramètres de la carte Ethernet comme l'auto-négociation, la vitesse des ports, le mode duplex et le « Wake-on-LAN ». Elle n'est pas installée par défaut, mais elle est disponible à l'installation dans les dépôts.

```
sudo apt install ethtool
```

Ce qui suit est un exemple de la façon de voir les fonctions prises en charge et les paramètres configurés d'une interface Ethernet.

```
sudo ethtool eth0
```

```
Settings for eth0:
        Supported ports: [ TP ]
        Supported link modes: 10baseT/Half 10baseT/Full
                              100baseT/Half 100baseT/Full
                              1000baseT/Half 1000baseT/Full
        Supports auto-negotiation: Yes
        Advertised link modes: 10baseT/Half 10baseT/Full
                               100baseT/Half 100baseT/Full
                               1000baseT/Half 1000baseT/Full
        Advertised auto-negotiation: Yes
        Speed: 1000Mb/s
        Duplex: Full
        Port: Twisted Pair
        PHYAD: 1
        Transceiver: internal
        Auto-negotiation: on
        Supports Wake-on: g
        Wake-on: d
        Current message level: 0x000000ff (255)
        Link detected: yes
```

Les modifications effectuées avec la commande **ethtool** sont temporaires et seront perdues au prochain redémarrage. Si vous souhaitez conserver ces paramètres, ajoutez simplement la commande **ethtool** sur une ligne **pre-up** du fichier de configuration de l'interface /etc/network/interfaces.

Vous trouverez ci-après la manière dont l'interface, identifiée comme **eth0**, peut être configurée de manière permanente avec une vitesse de port égale à 1000Mb/s en mode full duplex.

```
auto eth0
iface eth0 inet static
pre-up /sbin/ethtool -s eth0 speed 1000 duplex full
```

Bien que l'exemple ci-dessus montre l'interface configurée utilisant la méthode **statique**, cela fonctionne également avec les autres méthodes, comme DHCP. L'exemple a uniquement pour but de démontrer le placement approprié de l'élément **pre-up** en relation avec le reste de la configuration d'interface.

4.1.2. Adressage IP

La section qui suit décrit le processus de configuration de l'adresse IP et de la passerelle par défaut de votre système afin de le connecter à un réseau local et à Internet.

4.1.2.1. Assignation d'une adresse IP temporaire

Pour les configurations réseau temporaires, vous pouvez utiliser les commandes standard telles que **ip**, **ifconfig** et **route**, qui sont également présentes sur la plupart des systèmes d'exploitation GNU/Linux. Elles vous permettront de configurer les paramètres de façon à ce que les changements s'appliquent immédiatement, mais ces derniers seront perdus après un redémarrage.

Pour configurer temporairement une adresse IP, vous pouvez utiliser la commande **ifconfig** de la manière suivante. Modifiez simplement l'adresse IP et le masque de sous-réseau en fonction des besoins de votre réseau.

```
sudo ifconfig eth0 10.0.0.100 netmask 255.255.255.0
```

Afin de vérifier la configuration d'adresse IP de **eth0**, vous pouvez utiliser la commande **ifconfig** de la manière suivante.

```
ifconfig eth0
```

```
eth0 Link encap:Ethernet HWaddr 00:15:c5:4a:16:5a
          inet addr:10.0.0.100 Bcast:10.0.0.255 Mask:255.255.255.0
          inet6 addr: fe80::215:c5ff:fe4a:165a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:466475604 errors:0 dropped:0 overruns:0 frame:0
          TX packets:403172654 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2574778386 (2.5 GB) TX bytes:1618367329 (1.6 GB)
          Interrupt:16
```

Afin de configurer une passerelle par défaut, vous pouvez utiliser la commande **route**. Modifiez l'adresse de la passerelle par défaut en fonction de vos pré-requis réseau.

```
sudo route add default gw 10.0.0.1 eth0
```

Afin de vérifier la configuration de votre passerelle par défaut, vous pouvez utiliser la commande **route** de la manière suivante.

```
route -n
```

```
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
10.0.0.0 0.0.0.0 255.255.255.0 U 1 0 0 eth0
0.0.0.0 10.0.0.1 0.0.0.0 UG 0 0 0 eth0
```

Si vous avez besoin de DNS pour votre configuration réseau temporaire, vous pouvez ajouter les adresses IP du serveur DNS dans le fichier /etc/resolv.conf. En général, l'édition directe de /etc/resolv.conf n'est pas recommandée, sauf dans notre cas qui est une configuration temporaire et non persistante. L'exemple ci-dessous montre comment ajouter deux serveurs DNS à /etc/resolv.conf, adresses à modifier en fonction des

serveurs de votre réseau. Une meilleure description de la façon définitive de configurer le client DNS est dans la section suivante.

```
nameserver 8.8.8.8
Nameserver 8.8.4.4
```

Si vous n'avez plus besoin de cette configuration et que vous souhaitez supprimer toutes les configurations d'IP d'une interface, vous pouvez utiliser la commande **ip** avec l'option de purge comme indiqué ci-dessous.

```
ip addr flush eth0
```

Le nettoyage de la configuration IP en utilisant la commande **ip** n'efface pas les contenus de /etc/resolv.conf. Vous devez supprimer ou modifier ces entrées manuellement, ou redémarrer, ce qui devrait faire également que /etc/resolv.conf, qui est en fait maintenant un lien symbolique vers /run/resolvconf/resolv.conf, sera réécrit.

4.1.2.2. Attribution dynamique d'adresse IP (client DHCP)

Afin de configurer votre serveur pour qu'il utilise DHCP pour l'attribution dynamique d'adresse, ajoutez la méthode **dhcp** à la condition de famille d'adresse inet pour l'interface appropriée dans le fichier /etc/network/interfaces. L'exemple ci-dessous suppose que vous configurez votre première interface Ethernet identifiée comme **eth0**.

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

En ajoutant une configuration d'interface comme démontré ci-dessus, vous pouvez activer manuellement l'interface grâce à la commande **ifup** qui amorce le processus DHCP via **dhclient**.

```
sudo ifup eth0
```

Afin de désactiver manuellement l'interface, vous pouvez utiliser la commande **ifdown**, qui vous permettra d'amorcer l'annulation du processus DHCP et l'extinction de l'interface.

```
sudo ifdown eth0
```

4.1.2.3. Attribution statique d'adresse IP

Afin de configurer votre système pour utiliser l'attribution statique d'adresse IP, ajoutez la méthode **static** à la condition de famille d'adresse inet pour l'interface appropriée dans le fichier /etc/network/interfaces. L'exemple ci-dessous suppose que vous configurez votre première interface Ethernet identifiée comme **eth0**. Modifiez l'**adresse**, le **masque réseau**, et la **passerelle** en fonction des pré-requis de votre réseau.

```
auto eth0
iface eth0 inet static
address 10.0.0.100
netmask 255.255.255.0
Gateway 10.0.0.1
```

En ajoutant une configuration d'interface comme démontré ci-dessus, vous pouvez activer manuellement une interface grâce à la commande **ifup**.

```
sudo ifup eth0
```

Pour désactiver manuellement l'interface, vous pouvez utiliser la commande **ifdown**.

```
sudo ifdown eth0
```

4.1.2.4. Interface loopback

L'interface de boucle locale est identifiée par le système par **lo**, et possède l'adresse IP par défaut « 127.0.0.1 ». Elle est visible via la commande ifconfig.

```
ifconfig lo
```

```
lo Link encap:Local Loopback
         inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:2718 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2718 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:183308 (183.3 KB) TX bytes:183308 (183.3 KB)
```

Par défaut, il devrait y avoir deux lignes dans /etc/network/interfaces responsables de la configuration automatique de votre interface de boucle locale. Il est recommandé de conserver les paramètres par défaut, sauf si vous avez une raison spécifique de les modifier. un exemple des deux lignes par défaut est montré ci-dessous.

```
auto lo
iface lo inet loopback
```

4.1.3. Résolution de noms

La résolution de noms dans le domaine des réseaux IP est le processus de cartographie d'adresses IP en noms d'hôtes, facilitant l'identification des ressources sur un réseau. La section suivante expliquera comment configurer correctement votre système pour la résolution de noms en utilisant les enregistrements de noms d'hôte DNS et statiques.

4.1.3.1. Configuration de client DNS

Traditionnellement, le fichier /etc/resolv.conf était un fichier de configuration statique qui devait rarement être changé ou modifié automatiquement via les accroches client DCHP. Aujourd'hui, un ordinateur peut passer d'un réseau à un autre assez souvent et la structure de **resolvconf** est maintenant utilisée pour suivre ces changements et mettre à jour la configuration du solveur automatiquement. Il agit comme un intermédiaire entre les programmes qui fournissent l'information du serveur de noms et les applications qui ont besoin de cette information. Resolvconf s'est popularisé grâce à la fourniture de l'information via un ensemble de scripts accroche liés à la configuration de l'interface réseau. La différence la plus notable pour l'utilisateur est que tout changement effectué manuellement à /etc/resolv.conf sera perdu car il sera écrasé à chaque fois que quelque chose déclenche resolvconf. Au lieu de cela, resolvconf utilise les accroches client DHCP et /etc/network/interfaces pour générer une liste de serveurs de noms et de domaines à mettre dans le fichier

/etc/resolv.conf, qui est maintenant un lien symbolique :

```
/etc/resolv.conf -> ../run/resolvconf/resolv.conf
```

Pour configurer le solveur, ajouter les adresses IP des serveurs de noms, qui sont appropriés à votre réseau, dans le fichier /etc/network/interfaces. Vous pouvez également ajouter une liste de recherche avec un suffixe DNS pour correspondre à vos noms de domaine réseau. Pour toute autre option valide de configuration de resolv.conf, vous pouvez inclure, dans la strophe, une ligne commençant par ce nom d'option avec un préfixe **dns**-. Le fichier résultant peut ressembler à ce qui suit:

```
iface eth0 inet static
    address 192.168.3.3
    netmask 255.255.255.0
    gateway 192.168.3.1
    dns-search example.com
    Dns-nameservers 192.168.3.45 192.168.8.10
```

L'option de **recherche** peut également être utilisée avec plusieurs noms de domaine, de cette façon, les requêtes DNS seront ajoutées dans l'ordre dans lequel elles sont saisies. Par exemple, votre réseau peut avoir plusieurs sous-domaines à rechercher ; un domaine parent de **example.com**, et deux sous-domaines, **sales.example.com** et **dev.example.com**.

Si vous souhaitez rechercher plusieurs domaines, votre configuration pourrait ressembler à ce qui suit :

```
iface eth0 inet static
    address 192.168.3.3
    netmask 255.255.255.0
    gateway 192.168.3.1
    dns-search example.com sales.example.com dev.example.com
    Dns-nameservers 192.168.3.45 192.168.8.10
```

Si vous effectuez un ping sur l'hôte ayant le nom du **server1**, votre système interrogera automatiquement le DNS afin d'obtenir son nom de domaine complètement qualifié (FQDN : Fully Qualified Domain Names) dans l'ordre suivant :

1. server1**.exemple.com**
2. server1**.ventes.exemple.com**
3. server1**.dev.exemple.com**

Si aucun résultat n'est trouvé, le serveur DNS fournira un résultat de **notfound**, et la requête DNS échouera.

4.1.3.2. Noms d'hôte statiques

Les noms d'hôte statiques sont des cartographies noms d'hôte-à-IP définies localement et situés dans le fichier /etc/hosts. Les entrées du fichier hosts ont par défaut priorité sur le DNS. Cela signifie que si votre système essaye de résoudre un nom d'hôte et qu'il correspond à une entrée de /etc/hosts, il ne tentera pas de trouver un enregistrement dans le DNS. Dans certaines configurations, particulièrement lorsque l'accès Internet n'est pas requis, les serveurs communiquant avec un nombre limité de ressources peuvent être paramétrés avec commodité afin d'utiliser des noms d'hôtes statiques au lieu du DNS.

Ce qui suit est un exemple de fichier hosts où un nombre de serveurs locaux ont été identifiés par de simples noms d'hôtes, alias et leurs noms de domaine complètement qualifiés équivalents (FQDN).

```
127.0.0.1localhost
127.0.1.1ubuntu-server
```

```
10.0.0.11server1 server1.example.com vpn
10.0.0.12server2 server2.example.com mail
10.0.0.13server3 server3.example.com www
10.0.0.14server4 server4.example.com file
```

Dans l'exemple ci-dessus, notez que chaque serveur a reçu un alias en complément de son nom propre et FQDN. Le **Serveur1** a été défini par **vpn**, tandis que le **serveur2** est défini par **mail**, le **serveur3** par **www**, et le **serveur4** par **file**.

4.1.3.3. Configuration du Service de Changement de Nom

L'ordre dans lequel votre système sélectionne la méthode de résolution des noms d'hôtes en adresses IP est contrôlé par le fichier de configuration du Service de Changement de Nom (NSS : Name Service Switch) /etc/nsswitch.conf. Comme mentionné dans la section précédente, les noms d'hôtes typiquement statiques définis dans le fichier système /etc/hosts ont la préséance sur les noms résolus par DNS. Ci-dessous, un exemple de la ligne responsable de cet ordre de recherches de noms d'hôtes dans le fichier /etc/nsswitch.conf.

```
hosts: files mdns4_minimal [NOTFOUND=return] dns mdns4
```

- **files** essaie en premier lieu de résoudre les noms d'hôtes statiques situés dans le fichier /etc/hosts.
- **mdns4_minimal** tente de résoudre le nom utilisant la multidiffusion DNS.
- **[NOTFOUND=return]** signifie que n'importe quelle réponse de **notfound** par le processus précédent **mdns4_minimal** devrait être considérée comme autorité et que le système devrait arrêter de chercher une réponse.
- **dns** représente une ancienne requête mono-diffusion DNS.
- **mdns4** représente une requête multidiffusion DNS.

Afin de modifier l'ordre de la méthode de résolution de noms mentionnée ci-dessus, vous pouvez simplement modifier la chaîne de définition **hosts:** par la valeur de votre choix. Par exemple, si vous préférez utiliser la mono-diffusion DNS ancienne plutôt que la multidiffusion DNS, vous pouvez modifier la chaîne de définition dans le fichier /etc/nsswitch.conf comme expliqué ci-dessous.

```
hosts: files dns [NOTFOUND=return] mdns4_minimal mdns4
```

4.1.4. Pont réseau

Ponter plusieurs interfaces est une configuration plus élaborée, mais elle est très utile dans beaucoup de cas. Un premier scénario est de créer un pont avec plusieurs interfaces réseaux, puis d'utiliser un pare-feu pour filtrer le trafic entre les deux segments de réseau. Un autre scénario est d'utiliser un pont sur un système avec une seule interface pour autoriser plusieurs machines virtuelles à accéder au réseau extérieur. L'exemple suivant couvre ce dernier scénario.

Avant de configurer un pont, vous devez installer le paquet **bridge-utils**. Pour l'installer, tapez dans un terminal :

```
sudo apt install bridge-utils
```

Ensuite, configurez le pont en modifiant /etc/network/interfaces :

```
auto lo
```

```
iface lo inet loopback

auto br0
iface br0 inet static
        address 192.168.0.10
        network 192.168.0.0
        netmask 255.255.255.0
        broadcast 192.168.0.255
        gateway 192.168.0.1
        bridge_ports eth0
        bridge_fd 9
        bridge_hello 2
        bridge_maxage 12
        bridge_stp off
```

S aisissez les valeurs appropriées pour votre réseau et votre interface physique.

Maintenant, activez le pont :

```
sudo ifup br0
```

La nouvelle interface de pont doit maintenant être active et fonctionnelle. L'application **brctl** fournit des informations utiles à propos de l'état du pont, contrôle quelle interface fait partie du pont, etc... Consultez la page de **man brctl** pour plus d'informations.

La page du réseau du wiki Ubuntu contient des liens vers des articles traitant de la configuration avancée de réseaux : https://help.ubuntu.com/community/Network

La page de manuel pour resolvconf contient plus d'informations sur resolvconf : http://manpages.ubuntu.com/manpages/man8/resolvconf.8.html

La page de manuel sur la configuration des interfaces réseau contient des détails sur d'autres options pour /etc/network/interfaces : http://manpages.ubuntu.com/manpages/man5/interfaces.5.html

La page de manuel dhclient contient des détails sur d'autres options pour configurer les clients DHCP : http://manpages.ubuntu.com/manpages/man8/dhclient.8.html

Pour plus d'informations sur la configuration des clients DNS voir la page de manuel resolver : http://manpages.ubuntu.com/manpages/raring/fr/man5/resolver.5.html. En outre, le chapitre 6 du Guide d'Administration des Réseaux Linux de O'Reilly est une bonne source d'informations sur la configuration de resolver et du nom des services : http://oreilly.com/catalog/linag2/book/ch06.html

Pour plus d'informations sur le **pontage**, voir la page de manuel brctl : http://manpages.ubuntu.com/manpages/man8/brctl.8.html et la page Pontage-réseau du site de la fondation Linux : http://www.linuxfoundation.org/collaborate/workgroups/networking/bridge .

4.2. TCP/IP

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

4.2.1. Introduction à TCP/IP

TCP/IP sont en fait deux protocoles couvrant des aspects différents de la mise en réseau. **Internet Protocol - IP** s'occupe simplement de router les paquets en utilisant le **datagramme IP** comme unité de base d'information réseau. Le datagramme IP consiste en un en-tête suivi d'un message. **Transmission Control Protocol - TCP** permet aux hôtes d'établir des connexions pour échanger des flux de données. TCP garantit que les données sont bien délivrées d'un hôte vers un autre, dans l'ordre dans lequel elles sont parties.

4.2.2. Configuration TCP/IP

La configuration du protocole TCP/IP consiste en plusieurs éléments qui doivent être paramétrés en éditant les fichiers de configuration adaptés, ou en déployant des solutions telles qu'un serveur de Protocole de Configuration Dynamique des Hôtes (DHCP : Dynamic Host Configuration Protocol) qui, en retour, peut être configuré pour fournir automatiquement aux clients des définitions de configuration TCP/IP appropriées. Ces données de configuration doivent être définies correctement pour assurer un fonctionnement approprié du réseau avec votre système Ubuntu.

Les paramètres courants de configuration TCP/IP et leurs objectifs 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 d'une adresse qui fait au total 32 bits. Ce format est appelé **notation décimale pointée**.
- **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 sous-réseau.
- **Adresse Réseau** L'Adresse Réseau représente les octets constituant la partie réseau d'une adresse IP. Par exemple, l'hôte 12.128.1.2 dans un réseau de classe A utilisera l'adresse réseau 12.0.0.0, dans laquelle douze (12) représente le premier octet de l'adresse IP, (la partie réseau) et les zéros (0) des autres octets suivants représentent les valeurs d'hôtes potentiels. Un hôte réseau utilisant l'adresse privée 192.168.1.100 utilisera lui une Adresse Réseau de 192.168.1.0 qui indique les trois premiers octets du réseau de classe C 192.168.1 et un zéro (0) pour tous les hôtes possibles sur le réseau.
- **Broadcast Address** L'adresse de diffusion est une adresse IP utilisée pour envoyer un message à tous les hôtes d'un réseau local, plutôt qu'à un hôte en particulier. L'adresse de diffusion générale standard des réseaux IP est 255.255.255.255, mais cette adresse de diffusion ne peut toutefois pas être utilisée pour envoyer un message à tous les ordinateurs sur l'Internet car elle est bloquée par les routeurs. Une adresse de diffusion plus appropriée est déterminée pour correspondre à un sous-réseau particulier. Par exemple, sur le réseau IP privé de classe C, 192.168.1.0, l'adresse de

diffusion est 192.168.1.255. De tels messages de diffusion sont généralement produits par des protocoles réseaux tels que ARP (Address Resolution Protocol) et RIP (Router Information Protocol).

- **Adresse de la passerelle** Une adresse de passerelle est l'adresse IP à travers laquelle un réseau ou un hôte d'un autre réseau peuvent être atteints. Si un hôte veut communiquer avec un hôte d'un autre réseau, alors il doit utiliser la **passerelle**. En général cette passerelle sera le routeur du réseau, qui transmettra les données aux réseaux ou hôtes extérieurs n'appartenant au réseau privé, sur Internet par exemple. L'adresse de la passerelle doit être définie, sans quoi votre système sera incapable de communiquer avec des hôtes extérieurs à votre réseau.
- **Nameserver Address (adresse de serveur de noms)** représente les adresses IP d'un DNS (serveur de noms de domaine), qui résout les noms de domaines en adresses IP. Il y a trois niveaux d'adresses de serveur de noms qui peuvent être par ordre de priorité : serveur de noms **primaire**, serveur de noms **secondaire** et serveur de noms **tertiaire**. Pour que votre système puisse résoudre les noms d'hôtes, vous devez spécifier une adresse de serveur de noms correcte que vous êtes autorisés à utiliser sur votre réseau. Dans bien des cas, ces adresses seront fournies par votre fournisseur de service réseau mais vous pouvez aussi utiliser des serveurs de noms publics tel que les serveurs Verizon (IP 4.2.2.1 à 4.2.2.6).

L'adresse IP, le masque de réseau, l'adresse réseau, l'adresse de diffusion, l'adresse de la passerelle et les adresses de serveurs de noms sont généralement spécifiées par les directives appropriées dans le fichier /etc/network/interfaces. Pour plus d'informations, voir la page de manuel système concernant les interfaces, avec la commande suivante tapée dans un terminal :

Accédez au manuel du fichier interfaces avec la commande suivante :

```
man interfaces
```

4.2.3. Routage IP

Le routage IP est une technique pour spécifier et découvrir des chemins dans un réseau TCP/IP dans lequel les données sont amenées à transiter. Le routage utilise un ensemble de tables appelées **tables de routage** pour acheminer les paquets de données de leur source vers leur destination, souvent via plusieurs nœuds intermédiaires du réseau dénommés **routeurs**. Il existe deux principales formes de routage IP : **le routage statique** et **le routage dynamique.**

Le routage statique implique l'ajout manuel de règle de routage IP à la table de routage du système et généralement cela se fait en manipulant la table de routage avec la commande **route**. Le routage statique bénéficie de plusieurs avantages par rapport au routage dynamique, comme la simplicité de son implantation dans des petits réseaux, la prévisibilité (la table de routage est toujours calculée à l'avance et donc, la route est toujours la même à chaque fois qu'elle est utilisée), et la faible charge sur les autres routeurs et les liaisons réseaux du fait de l'absence de routage dynamique. Cependant, le routage statique présente également quelques désavantages. Par exemple, le routage statique est limité aux petits réseaux et n'est pas très extensible. Le routage statique n'arrive absolument pas à s'adapter aux pannes et aux erreurs du réseau rencontrés le long de la route, du fait même de sa nature fixe.

Le routage dynamique concerne les grands réseaux qui offrent de multiples routes IP possibles entre une source et une destination et qui utilisent des protocoles de routage spéciaux comme RIP (Router Information Protocol) lesquels gèrent automatiquement les tables de routage qui rendent le routage dynamique possible. Le routage dynamique possède de nombreux avantages sur le routage statique, comme une expansibilité supérieure, et la capacité à surmonter les erreurs et les pannes rencontrées au cours de l'acheminement des données. De plus, il nécessite moins de configuration manuelle dans les tables de routage car les routeurs apprennent entre eux leurs existences et les routes disponibles. Cette caractéristique permet également d'éliminer les possibilités d'introduction d'erreurs humaines dans les tables de routage. Mais le routage dynamique n'est pas parfait et présente des désavantages comme une complexité accrue et un temps de latence supplémentaire dû aux communications entre les routeurs qui ne

profite pas directement à l'utilisateur mais consomme néanmoins de la bande passante.

4.2.4. TCP et UDP

TCP est un protocole dit "connecté", qui permet la correction d'erreurs, et garantit que les données arriveront à destination grâce à un **contrôle de transmission**. Le contrôle de transmission détermine quand le flux de données doit être stoppé, et les paquets précédents devraient être retransmis 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 transmission 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 transmission, mais aussi car la perte de quelques paquets n'est généralement pas importante pour ces applications.

4.2.5. ICMP

Le Protocole de Contrôle de Messagerie Internet (ICMP : Internet Control Messaging Protocol) est une extension du Protocole Internet (IP) défini dans la Demande Pour Commentaires (RFC : Request For Comments) #792 et qui supporte les paquets réseau contenant 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.

4.2.6. Démons

Les démons sont des applications particulières qui s'exécutent généralement en permanence en tâche de fond, et qui attendent des requêtes venant d'autres applications pour les fonctions qu'ils exercent. De nombreux démons sont liés au réseau, et donc beaucoup de démons 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.

4.2.7. Ressources

Il y a des pages de man pour TCP : http://manpages.ubuntu.com/manpages/xenial/en/man7/tcp.7.html et IP : http://manpages.ubuntu.com/manpages/xenial/man7/ip.7.html qui contiennent d'autres informations utiles.

Voir aussi le Livre Rouge d'IBM Tutoriel et Survol Technique de TCP/IP : http://www.redbooks.ibm.com/abstracts/gg243376.html .

Une autre ressource est celle d'O'Reilly : Administration de réseau TCP/IP : http://oreilly.com/catalog/9780596002978/

4.3. Protocole de Configuration Dynamique des Hôtes (DHCP)

Le protocole DHCP (Dynamic Host Configuration Protocol) est un service réseau qui permet aux ordinateurs hôtes clients d'être configurés automatiquement à partir d'un serveur. Cela évite la configuration manuelle de chaque client du réseau. Les ordinateurs configurés pour être clients DHCP n'ont aucun contrôle sur les paramètres qu'ils reçoivent du serveur DHCP, et cette configuration est totalement transparente pour l'utilisateur.

Les éléments de configuration les plus communs fournis par un serveur DHCP à un client DHCP comprennent :

- Adresse IP et netmask (masque réseau)
- Adresse IP de la passerelle par défaut à utiliser
- Adresses IP des serveurs DNS à utiliser

Cependant, un serveur DHCP peut également fournir des éléments de configuration tels que :

- Nom d'hôte
- Nom de domaine
- Serveur de temps
- Serveur d'impression

L'avantage d'utiliser un serveur DHCP est qu'un changement dans la configuration du réseau, par exemple un changement d'adresse d'un serveur DNS, n'a alors besoin d'être changé que sur le serveur DHCP. Tous les clients réseau seront reconfigurés lors de leur prochaine connexion au serveur DHCP. Un autre avantage est l'intégration plus facile de nouveaux ordinateurs dans le réseau, puisqu'il n'y a pas besoin de vérifier les adresses IP disponibles. Les conflits dans les allocations d'adresses IP sont également réduits.

Un serveur DHCP peut fournir des paramètres de configuration à l'aide des méthodes suivantes :

- **Allocation manuelle (adresse MAC)**

  Cette méthode implique l'utilisation du protocole DHCP pour identifier l'adresse matérielle unique (MAC) de chaque carte réseau connectée au réseau et ensuite de continuellement fournir une configuration constante chaque fois que le client DHCP effectue une demande vers le serveur DHCP en utilisant ce dispositif de réseau. Cela garantit qu'une adresse particulière est attribuée automatiquement à cette carte réseau, basée sur son adresse MAC.

- **Allocation dynamique (pool d'adresses)**

  Dans cette méthode, le serveur DHCP attribue une adresse IP à partir d'un pool d'adresses (parfois aussi appelé une gamme ou étendue) pour une période de temps ou de la location, qui est configuré sur le serveur ou jusqu'à ce que le client informe le serveur qu'il doesn plus 't besoin de l'adresse. De cette façon, les clients recevront leur propriétés de configuration dynamique et sur une "premier arrivé, premier servi " base. Quand un client DHCP ne est plus sur le réseau pour une période déterminée, la configuration est expire et est remise à la piscine d'adresse pour une utilisation par d'autres clients DHCP. De cette façon, une adresse peut être loué ou utilisé pour une période de temps. Après cette période, le client doit renégocier le bail avec le serveur de maintenir l'utilisation de l'adresse.

- **Allocation automatique**

  Avec cette méthode, le serveur DHCP attribue automatiquement une adresse IP permanente à un appareil en la sélectionnant parmi une gamme d'adresses disponibles. Habituellement, DHCP est

utilisé afin d'attribuer une adresse temporaire à un client, mais cependant, un serveur DHCP peut permettre un bail infini.

Les deux dernières méthodes peuvent être considérées comme "automatique " parce que dans chaque cas, le serveur DHCP attribue une adresse sans aucune intervention supplémentaire nécessaire. La seule différence entre eux est dans combien de temps l'adresse IP est louée, en d'autres termes si l'adresse d'un client varie au fil du temps. Ubuntu est livré avec deux serveurs DHCP et le client. Le serveur est **dhcpd** (démon de protocole de configuration d'hôte dynamique). Le client fourni avec Ubuntu est **dhclient** et doit être installé sur tous les ordinateurs devant être configuré automatiquement. Les deux programmes sont faciles à installer et à configurer et seront lancés automatiquement au démarrage du système.

4.3.1. Installation

Pour installer **dhcpd**, exécutez la commande suivante dans un terminal :

```
sudo apt install isc-dhcp-server
```

Vous devrez probablement changer la configuration par défaut en éditant le fichier /etc/dhcp/dhcpd.conf afin de répondre à vos besoins et ceux des configurations particulières.

Vous pourrez également avoir besoin d'éditer le fichier /etc/default/isc-dhcp-server pour spécifier les interfaces que dhcpd doit écouter.

NOTE : les messages de dhcpd sont envoyés à syslog. Consultez ce journal pour récupérer les messages de diagnostiques.

4.3.2. Configuration

Le message d'erreur qui termine l'installation est un peu déroutant, mais les étapes suivantes vont vous aider à configurer proprement le service :

Le plus souvent, vous voudrez allouer les adresses IP aléatoirement. Ceci peut être fait avec la configuration suivante :

```
# minimal sample /etc/dhcp/dhcpd.conf
default-lease-time 600;
max-lease-time 7200;

subnet 192.168.1.0 netmask 255.255.255.0 {
 range 192.168.1.150 192.168.1.200;
 option routers 192.168.1.254;
 option domain-name-servers 192.168.1.1, 192.168.1.2;
 option domain-name "mydomain.example";
}
```

Ceci fera que le serveur DHCP donnera aux clients une adresse IP dans la plage 192.168.1.150-192.168.1.200. Il allouera une adresse IP pendant 600 secondes si le client ne demande pas un délai précis. Sinon, le bail maximum (autorisé) sera de 7 200 secondes. Le serveur « conseillera » également au client d'utiliser 192.168.1.254 en tant que passerelle par défaut et les adresses 192.168.1.1 et 192.168.1.2 comme serveurs DNS.

Après un changement dans le fichier de configuration, vous devez redémarrer **dhcpd** :

```
sudo systemctl restart isc-dhcp-server.service
```

4.3.3. Références

La page wiki Ubuntu dhcp3-server possède de plus amples informations. : https://help.ubuntu.com/community/dhcp3-server

Pour plus d'options pour /etc/dhcp/dhcpd.conf, consultez le manuel de dhcpd.conf : http://manpages.ubuntu.com/manpages/xenial/en/man5/dhcpd.conf.5.html

ISC dhcp-server : http://www.isc.org/software/dhcp

4.4. Synchronisation temporelle avec NTP

NTP est un protocole TCP/IP permettant de synchroniser les horloges à travers un réseau. De manière basique, un client demande l'heure actuelle à un serveur et l'utilise pour ajuster sa propre horloge.

Derrière cette simple description, il y a beaucoup de complexité - il y a un plusieurs niveaux de serveurs NTP, les serveurs NTP de niveau un reliés à des horloges atomiques, et les serveurs de niveau deux et trois partageant la charge de traitement des demandes à travers Internet. De plus, le logiciel client est beaucoup plus complexe que vous ne le pensez - il doit tenir compte des délais de communication, et de régler le temps d'une manière qui ne perturbe pas les autres processus qui s'exécutent sur le serveur. Mais heureusement, toute cette complexité vous-est cachée !

Ubuntu utilise ntpdate et ntpd.

4.4.1. timedatectl

Dans les versions récentes d'Ubuntu **timedatectl** remplace **ntpdate**. Pas défaut, **timedatectl** synchronise l'heure une fois au boot, et plus tard, à l'activation des sorties(sockets) utilisées pour tester à nouveau lorsque les connexions au réseau deviennent actives.

Si **ntpdate / ntp** est installé, **timedatectl** s'interdit d'agir pour vous laisser garder votre ancienne installation. Cela assurera qu'il n'y a pas deux services de synchronisation de l'heure qui s'affrontent et, également, pour conserver n'importe quelle sorte de configuration ancienne ou comportement que vous avez acquis lors d'une mise à jour. Mais cela implique qu'une mise à jour ancienne, par le biais de ntp/ntpdate, resterait toujours installée et, donc, rend les nouveaux services basés sur systemd inactifs.

4.4.2. timesynsd

Dans les récentes versions d'Ubuntu, **timesyncd** remplace la partie client de **ntpd**. Par défaut, **timesyncd** teste et conserve régulièrement l'heure dans sync. Il enregistre également localement les mises à jours de l'heure, et donc après les redémarrages, il avance de façon monotone, si cela est applicable.

L'heure courante et sa configuration via **timedatectl** et **timesyncd** peuvent être testés par la commande **timedatectl status**.

```
timedatectl status
      Local time: Fri 2016-04-29 06:32:57 UTC
  Universal time: Fri 2016-04-29 06:32:57 UTC
        RTC time: Fri 2016-04-29 07:44:02
       Time zone: Etc/UTC (UTC, +0000)
 Network time on: yes
NTP synchronized: no
 RTC in local TZ: no
```

Si NTP est installé et remplace la fonction de la commande **timedatectl**, la ligne "NTP synchronized" est à la valeur yes.

Le nom du serveur pour aller chercher l'heure des commandes **timedatectl** et **timesyncd** peut être désigné dans /etc/systemd/timesyncd.conf et à l'aide de fichiers de configuration additionnels souples dans /etc/systemd/timesyncd.conf.d/.

4.4.3. ntpdate

La commande **ntpdate** est considéré abandonnée, en faveur de la commande **timedatectl**, et ainsi, n'est plus installé par défaut. Si installée, elle se lancera une fois pendant l'initialisation pour fixer l'heure de votre système, en accord avec le serveur NTP d'Ubuntu. Ensuite, dès qu'une nouvelle interface se lance, elle réessaie de mettre à jour l'heure – en faisant cela, elle tentera de ralentir le mouvement de l'heure, tant que l'écart à couvrir n'est pas trop grand. Ce comportement peut être contrôlé par les boutons **-B/-b**.

```
ntpdate ntp.ubuntu.com
```

4.4.4. timeservers

Par défaut, les outils basés sur systemd demandent les informations de l'heure à l'adresse ntp.ubuntu.com. Selon la base classique ntpd, le service utilise le groupe de [0-3].ubuntu.pool.ntp.org Of the pool number 2.ubuntu.pool.ntp.org, bien que le site ntp.ubuntu.com supporte également ipv6 si nécessaire. Si un utilisateur a besoin de forcer ipv6, il y a aussi ipv6.ntp.ubuntu.com qui n'est pas configuré par défaut.

4.4.5. ntpd

Le démon ntp, appelé ntpd, calcule la dérive de l'horloge de votre système et l'ajuste en permanence, donc il n'y a pas de fortes corrections qui pourraient conduire à des journaux incohérents par exemple. Son coût est un peu de temps de processeur et de mémoire, mais pour un serveur moderne, cela est négligeable.

4.4.6. Installation

Pour installer ntpd, saisissez à partir d'une invite de terminal :

```
sudo apt install ntp
```

4.4.7. Configuration

Modifiez /etc/ntp.conf pour ajouter ou supprimer des lignes de serveur. Par défaut, ces serveurs sont configurés :

```
# Use servers from the NTP Pool Project. Approved by Ubuntu Technical Board
# on 2011-02-08 (LP: #104525). See http://www.pool.ntp.org/join.html for
# more information.
server 0.ubuntu.pool.ntp.org
server 1.ubuntu.pool.ntp.org
server 2.ubuntu.pool.ntp.org
server 3.ubuntu.pool.ntp.org
```

Après un changement dans le fichier de configuration, vous devez recharger **ntpd** :

```
sudo systemctl reload ntp.service
```

4.4.8. Afficher l'état

Utilisez ntpq pour voir plus d'informations :

```
# sudo ntpq -p
     remote           refid              st t when     poll  reach        delay
offset   jitter
==============================================================================  ====
+stratum2-2.NTP.  129.70.130.70   2  u   5       64   377   68.461 -44.274  110.334
+ntp2.m-online.n  212.18.1.106    2  u   5       64   377   54.629 -27.318   78.882
*145.253.66.170   .DCFa.         1  u  10       64   377   83.607 -30.159   68.343
+stratum2-3.NTP.  129.70.130.70   2  u   5       64   357   68.795 -68.168  104.612
+europium.canoni  193.79.237.14   2  u  63       64   337   81.534 -67.968   92.792
```

4.4.9. Prise en charge de PPS

Depuis la version 16.04, ntp supporte la discipline PPS qui peut être utilisé pour améliorer ntp avec des sources de référence d'heure pour une meilleure précision. Pour plus de détails sur la configuration, voir les ressources externes à PPS, listées ci-dessous.

4.4.10. Références

Veuillez consulter la page wiki en anglais **Ubuntu Time** pour de plus amples informations : https://help.ubuntu.com/community/UbuntuTime

ntp.org, page d'accueil du projet Network Time Protocol : http://www.ntp.org/

Foire aux questions de ntp.org sur la configuartion de PPS : http://www.ntp.org/ntpfaq/NTP-s-config-adv.htm#S-CONFIG-ADV-PPS

4.5. Kit de développement de plans de données

Le kit de développement de plans de données (Data Plane Development Kit, DPKP) est un jeu de bibliothèques et de pilotes pour le traitement rapide de paquets qui fonctionne principalement dans le monde de Linux. C'est une de bibliothèques qui fournit la couche d'abstraction de l'environnement (« Environment Abstraction Layer » ou EAL). L'EAL masque les détails de l'environnement et fournit une interface de programmation standard. Elle est communément utilisée dans des solutions spécifiques par exemple la virtualisation de fonctions réseau et les changements avancés de réseaux à haute capacité de traitement. Le DPDK utilise un modèle d'auto-exécution pour la réalisation rapide de plans de données et accède aux périphériques par interrogation active pour éliminer la latence d'interruption de processus. En contrepartie, il est gourmand en ressources CPU. Il a été conçu pour fonctionner avec n'importe quel processeur. Si les processeurs Intel x86 ont été les premiers à être pris en charge, DPDK a été étendu à IBM Power 8, EZchip ILE-Gx et ARM.

En ce moment, Ubuntu prend en charge la version 2.2 de DPDK et fournit une infrastructure pour faciliter son utilisation.

4.5.1. Prérequis

Ce paquet est compilé de manière à limiter autant que possible l'utilisation des ressources CPU. Néanmoins, sa prise en charge par la CPU nécessite au moins SSE3.

La liste des cartes réseau génériques supportant DPDK peut être trouvée à l'adresse NICs supportées : http://dpdk.org/doc/nics. Mais un grand nombre d'entre-elles sont désactivées pas défaut dans le Projet générique parce qu'elle ne sont pas dans un état totalement stable. Le sous-groupe de cartes réseau que DPDK a activées comme disponibles dans le paquet, pour Ubuntu 16.04 sont :

Intel

- e1000em.htmle1000 (82540, 82545, 82546) : http://dpdk.org/doc/guides/nics/
- e1000e (82571..82574, 82583, ICH8..ICH10, PCH..PCH2) : http://dpdk.org/browse/dpdk/tree/drivers/net/e1000/
- igb (82575..82576, 82580, I210, I211, I350, I354, DH89xx) : http://dpdk.org/browse/dpdk/tree/drivers/net/e1000/
- ixgbe (82598..82599, X540, X550) : http://dpdk.org/doc/guides/nics/ixgbe.html
- i40e (X710, XL710, X722) : http://dpdk.org/browse/dpdk/tree/drivers/net/i40e/
- fm10k (FM10420) : http://dpdk.org/doc/guides/nics/fm10k.html

Chelsio

- cxgbe (Terminator 5) : http://dpdk.org/doc/guides/nics/cxgbe.html

Cisco

- enic (UCS Virtual Interface Card) : http://dpdk.org/browse/dpdk/tree/drivers/net/enic
- Paravirtualization
- virtio-net (QEMU) : http://dpdk.org/doc/guides/nics/virtio.html
- vmxnet3 : http://dpdk.org/doc/guides/nics/vmxnet3.html

Autres

- af_packet (Linux AF_PACKET socket) : http://dpdk.org/browse/dpdk/tree/drivers/net/af_packet
- ring (memory) : http://dpdk.org/doc/guides/nics/pcap_ring.html#rings-based-pmd

En plus, la version permet de façon expérimentale les deux pilotes PMD suivants parce qu'ils représentent des périphériques (virtuels) qui sont très accessibles par les utilisateurs finaux.

Paravirtualization

- xenvirt (Xen) : http://dpdk.org/doc/guides/xen/pkt_switch.html#xen-pmd-frontend-prerequisites

Autres

- pcap (file or kernel driver) : http://dpdk.org/doc/guides/nics/pcap_ring.html#libpcap-based-pmd

Les cartes doivent perdre l'assignation à leur noyau, et à la place, être assignées au pilote uio_pci_generic ou vfio-pci. Le pilote uio_pci_generic est plus ancien et habituellement s'active plus facilement.

Le nouveau pilote vfio-pci nécessite que vous activiez les paramètres du noyau suivants pour rendre actif iommu.

```
iommu=pt intel_iommu=on
```

En plus, pour vfio-pci vous avez donc à configurer et assigner au groupe iommu correspondant.

Note : dans l'environnement basé sur virtio, il est suffisant de dé-assigner les périphériques du pilote du noyau. Sans cela, DPDK refusera d'utiliser le périphérique pour éviter les dysfonctionnements avec le noyau et DPDK travaillant avec le périphérique en même temps. Depuis que DPDK peut travailler directement sur les périphériques virtio, il n'est pas nécessaire d'assigner uio_pci_generic à ces périphériques.

La configuration manuelle et des vérifications d'état peuvent se faire via sysfs ou avec l'outil dpdk_nic_bind

```
dpdk_nic_bind --help

Syntaxe :
------

dpdk_nic_bind [options] PÉRIPHÉRIQUE1 PÉRIPHÉRIQUE2 ....

où PÉRIPHÉRIQUE1, PÉRIPHÉRIQUE2, etc., son spécifiés avec la syntaxe PCI
« domain:bus:slot.func » ou la syntaxe « bus:slot.func ».
Pour les périphériques liés aux pilotes du noyau Linux, on peut aussi
indiquer leur nom d'interface Linux, par exemple eth0, eth1, em0, em1, etc.

Options :
--help, --usage:
Afficher les informations d'utilisation et quitter

-s, --status :
Afficher l'état actuel de toutes les interfaces réseau connues.
Pour chaque périphérique, la commande affiche les domaine PCI, bus,
connecteur d'extension et fonction, ainsi qu'une description textuelle
du périphérique. Selon que le périphérique est utilisé par un pilote
du noyau, le pilote igb_uio ou aucun pilote, d'autres informations
pertinentes seront affichées :
* le nom de l'interface Linux, par exemple if=eth0
```

```
* le pilote utilisé, par exemple drv=igb_uio
* tout pilote adapté qui n'utilise pas le périphérique actuellement,
par exemple unused=igb_uio
NOTE : si cette option est passée avec une option bind/unbind,
l'affichage de l'état se fera toujours après que les autres opérations
ont eu lieu.

-b pilote, --bind=pilote :
Choisir le pilote à utiliser ou « none » (aucun) pour dissocier le périphérique

-u, --unbind :
Dissocier un périphérique (équivalent à « -b none »)

--force :
Par défaut, les périphériques qui sont utilisés par Linux - indiqués
comme ayant des routes dans la table de routage - ne peuvent pas
être modifiés. L'utilisation de l'option --force ignore ce comportement
en autorisant le forçage de la dissociation des liens actifs.
AVERTISSEMENT : Ceci peut conduire à des pertes de connexion
réseau et devrait être utilisé avec prudence.

Exemples :
---------

Pour afficher l'état actuel des périphériques :
dpdk_nic_bind --status

Pour dissocier eth1 du pilote actuel et le lier à igb_uio :
dpdk_nic_bind --bind=igb_uio eth1

Pour dissocier 0000:01:00.0 de tout pilote :
dpdk_nic_bind -u 0000:01:00.0

Pour lier 0000:02:00.0 et 0000:02:00.1 au pilote du noyau ixgbe :
dpdk_nic_bind -b ixgbe 02:00.0 02:00.
```

4.5.2. Configuration des périphériques DPDK

Le paquet **dpdk** fournit des scripts pour la commande init qui facilite la configuration de l'assignation de périphérique et d'énormes pages. Il les rend également persistants.

Ce qui suit est un exemple du fichier /etc/dpdk/interfaces qui configure deux ports d'une carte réseau. Un avec uio_pci_genaric et l'autre avec cfio_pci.

```
# <bus> Currently only "pci" is supported
# <id> Device ID on the specified bus
# <driver> Driver to bind against (vfio-pci or uio_pci_generic)
#
# Be aware that the two DPDK compatible drivers uio_pci_generic and vfio-pci are
# part of linux-image-extra-<VERSION> package.
# This package is not always installed by default - for example in cloud-images.
```

```
# So please install it in case you run into missing module issues.
#
# <bus> <id> <driver>
pci 0000:04:00.0 uio_pci_generic
pci 0000:04:00.1 vfio-pci
```

Les cartes sont identifiées par leur PCI-ID. Si vous n'êtes pas sûr vous devriez utiliser l'outil dpdk_nic_bind pour montrer le périphérique courant disponible ainsi que les pilotes qui lui sont assignés.

dpdk_nic_bind --status

```
Network devices using DPDK-compatible driver
============================================
0000:04:00.0 'Ethernet Controller 10-Gigabit X540-AT2' drv=uio_pci_generic unused=ixgbe

Network devices using kernel driver
===================================
0000:02:00.0 'NetXtreme BCM5719 Gigabit Ethernet PCIe' if=eth0 drv=tg3
unused=uio_pci_generic *Active*
0000:02:00.1 'NetXtreme BCM5719 Gigabit Ethernet PCIe' if=eth1 drv=tg3
unused=uio_pci_generic
0000:02:00.2 'NetXtreme BCM5719 Gigabit Ethernet PCIe' if=eth2 drv=tg3
unused=uio_pci_generic
0000:02:00.3 'NetXtreme BCM5719 Gigabit Ethernet PCIe' if=eth3 drv=tg3
unused=uio_pci_generic
0000:04:00.1 'Ethernet Controller 10-Gigabit X540-AT2' if=eth5 drv=ixgbe
unused=uio_pci_generic

Other network devices
=====================
<none>
```

4.5.3. Configuration de DPDK HugePage

DPDK a une utilisation lourde d'énormes pages (hugepages) pour éliminer la pression sur TLB. Donc, hugepages doit être configurées dans votre système.

Le paquet **dpdk** possède un fichier de configuration et des scripts qui essaient de faciliter la configuration de hugepage pour DPDK, sous la forme **/etc/dpdk/dpdk.conf**. Si vous avez des clients de hugepages dans votre système en plus de DPDK, ou des demandes très spéciales sur comment configurer hugepages, il est probable que vous voudrez les allouer ou les contrôler par vous-même. Sinon cela peut être une grande simplification pour obtenir DPDK configuré pour vos besoins.

Ici, un exemple de configuration de Hugepages de 1024 octets de 2 Mo chacune et quatre pages de 1 Go.

```
NR_2M_PAGES=1024
NR_1G_PAGES=4
```

Comme montré ci-dessus, cela supporte des configurations de hugepages de 2 Mo et la plus grande de 1Go (ou un mélange des deux). Cela assurera qu'il y a des points de montage propre hugetlbfs pour DPDK pour trouver les deux dimensions, quel que soit la dimension par défaut d'énorme page de votre système.

Le fichier de configuration lui-même détient plus de détails sur certains cas particuliers et quelques conseils si vous voulez allouer manuellement des hugepages via un paramètre du noyau.

La dimension de page que vous voulez dépend de vos besoins, des pages d'une dimension de 1 Go sont sûrement plus efficace étant donné la pression sur TLB. Mais il y a eu des rapports de leur fragmentation dans les allocations de mémoire de DPDK. Également, il peut être plus difficile d'allouer assez d'espace libre pour paramétrer un certain nombre de pages de 1 Mo, plus tard, dans le cycle de vie d'un système.

4.5.4. Compiler les Applications DPDK

Actuellement, il n'y a pas beaucoup de clients de la bibliothèque DPDK qui sont stables et à jour. OpenVswitch-DPDK est un exception à cela (voir ci-dessous), mais, en général, il est très vraisemblable que vous voudriez ou deviez compiler une application en s'appuyant sur la bibliothèque.

Vous trouverez toujours ds guides qui vous diront d'aller chercher les sources DPDK, de les construire selon vos besoins et, éventuellement, construire votre application basée sur DPDK en configurant les valeurs RTE_* pour le système construit. Depuis que Ubuntu fournit un DPDK déjà compilé en ce sens, vous pouvez tout laisser tomber. Pour simplifier la configuration des variables appropriées, vous pouvez vous procurer le fichier /usr/share/dpdk/dpdk-sdk-env.sh avant de construire votre application. Ci-dessous, un extrait de construction d'un exemple d'application l2fwd fournie avec le paquet dpdk-doc.

```
sudo apt-get install dpdk-dev libdpdk-dev
. /usr/share/dpdk/dpdk-sdk-env.sh
make -C /usr/share/dpdk/examples/l2fwd
```

Selon ce que vous construisez, ce serait une bonne idée d'installer toutes les dépendances de construction de DPDK avant la construction.

```
sudo apt-get install build-dep dpdk
```

4.5.5. OpenVswitch-DPDK

L'état d'une bibliothèque ne fait pas grand chose par elle-même, ainsi, cela dépend des projets qui apparaissent et qui peuvent l'utiliser. Un client de la bibliothèque, qui est empaquetée dans la version 16.04 d'Ubuntu, est ouverte avec OpenVswitch et le support de DPDK dans le paquet openvswitch-switch-dpdk.

Ici, un exemple de comment installer et configurer basiquement OpenVswitch utilisant DPDK qui sera utilisé via libvirt/qemu-kvm par la suite.

```
sudo apt-get install openvswitch-switch-dpdk
sudo update-alternatives --set ovs-vswitchd /usr/lib/openvswitch-switch-dpdk/ovs-vswitchd-dpdk
echo "DPDK_OPTS='--dpdk -c 0x1 -n 4 -m 2048 --vhost-owner libvirt-qemu:kvm --vhost-perm 0664'" | sudo tee -a /etc/default/openvswitch-switch
sudo service openvswitch-switch restart
```

S'il vous plaît, souvenez-vous que vous avez à déclarer un périphérique à un pilote DPDK compatible (voir ci-dessus) avant de redémarrer.

La section **--vhost-owner libvirt-qemu:kvm --vhost-perm 0664** configurera à ouvert les ports vhost_user

avec le propriétaire et les permissions qui doivent être compatible avec l'utilisation de qemu-kvm/libvirt par Ubuntu,avec des privilèges limités, pour plus de sécurité.

S'il vous plaît, veuillez noter que la section **-m 2048** est la numa la plus basique pour un sytème muni d'une seule sortie (socket). Si vous avez plusieurs sorties, vous voudrez peu-être définir comment partager votre mémoire parmi celles-ci, par exemple **-m 1024, 1024**. S'il vous plaît, garder présent à l'esprit que DPDK essaiera de travailler uniquement avec la mémoire locale des cartes réseau qu'il connaît (pour des raisons de performance). Cela dit, si vous avez plusieurs nœuds, mais toutes les cartes réseau sur un seul, vous devriez envisager de disperser vos cartes. Sinon au moins, allouez la mémoire au nœud où les cartes résident, par exemple deux nœuds sur le nœud #2 : **-m 0, 2048**. Vous pouvez utiliser l'outil **lstopo** du paquet **hwloc-nox** pour voir sur quelle sortie vos cartes sont situées.

Le programme OpenVswitch que vous venez de démarrer supporte tous les types de ports qu'OpenVswitch supporte habituellement, les ports DPDK en plus. Ici, un exemple de comment créer un pont et – à l'inverse d'un port externe normal – y ajouter un port externe DPDK.

```
ovs-vsctl add-br ovsdpdkbr0 -- set bridge ovsdpdkbr0 datapath_type=netdev
ovs-vsctl add-port ovsdpdkbr0 dpdk0 -- set Interface dpdk0 type=dpdk
```

L'accès à DPDK dans Open vSwitch a changé dans la version 2.6. Alors, pour les utilisateurs des versions >= à 16.10, mais aussi pour les utilisateurs de https://wiki.ubuntu.com/OpenStack/CloudArchiveUbuntu Cloud Archive >= neutron, l'accès à DPDK a changé comparé à celui des utilisateurs d'Ubuntu 16.04. Les options passées antérieurement via **DPDK_OPTS** sont maintenant configurées via ovs-vsctl dans la base de données de configuration d'OpenvSwitch.

Le même exemple que ci-dessus, dans la nouvelle version, a cet aspect :

```
# Enable DPDK
ovs-vsctl set Open_vSwitch . "other_config:dpdk-init=true"
# run on core 0
ovs-vsctl set Open_vSwitch . "other_config:dpdk-lcore-mask=0x1"
# Allocate 2G huge pages (not Numa node aware)
ovs-vsctl set Open_vSwitch . "other_config:dpdk-alloc-mem=2048"
# group/permissions for vhost-user sockets (required to work with libvirt/qemu)
ovs-vsctl set Open_vSwitch . \
    "other_config:dpdk-extra=--vhost-owner libvirt-qemu:kvm --vhost-perm 0666"
```

Veuillez vous référez à la documentation générique associée et à la page de man de configuration de vSwitch, fournie dans le paquet, pour plus de détails :

```
/usr/share/doc/openvswitch-common/INSTALL.DPDK.md.gz
/usr/share/doc/openvswitch-common/INSTALL.DPDK-ADVANCED.md.gz
man ovs-vswitchd.conf.db
```

4.5.6. D'OpenVswitch DPDK aux Invités KVM

Si vous ne construisez pas une sorte d'interrupteur SDN ou NFV au-dessus de DPDK, c'est comme vouloir envoyer le trafic de communication à des invités KVM. La bonne nouvelle est que, avec les nouvelles versions de qemu/libvirt/dpdk/openvswitch dans Ubuntu 16.04, ce n'est rien de plus que d'ajouter des chaînes de caractères en ligne de commandes. Ce chapitre couvre la configuration basique de comment connecter un invité KVM à une instance OpenVswitch-DPDK.

L'invité doit être mis à l'arrière plan grâce aux pages énormes partagées de DPDK/vhost_user pour fonctionner. Pour s'assurer en général que libvirt/qemu-kvm trouve un point de montage approprié de page

énorme, vous pouvez juste activer KVM_HUGEPAGES dans le fichier /etc/default/qemu-kvm. Ensuite, redémarrer le service pour reprendre la configuration modifiée.

```
sed -ri -e 's,(KVM_HUGEPAGES=).*,\11,' /etc/default/qemu-kvm
service qemu-kvm restart
```

Laisser un invité être mis en arrière plan par des pages énormes est maintenant également supporté par la commande libvirt récente, vous devez juste ajouter le fragment suivant à votre interface virsh xml (ou l'interface libvirt équivalente que vous utilisez). Ces interfaces xml peuvent aussi être utilisées comme des modèles pour engendrer facilement des invités avec "uvt-kvm create".

```
<numa>
<cell id='0' cpus='0' memory='6291456' unit='KiB' memAccess='shared'/>
</numa>
[...]
<memoryBacking>
<hugepages/>
</memoryBacking>
```

Le chemin nouveau et recommandé pour parvenir à un invité KVM c'est d'utiliser vhost_user. Cela fera créer à DPDK une prise sur laquelle gemu connectera l'invité. Ici, un exemple de comment ajouter un tel port au pont que vous avez créé (voir ci-dessus).

```
ovs-vsctl add-port ovsdpdkbr0 vhost-user-1 -- set Interface vhost-user-1
type=dpdkvhostuser
```

Cela créera une prise vhost_user à l'adresse /var/run/openvswitch/vhost-user-1 .

Pour laisser libvirt/kvm utiliser cette prise et créer pour elle un périphérique réseau virtio invité, ajoutez un fragment comme ceci à votre définition d'invité, comme la définition du réseau.

```
<interface type='vhostuser'>
<source type='unix'
path='/var/run/openvswitch/vhost-user-1'
mode='client'/>
<model type='virtio'/>
</interface>
```

4.5.7. DPDK dans les Invités KVM

Si vous n'avez pas d'accès aux cartes réseau supportant DPDK, vous pouvez toujours travailler avec DPDK en utilisant son support pour virtio. Pour faire cela, vous devez créer la mis en arrière plan de vos invités par des pages énormes (voir ci-dessus).

Le point le plus important, c'est de posséder au minimum SSE3. Le modèle par défaut de CPU que qemu/libvert utilise ne va pas au-delà de SSE2. Donc, vous devez définir un modèle qui passe les indicateurs de caractéristique appropriés et, évidemment, posséder un système Hôte qui les supporte. Un exemple peut être trouvé dans le fragment suivant de votre interface virsh xml (ou l'interface virsh équivalente que vous utilisez).

```
<cpu mode='host-passthrough'>
```

Cet exemple est plus offensif et passe toutes les caractéristiques d'hôte. Ce qui, en retour, ne permet pas de migrer vraiment l'invité alors que la cible aurait besoin de toutes les caractéristiques. Une approche plus souple, est d'ajouter simplement sse3 au modèle par défaut, comme dans l'exemple suivant :

```
<cpu mode='custom' match='exact'>
<model fallback='allow'>qemu64</model>
<feature policy='require' name='sse3'/>
</cpu>
```

De nos jours, virtio supporte plusieurs queues, qu'en retour, DPDK peut exploiter pour une meilleure vitesse. Pour modifier une définition normale de virtio, pour obtenir plusieurs queues, ajoutez ce qui suit à votre définition d'interface. Cela revient à augmenter un « nic » virtio normal pour avoir plusieurs queues, pour être consommé plus tard par DPDK dans l'invité par exemple.

```
<driver name="vhost" queues="4"/>
```

4.5.8. Personnaliser Openvswitch-DPDK

DPDK comprend plein d'options, en combinaison avec Openvswitch. Les deux options de DPDK les plus utilisées sont :

```
ovs-vsctl set Open_vSwitch . other_config:n-dpdk-rxqs=2
ovs-vsctl set Open_vSwitch . other_config:pmd-cpu-mask=0x6
```

La première sélectionne combien de queues rx vont être utilisées par interface DPDK, alors que la seconde contrôle combien et où les cœurs PMD opéreront. L'exemple ci-dessus utilisera deux queues rx et opérera des cœurs PMD sur les CPU 1 et 2. Voyez les liens associés à "Options des lignes de commandes EAL" et "Installation d'OpenVswitch pour DPDK"

Comme d'habitude avec la personnalisation, vous devez bien connaître votre système ainsi que votre charge de travail, donc, s'il vous plaît, vérifiez que toute personnalisation avec les charges de travail soit compatible avec votre cas d'utilisation réel.

4.5.9. Support et Résolution de pannes

DPDK est un projet qui évolue rapidement. Dans tous les cas de recherche de support et d'autres guides, en premier, il est fortement recommandé de contrôler s'ils correspondent à la version courante.

- Liste de mailing DPDK : http://dpdk.org/ml
- Pour OpenVswitch-DPDK, Liste de mailing OpenStack : http://openvswitch.org/mlists
- Problèmes connus dans DPDK Launchpad Area : https://bugs.launchpad.net/ubuntu/+source/dpdk
- Rejoignez les canaux IRC #DPDK or #openvswitch sur freenode.

Les difficultés rencontrées sont toujours dus à des détails manquants dans la configuration générale. Plus tard, ces détails manquants causent des problèmes dont la cause originelle peut être difficile à retrouver. Un cas courant ressemble à la difficulté « Le périphérique réseau dpdk0 ne peut être ouvert (ce périphérique

n’existe pas) ». Cela arrive plus tard lors de la configuration d’un port dans Open vSwitch avec DPDK. Mais la cause originelle, la plupart du temps, se situe vraiment tôt dans la configuration et l’initialisation. Ici, un exemple de comment apparaît une initialisation appropriée d’un périphérique, cela peut être trouvé dans le journal syslog/journal lorsque démarre Open vSwitch avec DPDK activé.

```
ovs-ctl[3560]: EAL: PCI device 0000:04:00.1 on NUMA socket 0
ovs-ctl[3560]: EAL: probe driver: 8086:1528 rte_ixgbe_pmd
ovs-ctl[3560]: EAL: PCI memory mapped at 0x7f2140000000
ovs-ctl[3560]: EAL: PCI memory mapped at 0x7f2140200000
```

Si cela est manquant, également par des cartes ignorées, initialisation avortées ou pour d’autres raisons, plus tard il n’y aura pas de périphérique DPDK sur lequel se référer. Malheureusement, la journalisation est diffusée parmi les journaux syslog/journal et openvswitch. Pour avoir des tests transversaux, ci-dessous un exemple de ce que l’on peut trouver dans ces journaux, selon la commande entrée.

```
#Note: This log was taken with dpdk 2.2 and openvswitch 2.5
Captions:
CMD: that you enter
SYSLOG: (Inlcuding EAL and OVS Messages)
OVS-LOG: (Openvswitch messages)

#PREPARATION
Bind an interface to DPDK UIO drivers, make Hugepages available, enable DPDK on OVS

CMD: sudo service openvswitch-switch restart

SYSLOG:
2016-01-22T08:58:31.372Z|00003|daemon_unix(monitor)|INFO|pid 3329 died, killed
(Terminated), exiting
2016-01-22T08:58:33.377Z|00002|vlog|INFO|opened log file /var/log/openvswitch/ovs-
vswitchd.log
2016-01-22T08:58:33.381Z|00003|ovs_numa|INFO|Discovered 12 CPU cores on NUMA node 0
2016-01-22T08:58:33.381Z|00004|ovs_numa|INFO|Discovered 1 NUMA nodes and 12 CPU cores
2016-01-22T08:58:33.381Z|00005|reconnect|INFO|unix:/var/run/openvswitch/db.sock:
connecting...
2016-01-22T08:58:33.383Z|00006|reconnect|INFO|unix:/var/run/openvswitch/db.sock:
connected
2016-01-22T08:58:33.386Z|00007|bridge|INFO|ovs-vswitchd (Open vSwitch) 2.5.0

OVS-LOG:
systemd[1]: Stopping Open vSwitch...
systemd[1]: Stopped Open vSwitch.
systemd[1]: Stopping Open vSwitch Internal Unit...
ovs-ctl[3541]: * Killing ovs-vswitchd (3329)
ovs-ctl[3541]: * Killing ovsdb-server (3318)
systemd[1]: Stopped Open vSwitch Internal Unit.
systemd[1]: Starting Open vSwitch Internal Unit...
ovs-ctl[3560]: * Starting ovsdb-server
ovs-vsctl: ovs|00001|vsctl|INFO|Called as ovs-vsctl --no-wait -- init -- set
Open_vSwitch . db-version=7.12.1
ovs-vsctl: ovs|00001|vsctl|INFO|Called as ovs-vsctl --no-wait set Open_vSwitch . ovs-
version=2.5.0 "external-ids:system-id=\"e7c5ba80-bb14-45c1-b8eb-628f3ad03903\""
```

```
"system-type=\"Ubuntu\"" "system-version=\"16.04-xenial\""
ovs-ctl[3560]: * Configuring Open vSwitch system IDs
ovs-ctl[3560]: 2016-01-22T08:58:31Z|00001|dpdk|INFO|No -vhost_sock_dir provided -
defaulting to /var/run/openvswitch
ovs-vswitchd: ovs|00001|dpdk|INFO|No -vhost_sock_dir provided - defaulting to
/var/run/openvswitch
ovs-ctl[3560]: EAL: Detected lcore 0 as core 0 on socket 0
ovs-ctl[3560]: EAL: Detected lcore 1 as core 1 on socket 0
ovs-ctl[3560]: EAL: Detected lcore 2 as core 2 on socket 0
ovs-ctl[3560]: EAL: Detected lcore 3 as core 3 on socket 0
ovs-ctl[3560]: EAL: Detected lcore 4 as core 4 on socket 0
ovs-ctl[3560]: EAL: Detected lcore 5 as core 5 on socket 0
ovs-ctl[3560]: EAL: Detected lcore 6 as core 0 on socket 0
ovs-ctl[3560]: EAL: Detected lcore 7 as core 1 on socket 0
ovs-ctl[3560]: EAL: Detected lcore 8 as core 2 on socket 0
ovs-ctl[3560]: EAL: Detected lcore 9 as core 3 on socket 0
ovs-ctl[3560]: EAL: Detected lcore 10 as core 4 on socket 0
ovs-ctl[3560]: EAL: Detected lcore 11 as core 5 on socket 0
ovs-ctl[3560]: EAL: Support maximum 128 logical core(s) by configuration.
ovs-ctl[3560]: EAL: Detected 12 lcore(s)
ovs-ctl[3560]: EAL: VFIO modules not all loaded, skip VFIO support...
ovs-ctl[3560]: EAL: Setting up physically contiguous memory...
ovs-ctl[3560]: EAL: Ask a virtual area of 0x100000000 bytes
ovs-ctl[3560]: EAL: Virtual area found at 0x7f2040000000 (size = 0x100000000)
ovs-ctl[3560]: EAL: Requesting 4 pages of size 1024MB from socket 0
ovs-ctl[3560]: EAL: TSC frequency is ~2397202 KHz
ovs-vswitchd[3592]: EAL: TSC frequency is ~2397202 KHz
ovs-vswitchd[3592]: EAL: Master lcore 0 is ready (tid=fc6cbb00;cpuset=[0])
ovs-vswitchd[3592]: EAL: PCI device 0000:04:00.0 on NUMA socket 0
ovs-vswitchd[3592]: EAL: probe driver: 8086:1528 rte_ixgbe_pmd
ovs-vswitchd[3592]: EAL: Not managed by a supported kernel driver, skipped
ovs-vswitchd[3592]: EAL: PCI device 0000:04:00.1 on NUMA socket 0
ovs-vswitchd[3592]: EAL: probe driver: 8086:1528 rte_ixgbe_pmd
ovs-vswitchd[3592]: EAL: PCI memory mapped at 0x7f2140000000
ovs-vswitchd[3592]: EAL: PCI memory mapped at 0x7f2140200000
ovs-ctl[3560]: EAL: Master lcore 0 is ready (tid=fc6cbb00;cpuset=[0])
ovs-ctl[3560]: EAL: PCI device 0000:04:00.0 on NUMA socket 0
ovs-ctl[3560]: EAL: probe driver: 8086:1528 rte_ixgbe_pmd
ovs-ctl[3560]: EAL: Not managed by a supported kernel driver, skipped
ovs-ctl[3560]: EAL: PCI device 0000:04:00.1 on NUMA socket 0
ovs-ctl[3560]: EAL: probe driver: 8086:1528 rte_ixgbe_pmd
ovs-ctl[3560]: EAL: PCI memory mapped at 0x7f2140000000
ovs-ctl[3560]: EAL: PCI memory mapped at 0x7f2140200000
ovs-vswitchd[3592]: PMD: eth_ixgbe_dev_init(): MAC: 4, PHY: 3
ovs-vswitchd[3592]: PMD: eth_ixgbe_dev_init(): port 0 vendorID=0x8086 deviceID=0x1528
ovs-ctl[3560]: PMD: eth_ixgbe_dev_init(): MAC: 4, PHY: 3
ovs-ctl[3560]: PMD: eth_ixgbe_dev_init(): port 0 vendorID=0x8086 deviceID=0x1528
ovs-ctl[3560]: Zone 0: name:<RG_MP_log_history>, phys:0x83fffdec0, len:0x2080,
virt:0x7f213fffdec0, socket_id:0, flags:0
ovs-ctl[3560]: Zone 1: name:<MP_log_history>, phys:0x83fd73d40, len:0x28a0c0,
virt:0x7f213fd73d40, socket_id:0, flags:0
ovs-ctl[3560]: Zone 2: name:<rte_eth_dev_data>, phys:0x83fd43380, len:0x2f700,
virt:0x7f213fd43380, socket_id:0, flags:0
```

```
ovs-ctl[3560]: * Starting ovs-vswitchd
ovs-ctl[3560]: * Enabling remote OVSDB managers
systemd[1]: Started Open vSwitch Internal Unit.
systemd[1]: Starting Open vSwitch...
systemd[1]: Started Open vSwitch.


CMD: sudo ovs-vsctl add-br ovsdpdkbr0 -- set bridge ovsdpdkbr0 datapath_type=netdev

SYSLOG:
2016-01-22T08:58:56.344Z|00008|memory|INFO|37256 kB peak resident set size after 24.5
seconds
2016-01-22T08:58:56.346Z|00009|ofproto_dpif|INFO|netdev@ovs-netdev: Datapath supports
recirculation
2016-01-22T08:58:56.346Z|00010|ofproto_dpif|INFO|netdev@ovs-netdev: MPLS label stack
length probed as 3
2016-01-22T08:58:56.346Z|00011|ofproto_dpif|INFO|netdev@ovs-netdev: Datapath supports
unique flow ids
2016-01-22T08:58:56.346Z|00012|ofproto_dpif|INFO|netdev@ovs-netdev: Datapath does not
support ct_state
2016-01-22T08:58:56.346Z|00013|ofproto_dpif|INFO|netdev@ovs-netdev: Datapath does not
support ct_zone
2016-01-22T08:58:56.346Z|00014|ofproto_dpif|INFO|netdev@ovs-netdev: Datapath does not
support ct_mark
2016-01-22T08:58:56.346Z|00015|ofproto_dpif|INFO|netdev@ovs-netdev: Datapath does not
support ct_label
2016-01-22T08:58:56.360Z|00016|bridge|INFO|bridge ovsdpdkbr0: added interface
ovsdpdkbr0 on port 65534
2016-01-22T08:58:56.361Z|00017|bridge|INFO|bridge ovsdpdkbr0: using datapath ID
00005a4a1ed0a14d
2016-01-22T08:58:56.361Z|00018|connmgr|INFO|ovsdpdkbr0: added service controller
"punix:/var/run/openvswitch/ovsdpdkbr0.mgmt"

OVS-LOG:
ovs-vsctl: ovs|00001|vsctl|INFO|Called as ovs-vsctl add-br ovsdpdkbr0 -- set bridge
ovsdpdkbr0 datapath_type=netdev
systemd-udevd[3607]: Could not generate persistent MAC address for ovs-netdev: No such
file or directory
kernel: [50165.886554] device ovs-netdev entered promiscuous mode
kernel: [50165.901261] device ovsdpdkbr0 entered promiscuous mode


CMD: sudo ovs-vsctl add-port ovsdpdkbr0 dpdk0 -- set Interface dpdk0 type=dpdk

SYSLOG:
2016-01-22T08:59:06.369Z|00019|memory|INFO|peak resident set size grew 155% in last
10.0 seconds, from 37256 kB to 95008 kB
2016-01-22T08:59:06.369Z|00020|memory|INFO|handlers:4 ports:1 revalidators:2 rules:5
2016-01-22T08:59:30.989Z|00021|dpdk|INFO|Port 0: 8c:dc:d4:b3:6d:e9
2016-01-22T08:59:31.520Z|00022|dpdk|INFO|Port 0: 8c:dc:d4:b3:6d:e9
2016-01-22T08:59:31.521Z|00023|dpif_netdev|INFO|Created 1 pmd threads on numa node 0
2016-01-22T08:59:31.522Z|00001|dpif_netdev(pmd16)|INFO|Core 0 processing port 'dpdk0'
2016-01-22T08:59:31.522Z|00024|bridge|INFO|bridge ovsdpdkbr0: added interface dpdk0 on
port 1
```

```
2016-01-22T08:59:31.522Z|00025|bridge|INFO|bridge ovsdpdkbr0: using datapath ID
00008cdcd4b36de9
2016-01-22T08:59:31.523Z|00002|dpif_netdev(pmd16)|INFO|Core 0 processing port 'dpdk0'


OVS-LOG:
ovs-vsctl: ovs|00001|vsctl|INFO|Called as ovs-vsctl add-port ovsdpdkbr0 dpdk0 -- set
Interface dpdk0 type=dpdk
ovs-vswitchd[3595]: PMD: ixgbe_dev_tx_queue_setup(): sw_ring=0x7f211a79ebc0
hw_ring=0x7f211a7a6c00 dma_addr=0x81a7a6c00
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Using simple tx code path
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Vector tx enabled.
ovs-vswitchd[3595]: PMD: ixgbe_dev_rx_queue_setup(): sw_ring=0x7f211a78a6c0
sw_sc_ring=0x7f211a786580 hw_ring=0x7f211a78e800 dma_addr=0x81a78e800
ovs-vswitchd[3595]: PMD: ixgbe_set_rx_function(): Vector rx enabled, please make sure
RX burst size no less than 4 (port=0).
ovs-vswitchd[3595]: PMD: ixgbe_dev_tx_queue_setup(): sw_ring=0x7f211a79ebc0
hw_ring=0x7f211a7a6c00 dma_addr=0x81a7a6c00
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Using simple tx code path
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Vector tx enabled.
ovs-vswitchd[3595]: PMD: ixgbe_dev_tx_queue_setup(): sw_ring=0x7f211a76e4c0
hw_ring=0x7f211a776500 dma_addr=0x81a776500
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Using simple tx code path
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Vector tx enabled.
ovs-vswitchd[3595]: PMD: ixgbe_dev_tx_queue_setup(): sw_ring=0x7f211a756440
hw_ring=0x7f211a75e480 dma_addr=0x81a75e480
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Using simple tx code path
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Vector tx enabled.
ovs-vswitchd[3595]: PMD: ixgbe_dev_tx_queue_setup(): sw_ring=0x7f211a73e3c0
hw_ring=0x7f211a746400 dma_addr=0x81a746400
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Using simple tx code path
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Vector tx enabled.
ovs-vswitchd[3595]: PMD: ixgbe_dev_tx_queue_setup(): sw_ring=0x7f211a726340
hw_ring=0x7f211a72e380 dma_addr=0x81a72e380
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Using simple tx code path
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Vector tx enabled.
ovs-vswitchd[3595]: PMD: ixgbe_dev_tx_queue_setup(): sw_ring=0x7f211a70e2c0
hw_ring=0x7f211a716300 dma_addr=0x81a716300
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Using simple tx code path
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Vector tx enabled.
ovs-vswitchd[3595]: PMD: ixgbe_dev_tx_queue_setup(): sw_ring=0x7f211a6f6240
hw_ring=0x7f211a6fe280 dma_addr=0x81a6fe280
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Using simple tx code path
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Vector tx enabled.
ovs-vswitchd[3595]: PMD: ixgbe_dev_tx_queue_setup(): sw_ring=0x7f211a6de1c0
hw_ring=0x7f211a6e6200 dma_addr=0x81a6e6200
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Using simple tx code path
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Vector tx enabled.
ovs-vswitchd[3595]: PMD: ixgbe_dev_tx_queue_setup(): sw_ring=0x7f211a6c6140
hw_ring=0x7f211a6ce180 dma_addr=0x81a6ce180
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Using simple tx code path
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Vector tx enabled.
ovs-vswitchd[3595]: PMD: ixgbe_dev_tx_queue_setup(): sw_ring=0x7f211a6ae0c0
hw_ring=0x7f211a6b6100 dma_addr=0x81a6b6100
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Using simple tx code path
```

```
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Vector tx enabled.
ovs-vswitchd[3595]: PMD: ixgbe_dev_tx_queue_setup(): sw_ring=0x7f211a696040
hw_ring=0x7f211a69e080 dma_addr=0x81a69e080
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Using simple tx code path
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Vector tx enabled.
ovs-vswitchd[3595]: PMD: ixgbe_dev_tx_queue_setup(): sw_ring=0x7f211a67dfc0
hw_ring=0x7f211a686000 dma_addr=0x81a686000
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Using simple tx code path
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Vector tx enabled.
ovs-vswitchd[3595]: PMD: ixgbe_dev_tx_queue_setup(): sw_ring=0x7f211a665e40
hw_ring=0x7f211a66de80 dma_addr=0x81a66de80
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Using simple tx code path
ovs-vswitchd[3595]: PMD: ixgbe_set_tx_function(): Vector tx enabled.
ovs-vswitchd[3595]: PMD: ixgbe_dev_rx_queue_setup(): sw_ring=0x7f211a78a6c0
sw_sc_ring=0x7f211a786580 hw_ring=0x7f211a78e800 dma_addr=0x81a78e800
ovs-vswitchd[3595]: PMD: ixgbe_set_rx_function(): Vector rx enabled, please make sure
RX burst size no less than 4 (port=0).


CMD: sudo ovs-vsctl add-port ovsdpdkbr0 vhost-user-1 -- set Interface vhost-user-1
type=dpdkvhostuser

OVS-LOG:
2016-01-22T09:00:35.145Z|00026|dpdk|INFO|Socket /var/run/openvswitch/vhost-user-1
created for vhost-user port vhost-user-1
2016-01-22T09:00:35.145Z|00003|dpif_netdev(pmd16)|INFO|Core 0 processing port 'dpdk0'
2016-01-22T09:00:35.145Z|00004|dpif_netdev(pmd16)|INFO|Core 0 processing port 'vhost-
user-1'
2016-01-22T09:00:35.145Z|00027|bridge|INFO|bridge ovsdpdkbr0: added interface vhost-
user-1 on port 2

SYSLOG:
ovs-vsctl: ovs|00001|vsctl|INFO|Called as ovs-vsctl add-port ovsdpdkbr0 vhost-user-1 --
set Interface vhost-user-1 type=dpdkvhostuser
ovs-vswitchd[3595]: VHOST_CONFIG: socket created, fd:46
ovs-vswitchd[3595]: VHOST_CONFIG: bind to /var/run/openvswitch/vhost-user-1

Eventually we can see the poll thread in top
  PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
 3595 root 10 -10 4975344 103936 9916 S 100.0 0.3 33:13.56 ovs-vswitchd
```

4.5.10. Ressources

Documentation DPDK : http://dpdk.org/doc

Notes de mise à jour correspondant aux paquets de version dans Ubuntu 16.04 : http://dpdk.org/doc/guides/rel_notes/release_2_2.html

Utilisateur débutant de Linux DPDK : http://dpdk.org/doc/guides/linux_gsg/index.html

Options des lignes de commande EAL : http://dpdk.org/doc/guides/testpmd_app_ug/run_app.html

Documentation Api DPDK : http://dpdk.org/doc/api/

Installation d'OpenVswitch pour DPDK : https://github.com/openvswitch/ovs/blob/branch-

2.5/INSTALL.DPDK.md

Définitions dans Wikipedias de DPDK : https://en.wikipedia.org/wiki/Data_Plane_Development_Kit

Chapitre 5. DM-Multipath

5.1. Cartographie Multivoie de Périphérique

La Cartographie Multivoie des Périphériques (DM-Multipath : Device Mapper Multipathing) vous permet de configurer plusieurs chemins d'E/S entre les nœuds de serveurs et les baies de stockage par le biais d'un seul périphérique. Ces chemins d'E/S physiques sont des connexions SAN qui peuvent inclure des câbles séparés, des commutateurs et des contrôleurs. La cartographie multivoie enregistre les chemins d'E/S en créant un nouveau périphérique qui n'est autre que l'agrégation des chemins d'accès. Ce chapitre présente un sommaire des concepts de DM-Multipath qui sont nouveaux pour la version initiale d'Ubuntu Serveur 12.04. En conséquence, celui-ci présente un haut niveau de vue d'ensemble de DM-Multipath et de ses composants, comme une vue d'ensemble de la configuration de DM-Multipath.

5.1.1. Fonctionnalités nouvelles et modifiées pour Ubuntu Serveur 12.04

Migrées de multipath-0.4.8 à multipath-0.4.9

5.1.1.1. Migration depuis 0.4.8

Les vérificateurs de priorité ne fonctionnent plus sous forme de binaires autonomes, mais comme des bibliothèques partagées. Le nom de la valeur clé pour cette fonctionnalité a aussi légèrement changé. Copiez l'attribut nommé **prio_callout** sur **prio**, également modifiez l'argument de nom du vérificateur de priorité, le chemin de système n'est plus nécessaire. Exemple de conversion :

```
device  {
        vendor "NEC"
        product "DISK ARRAY"
        prio_callout mpath_prio_alua /dev/%n
        prio alua
}
```

Voir le tableau *5.1. Conversion des Vérificateurs* en priorité pour une liste complète

Tableau 5.1. Conversion des Vérificateurs de priorité

v0.4.8	v0.4.9
prio_callout mpath_prio_emc /dev/%n	**prio emc**
prio_callout mpath_prio_alua /dev/%n	**prio alua**
prio_callout mpath_prio_netapp /dev/%n	**prio netapp**
prio_callout mpath_prio_rdac /dev/%n	**prio rdac**
prio_callout mpath_prio_hp_sw /dev/%n	**prio hp_sw**
prio_callout mpath_prio_hds_modular %b	**prio hds**

Puisque l'analyseur de fichiers de configuration multipath analyse essentiellement toutes les paires clé/valeur, qu'il trouve et fait alors usage de ceux-ci, il est sans danger autant pour **prio_callout** que pour **prio** de coexister et il est recommandé que l'attribut **prio** soit inséré avant le début de la migration. Après quoi, vous pouvez supprimer en toute sécurité l'attribut **prio_callout** sans interrompre le service.

5.1.2. Présentation

DM-Multipath peut être utilisé pour fournir :

- **La redondance** DM-Multipath peut fournir un basculement dans une configuration active/passive. Dans une configuration active/passive, uniquement la moitié des voies sont utilisées à tout moment pour les E/S. Si un quelconque élément d'un chemin d'E/S (le câble, le commutateur ou contrôleur) échoue, DM-Multipath bascule vers un autre chemin.
- **Des performances améliorées** Performance DM-Multipath peut être configuré en mode actif/actif, où les E/S sont réparties sur les chemins de façon circulaire. Dans certaines configurations, DM-Multipath peut détecter le chargement sur les chemins d'E/S et dynamiquement re-équilibrer la charge.

5.1.3. Présentation des baies de stockage

Par défaut, DM-Multipath inclut le support pour la plupart des baies de stockage les plus courantes qui supportent DM-Multipath. Les périphériques pris en charge peuvent être trouvés dans le fichier multipath.conf.defaults. Si votre baie de stockage prend en charge DM-Multipath et n'est pas configurée par défaut dans ce fichier, vous devrez peut-être l'ajouter au fichier de configuration DM-Multipath, multipath.conf. Pour plus d'informations sur le fichier de configuration DM-Multipath, voir le *Chapitre 5, paragraphe 4. Le fichier de configuration DM-Multipath*. Certaines baies de stockage nécessitent un traitement spécial des erreurs d'E/S et de commutation de chemin. Ceux-ci requièrent des modules de noyau gestionnaires de matériels séparé.

5.1.4. Composants DM-Multipath

Le tableau *5.2. Composants DM-Multipath* décrit les composants du paquet DM-Multipath.

Tableau 5.2 Composants DM-Multipath

Composant	Description
module du noyau dm_multipath	Réachemine les E/S et supporte le basculement pour les chemins et les groupes de chemin.
commande multipath	Liste et configure les périphériques **multivoie**. Normalement démarré avec /etc/rc.sysinit, il peut également être démarré par un programme **udev** chaque fois qu'un périphérique en mode bloc est ajouté ou il peut être exécuté par le système de fichiers **initramfs**.
démon multipathd	Surveille les chemins; comme les chemins échouent et se rétablissent, il peut initialiser les commutateurs de groupe de chemins. Il fournit des modifications interactives aux périphériques **multivoie**. Ce démon doit être redémarré après toute modification apportée au fichier /etc/multipath.conf pour qu'elle prenne effet.
commande kpartx	Crée un périphérique cartographe de périphériques, pour les partitions sur un périphérique. Il est nécessaire d'utiliser cette commande pour les partitions générées sous DOS avec DM-Multipath. La commande kpartx est fournie dans son propre package, mais le paquet **multipath-tools** en dépend.

5.1.5. Présentation de la configuration de DM-Multipath

DM-Multipath comprend les paramètres compilés par défaut qui conviennent pour les configurations multivoies courantes. La configuration de DM-multipath est souvent une procédure simple. La procédure de base pour configurer votre système avec DM-Multipath est la suivante :

1. Installez les paquets **multipath-tools** et **multipath-tools-boot**
2. Créez un fichier de configuration vide, /etc/multipath.conf, ceci redéfinit *cela (3. Présentation de la Configuration de DM-Multipath.1. Configuration de DM-Multipath)*
3. Si nécessaire, éditez le fichier de configuration **multipath.conf** pour modifier les valeurs par défaut et enregistrez le fichier mis à jour.
4. Démarrez le démon multipath
5. Mettez à jour le disque virtuel initial

Pour obtenir des instructions détaillées pour la configuration de multipath voir le *Chapitre 5, paragraphe 3. Présentation de la Configuration de DM-Multipath.1. Configuration de DM-Multipath*.

5.2. Périphériques multivoie

Sans DM-Multipath, chaque chemin à partir d'un nœud serveur jusqu'à un contrôleur de stockage est traité par le système comme un périphérique distinct, même si le chemin d'accès d'E/S se connecte du même noeud de serveur au même contrôleur de stockage. DM-Multipath fournit une façon d'organiser les chemins d'E/S logiquement, par la création d'un périphérique multivoie unique au-dessus des périphériques sous-jacents.

5.2.1. Identificateurs de périphériques multivoie

Chaque périphérique multivoie a un Identifiant Monde Entier (WWID : World Wide Identifier), qui est assuré d'être mondialement unique et immuable. Par défaut, le nom d'un périphérique multivoie est défini par son WWID. Alternativement, vous pouvez définir l'option ***user_friendly_names*** (noms_conviviaux) dans le fichier de configuration multivoie, ce qui implique l'utilisation par DM-Multipath d'un alias de nœud-unique de la forme **mpathn** comme nom. Par exemple, un nœud avec deux Adaptateurs de Bus Hôte (HBA : Host Bus Adaptor) connectés à un contrôleur de stockage avec deux ports via un simple commutateur FC non-zoné voit quatre périphériques : **/dev/sda**, **/dev/sdb**, **/dev/sdc** et **/dev/sdd**. DM-Multipath crée un seul dispositif avec un WWID unique qui redirige les Entrées/Sorties pour les quatre périphériques sous-jacents selon la configuration multivoie. Lorsque l'option **noms_conviviaux** de configuration est réglé sur **oui**, le nom du périphérique multivoie est réglée sur **mpathn**. Lorsque de nouveaux périphériques sont placées sous le contrôle de DM-Multipath, les nouveaux périphériques peuvent être vus dans deux endroits différents dans le répertoire **/dev** : **/dev/mapper/mpathn** et **/dev/dm-n**.

- Les périphériques dans **/dev/mapper** sont créés très tôt dans le processus de démarrage. Utilisez ces périphériques pour accéder aux périphériques en multivoie, par exemple lors de la création de volumes logiques.
- Tout périphériques de la forme **/dev/dm-n** sont à usage interne uniquement et ne doivent jamais être utilisés.

Pour plus d'informations sur la configuration par défaut de la configuration multivoie, y compris l'option de configuration **noms_conviviaux**, voir le *Chapitre 5, paragraphe 4. Le fichier de configuration DM-Multipath.3. La section Valeurs par défaut du fichier de configuration*. Vous pouvez également définir le nom d'un périphérique multivoie à un nom de votre choix en utilisant l'option *alias* dans la section **Multivoies** du fichier de configuration multivoie. Pour plus d'informations sur la section **Multivoies** du fichier de configuration multivoie, référez-vous au *Chapitre 5, paragraphe 4. Le fichier de configuration DM-Multipath.4. Attributs Multivoie du fichier de configuration*.

5.2.2. Noms cohérents de périphériques multivoie dans un amas

Lorsque l'option **noms conviviaux** de configuration est réglé sur oui, le nom du périphérique multivoie est unique à un nœud, mais il n'est pas garanti d'être le même sur tous les nœuds en utilisant le périphérique multivoie. De même, si vous définissez l'option **alias** pour un périphérique dans la section **Multivoies** du fichier de configuration multipath.conf, le nom n'est pas automatiquement constant à travers tous les nœuds dans l'amas. Cela ne devrait pas poser de difficultés si vous utilisez LVM pour créer des dispositifs logiques du périphérique multivoie, mais si vous avez besoin que vos noms de périphériques multivoie soient cohérents dans chaque nœud, il est recommandé de laisser l'option **noms_conviviaux** réglée sur **non** et que vous ne configurez pas d'alias pour les périphériques. Par défaut, si vous ne fixez pas **noms_conviviaux** sur **oui** ou configurez un alias pour un périphérique, le nom d'un périphérique sera l'identifiant WWID de celui-ci, qui est toujours le même. Si vous voulez que des noms conviviaux cohérents soient définis par le système sur tous les nœuds de l'amas, cependant, vous pouvez suivre cette

procédure :

1. Installez tous les périphériques multivoie sur une machine.
2. Désactiver tous vos périphériques multivoie sur vos autres machines en exécutant les commandes suivantes :

```
# systemctl stop multipath-tools.service
# multipath -F
```

3. Copiez le fichier /etc/multipath/bindings de la première machine sur toutes les autres machines de l'amas.
4. Re-activer le démon multipathd sur toutes les autres machines de l'amas en exécutant la commande suivante :

```
# systemctl start multipath-tools.service
```

Si vous ajoutez un nouveau périphérique, vous devrez répéter ce processus.

De même, si vous configurez un alias pour un périphérique et que vous souhaitez qu'il soit cohérent sur les nœuds de l'amas, vous devez vous assurer que le fichier /etc/multipath.conf est la même pour chaque nœud de l'amas en suivant la même procédure :

1. Configurez les alias pour les périphériques multivoie dans le fichier multipath.conf sur une seule machine.
2. Désactiver tous vos périphériques multivoie sur vos autres machines en exécutant les commandes suivantes :

```
# systemctl stop multipath-tools.service
# multipath -F
```

3. Copiez le fichier multipath.conf de la première machine à toutes les autres machines de l'amas.
4. Re-activer le démon multipathd sur toutes les autres machines de l'amas en exécutant la commande suivante :

```
# systemctl start multipath-tools.service
```

Lorsque vous ajouterez un nouveau périphérique, vous devrez répéter ce processus.

5.2.3. Attributs de périphériques multivoie

En plus des options **noms_conviviaux** et **alias**, un périphérique multivoie possède de nombreux attributs. Vous pouvez modifier ces attributs pour un périphérique multivoie spécifique en créant une entrée pour ce périphérique dans la section **Multitvoies** du fichier de configuration **multitvoie**. Pour plus d'informations sur la section **Multitvoies** du fichier de configuration multivoie, voir le *Chapitre 5, paragraphe 4. Le fichier de configuration DM-Multipath.4. Attributs Multivoie du fichier de configuration*.

5.2.4. Périphériques Multivoie dans des Volumes Logiques

Après la création de périphériques multivoie, vous pouvez utiliser les noms des périphériques multivoie comme vous le feriez pour un nom de périphérique physique lors de la création d'un Volume Logique Multivoie. Par exemple, si /dev/mapper/mpatha est le nom d'un périphérique multivoie, la commande suivante

va marquer /dev/mapper/mpatha comme un volume physique.

```
# pvcreate /dev/mapper/mpatha
```

Vous pouvez utiliser l'appareil physique VLM résultant lorsque vous créez un groupe de volumes VLM juste comme vous utiliseriez n'importe quel autre périphérique VLM physique.

> Si vous tentez de créer un volume physique VLM sur un ensemble de périphériques, sur lesquels vous avez configuré des partitions, la commande **pvcreate** échouera.

Lorsque vous créez un volume logique VLM qui utilise des matrices multivoie actifs/passifs pour les périphériques physiques sous-jacents, vous devriez inclure des filtres dans le fichier **lvm.conf** pour exclure les disques qui supportent les périphériques multivoie. Ceci parce que si le système de stockage change automatiquement le chemin actif pour le chemin passif quand il reçoit les E/S, la fonction multivoie basculera et se rétablira à chaque fois que le VLM scannera le chemin passif, si ces périphériques ne sont pas filtrés. Pour les matrices actives/passives qui nécessitent une commande pour rendre le chemin passif, actif, le VLM affiche un message d'avertissement lorsque cela se produit. Pour filtrer tous les périphériques SCSI dans le fichier de configuration de VLM (lvm.conf), incluez le filtre suivant dans la section **Périphériques** du fichier.

```
 filter = [ "r/block/", "r/disk/", "r/sd.*/", "a/.*/" ]
```

Après la mise à jour de /etc/lvm.conf, il est nécessaire de mettre à jour **initrd** de sorte que ce fichier sera copié là où le filtre qui compte le plus, pendant le démarrage. Effectuez :
`update-initramfs -u -k all`

> A chaque fois que les fichiers /etc/lvm.conf ou /etc/multipath.conf sont mis à jour, l'initrd doit être reconstruit pour refléter ces changements. C'est impératif lorsque les listes noires et les filtres sont nécessaires pour maintenir une configuration de stockage stable.

5.3. Présentation de la Configuration de DM-Multipath

Cette section fournit des exemples de procédures étape par étape pour la configuration de DM-Multipath. Il comprend les procédures suivantes :

- Configuration DM-Multipath de base
- Occultation des disques locaux
- Ajout de plus de périphériques au fichier de configuration

5.3.1. Configuration de DM-Multipath

Avant de configurer DM-Multipath sur votre système, assurez-vous que celui-ci ait été mis à jour et inclut le paquet **multipath-tools**. Si vous voulez que le démarrage soit fait depuis le SAN (réseau de stockage), le paquet **multipath-tools-boot** est également requis.

Un fichier **/etc/multipath.conf** n'est pas forcément nécessaire, lorsque **DM-Multipath** est exécuté sans ce fichier, il puise dans sa base de données interne pour trouver une configuration appropriée, il s'appuie également sur sa liste noire interne. Si après l'exécution de **multipath-ll** sans fichier de configuration, aucun multi-acheminement n'est découvert, il faut procéder à une augmentation de la verbosité pour découvrir pourquoi une configuration multivoie n'a pas été créée. Pensez à vous référer à la documentation du fournisseur SAN, les fichiers de configuration multivoie en exemple, trouvés dans le fichier /usr/share/doc/multipath-tools/exemples, et la base de données active multipathd :

```
# echo 'show config' | multipathd -k > multipath.conf-live
```

Pour préciser une particularité de multipathd, lorsqu'un fichier /etc/multipath.conf n'existe pas, la commande précédente ne retourne rien, comme si le résultat était une **fusion** entre le fichier /etc/multipath.conf et la base de données dans la mémoire. Pour y remédier, soit définir un fichier vide /etc/multipath.conf, en utilisant **touch**, ou en créer un qui redéfinit une valeur par défaut comme :

```
defaults {
       user_friendly_names no
 }
```

et redémarrez multipathd :

```
# systemctl restart multipath-tools.service
```

M aintenant, la commande « montrer la configuration » retournera la base de donnée active.

5.3.2. Installation du support multivoie

Pour activer **le support multivoie lors de l'installation :**
http://wiki.debian.org/DebianInstaller/MultipathSupport , utilisez la commande

```
install disk-detect/multipath/enable=true
```

à l'invite d'installation. Si les périphériques multivoie sont trouvés, ceux-ci apparaîtront tels que **/dev/mapper/mpath<X>** lors de l'installation.

5.3.3. Occultation des disques locaux lors de la génération des périphériques multivoie

Certaines machines ont des cartes SCSI locales pour leurs disques internes. DM-Multipath n'est pas recommandé pour ces appareils. La procédure suivante montre comment modifier le fichier de configuration multivoie afin d'ignorer les disques locaux lors de la configuration multivoie.

1. Déterminez quels sont les disques internes et les marquez-les comme appartenant à la liste noire. Dans cet exemple, /dev/sda est le disque interne. Notez que, comme initialement configuré dans le fichier de configuration multivoie par défaut, l'exécution de **multipath-v2** montre le disque local, **/dev/sda**, dans la carte multivoie. Pour de plus amples informations sur la sortie de la commande **multipath**, voir le *Chapitre 5, paragraphe 5. Administration et dépannage DM-Multipath.6. Sortie de la commande Multipath*.

```
# multipath -v2
create: SIBM-ESXSST336732LC____F3ET0EP0Q000072428BX1 undef WINSYS,SF2372
size=33 GB features="0" hwhandler="0" wp=undef
`-+- policy='round-robin 0' prio=1 status=undef
  |- 0:0:0:0 sda 8:0 [---------

device-mapper ioctl cmd 9 failed: Invalid argument
device-mapper ioctl cmd 14 failed: No such device or address
create: 3600a0b80001327d80000006d43621677 undef WINSYS,SF2372
size=12G features='0' hwhandler='0' wp=undef
`-+- policy='round-robin 0' prio=1 status=undef
  |- 2:0:0:0 sdb 8:16 undef ready running
    `- 3:0:0:0 sdf 8:80 undef ready running

create: 3600a0b80001327510000009a436215ec undef WINSYS,SF2372
size=12G features='0' hwhandler='0' wp=undef
`-+- policy='round-robin 0' prio=1 status=undef
  |- 2:0:0:1 sdc 8:32 undef ready running
    `- 3:0:0:1 sdg 8:96 undef ready running

create: 3600a0b80001327d800000070436216b3 undef WINSYS,SF2372
size=12G features='0' hwhandler='0' wp=undef
`-+- policy='round-robin 0' prio=1 status=undef
  |- 2:0:0:2 sdd 8:48 undef ready running
    `- 3:0:0:2 sdg 8:112 undef ready running

create: 3600a0b80001327510000009b4362163e undef WINSYS,SF2372
```

```
size=12G features='0' hwhandler='0' wp=undef
`-+- policy='round-robin 0' prio=1 status=undef
  |- 2:0:0:3 sdd 8:64 undef ready running
    `- 3:0:0:3 sdg 8:128 undef ready running
```

2. Afin d'empêcher le périphériques cartographe de tracer **/dev/sda** dans ses cartes multivoie, éditez la section **Liste Noire** du fichier /etc/multipath.conf pour inclure ce périphérique. Bien que vous puissiez mettre en liste noire le périphérique **sda** en utilisant un type **devnode**, qui ne serait pas une procédure sans danger puisque **/dev/sda** n'est pas garanti d'être le même au redémarrage. Pour mettre en liste noire des périphériques individuels, vous pouvez utiliser l'WWID de ce périphérique. Notez que dans la sortie de la commande **multipath-v2**, l'identifiant WWID du périphérique /dev/sda est SIBM-ESXSST336732LC____F3ET0EP0Q000072428BX1. Pour mettre en liste noire ce disque, incluez les éléments suivants dans le fichier /etc/multipath.conf.

```
blacklist {
      wwid SIBM-ESXSST336732LC____F3ET0EP0Q000072428BX1
}
```

3. Après avoir mis à jour le fichier /etc/multipath.conf, vous devez indiquer manuellement au démon **multipathd** de le recharger. La commande suivante recharge le fichier /etc/multipath.conf qui a été mis à jour.

```
# systemctl reload multipath-tools.service
```

4. Exécutez la commande suivante pour supprimer le périphérique multipath :

```
# multipath -f SIBM-ESXSST336732LC____F3ET0EP0Q000072428BX1
```

5. Pour vérifier si le retrait du périphérique a fonctionné, vous pouvez exécuter la commande **multipath -ll** pour afficher la configuration multivoie courante. Pour plus d'informations sur la commande **multipath -ll**, voir le *Chapitre 5, paragraphe 5. Administration et dépannage DM-Multipath.7. Requêtes trajets multiples avec la commande multipath*. Pour vérifier que l'appareil occulté n'a pas été ajouté sur la liste noire à posteriori, vous pouvez exécuter la commande multipath, comme dans l'exemple suivant. La commande multipath est à un niveau de verbosité de **v2** si vous ne spécifiez pas l'option **-v**.

```
# multipath

create: 3600a0b80001327d80000006d43621677 undef WINSYS,SF2372
size=12G features='0' hwhandler='0' wp=undef
`-+- policy='round-robin 0' prio=1 status=undef
  |- 2:0:0:0 sdb 8:16 undef ready running
    `- 3:0:0:0 sdf 8:80 undef ready running

create: 3600a0b8000132751000009a436215ec undef WINSYS,SF2372
size=12G features='0' hwhandler='0' wp=undef
`-+- policy='round-robin 0' prio=1 status=undef
  |- 2:0:0:1 sdc 8:32 undef ready running
    `- 3:0:0:1 sdg 8:96 undef ready running
```

```
create: 3600a0b80001327d800000070436216b3 undef WINSYS,SF2372
size=12G features='0' hwhandler='0' wp=undef
`-+- policy='round-robin 0' prio=1 status=undef
  |- 2:0:0:2 sdd 8:48 undef ready running
    `- 3:0:0:2 sdg 8:112 undef ready running

create: 3600a0b8000132751000000 9b4362163e undef WINSYS,SF2372
size=12G features='0' hwhandler='0' wp=undef
`-+- policy='round-robin 0' prio=1 status=undef
  |- 2:0:0:3 sdd 8:64 undef ready running
`- 3:0:0:3 sdg 8:128 undef ready running
```

5.3.4. Configuration des périphériques de stockage

Par défaut, DM-Multipath inclut le support pour les systèmes de stockage les plus courantes qui supportent DM-Multipath. Les valeurs de configuration par défaut, y compris les périphériques pris en charge, peut être trouvée dans le fichier multipath.conf.defaults.

Si vous avez besoin d'ajouter un périphérique de stockage multivoie qui n'est pas supporté par défaut comme périphérique connu, éditez le fichier /etc/multipath.conf et insérer les informations appropriées du périphérique.

Par exemple, pour ajouter de l'information sur la série HP Open-V, la saisie ressemble à ceci, où **%n** est le nom du périphérique :

```
devices {
     device {
            vendor "HP"
            product "OPEN-V."
            getuid_callout "/lib/udev/scsi_id --whitelisted --device=/dev/%n"
     }
}
```

Pour plus d'informations sur la section **Périphériques** du fichier de configuration, voir le *Chapitre 5, paragraphe 4. Le fichier de configuration DM-Multipath.5. La section Périphériques du fichier de configuration.*

5.4. Le fichier de configuration DM-Multipath

Par défaut, DM-Multipath fournit des valeurs de configuration pour les utilisations les plus courantes de mise en multivoie. En outre, DM-Multipath inclut le support pour les systèmes de stockage les plus courantes qui supportent DM-Multipath. Les valeurs de configuration par défaut et les périphériques pris en charge peuvent être trouvés dans le fichier multipath.conf.defaults.

Vous pouvez remplacer les valeurs de configuration par défaut pour DM-Multipath en éditant le fichier de configuration/etc/multipath.conf. Si nécessaire, vous pouvez également ajouter une baie de stockage qui n'est pas supporté par défaut dans le fichier de configuration. Ce chapitre fournit des informations sur l'analyse et la modification du fichier multipath.conf. Il contient des sections sur les sujets suivants :

- *4.1. Vue d'ensemble du fichier de configuration*
- *4.2. La section Liste Noire du fichier de configuration*
- *4.3. La section Valeurs par défaut du fichier de configuration*
- *4.4. Les Attributs Multivoie du fichier de configuration*
- *4.5. La section Périphériques du fichier de configuration*

Dans le fichier de configuration multivoie, vous devez spécifier uniquement les sections dont vous avez besoin pour votre configuration, ou les valeurs par défaut spécifiées que vous désirez changer dans le fichier multipath.conf.defaults. S'il y a des sections du fichier qui ne sont pas pertinentes pour votre environnement ou pour lesquels vous n'avez pas besoin de remplacer les valeurs par défaut, vous pouvez les laisser en commentaire, tels qu'ils sont dans le fichier initial.

Le fichier de configuration autorise la syntaxe de description par des expressions régulières.

Une version annotée du fichier de configuration peut être trouvée dans le fichier /usr/share/doc/multipath-tools/examples/multipath.conf.annotated.gz.

5.4.1. Vue d'ensemble du fichier de configuration

Le fichier de configuration multipath est divisé selon les sections suivantes :

Liste Noire

Liste des périphériques spécifiques qui ne seront pas pris en considération pour la mise en multivoie.

Exceptions de la Liste Noire

Liste des candidats à la mise en multivoie qui seront autrement mis en liste noire selon les paramètres de la section **Liste Noire**.

Valeurs par défaut

Paramètres généraux par défaut pour DM-Multipath.

Multivoies

Réglages pour les caractéristiques des périphériques individuels multivoie. Ces valeurs remplacent ce qui est spécifié dans les sections **Valeurs par défaut** et **Périphériques** du fichier de configuration.

Périphériques

Réglages des contrôleurs de stockage individuels. Ces valeurs remplacent ce qui est spécifié dans la section **Valeurs par défaut** du fichier de configuration. Si vous utilisez une baie de stockage qui n'est pas supporté par défaut, vous devrez peut-être créer une sous-section de périphériques pour votre baie.

Lorsque le système détermine les attributs d'un périphérique multivoie, d'abord il vérifie les paramètres multivoie, puis les paramètres par périphérique, puis les valeurs par défaut du système multivoie.

5.4.2. La section Liste Noire du fichier de configuration

La section **Liste Noire** du fichier de configuration multivoie spécifie les périphériques qui ne seront pas utilisés lorsque le système configure les périphériques multivoie. Les périphériques qui sont sur la **Liste Noire** ne seront pas regroupées dans un périphérique multivoie.

Si vous souhaitez mettre des périphériques en liste noire, vous pouvez le faire en fonction des critères suivants :

- Par WWID, comme décrit dans config-blacklist-by-wwid-title multipath-config-blacklist-by-wwid
- Par nom de périphérique, comme décrit dans config-blacklist-by-device-name-title multipath-config-blacklist-by-device-name
- Par type de dispositif, tel que décrit dans config-blacklist-by-device-type-title multipath-config-blacklist-by-device-type

Par défaut, une variété de types d'appareils sont sur la liste noire, même après que vous commentiez la section **Liste Noire** initiale du fichier de configuration. Pour plus d'informations, voir 4*.2.2. Mise en Liste Noire par nom de périphérique.*

5.4.2.1. Mise en Liste Noire en fonction de l'identifiant WWID (identifiant mondial)

Vous pouvez spécifier des périphériques individuels à mettre en liste noire en fonction de leur identifiant mondial avec une entrée **wwid** dans la section **Liste Noire** du fichier de configuration.

L'exemple suivant montre les lignes dans le fichier de configuration qui permettent la mise en liste noire d'un appareil avec un WWID qui est 26353900f02796769.

```
blacklist {
       wwid 26353900f02796769
}
```

5.4.2.2. Mise en Liste Noire par nom de périphérique

Vous pouvez mettre en liste noire des types de périphériques par nom de périphérique de sorte qu'ils ne seront pas regroupés dans un périphérique multivoie en spécifiant une entrée **devnode** dans la section **Liste Noire** du fichier de configuration.

L'exemple suivant montre les lignes dans le fichier de configuration, pour mettre dans la **Liste Noire** tous les périphériques SCSI, puisque cela impacte tous les périphériques ayant le nom commençant par sd*.

```
blacklist {
       devnode "^sd[a-z]"
}
```

Vous pouvez utiliser une entrée **devnode** dans la section **Liste Noire** du fichier de configuration pour spécifier des périphériques individuels à mettre dans la liste noire plutôt que tous les périphériques d'un type spécifique. Ce n'est pas recommandé, cependant, puisque à moins qu'elle ne soit statiquement cartographié par des règles udev, il n'y a aucune garantie qu'un périphérique spécifique aurait le même nom lors du redémarrage. Par exemple, un nom de périphérique peut changer de /dev/sda pour /dev/sdb au redémarrage.

Par défaut, les entrées **devnode** suivantes sont compilées dans la liste noire par défaut ; les périphériques concernés ne supportent pas DM-Multipath généralement. Pour activer le multi-acheminement sur l'un quelconque de ces périphériques, il est nécessaire de le spécifier dans la section **Exceptions de la Liste Noire** du fichier de configuration, comme décrit dans le *Chapitre 5, paragraphe 4. Le fichier de configuration DM-Multipath.2.4. Exceptions de Liste Noire.*

```
blacklist {
       devnode "^(ram|raw|loop|fd|md|dm-|sr|scd|st)[0-9]*"
       devnode "^hd[a-z]"
}
```

5.4.2.3. Mise en Liste Noire par type de périphérique

Vous pouvez spécifier les types de périphériques spécifiques dans la section **Liste Noire** du fichier de configuration avec une section périphérique. L'exemple suivant met en liste noire tous les périphériques IBM DS4200 et HP.

```
blacklist {
       device {
               vendor "IBM"
               product "3S42" #DS4200 Product 10
       }
       device {
               vendor "HP"
               product "*"
       }
}
```

5.4.2.4. Exceptions de Liste Noire

Vous pouvez utiliser la section **Exceptions de la Liste Noire** du fichier de configuration pour activer le multi-acheminement sur des périphériques qui ont été mis en liste noire par défaut.

Par exemple, si vous avez un grand nombre de périphériques et que vous voulez utiliser uniquement l'un d'entre eux en multivoie (avec l'identifiant WWID 3600d0230000000000e13955cc3757803), plutôt que de mettre en liste noire individuellement chacun des périphériques, excepté un seul, vous pourriez plutôt mettre en liste noire l'ensemble, et alors ne permettre l'utilisation d'un seul en ajoutant les lignes suivantes au fichier /etc/multipath.conf.

```
blacklist {
        wwid "*"
}

blacklist_exceptions {
        wwid "3600d0230000000000e13955cc3757803"
```

```
}
```

Lors de la spécification des périphériques dans la section **Exceptions de la Liste Noire** du fichier de configuration, vous devez spécifier les exceptions de la même manière qu'elles ont été précisées dans la **liste noire**. Par exemple, une exception WWID ne s'appliquera pas aux périphériques spécifiés par une entrée de la liste noire **devnode**, même si le périphérique défini dans la liste noire est associé à ce WWID. De même, les exceptions devnode ne s'appliquent qu'aux entrées devnode, et les exceptions de périphériques ne s'appliquent seulement qu'aux entrées de périphériques.

5.4.3. La section Valeurs par défaut du fichier de configuration

Le fichier de configuration /etc/multipath.conf inclut une section **Valeurs par défaut** qui définit les paramètres **noms_conviviaux** à **oui**, comme suit.

```
defaults {
        user_friendly_names yes
}
```

Cela sur-écrit la valeur par défaut du paramètre **noms_conviviaux**.

Le fichier de configuration comprend un modèle de configuration par défaut. Cette section est mise en commentaire, comme suit.

```
#defaults {
# udev_dir /dev
# polling_interval 5
# selector "round-robin 0"
# path_grouping_policy failover
# getuid_callout "/lib/dev/scsi_id --whitelisted --device=/dev/%n"
#prioconst
#path_checkerdirectio
#rr_min_io1000
#rr_weightuniform
#failbackmanual
#no_path_retryfail
#user_friendly_namesno
#}
```

Pour sur-écrire la valeur par défaut de l'un des paramètres de configuration, vous pouvez copier la ligne correspondante à partir de ce modèle dans la section **Valeurs par défaut** et décommentez-la. Par exemple, pour remplacer le paramètre **path_grouping_policy** de sorte qu'il soit défini à **multibus** plutôt qu'à la valeur par défaut de **failover**, copiez la ligne appropriée, depuis le modèle, dans la section initiale **Valeurs par défaut** du fichier de configuration, et dé-commentez-la, comme suit :

```
defaults {
        user_friendly_names yes
        path_grouping_policy multibus
}
```

Le tableau 5.3 décrit les attributs qui sont définis dans la section **Valeurs par défaut** du fichier de configuration multipath.conf. Ces valeurs sont utilisées par DM-Multipath à moins qu'elles ne soient sur-écrites par les attributs spécifiés dans les sections **périphériques** et **multivoie** du fichier multipath.conf.

Tableau 5.3 Configuration des Valeurs par défaut **de DM-Multipath**

Attribut	Description
polling_interval	Spécifie l'intervalle entre deux vérifications de chemin en quelques secondes. Pour les chemins qui fonctionnent bien, l'intervalle entre les contrôles augmentera progressivement à (4 * **polling_interval**). La valeur par défaut est **5**.
udev_dir	Le répertoire où les nœuds de périphériques udev sont créés. La valeur par défaut est /dev.
multipath_dir	Le répertoire où les objets partagés dynamiques sont stockés. La valeur par défaut dépend du système, communément /lib/multipath.
verbosity	Le niveau de verbosité par défaut. Des valeurs plus élevées augmentent le niveau de verbosité. Les niveaux valides sont compris entre 0 et 6. La valeur par défaut est 2.
path_selector	Spécifie l'algorithme à utiliser par défaut afin de déterminer quel chemin utiliser pour la prochaine opération d'E/S. Les valeurs possibles sont : • **round-robin 0**: Boucle par tous les chemins dans le groupe de chemins, d'envoyer la même quantité d'E/S à chacun. • **file d'attente de longueur 0**: Envoyer le tas à côté de l'I/O sur le chemin avec le moins de circulation requêtes E/S. • **service de temps 0**: Envoyer le tas à côté de l'I/O sur le chemin avec le temps de service plus courte estimée, qui est déterminée en divisant la taille totale de l'encours I/O à chaque chemin de son débit relatif. La valeur par défaut est **round-robin 0**.
path_grouping_policy	Spécifie la politique de regroupement chemin par défaut à appliquer à trajets multiples non spécifiés. Les valeurs possibles sont: • **basculement** = 1 chemin par groupe de priorité • **multibus** = tous les chemins valides dans 1 groupe de priorité • **group_by_serial** = 1 groupe de priorité par numéro de série détecté • **group_by_prio** valeur de priorité = 1 groupe de priorité par voie de • **group_by_node_name** = 1 groupe prioritaire par nom de noeud cible. La valeur par défaut est **failover.**
getuid_callout	Indique le programme par défaut et les arguments pour appeler de manière à obtenir un identifiant unique chemin. Un chemin absolu est requis. La valeur par défaut est **/lib/udev/scsi_id --whitelisted --device=/dev/%n.**
prio	Indique la fonction par défaut à appeler pour obtenir une valeur de priorité chemin. Par exemple, les bits ALUA en SPC-3 fournissent une valeur prio exploitable. Les valeurs possibles sont: • **const** : Définit une priorité de 1 à tous les chemins.

	• **emc** : génèrer la priorité de chemin pour les ensembles EMC. • **alua**: : Génère la priorité de chemin en fonction des paramètres ALUA SCSI-3. • **netapp** : génèrer la priorité de chemin pour les ensembles NetApp. • **rdac** : Génère la priorité de chemin pour les contrôleurs RDAC LSI et Engenio. • **hp_sw** : Génère la priorité de chemin pour les contrôleurs Compaq et HP en mode actif ou veille. • **hds** : génèrer la priorité de chemin pour les ensembles modulaires de stockage Hitachi HDS. La valeur par défaut est **const**.
prio_args	La chaîne d'arguments passés à la fonction prio La plupart des fonctions prio n'avez pas besoin d'arguments. Le prioritizer DataCore besoin. Par exemple, **"timeout = 1000 preferredsds = foo "**. La valeur par défaut est (null) **""**.
features	Les fonctionnalités supplémentaires de périphériques multivoie. Le seul élément existant est **queue_if_no_path**, qui est la même que la mise en **no_path_retry** à **queue**. Pour plus d'informations sur les problèmes qui peuvent survenir lors de l'utilisation de cette fonctionnalité, voyez Section, *5.5. Problèmes avec queue_if_no_path*.
path_checker	Spécifie la méthode utilisée par défaut pour déterminer l'état des chemins. Les valeurs possibles sont : **readsector0** : Lit le premier secteur du périphérique. **tur**: émission d'un TEST UNIT READY de l'appareil. **emc_clariion**: Requête la EMC Clariion page spécifique EVPD 0xC0 pour déterminer le chemin. **hp_sw**: Vérifiez l'état de chemin pour les baies de stockage HP avec Active/Standby du firmware. **rdac** : Vérifie l'état du chemin pour les contrôleurs de stockage RDAC LSI et Engenio. **directio** : Lit le premier secteur avec E/S directe. La valeur par défaut est **directio**.
failback	Gère le rétablissement du groupe de chemin. • Une valeur de **immédiate** spécifie rétablissement immédiat pour le groupe de chemin de plus haute priorité qui contient des chemins actifs. • Une valeur de **manuel** indique qu'il ne devrait pas être immédiat, mais que le rétablissement ne peut se faire que par intervention de l'opérateur. • Une valeur numérique supérieure à zéro indique un rétablissement différé à l'état d'origine et s'exprime en secondes. La valeur par défaut est **manual**.

rr_min_io	Indique le nombre de demandes d'E/S pour acheminer vers un chemin avant de passer à la voie suivante dans le groupe trajet de courant. La valeur par défaut est **1000**.
rr_weight	S'il est réglé sur **priorités**, alors au lieu d'envoyer des demandes **rr_min_io** à un chemin avant d'appeler **path_selector** pour choisir la voie suivante, le nombre de demandes à envoyer est déterminé par **rr_min_io** fois le chemin prioritaire, tel que déterminé par la fonction **prio**. S'il est réglé sur **uniform**, tous les poids des chemins sont égaux. La valeur par défaut est **uniform**.
no_path_retry	Une valeur numérique pour cet attribut spécifie le nombre de fois que le système devrait tenter d'utiliser un chemin défaillant avant de désactiver la mise en liste d'attente. Une valeur d'échec indiquant **immediate**, il n'y a pas de mise en file d'attente. Une valeur de mise en file d'attente indique que la mise en file d'attente ne doit pas s'arrêter jusqu'à ce que le chemin soit réparé. La valeur par défaut est **0**.
user_friendly_names	Si la valeur est réglée sur oui, cela spécifie que le système doit utiliser le fichier /etc/multipath/bindings pour attribuer un **alias** unique et immuable à un périphérique **multivoie**, sous la forme mpathn. Si la valeur est réglée sur non, cela spécifie que le système doit utiliser l'identifiant WWID comme **alias** pour le périphérique **multivoie**. Dans les deux cas, ce qui est spécifié ici sera remplacée par tout alias spécifique de périphérique que vous indiquez dans la section **Multivoies** du fichier de configuration. La valeur par défaut est **non**.
queue_without_daemon	Si la valeur est réglée sur non, le démon **multipathd** désactivera la file d'attente pour tous les périphériques quand il sera fermé. La valeur par défaut est **oui**.
flush_on_last_del	Si elle est définie à oui, alors **DM-Multipath** désactivera la file d'attente lorsque le dernier chemin d'un périphérique a été supprimé. La valeur par défaut est **non**.
max_fds	Définit le nombre maximal de descripteurs de fichiers ouverts qui peuvent être ouverts par **DM-Multipath** et le démon **multipathd**. Ceci est équivalent à la commande **ulimit-n**. Une valeur de max fixera ce nombre à la limite du système défini dans /proc/sys/fs/nr_open. Si ce nombre n'est pas défini, le nombre maximal de descripteurs de fichiers ouverts est tiré du processus appelant, il est généralement de 1024. Pour être sûr, cela doit être réglé sur le nombre maximum de chemins plus 32, si ce nombre est supérieur à 1024.

checker_timer	Définit le délai d'attente à utiliser pour les testeurs de chemin qui émettent des commandes SCSI avec un délai d'attente explicite, en secondes. La valeur par défaut provient de /sys/block/sdx/device/timeout, qui est de **30** secondes à partir de la version 12.04 LTS.
fast_io_fail_tmo	Définit le nombre de secondes que la couche SCSI attendra après qu'un problème ait été détecté sur un port distant FC avant d'interrompre les E/S vers les périphériques sur ce port distant. Cette valeur doit être inférieure à la valeur de dev_loss_tmo. Mettre ce paramètre à off désactivera le délai d'attente. La valeur par défaut est définie par le système d'exploitation.
dev_loss_tmo	Définit le nombre de secondes que la couche SCSI attendra après qu'un problème ait été détecté sur un port FC distant avant de le retirer du système. La définition de cette valeur à infini la fixe à 2147483647 secondes, ou 68 ans. La valeur par défaut est déterminée par le système d'exploitation.

5.4.4. Attributs multivoie du fichier de configuration

Le tableau *5.4. Attributs multivoie* montre les attributs que vous pouvez définir dans la section **Multivoies** du fichier de configuration multipath.conf pour chaque périphérique multivoie spécifique. Ces attributs s'appliquent uniquement à celui qui est spécifié multivoie. Ces valeurs par défaut sont utilisées par DM-Multipath et l'emportent sur les attributs définis dans les sections **Valeurs par défaut** et **périphériques** du fichier multipath.conf.

Tableau 5.4 Attributs multivoie

Attribut	Description
wwid	Spécifie l'identifiant WWID du périphérique **multivoie** auquel les attributs multivoie s'appliquent. Ce paramètre est obligatoire pour cette section du fichier **multipath.conf**.
alias	Spécifie le nom symbolique pour le périphérique **multivoie** auquel les attributs multivoie s'appliquent. Si vous utilisez les **noms_conviviaux**, ne les définissez pas à mpathn, ce qui peut entrer en conflit avec un nom convivial d'utilisateur attribué automatiquement et vous donner des noms de nœuds de périphériques incorrects.

En plus, les paramètres suivants peuvent être sur-écrits dans cette section **Multivoies**.

- *path_grouping_policy*
- *Path_selector*
- *failback*

- *prio*
- *prio_args*
- *no_path_retry*
- *rr_min_io*
- *rr_weight*
- *flush_on_last_del*

L'exemple suivant montre les attributs multivoie spécifiés dans le fichier de configuration pour deux périphériques multivoie spécifiques. Le premier périphérique a un identifiant WWID qui est 3600508b4000156d70001200000b0000 et un nom symbolique (alias) qui est yellow.

Le second périphérique multivoie, dans l'exemple, a un identifiant WWID qui est 1DEC_____321816758474 et un nom symbolique (alias) qui est red. Dans cet exemple, les attributs *rr_weight* sont définis prioritaires.

```
multipaths {
        multipath {
                wwid 3600508b4000156d70001200000b0000
                alias yellow
                path_grouping_policy multibus
                path_selector "round-robin 0"
                failback manual
                rr_weight priorities
                no_path_retry 5
        }
        multipath {
                wwid 1DEC_____321816758474
                alias red
                rr_weight priorities
         }
}
```

5.4.5. La section Périphériques du fichier de configuration

Le tableau *5.5. Attributs de périphériques* renseigne sur les attributs que vous pouvez définir pour chaque périphérique de stockage individuel dans la section **Périphériques** du fichier de configuration multipath.conf. Ces attributs sont utilisés par DM-Multipath à moins qu'ils ne soient sur-écrits par les attributs spécifiés dans la section **Multivoies** du même fichier, pour les chemins que contiennent le périphérique. Ces attributs sur-écrivent les attributs définis dans la section **Valeurs par défaut** du fichier de configuration.

De nombreux périphériques qui prennent en charge la configuration multivoie sont inclus par défaut dans une configuration multivoie. Les valeurs, pour les périphériques pris en charge par défaut, sont répertoriées dans le fichier multipath.conf.defaults. Vous n'aurez probablement pas besoin de modifier les valeurs de ces périphériques, mais si vous le faites, vous pouvez sur-écrire les valeurs par défaut en ajoutant une entrée dans le fichier de configuration, pour le périphérique concerné, qui sur-écrit ces valeurs. Vous pouvez copier les valeurs par défaut de configuration du périphérique à partir du fichier multipath.conf.annotated.gz ou si vous souhaitez avoir un fichier de configuration bref, depuis le fichier multipath.conf.synthetic pour le périphérique, et sur-écrire les valeurs que vous voulez changer.

Pour ajouter un périphérique à cette section du fichier de configuration qui n'est pas configuré automatiquement par défaut, vous devez définir les paramètres **vendor** et **product**. Vous pouvez trouver

ces valeurs aux lignes **/sys/block/device_name/device/vendor** et **/sys/block/device_name/device/model**, où device_name est le périphérique à mettre en multivoie, comme dans l'exemple suivant :

```
# cat /sys/block/sda/device/vendor
WINSYS
# cat /sys/block/sda/device/model
SF2372
```

Les paramètres supplémentaires à préciser dépendent des spécifications de votre périphérique. Si le dispositif est actif/actif, vous n'aurez généralement pas besoin de définir de paramètres supplémentaires. Vous voudrez peut-être définir *path_grouping_policy* à **multibus**. Les autres paramètres que vous aurez besoin de régler sont *no_path_retry* et *rr_min_io*, tel que décrit dans le tableau *5.4. Attributs multivoie*.

Si le dispositif est actif/passif, mais s'il commute automatiquement les chemins d'E/S sur le chemin passif, vous devez modifier la fonction de contrôleur pour qu'il ne puisse pas envoyer des E/S sur le chemin à tester si cela fonctionne (sinon, votre périphérique gardera la commutation). Ceci signifie presque toujours que vous réglez le *path_checker* à **tur**, cela fonctionne pour tous les périphériques SCSI qui prennent en charge la commande "Test Unit Ready", ce que la plupart font.

Si le périphérique a besoin d'une commande spéciale pour commuter les chemins, alors la configuration de celui-ci pour la mise en multivoie nécessite un module du noyau gestionnaire de matériel. Le module courant disponible gestionnaire de matériel est **emc**. Si cela n'est pas suffisant pour votre périphérique, vous ne serez pas à même de configurer votre périphérique pour la mise en multivoie.

Tableau 5.5 Attributs de périphériques

Attribut	Description
vendor	Spécifie le nom du fabricant du périphérique de stockage auquel les attributs de périphériques s'appliquent, par exemple COMPAQ.
product	Spécifie le nom de produit de l'unité de stockage auquel les attributs de périphériques s'appliquent, par exemple HSV110 (C)COMPAQ.
revision	Indique l'identifiant de version de produit du périphérique de stockage.
product_blacklist	Spécifie une expression régulière utilisée à la Liste Noire des périphériques par produit.
hardware_handler	Spécifie un module qui sera utilisé pour effectuer des actions spécifiques au matériel lors de la commutation des groupes de chemins ou de traitement des erreurs d'E/S. Les valeurs possibles sont : • **1 emc** : gestionnaire de matériel pour les baies de stockage EMC • **1 alua** : gestionnaire de matériel pour les baies ALUA SCSI-3. • **1 hp_sw** : gestionnaire de matériel pour les contrôleurs Compaq/HP • **1 rdac** : gestionnaire de matériel pour les contrôleurs RDAC LSI/Engenio.

En outre, les paramètres suivants peuvent être remplacés dans la section **Périphérique**

- *path_grouping_policy*

- *getuid_callout*
- *path_selector*
- *path_checker*
- *features*
- *failback*
- *prio*
- *prio_args*
- *no_path_retry*
- *rr_min_io*
- *rr_weight*
- *fast_io_fail_tmo*
- *dev_loss_tmo*
- *flush_on_last_del*

Chaque fois qu'un hardware_handler est spécifié, il est de votre responsabilité de vous assurer que le module noyau approprié est chargé pour supporter l'interface spécifiée. Ces modules peuvent être trouvés dans /lib/modules/`uname-r`/kernel/drivers/scsi/device_handler/. Le module requis devrait être intégrée dans l'initrd afin d'assurer sa reconnaissance nécessaire et que la capacité de basculement-rétablissement soit disponible lors de l'initialisation. Par exemple,

```
# echo scsi_dh_alua >> /etc/initramfs-tools/modules ## ajout du module au fichier
# update-initramfs -u -k all
```

L'exemple suivant montre une entrée de périphérique dans le fichier de configuration multivoie.

```
#devices {
#device {
#vendor"COMPAQ "
#product"MSA1000 "
#path_grouping_policymultibus
#path_checkertur
#rr_weightpriorities
#}
#}
```

L'espace réservé dans les champs **vendor**, **product** et **revision** ont un sens parce que la mise en multivoie effectue une correspondance directe sur ces attributs, dont le format est défini par la spécification SCSI, en particulier la commande **Standard INQUIRY :** http://en.wikipedia.org/wiki/SCSI_Inquiry_Command . Lorsque des guillemets sont utilisés, les champs **vendor**, **product** et **revision** seront interprétés strictement selon les spécifications. Les expressions régulières peuvent être intégrées dans les chaînes entre guillemets. Si un champ est défini sans l'espacement requis, la mise en multivoie copiera la chaîne dans la mémoire tampon de taille appropriée et enregistrera le nombre approprié d'espaces. Le cahier des charges prévoit que l'ensemble du champs sera diffusé avec des caractères imprimables ou des espaces, comme on le voit dans l'exemple ci-dessus.

- vendor : 8 caractères
- product : 16 caractères

- revision : 4 caractères

Pour créer un fichier de configuration plus robuste, les expressions régulières peuvent également être utilisés. Les opérateurs intègrent **^ $ []. *? +**. Des exemples de fonctions d'expressions régulières peuvent être trouvées en examinant la base de données multivoie en direct et le fichier exemple multipath.conf trouvés à l'adresse /usr/share/doc/multipath-tools/exemples :

```
# echo 'show config' | multipathd -k
```

5.5. Administration et dépannage DM-Multipath

5.5.1. Redimensionnement d'un périphérique multipath en ligne

Si vous voulez redimensionner un périphérique multipath en ligne, utilisez la procédure suivante :

1. Redimensionnez votre périphérique physique. Ceci est spécifique des plateformes de stockage.
2. Utilisez la commande suivante pour trouver les chemins d'accès aux Numéros d'Unité Logique (LUN : Logical Unity Number) :

```
# multipath -l
```

3. Mettez à jour vos chemins. Pour les périphériques SCSI, écrire 1 dans le fichier rescan de l'appareil, occasionne une nouvelle analyse par le pilote SCSI, comme dans la commande suivante :

```
# echo 1 > /sys/block/device_name/device/rescan
```

4. Redimensionnez votre périphérique multivoie en exécutant la commande multipathd de redimensionnement :

```
# multipathd -k 'resize map mpatha'
```

5. Redimensionnez le système de fichiers (en supposant qu'aucune partition LVM ou DOS n'est utilisée) :

```
# resize2fs /dev/mapper/mpatha
```

5.5.2. Déplacer des Systèmes de fichiers racine d'un périphérique à chemin unique à un périphérique multivoie

Ceci est considérablement simplifié par l'utilisation des références UUID pour identifier les périphériques comme une étiquette intrinsèque. Il suffit d'installer **multipath-tools-boot** et redémarrez. Ceci reconstruira le disque virtuel initial et donnera les moyens à DM-Multipath, la possibilité de construire ses chemins avant que le système de fichiers racine soit monté par référence UUID.

Chaque fois que le fichier multipath.conf est mis à jour, alors le démon initrd doit l'être, en exécutant la commande **update-initramfs-u -k all**. La raison est que le fichier multipath.conf est copié sur le disque virtuel et fait partie intégrante pour déterminer les périphériques disponibles pour le regroupement via ses sections Liste Noire et Périphériques.

5.5.3. Déplacer des Systèmes de fichiers swap d'un périphérique à chemin unique à un périphérique multivoie

La procédure est exactement la même que celle illustrée dans le paragraphe précédent intitulé *5.2.*

Déplacer des Systèmes de fichiers racine d'un périphérique à chemin unique à un périphérique multivoie.

5.5.4. Le démon Multipathd

Si vous rencontrez des difficultés lors de la définition d'une configuration multivoie, vous devriez vous assurer que le démon de DM-Multipath est en fonctionnement, comme décrit dans le *Chapitre 5, paragraphe 3. Présentation de la Configuration de DM-Multipath.1. Configuration de DM-Multipath*. Le démon **multipathd** doit fonctionner dans le but d'utiliser les périphériques multivoie. Regardez également le *Chapitre 5, paragraphe 5. Administration et dépannage DM-Multipath.10. Dépannage à l'aide de la console interactive de multipathd* qui concerne l'interaction avec **multipathd**, comme une aide de débogage.

5.5.5. Questions avec queue_if_no_path

Si **features "1 queue_if_no_path "** est spécifié dans le fichier /etc/multipath.conf, alors tout processus qui utilise des E/S sera suspendu jusqu'à ce que une ou plusieurs chemins soient restaurés. Pour éviter cela, réglez le paramètre **no_path_retry** N dans le fichier /etc/multipath.conf.

Lorsque vous réglez le paramètre **no_path_retry**, retirez également l'option **features "1 queue_if_no_path"** depuis le fichier /etc/multipath.conf. Toutefois, si vous utilisez un périphérique multivoie pour lequel l'option **features "1 queue_if_no_path"** est définie et compilée par défaut, comme pour de nombreux périphériques SAN, vous devez ajouter l'option **features "0"** pour occulter cette valeur par défaut. Vous pouvez le faire en copiant la section existante **périphériques**, et juste cette section (et non le fichier entier), de /usr/share/doc/multipath-tools/examples/multipath.conf.annotated.gz dans le fichier /etc/multipath.conf et le modifier en fonction de vos besoins.

Si vous avez besoin d'utiliser l'option **"1 queue_if_no_path"** et que vous rencontrez la difficulté notée ici, utiliser la commande **dmsetup** pour modifier la stratégie à l'exécution pour un LUN particulier (c'est-à-dire, pour lequel tous les chemins sont indisponibles). Par exemple, si vous souhaitez modifier la stratégie sur le périphérique multivoie mpathc de **"queue_if_no_path"** pour **"fail_if_no_path"**, exécutez la commande suivante :

```
# dmsetup message mpathc 0 "fail_if_no_path"
```

V ous devez spécifier l'alias mpathN plutôt que le chemin.

5.5.6. Sortie de la commande multipath

Lorsque vous créez, modifiez ou listez un périphérique multivoie, vous obtenez une impression du paramétrage courant du périphérique. Le format est le suivant, pour chaque périphérique multivoie :

```
action_if_any: alias (wwid_if_different_from_alias) dm_device_name_if_known vendor,
product
   size=size features='features' hwhandler='hardware_handler'
wp=write_permission_if_known
```

Pour chaque groupe de chemins :

```
  -+- policy='scheduling_policy' prio=prio_if_known
  status=path_group_status_if_known
```

Pour chaque chemin :

```
   `- host:channel:id:lun devnode major:minor dm_status_if_known path_status
  online_status
```

Par exemple, la sortie d'une commande multipath pourrait se présenter comme suit :

```
  3600d0230000000000e13955cc3757800 dm-1 WINSYS,SF2372
  size=269G features='0' hwhandler='0' wp=rw
  |-+- policy='round-robin 0' prio=1 status=active
  | `- 6:0:0:0 sdb 8:16 active ready running
  `-+- policy='round-robin 0' prio=1 status=enabled
    `- 7:0:0:0 sdf 8:80 active ready running
```

Si le chemin est en place et prêt pour les E/S, le statut du chemin est **prêt** ou **fantôme**. Si le chemin n'est plus accessible, le statut est **défectueux** ou **précaire**. Le statut du chemin est mis à jour périodiquement par le démon **multipathd** basé sur l'intervalle d'interrogation défini dans le fichier /etc/multipath.conf.

Les statuts du cartographe de périphérique (dm : device mapper) sont similaires aux statuts du chemin, mais du point de vue du noyau. Le statut du cartographe de périphériques a deux états: **en panne**, qui est analogue à **défectueux**, et **actif**, qui couvre tous les autres états du chemin. De temps en temps, l'état de chemin et l'état du cartographe de périphérique, pour un même périphérique, ne seront temporairement pas en accord.

Les valeurs possibles pour **online_status** sont **fonctionne** et **déconne cté**. Un état **déconnecté** signifie que le périphérique SCSI a été désactivé.

> Lorsqu'un périphérique multivoie est en cours de création ou de modification, le statut de groupe chemin, le nom du périphérique cartographe de périphérique, les permissions d'écriture, et le statut du cartographe de périphérique ne sont pas connus. En outre, les fonctionnalités ne sont pas toujours correctes.

5.5.7. Requêtes trajets multiples avec la commande multipath

Vous pouvez utiliser les options **-l** et **-ll** de la commande **multipath** pour afficher la configuration courante multivoie. L'option **-l** affiche la topologie multivoie recueillie dans les informations de sysfs et auprès du cartographe de périphériques. L'option **-ll** affiche les informations que l'option **-l** permet d'afficher en plus de tous les autres éléments disponibles du système.

Lors de l'affichage de la configuration multivoie, il y a trois niveaux de verbosité que vous pouvez spécifier avec l'option **-v** de la commande multipath. Spécifier **-v0** ne donne aucune sortie. Spécifier **-v1** ne donne que les noms multivoie créés ou mis à jour uniquement, que vous pouvez ensuite transmettre à d'autres outils tels que kpartx. Spécifier **-v2** imprime tous les chemins détectés, les multivoies et la cartographie des périphériques.

> Le niveau de **verbosité** de multivoie est de **2** et peut être globalement modifié en définissant l'*attribut de verbosité* dans la section **Valeurs par défaut** du fichier multipath.conf.

L'exemple suivant montre la sortie d'une commande **multipath-l**.

```
# multipath -l
  3600d0230000000000e13955cc3757800 dm-1 WINSYS,SF2372
  size=269G features='0' hwhandler='0' wp=rw
  |-+- policy='round-robin 0' prio=1 status=active
  | `- 6:0:0:0 sdb 8:16 active ready running
  `-+- policy='round-robin 0' prio=1 status=enabled
    `- 7:0:0:0 sdf 8:80 active ready running
```

L'exemple suivant montre la sortie d'une commande **multipath-ll**.

```
# multipath -ll
  3600d0230000000000e13955cc3757801 dm-10 WINSYS,SF2372
  size=269G features='0' hwhandler='0' wp=rw
  |-+- policy='round-robin 0' prio=1 status=enabled
  | `- 19:0:0:1 sdc 8:32 active ready running
  `-+- policy='round-robin 0' prio=1 status=enabled
    `- 18:0:0:1 sdh 8:112 active ready running
    3600d0230000000000e13955cc3757803 dm-2 WINSYS,SF2372
    size=125G features='0' hwhandler='0' wp=rw
    `-+- policy='round-robin 0' prio=1 status=active
      |- 19:0:0:3 sde 8:64 active ready running
        `- 18:0:0:3 sdj 8:144 active ready running
```

5.5.8. Options de la commande multipath

Le tableau 5.6. décrit certaines options de la commande **multipath** que vous pourriez trouver utiles.

Tableau 5.6. Options utiles de la commande multipath

Option	Description
-l	Affiche la configuration multivoie courante recueillie auprès de **sysfs** et le cartographe de périphériques.
-ll	Affiche la configuration multivoie courante recueillie auprès de **sysfs** et du cartographe de périphériques ainsi que tous les autres éléments disponibles sur le système.
-f device	Retire le périphérique multivoie nommé.
-F	Retirez tous les périphériques multivoie inutilisés.

5.5.9. Déterminer les entrées du cartographe de périphérique avec la commande dmsetup

Vous pouvez utiliser la commande **dmsetup** pour savoir quelles entrées du cartographe de périphérique correspondent aux périphériques définis en **multivoie**.

La commande suivante affiche tous les périphériques cartographes de périphériques et leurs numéros majeur et mineur. Les numéros mineurs déterminent le nom du périphérique cartographe. Par exemple, un numéro mineur de **3** correspond au périphérique cartographié /dev/dm-3.

```
# dmsetup ls
```

```
mpathd (253, 4)
mpathep1 (253, 12)
mpathfp1 (253, 11)
mpathb (253, 3)
mpathgp1 (253, 14)
mpathhp1 (253, 13)
mpatha (253, 2)
mpathh (253, 9)
mpathg (253, 8)
VolGroup00-LogVol01 (253, 1)
mpathf (253, 7)
VolGroup00-LogVol00 (253, 0)
mpathe (253, 6)
mpathbp1 (253, 10)
mpathd (253, 5)
```

5.5.10. Dépannage à l'aide de la console interactive de multipathd

La commande **multipathd -k** est une interface interactive au démon **multipathd**. Le lancement de cette commande ouvre une console multivoie interactive. Après avoir entré cette commande, vous pouvez entrer aider à obtenir une liste des commandes disponibles, vous pouvez saisir **help** pour obtenir une liste de commandes disponibles, vous pouvez saisir une commande interactive ou vous pouvez entrer **CTRL-D** pour quitter.

La console interactive de multipathd peut être utilisée pour résoudre les problèmes que vous pouvez rencontrer avec votre système. Par exemple, la séquence de commande suivante affiche la configuration multipath, y compris les valeurs par défaut, avant de quitter la console. Voir l'article d'IBM http://www-01.ibm.com/support/docview.wss?uid=isg3T1011985 **"Astuces avec multipathd "** pour plus d'exemples.

```
# multipathd -k
  > > show config
  > > CTRL-D
```

La séquence de commandes suivante garantit que DM-multipath n'a rien modifié de la configuration contenue dans le fichier multipath.conf.

```
# multipathd -k
> > reconfigure
> > CTRL-D
```

Utilisez les commandes suivantes pour s'assurer que le vérificateur de chemin fonctionne correctement.

```
# multipathd -k
> > show paths
> > CTRL-D
```

Les commandes peuvent également être transmis en continu vers multipathd en utilisant stdin comme ceci :

```
# echo 'show config' | multipathd-k
```

Chapitre 6. Administration à distance

Il y a plusieurs façons d'administrer un serveur Linux à distance. Ce chapitre couvrira trois des applications les plus populaires en la matière, **OpenSSH**, **Puppet**, et **Zentyal**.

6.1. Serveur OpenSSH

6.1.1. Introduction

Cette section du guide du serveur Ubuntu présente un ensemble d'outils puissants appelé **OpenSSH** pour le contrôle à distance et le transfert de données entre des ordinateurs en réseau. Vous apprendrez également quelques paramètres de configuration possibles avec l'application serveur OpenSSH et comment les changer sur votre système Ubuntu.

OpenSSH est une version libre de la famille d'outils du protocole Secure Shell (SSH) pour le contrôle à distance ou le transfert des fichiers entre les ordinateurs. Les outils traditionnels utilisés pour accomplir ces fonctions tels que **telnet** ou **rcp** ne sont pas sécurisés et transmettent le mot de passe utilisateur en clair lors de leurs utilisations. OpenSSH fournit un démon de serveur et des outils pour les clients afin de sécuriser le contrôle à distance chiffré et les opérations de transfert de fichiers, remplaçant ainsi les anciens outils.

Le serveur OpenSSH, **sshd**, attend en permanence des connexions depuis des clients. Quand une requête de connexion a lieu, **sshd** établit la connexion correcte en fonction du type de client. Par exemple, si un client se connecte avec le client **ssh**, le serveur OpenSSH va établir une connexion sécurisée après une authentification. Si un client se connecte 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**.

6.1.2. 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 install openssh-client
```

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

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

Le paquet **openssh-server** peut aussi être sélectionné pour s'installer pendant la procédure d'installation de l'édition serveur.

6.1.3. Configuration

Vous pouvez configurer le comportement par défaut du serveur OpenSSH, **sshd**, en modifiant le fichier /etc/ssh/sshd_config. Pour des informations sur les options de configuration utilisées dans ce fichier, veuillez lire le manuel approprié en tapant la commande suivante dans un terminal :

```
man sshd_config
```

Il existe de nombreuses directives dans le fichier de configuration **sshd** contrôlant des choses telles que les paramètres de communication et les modes d'authentification. Ce qui suit sont des exemples de directives de configuration modifiables en éditant le fichier /etc/ssh/sshd_config.

Avant de modifier 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.

Copiez le fichier /etc/ssh/sshd_config et protégez le en écriture en tapant la commande suivante dans un terminal :

```
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 pouvez changer :

- Pour que OpenSSH écoute sur le port TCP 2222 au lieu du port par défaut 22, changez la directive Port comme ceci :

  ```
  Port 2222
  ```

- Pour que **sshd** accepte les informations de connexion basées sur une clef publique, il suffit d'ajouter ou de modifier la ligne :

  ```
  PubkeyAuthentication yes
  ```

  Si la ligne est déjà présente, alors assurez-vous qu'elle n'est pas commentée.

- Pour que le serveur OpenSSH affiche le contenu du fichier /etc/issue.net comme une invite avant l'affichage de l'écran de connexion, il suffit d'ajouter ou de modifier la ligne :

  ```
  Banner /etc/issue.net
  ```

  dans le fichier /etc/ssh/sshd_config.

Après avoir modifié le fichier /etc/ssh/sshd_config, enregistrez-le et redémarrez le service **sshd** afin de prendre en compte les changements. Pour cela, saisissez la commande suivante dans un terminal :

```
sudo systemctl restart sshd.service
```

! Beaucoup d'autres directives de configuration **sshd** sont disponibles pour changer le comportement de l'application serveur en fonction de vos besoins. Soyez averti, cependant, si votre seul moyen d'accès à un serveur est **ssh** et que vous faites une erreur dans la configuration **sshd** dans le fichier /etc/ssh/sshd_config, vous pouvez vous retrouver bloqué sur le serveur lors de son redémarrage. En outre, si une directive de configuration incorrecte est fournie, le serveur **sshd** peut refuser de démarrer, soyez donc très prudent lorsque vous modifiez ce fichier sur un serveur distant.

6.1.4. Clés SSH

Les **clés** SSH permettent l'authentification entre deux hôtes sans avoir besoin de mot de passe. L'authentification par clé SSH utilise deux clés, une clé **privée** et une clé **publique**.

Pour générer les clés, dans un terminal tapez :

```
ssh-keygen -t rsa
```

Cela générera les clés à l'aide de l'**Algorithme RSA**. Pendant le processus, vous serez invité à entrer un mot de passe. Appuyez simplement sur **Entrée** lorsque vous y êtes invité pour créer la clé.

Par défaut, la clé **publique** est sauvegardée dans le fichier ~/.ssh/id_rsa.pub, alors que la clé **privée** est dans ~/.ssh/id_rsa. Copiez maintenant le fichier id_rsa.pub sur l'hôte distant et ajoutez le à ~/.ssh/authorized_keys en entrant :

```
ssh-copy-id identifiant@hôte
```

Pour finir, vérifiez les permissions du fichier authorized_keys. Seul l'utilisateur authetifié doit avoir les droits en lecture et écriture. Si les permissions sont incorrectes, changez-les en tapant :

```
chmod 600 .ssh/authorized_keys
```

Vous devriez maintenant pouvoir établir une connexion SSH vers l'hôte sans avoir à saisir de mot de passe.

6.1.5. Références

Pour plus d'information, consultez la page du **Wiki Ubuntu consacrée à SSH :** https://help.ubuntu.com/community/SSH

Site Web de OpenSSH : http://www.openssh.org/

La page Wiki sur OpenSSH avancé : https://wiki.ubuntu.com/AdvancedOpenSSH

6.2. Puppet

Puppet est une structure multiplate-forme permettant aux administrateurs système d'effectuer des tâches courantes à l'aide de code. Le code peut effectuer une grande variété de tâches, de l'installation de nouveaux logiciels, à la vérification des autorisations de fichiers, ou mettre à jour des comptes utilisateur. **Puppet** n'est pas seulement génial pour l'installation initiale d'un système, mais aussi pendant tout le cycle de vie du système. Dans la plupart des circonstances **Puppet** sera utilisé dans une configuration client/serveur.

Cette section couvrira l'installation et la configuration de **Puppet** dans une configuration client/serveur. Cet exemple simple vous expliquera comment installer **Apache** en utilisant **Puppet**.

6.2.1. Pré-configuration

Avant de configurer **Puppet** vous voudrez peut-être ajouter un dossier **CNAME** DNS pour **puppet.exemple.com**, où **exemple.com** est votre nom de domaine. Par défaut les clients **Puppet** vérifient le DNS de puppet.example.com comme le nom du serveur Puppet, ou **Puppet Master**. Voir *Chapitre 8. Service de nom de domaine (DNS)* pour plus de détails.

Si vous ne souhaitez pas utiliser le DNS, vous pouvez ajouter des entrées dans le fichier /etc/hosts du serveur et du client. Par exemple, dans le fichier /etc/hosts du serveur **Puppet**, ajoutez :

```
127.0.0.1 hôte_local.domaine_local hôte_local puppet
192.168.1.17 client_puppet.exemple.com clientpuppet
```

Sur chaque client **Puppet**, ajoutez une entrée pour le serveur :

```
192.168.1.16 puppetmaster.example.com puppetmaster puppet
```

> Remplacez les exemples d'adresses IP et noms de domaine ci-dessus avec vos adresses actuelles de serveur, de client et noms de domaine.

6.2.2. Installation

Pour installer **Puppet**, saisissez dans un terminal sur le **serveur** :

```
sudo apt install puppetmaster
```

Sur la ou les machines **client**, saisissez :

```
sudo apt install puppet
```

6.2.3. Configuration

Créer un chemin de dossier pour la classe apache2 :

```
sudo mkdir -p /etc/puppet/modules/apache2/manifests
```

Maintenant, configurez quelques ressources pour **apache2**. Créez un fichier /etc/puppet/modules/apache2/manifests/init.pp contenant ce qui suit :

```
class apache2 {
  package { 'apache2':
    ensure => installed,
  }

  service { 'apache2':
    ensure => true,
    enable => true,
    require => Package['apache2'],
  }
}
```

Ensuite, créez un fichier nœud /etc/puppet/manifests/site.pp avec :

```
node 'puppetclient.example.com' {
   include apache2
}
```

R emplacez **puppetclient.example.com** par votre nom d'hôte actuel de client **Puppet**.

La dernière étape pour ce serveur **Puppet** est de redémarrer le démon :

```
sudo systemctl restart puppetmaster.service
```

Maintenant que tout est configuré sur le serveur **Puppet**, il est temps de configurer le client.

Tout d'abord, configurer le **Puppet** démon de l'agent pour commencer. Éditez /etc/default/puppet et changez **START** à yes :

```
START=yes
```

Puis démarrez le service :

```
sudo systemctl start puppet.service
```

Regardez l'empreinte numérique de certification du client :

```
sudo puppet agent --fingerprint
```

De retour sur le serveur **Puppet**, regardez les demandes de signature de certificats en attente :

```
sudo puppet cert list
```

Sur le serveur **Puppet**, vérifiez les empreintes numériques du client et signez la certification du client puppet :

```
sudo puppet cert sign puppetclient.example.com
```

Sur le client **Puppet**, lancez l'agent puppet manuellement au premier plan. Cette étape n'est pas à

proprement parler nécessaire, mais c'est la meilleure façon de tester et de déboguer le service puppet :

```
sudo puppet agent --test
```

Vérifiez /var/log/syslog sur les deux hôtes pour toute erreur de configuration. Si tout va bien, le paquet **apache2** et ses dépendances seront installés sur le client **Puppet**.

Cet exemple est **très** simple et ne met pas beaucoup de fonctionnalités et d'avantages de **Puppet** en évidence . Pour plus d'informations, voir puppet-resources.

6.2.4. Ressources

Voir le site de la **Documentation officielle Puppet :** http://docs.puppetlabs.com/

Voir le dépôt de modules puppet en ligne, **Puppet forge :** http://forge.puppetlabs.com/

Voyez également **Pro Puppet :** http://www.apress.com/9781430230571

6.3. Zentyal

Zentyal est un petit serveur Linux qui peut être configuré comme une passerelle, gestionnaire d'infrastructure, gestionnaire de menace unifiée, serveur de bureau, serveur de communication unifiée ou une combinaison de celles-ci. Tous les services de réseaux gérés par **Zentyal** sont strictement intégrés, en automatisant la plupart des tâches. Cela économise du temps et aide à éviter des erreurs dans la configuration et l'administration du réseau. **Zentyal** est open source, disponible sous la licence générale et publique GNU (« GPL ») et fonctionne au-dessus d'Ubuntu GNU/Linux.

Zentyal est un ensemble de paquets (généralement un pour chaque module) qui fournit une interface web pour configurer les différents serveurs ou services. La configuration est enregistrée dans une base de données **Redis** de valeurs-clefs mais la configuration relative aux utilisateurs, groupes et domaines est sur **OpenLDAP** . Lorsque vous configurez l'un des paramètres disponibles au moyen de l'interface web, les fichiers de configuration finaux sont écrasés et remplacés par les modèles fournis par les modules. L'avantage principal de **Zentyal** est son interface utilisateur graphique unifiée qui permet de configurer tous les services réseau et son niveau d'intégration, élevé et innovant.

Zentyal publie une version majeure stable par an, fondée sur la version LTS d'Ubuntu la plus récente.

6.3.1. Installation

Pour créer un nouvel utilisateur pour accéder à l'interface web de **Zentyal**, exécutez :

```
sudo adduser username sudo
```

Ajoutez le dépôt de **Zentyal** à votre liste de dépôts :

(commande sur 2 lignes)

```
sudo add-apt-repository "deb http://archive.zentyal.org/zentyal 3.5 main
extra"
```

Importez la clefs publiques de **Zentyal** :

```
sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 10E239FF
```

(commande sur 2 lignes)

```
wget -q http://keys.zentyal.org/zentyal-4.2-archive.asc -O- | sudo apt-key
add -
```

Mettez à jour vos paquets et installez **Zentyal** :

```
sudo apt update
```

```
sudo apt install zentyal
```

Pendant l'installation, il vous sera demandé de choisir un mot de passe racine pour MySQL et de confirmer le port 443.

6.3.2. Premiers pas

Tout compte système appartenant au groupe sudo est autorisé à se connecter à l'interface web de Zentyal. Par défaut, l'utilisateur créé lors de l'installation d'Ubuntu server appartient au groupe sudo.

Pour accéder à l'interface web de **Zentyal**, dans un navigateur, allez à https://localhost/ ou à l'adresse IP de votre serveur distant. Comme **Zentyal** crée son propre certificat SSL auto-signé, vous devrez accepter une exception de sécurité dans votre navigateur. Connectez-vous avec le même nom d'utilisateur et mot de passe que vous utilisez pour vous connecter au serveur.

Une fois connecté, vous verrez un aperçu de votre serveur. Les modules individuels, comme Antivirus et Pare-feu, peuvent-être installés simplement, en cliquant dessus puis sur Installer. On peut choisir des rôles de serveur comme **Gateway** ou **Infrastructure** pour installer plusieurs modules en même temps.

Les modules peuvent également être installés via la ligne de commande :

```
sudo apt install <zentyal-module>
```

Voir la liste des modules disponibles ci-dessous.

Pour activer un module, allez dans le Tableau de bord, puis cliquez sur État des modules. Cochez la case du module, puis cliquez sur Enregistrer les modifications.

Pour configure l'un des fonctionnalités des modules installés, cliquez sur les différentes sections du menu de gauche. Quand vous faites des modifications, un bouton rouge « Enregistrer les modifications » apparaît dans le coin supérieur droit.

Si vous avez besoin de personnaliser un fichier de configuration ou d'exécuter certaines actions (scripts ou commandes) pour configurer des fonctionnalités non disponibles sur **Zentyal**, placez les modèles de fichier de configuration de personnalisation (fichiers d'incorporation ou stubs) dans /etc/zentyal/stubs/<module>/ et les attaches dans /etc/zentyal/hooks/<module>.<action> . Pour en savoir plus sur les fichiers d'incorporation et les attaches, consultez cet article : https://wiki.zentyal.org/wiki/En/4.0/Appendix_B:_Development_and_advanced_configuration#Advanced_Service_Customization .

6.3.3. Modules

Zentyal 2.3 est disponible dans les dépôts Universe d'Ubuntu 13.04. Les modules disponibles sont :

- zentyal-core & zentyal-common: le cœur de l'interface **Zentyal** et les bibliothèques courantes de la structure. Y est inclus également les modules journaux de connexion et événements qui donnent, à l'administrateur, une interface pour voir les journaux de connexion et les événements générés.
- zentyal-network : gère la configuration du réseau. Depuis les interfaces (gérant IP statiques, DHCP, VLAN, pont ou PPPoE), aux passerelles multiples avec plus d'une connexion Internet, répartition du trafic et routage avancé, routes statiques ou DNS dynamiques.
- zentyal-objects & zentyal-services : permet un niveau d'abstraction pour les adresses réseau (p. ex. LAN à la place de 192.168.1.0/24) ainsi que l'identification des ports en tant que services (p. ex. HTTP à la place de 80/TCP).
- zentyal-firewall : configure les règles de **iptables** afin de bloquer les connexions interdites, les NAT et aussi les redirections de ports.
- zentyal-ntp : installe le démon NTP afin de maintenir le serveur à l'heure et d'autoriser les clients sur le réseau à synchroniser leurs horloges sur celle du serveur.

- zentyal-dhcp : configure le serveur **ISC DHCP** gérant les plages réseau, les baux statiques et autres options avancées telles que NTP, WINS, DNS dynamiques, mises à jour et initialisation réseau avec PXE.
- zentyal-dns : apporte le serveur DNS **ISC Bind9** dans votre serveur pour la mise en cache des requêtes locales en tant que transitaire ou serveur faisant autorité pour les domaines configurés. Permet de configurer les enregistrements des types A, CNAME, MX, NS, TXT et SRV.
- zentyal-ca : intègre la gestion d'une autorité de certification à Zentyal afin que les utilisateurs puissent utiliser des certificats pour s'authentifier aux services, comme avec **OpenVPN**.
- Zentyal-openvpn : permet de configurer plusieurs serveurs et clients VPN utilisant **OpenVPN** avec une configuration de routage dynamique à l'aide de **Quagga**.
- zentyal-users : fournit une interface pour configurer et gérer les utilisateurs et les groupes dans **OpenLDAP**. Les autres services dans Zentyal sont authentifiés vis à vis de LDAP qui a une gestion centralisée des utilisateurs et des groupes. Il est également possible de synchroniser les utilisateurs, les mots de passe et les groupes à partir d'un domaine **Microsoft Active Directory**.
- zentyal-squid : configure **Squid** et **Dansguardian** pour accélérer la navigation grâce aux capacités de mise en cache et de filtrage de contenu.
- zentyal-samba : permet la configuration de **Samba** et l'intégration avec un LDAP existant. Depuis cette même interface, vous pouvez définir les politiques de mot de passe, créer des ressources partagées et attribuer des autorisations.
- zentyal-printers : intègre **CUPS** avec **Samba** et permet non seulement de configurer les imprimantes mais aussi de leur donner des autorisations basées sur les utilisateurs et les groupes LDAP.

Non présent sur les dépôts Universe d'Ubuntu, mais sur https://launchpad.net/~zentyal/ **le PPA de l'équipe Zentyal** vous trouverez ces autres modules :

- zentyal-antivirus : intègre l'antivirus **ClamAV** avec les autres modules tels que le proxy, le partage de fichiers ou le filtre des méls.
- zentyal-asterisk : configure **Asterisk** pour fournir un PBX (autocommutateur privé) simple avec une authentification basée sur LDAP.
- zentyal-bwmonitor : permet de surveiller l'utilisation de la bande passante par les clients de votre réseau local.
- zentyal-captiveportal : intègre un portail captif avec le pare-feu, les utilisateurs et les groupes LDAP.
- zentyal-ebackup : permet de faire des sauvegardes programmées de votre serveur à l'aide de l'outil de sauvegarde **duplicity**.
- zentyal-ftp : configure un serveur FTP avec authentification basée sur LDAP.
- zentyal-ids : intègre un système de détection d'intrusions réseau.
- zentyal-ipsec : permet de configurer des tunnels IPsec en utilisant **OpenSwan**.
- zentyal-jabber : intègre le serveur XMPP **ejabberd** avec les utilisateurs et groupes LDAP.
- zentyal-thinclients : une solution en clients légers basée sur **LTSP**.
- Zentyal-mail: une pile de courrier complet, y compris **Postfix** et **Dovecot** avec le backend LDAP.
- Zentyal-mailfilter: configure **amavisd** avec pile de courrier pour filtrer le spam et les virus ci-joint.
- zentyal-monitor : intègre **collectd** pour surveiller les performances du serveur et les services en cours d'exécution.
- zentyal-pptp : configure un serveur VPN **PPTP**.

- zentyal-radius : intègre **FreeRADIUS** avec les utilisateurs et groupes LDAP.
- zentyal-software : interface simple pour gérer les modules installés de **Zentyal** et les mises à jour du système.
- zentyal-trafficshaping : configure les règles de limitation de trafic pour faire de la restriction de bande passante et améliorer le temps de réponse.
- zentyal-usercorner : permet aux utilisateurs d'éditer leurs propres attributs LDAP à l'aide d'un navigateur web.
- zentyal-virt : interface simple pour créer et gérer des machines virtuelles basées sur **libvirt**.
- zentyal-webmail : permet d'accéder à votre messagerie en utilisant la messagerie en ligne populaire **Roundcube**.
- zentyal-webserver : configure le serveur **Apache** pour héberger différents sites sur votre machine.
- Zentyal-zarafa: intègre **Zarafa** Suite de travail collaboratif avec **Zentyal** mail pile et LDAP.

6.3.4. Références

Page de **documentation officielle Zentyal :** http://doc.zentyal.org/

Wiki de la communauté Zentyal : http://trac.zentyal.org/wiki/Documentation

Consultez le **forum de Zentyal** http://forum.zentyal.org/ pour obtenir de l'aide de la communauté, faire une retour sur votre expérience, demander des fonctionnalités, etc.

Chapitre 7. Authentification réseau

Cette section s’applique à LDAP pour l’authentification et l’autorisation réseau.

7.1. Serveur OpenLDAP

Le protocole d'accès au répertoire « poids léger » ou LDAP (Lightweight Directory Access Protocol) est un protocole pour l'interrogation et la modification d'un service de répertoire basé sur X.500 fonctionnant sous TCP/IP. LA verson actuelle de LDAP est LDAPv3, comme défini dans la règle **RFC4510** : http://tools.ietf.org/html/ , rfc4510 et l'implémentation dans Ubuntu est OpenLDAP.

Ainsi, le protocole LDAP accède aux répertoires LDAP. Voici quelques concepts et termes clé :

- Un répertoire LDAP est une arborescence d'**entrées** de données de nature hiérarchique qui est appelée Arborescence d'Information du Répertoire (Directory Information Tree : DIT).
- Une entrée se compose d'un ensemble d'**attributs**.
- Un attribut possède un **type** (un nom/description) et une ou plusieurs **valeurs**.
- Chaque attribut doit être défini dans au moins une **classe d'objet**.
- Les attributs et classes d'objets sont définis dans les **schémas** (une classe d'objet est en fait considérée comme un type particulier d'attribut).
- Chaque entrée possède un unique : son **Nom Distinctif** (Distinguished Name : DN ou dn). Celui-ci, à son tour, se compose d'un **Nom Distinctif Relatif** (Relative Distinguished Name : RDN), suivi par le DN de l'entrée parent.
- Le DN de l'entrée n'est pas un attribut. Il n'est pas considéré comme faisant partie de l'entrée elle-même.

> Les termes **objet**, **conteneur** et **nœud** ont une certaine connotations mais ils ont tous essentiellement la même signification que **entrée**, le terme techniquement correct.

Par exemple, ci-dessous, nous avons une seule entrée composée de 11 attributs où ce qui suit est exact :

- Le DN (Nom Distinctif) est " cn=John Doe, dc=exemple, dc=com "
- Le RDN (Nom Distinctif Relatif) est " cn=John Doe "
- Le DN parent est " dc=exemple, dc=com "

```
dn : cn=John Doe,dc=example,dc=com
cn : John Doe
givenName : John
sn : Doe
telephoneNumber : +1 888 555 6789
telephoneNumber : +1 888 555 1232
mail : john@example.com
manager : cn=Larry Smith,dc=example,dc=com
objectClass : inetOrgPerson
objectClass : organizationalPerson
objectClass : person
objectClass : top
```

L'entrée ci-dessus est au format **LDIF** (format d'échange de données : LDAP Data Interchange Format). Toute information que vous fournirez dans votre DIT (Arborescence d'Information du Répertoire) doit également être dans un tel format. Il est défini dans la norme **RFC2849** : http://tools.ietf.org/html/rfc2849 .

Bien que ce guide vous expliquera comment l'utiliser pour l'authentification central, LDAP est compétent pour tout ce qui implique un grand nombre de demandes d'accès en tâche de fond, la plupart du temps lu, basé sur les attributs (nom : valeur). Les exemples incluent un carnet d'adresses, une liste d'adresses e-mail, et la configuration d'un serveur de messagerie.

7.1.1. Installation

Installez le démon du serveur OpenLDAP et les utilitaires de gestion traditionnels de LDAP. On les trouve respectivement dans les paquets **slapd** et **ldap-utils**.

L'installation de slapd créera une configuration de travail. En particulier, il permettra de créer un exemple de base de données que vous pouvez utiliser pour stocker vos données. Cependant, le suffixe (ou DN de base) de cet exemple sera déterminé à partir du nom de domaine de l'hôte local. Si vous voulez quelque chose de différent, modifiez /etc/hosts et remplacez le nom de domaine avec celui qui vous donnera le suffixe que vous désirez. Par exemple, si vous voulez un suffixe **dc=exemple,dc=com**, votre fichier aura ensuite une ligne similaire à ceci :

```
127.0.1.1 hostname.example.com hostname
```

Vous pouvez annuler la modification après l'installation du paquet.

> C e guide utilisera un suffixe de base de données tel que **dc=exemple,dc=com**.

Procédez à l'installation :

```
sudo apt install slapd ldap-utils
```

Depuis Ubuntu 8.10 slapd est conçu pour être configuré dans slapd lui-même en lui dédiant un DIT distinct à cette fin. Cela permet de configurer dynamiquement slapd sans avoir besoin de redémarrer le service. Cette base de données de configuration se compose d'une collection de fichiers LDIF à base de texte située sous /etc/ldap/slapd.d. Cette façon de travailler est connu sous plusieurs noms : la méthode slapd-config, la méthode RTC (Real Time Configuration), ou la méthode cn=config. Vous pouvez toujours utiliser le traditionnel plat fichier de méthode (slapd.conf), mais ce n'est pas recommandé, la fonctionnalité sera finalement supprimée.

> U buntu utilise maintenant la méthode **slapd-config** pour la configuration de slapd et ce guide reflète cela.

Pendant l'installation vous avez été invité à définir les informations d'identification administratives. Ceux-ci sont basés sur LDAP d'identification pour le **rootdn** de votre instance de base de données. Par défaut, DN cet utilisateur est **cn=admin, dc=example, dc=com**. Également par défaut, il n'y a pas de compte administrateur créé pour la base de données slapd-config et vous aurez donc besoin de s'authentifier à l'extérieur de LDAP afin d'y accéder. Nous verrons comment faire cela plus tard.

De nos jours, certains schémas classiques (cosine, nis, inetorgperson) sont intégrés avec slapd. Il y a aussi un schéma « de base », un pré-requis pour que les schémas puissent fonctionner.

7.1.2. Inspection post-installation

Le processus d'installation met en place 2 DIT. Un pour slapd-config et un pour vos propres données (dc=exemple, dc=com). Jetons-y un coup d'œil.

- C'est ce à quoi la base de données slapd-config/DIT ressemble. Rappelons que cette base de données est basée sur LDIF et réside dans /etc/ldap/slapd.d :

```
/etc/ldap/slapd.d/
/etc/ldap/slapd.d/cn=config
/etc/ldap/slapd.d/cn=config/cn=module{0}.ldif
/etc/ldap/slapd.d/cn=config/cn=schema
/etc/ldap/slapd.d/cn=config/cn=schema/cn={0}core.ldif
/etc/ldap/slapd.d/cn=config/cn=schema/cn={1}cosine.ldif
/etc/ldap/slapd.d/cn=config/cn=schema/cn={2}nis.ldif
/etc/ldap/slapd.d/cn=config/cn=schema/cn={3}inetorgperson.ldif
/etc/ldap/slapd.d/cn=config/cn=schema.ldif
/etc/ldap/slapd.d/cn=config/olcBackend={0}hdb.ldif
/etc/ldap/slapd.d/cn=config/olcDatabase={0}config.ldif
/etc/ldap/slapd.d/cn=config/olcDatabase={-1}frontend.ldif
/etc/ldap/slapd.d/cn=config/olcDatabase={1}hdb.ldif
/etc/ldap/slapd.d/cn=config.ldif
```

Ne pas modifier la base de données slapd-config directement. Effectuez des modifications via le protocole LDAP (utilitaires).

- Voici ce à quoi le DIT slapd-config ressemble avec le protocole LDAP :

Sur Ubuntu serveur 14.10, et peut-être plus, la commande suivante peut ne pas fonctionner en raison d'un **bogue** : https ://bugs.launchpad.net/ubuntu/+source/apparmor/+bug/1392018

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi :/// -b cn=config dn
```

```
dn : cn=config

dn : cn=module{0},cn=config

dn : cn=schema,cn=config

dn : cn={0}core,cn=schema,cn=config

dn : cn={1}cosine,cn=schema,cn=config

dn : cn={2}nis,cn=schema,cn=config

dn : cn={3}inetorgperson,cn=schema,cn=config

dn : olcBackend={0}hdb,cn=config

dn : olcDatabase={-1}frontend,cn=config

dn : olcDatabase={0}config,cn=config

dn : olcDatabase={1}hdb,cn=config
```

Explication des entrées :

- **cn=config** : paramètres globaux
- **cn=module{0},cn=config** : un module chargé dynamiquement
- **cn=Schema, cn=configuration** : contient codées en dur au niveau du système de schéma
- **cn={0} de base, cn=Schema, cn=configuration** : le schéma de base codées en dur
- **cn={1}cosine,cn=schema,cn=config** : le schéma cosine
- **cn={2}nis,cn=schema,cn=config** : le schéma nis

- **cn={3}inetorgperson,cn=schema,cn=config** : le schéma inetorgperson
- **olcBackend={0}hdb,cn=config** : le type de stockage de backend « hdb »
- **olcDatabase={-1}frontend,cn=config** : base de données du frontend, paramètres par défaut pour les autres bases de données
- **olcDatabase={0}config,cn=config** : base de données de configuration slapd (cn=config)
- **olcDatabase={1}hdb,cn=config** : votre exemple de base de données (dc=exemle,dc=com)

- C'est ce à quoi le DIT de dc=exemple,dc=com ressemble :

```
ldapsearch -x -LLL -H ldap :/// -b dc=example,dc=com dn

dn : dc=example,dc=com

dn : cn=admin,dc=example,dc=com
```

Explication des entrées :

dc=example,dc=com : base du DIT
cn=admin,dc=exemple,dc=com : administrateur (rootDN) pour ce DIT (mis en place lors de l'installation du paquet)

7.1.3. Modification/Remplissage de votre base de données

Introduisons un peu de contenu dans notre base de données. Nous allons ajouter ce qui suit :

- un nœud appelé **Gens** (pour stocker les utilisateurs)
- un nœud appelé **Groupes** (pour stocker les groupes)
- un groupe appelé **miners**
- un utilisateur appelé **john**

Créez le fichier LDIF suivant et appelez le add_content.ldif :

```
dn : ou=Gens,dc=exemple,dc=com
objectClass : organizationalUnit
ou : Gens

dn : ou=Groupes,dc=exemple,dc=com
objectClass : organizationalUnit
ou : Groupes

dn : cn=mineurs,ou=Groupes,dc=exemple,dc=com
objectClass : posixGroup
cn : mineurs
gidNumber : 5000

dn : uid=john,ou=Gens,dc=exemple,dc=com
objectClass : inetOrgPerson
objectClass : posixAccount
objectClass : shadowAccount
```

```
uid : john
sn : Doe
givenName : John
cn : John Doe
displayName : John Doe
uidNumber : 10000
gidNumber : 5000
userPassword : johnldap
gecos : John Doe
loginShell : /bin/bash
homeDirectory : /home/john
```

> Il est important que les valeurs uid et gid dans votre répertoire n'entrent pas en collision avec les valeurs locales. Utilisez plages de numéros élevés, comme à partir de 5000. En réglant le uid gid et les valeurs de haute ldap, vous permettent également de faciliter le contrôle de ce qui peut être fait avec un utilisateur local vs un ldap. Plus sur cela plus tard.

Ajouter le contenu :

```
ldapadd -x -D cn=admin,dc=example,dc=com -W -f add_content.ldif
```

```
Entrez le mot de passe LDAP : ********

ajout de nouvelle entrée « ou=Gens,dc=exemple,dc=com »

ajout de nouvelle entrée « ou=Groupes,dc=exemple,dc=com »

ajout de nouvelle entrée « cn=mineurs,ou=Groupes,dc=exemple,dc=com »

ajout de nouvelle entrée « uid=john,ou=Gens,dc=exemple,dc=com »
```

Nous pouvons vérifier que l'information a été correctement ajoutée avec l'utilitaire **ldapsearch** :

```
ldapsearch -x -LLL -b dc=example,dc=com 'uid=john' cn gidNumber
```

```
dn : uid=john,ou=People,dc=example,dc=com
cn : John Doe
GidNumber : 5000
```

Explication des changements :

- La liaison« simple » **-x :** ; n'utilisera pas la méthode SASL par défaut
- **-LLL :** désactive les informations externes d'impression
- **uid=john :** un « filtre » pour trouver l'utilisateur john
- **cn gidNumber :** demande l'affichage de certains attributs (la valeur par défaut fait s'afficher tous les attributs)

7.1.4. Modification de la base de données de configuration slapd

Le DIT de slapd-config peut également être interrogé et modifié. Voici quelques exemples.

- Utilisez **ldapmodify** pour ajouter un « Index » (attribut DbIndex) à votre base de données **{1}hdb,cn=config** (dc=exemple,dc=com). Créez un fichier que vous appellerez uid_index.ldif contenant ce qui suit :

```
dn : olcDatabase={1}hdb,cn=config
add : olcDbIndex
olcDbIndex : uid eq,pres,sub
```

Puis, exécutez la commande suivante :

```
sudo ldapmodify -Q -Y EXTERNAL -H ldapi :/// -f uid_index.ldif
```

```
modification de l'entrée « olcDatabase={1}hdb,cn=config »
```

Vous pouvez confirmer le changement de cette manière :

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi :/// -b \
cn=config '(olcDatabase={1}hdb)' olcDbIndex
```

```
dn : olcDatabase={1}hdb,cn=config
olcDbIndex : objectClass eq
olcDbIndex : uid eq,pres,sub
```

- Ajoutons un schéma. Il devra d'abord être converti au format LDIF. Vous pouvez trouver des schémas non convertis, en plus de ceux convertis dans le dossier directory /etc/ldap/schema.

> Il n'est pas courant de supprimer un schéma de la base de données slapd-config. Entrainez vous à l'ajout de schémas sur un système de test.

Avant d'ajouter n'importe quel schéma, vous devez vérifier que les schémas sont déjà installés (représenté est un défaut, out-of-the-box de sortie) :

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi :/// -b \
cn=schema,cn=config dn
```

```
dn : cn=schema,cn=config

dn : cn={0}core,cn=schema,cn=config

dn : cn={1}cosine,cn=schema,cn=config

dn : cn={2}nis,cn=schema,cn=config

dn : cn={3}inetorgperson,cn=schema,cn=config
```

Dans l'exemple suivant, nous ajouterons le schéma CORBA.

1. Créez le fichier de configuration de conversion schema_convert.conf contenant les lignes suivantes :

```
include /etc/ldap/schema/core.schema
```

```
include /etc/ldap/schema/collective.schema
include /etc/ldap/schema/corba.schema
include /etc/ldap/schema/cosine.schema
include /etc/ldap/schema/duaconf.schema
include /etc/ldap/schema/dyngroup.schema
include /etc/ldap/schema/inetorgperson.schema
include /etc/ldap/schema/java.schema
include /etc/ldap/schema/misc.schema
include /etc/ldap/schema/nis.schema
include /etc/ldap/schema/openldap.schema
include /etc/ldap/schema/ppolicy.schema
include /etc/ldap/schema/ldapns.schema
include /etc/ldap/schema/pmi.schema
```

2. Créez le répertoire de sortie ldif_output.
3. Déterminez l'index du schéma :

```
slapcat -f schema_convert.conf -F ldif_output -n 0 | grep corba,cn=schema
```

```
cn={1}corba,cn=schema,cn=config
```

Lorsque slapd ingère des objets avec le même DN parent, il va créer un **index** pour cet objet. Un index est contenu entre des parentheses : **{X}**.

4. Utilisez **slapcat** pour effectuer la conversion :

```
slapcat -f schema_convert.conf -F ldif_output -n0 -H \
ldap :///cn={1}corba,cn=schema,cn=config -l cn=corba.ldif
```

Le schéma converti est maintenant dans cn=corba.ldif

5. Modifiez cn=corba.ldif pour atteindre les attributs suivants :

```
dn : cn=corba,cn=schema,cn=config
...
cn : corba
```

Supprimez également les lignes suivantes à partir du bas :

```
structuralObjectClass : olcSchemaConfig
entryUUID : 52109a02-66ab-1030-8be2-bbf166230478
creatorsName : cn=config
createTimestamp : 20110829165435Z
entryCSN : 20110829165435.935248Z#000000#000#000000
modifiersName : cn=config
modifyTimestamp : 20110829165435Z
```

Vos valeurs d'attributs varieront.

6. Enfin, utilisez **ldapadd** pour ajouter le nouveau schéma au DIT slapd-config :

```
sudo ldapadd -Q -Y EXTERNAL -H ldapi :/// -f cn\=corba.ldif
```

```
ajout de nouvelle entrée « cn=corba,cn=schema,cn=config »
```

7. Confirmez les schémas actuellement chargés :

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi :/// -b cn=schema,cn=config dn
```

```
dn : cn=schema,cn=config

dn : cn={0}core,cn=schema,cn=config

dn : cn={1}cosine,cn=schema,cn=config

dn : cn={2}nis,cn=schema,cn=config

dn : cn={3}inetorgperson,cn=schema,cn=config

dn : cn={4}corba,cn=schema,cn=config
```

Pour s'authentifier avec LDAP, chaque application ou client externe doit être configuré spécialement à cet effet. Consultez la documentation-client appropriée pour plus de détails.

7.1.5. Journalisation

La journalisation des activités pour slapd est indispensable lors de la mise en œuvre d'une solution basée sur OpenLDAP mais elle doit être activée manuellement après l'installation du logiciel. Dans le cas contraire, seuls les messages rudimentaires apparaissent dans les journaux. La journalisation, comme toute autre configuration de slapd, est activée via la base de données slapd-config.

OpenLDAP est livré avec plusieurs sous-systèmes (niveaux) de journalisation, chaque niveau contenant le niveau inférieur (systèmes additifs). Il est conseillé d'essayer le niveau **stats**. Le manuel de **slapd-config** contient des informations plus détaillées sur les différents sous-systèmes : http ://manpages.ubuntu.com/manpages/en/man5/slapd-config.5.html.

Créez le fichier logging.ldif avec le contenu suivant :

```
dn : cn=config
changetype : modify
replace : olcLogLevel
olcLogLevel : stats
```

Appliquez le changement :

```
sudo ldapmodify -Q -Y EXTERNAL -H ldapi :/// -f logging.ldif
```

Ceci crée de nombreuses entrées dans le journal. Il est préférable de revenir à un niveau de détail moindre une fois que votre système est en production. Dans ce mode détaillé, le moteur syslog de votre hôte (rsyslog) peut avoir du mal à suivre et peut envoyer des messages :

```
rsyslogd-2177 : imuxsock a perdu 228 messages du pid 2547 à cause de la limitation de débit
```

Vous pouvez envisager un changement dans la configuration de rsyslog. Dans /etc/rsyslog.conf, entrez :

```
# Désactivez la limitation de débit
# (la limitation par défaut est de 200 messages en 5 secondes ; ci-dessous nous faisons que le 5 devienne 0)
$SystemLogRateLimitInterval 0
```

Et puis redémarrez le démon rsyslog :

```
sudo systemctl restart syslog.service
```

7.1.6. Réplication

Le service LDAP gagne en importance car le nombre de systèmes en réseau qui en dépendent va croissant. Dans un tel environnement, il est de pratique courante de créer de la redondance (haute disponibilité) dans LDAP pour éviter des dégâts en cas d'indisponibilité du serveur LDAP. Cela se fait par **réplication LDAP**.

La réplication est assurée par le moteur **syncrepl**. Celui-ci permet de synchroniser les modifications à l'aide d'un modèle **consommateur** - **fournisseur**. Le type spécifique de la réplication mise en œuvre dans ce guide est une combinaison des modes suivants : **refreshAndPersist** et **delta-syncrepl**. Cela fait que le fournisseur pousse les entrées modifiées vers le consommateur dès qu'ils sont faits et, en outre, que seuls les modifications réelles sont envoyées, et non pas les entrées entières.

7.1.6.1. Configuration du fournisseur

Commencez par configurer le **Provider (Fournisseur)**.

1. Créez un fichier LDIF avec le contenu suivant et nommez-le provider_sync.ldif :

```
# Add indexes to the frontend db.
dn : olcDatabase={1}hdb,cn=config
changetype : modify
add : olcDbIndex
olcDbIndex : entryCSN eq
-
add : olcDbIndex
olcDbIndex : entryUUID eq

#Load the syncprov and accesslog modules.
dn : cn=module{0},cn=config
changetype : modify
add : olcModuleLoad
olcModuleLoad : syncprov
-
add : olcModuleLoad
olcModuleLoad : accesslog

# Accesslog database definitions
```

```
dn : olcDatabase={2}hdb,cn=config
objectClass : olcDatabaseConfig
objectClass : olcHdbConfig
olcDatabase : {2}hdb
olcDbDirectory : /var/lib/ldap/accesslog
olcSuffix : cn=accesslog
olcRootDN : cn=admin,dc=example,dc=com
olcDbIndex : default eq
olcDbIndex : entryCSN,objectClass,reqEnd,reqResult,reqStart

# Accesslog db syncprov.
dn : olcOverlay=syncprov,olcDatabase={2}hdb,cn=config
changetype : add
objectClass : olcOverlayConfig
objectClass : olcSyncProvConfig
olcOverlay : syncprov
olcSpNoPresent : TRUE
olcSpReloadHint : TRUE

# syncrepl Provider for primary db
dn : olcOverlay=syncprov,olcDatabase={1}hdb,cn=config
changetype : add
objectClass : olcOverlayConfig
objectClass : olcSyncProvConfig
olcOverlay : syncprov
olcSpNoPresent : TRUE

# accesslog overlay definitions for primary db
dn : olcOverlay=accesslog,olcDatabase={1}hdb,cn=config
objectClass : olcOverlayConfig
objectClass : olcAccessLogConfig
olcOverlay : accesslog
olcAccessLogDB : cn=accesslog
olcAccessLogOps : writes
olcAccessLogSuccess : TRUE
# scan the accesslog DB every day, and purge entries older than 7 days
OlcAccessLogPurge : 07+00 :00 01+00 :00
```

Changer le rootDN dans le fichier LDIF pour qu'il corresponde à celui que vous avez pour votre répertoire.

2. Le profil **apparmor** pour slapd n'a pas besoin d'être ajusté en ce qui concerne l'emplacement de base de données accesslog parce que /etc/apparmor.d/local/usr.sbin.slapd contient :

```
/var/lib/ldap/ r,
/var/lib/ldap/** rwk,
```

Créez un répertoire, mettez en place un fichier de configuration de base de données, et rechargez le profil apparmor :

```
sudo -u openldap mkdir /var/lib/ldap/accesslog
sudo -u openldap cp /var/lib/ldap/DB_CONFIG /var/lib/ldap/accesslog
sudo systemctl reload apparmor.service
```

3. Ajoutez le nouveau contenu et, en raison du changement dans apparmor, redémarrez le démon :

```
sudo ldapadd -Q -Y EXTERNAL -H ldapi :/// -f provider_sync.ldif
sudo systemctl restart slapd.service
```

Le fournisseur est maintenant configuré.

7.1.6.2. Configuration de l'utilisateur

Et maintenant configurez le **Consumer (Consommateur)**.

1. Installez le logiciel en passant par openldap-server-installation. Assurez-vous que la base de données slapd-config est identique à celle du fournisseur. En particulier, assurez-vous que les schémas et le suffixe de base de données sont les mêmes.
2. Créez un fichier LDIF avec le contenu suivant et nommez-le consumer_sync.ldif :

```
dn : cn=module{0},cn=config
changetype : modify
add : olcModuleLoad
olcModuleLoad : syncprov

dn : olcDatabase={1}hdb,cn=config
changetype : modify
add : olcDbIndex
olcDbIndex : entryUUID eq
-
add : olcSyncRepl
olcSyncRepl : rid=0 provider=ldap ://ldap01.exemple.com bindmethod=simple
binddn="cn=admin,dc=exemple,dc=com"
credentials=secret searchbase="dc=exemple,dc=com" logbase="cn=accesslog"
logfilter="(&amp;(objectClass=auditWriteObject)(reqResult=0))" schemachecking=on
type=refreshAndPersist retry="60 +" syncdata=accesslog
-
add : olcUpdateRef
olcUpdateRef : ldap ://ldap01.exemple.com
```

   Vérifiez que les attributs suivants ont les bonnes valeurs :

   - **fournisseur** (nom d'hôte du serveur fournisseur -- ldap01.exemple.com dans cet exemple -- ou l'adresse IP)
   - **binddn** (le DN administrateur que vous utilisez)
   - **credentials** (le mot de passe administrateur DN que vous utilisez)
   - **searchbase** (le suffixe de base de données que vous utilisez)

- **olcUpdateRef** (nom d'hôte du serveur fournisseur ou adresse IP)
- **rid** (réplique d' unique à 3 chiffres qui définie la réplique. Chaque utilisateur devrait avoir au moins une réplique d')

3. Ajoutez le nouveau contenu :

```
sudo ldapadd -Q -Y EXTERNAL -H ldapi :/// -f consumer_sync.ldif
```

Vous avez terminé. Les deux bases de données (suffixe : dc=exemple,dc=com) devraient maintenant se synchroniser.

7.1.6.3. Réalisation des tests

Une fois que la réplication démarre, vous pouvez la suivre en exécutant :

```
ldapsearch -z1 -LLLQY EXTERNAL -H ldapi :/// -s base -b dc=exemple,dc=com
contextCSN
```

```
dn : dc=example,dc=com
contextCSN : 20120201193408.178454Z#000000#000#000000
```

sur le fournisseur et l'utilisateur. Une fois que la sortie (`20120201193408.178454Z#000000#000#000000` dans l'exemple ci-dessus) correspond aux deux machines, vous avez la réplication. Chaque fois qu'une modification est effectuée pour le fournisseur, cette valeur changera, ainsi que celle des utilisateurs.

Si votre connexion est lente ou si votre base de données ldap est votre volumineuse, la mise en correspondance du **contextCSN** du consommateur avec celui du fournisseur peut prendre un certain temps. Un accroissement régulier du **contextCSN** du consommateur indique que l'opération est en cours.

Si le **contextCSN** du consommateur est absent ou s'il ne correspond pas à celui du fournisseur, il convient de s'arrêter et d'identifier le problème avant de continuer. Vérifiez les fichiers de journalisation de slapd (syslog) et d'authentification du fournisseur pour voir si les demandes d'authentification du consommateur ont réussi, ou si les requêtes d'accès aux données, qui prennent la forme de nombreuses instructions « ldapsearch », retournent des erreurs.

Pour tester si cela a fonctionné, simplement questionner, sur l'utilisateur, les noms distinctifs (DN) de la base de données :

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi :/// -b dc=example,dc=com dn
```

Vous devriez voir l'utilisateur « john » et le groupe « mineurs » ainsi que les nœuds « Gens » et « Groupes ».

7.1.7. Contrôle d'accès

La gestion du type d'accès (lecture, écriture, etc.) qui doit être attribué aux utilisateurs afin qu'ils puissent accéder aux ressources est connue sous le nom de **contrôle d'accès**. Les directives de configuration associées sont appelées **listes de contrôle d'accès** ou ACL.

Lors de l'installation du paquet slapd, diverses ACL (listes de contrôle d'accès) ont été mises en place automatiquement. Nous allons examiner quelques conséquences importantes de ces défauts et, ce faisant, nous aurons une idée sur la façon dont les ACL fonctionnent et sur la façon dont elles sont configurées.

Pour obtenir la liste ACL effective pour une requête LDAP, il faut regarder les entrées ACL de la base de données interrogée ainsi que celles de l'instance de base de données spéciale de l'interface utilisateur. Les ACL appartenant à cette dernière agissent comme valeurs par défaut dans le cas où celles des premières ne correspondent pas. La base de données de l'interface utilisateur est la deuxième à être consultée et l'ACL à appliquer est la première à correspondre parmi ces deux sources (« la première correspondance l'emporte »). Les commandes suivantes donnent respectivement les ACL de la base de données hdb (« dc=example, dc=com ») et celles de la base de données de l'interface utilisateur :

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi :/// -b \
cn=config '(olcDatabase={1}hdb)' olcAccess
```

```
dn : olcDatabase={1}hdb,cn=config
olcAccess : {0}to attrs=userPassword,shadowLastChange by self write by anonymous
             auth by dn="cn=admin,dc=example,dc=com" write by * none
olcAccess : {1}to dn.base="" by * read
olcAccess : {2}to * by self write by dn="cn=admin,dc=example,dc=com" write by *
  Read
```

Le rootDN a toujours un droit d'accès complet sur sa base de données. L'incorporer dans une ACL constitue une configuration explicite mais cela pénalise aussi la performance de slapd.

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi :/// -b \
cn=config '(olcDatabase={-1}frontend)' olcAccess
```

```
dn : olcDatabase={-1}frontend,cn=config
olcAccess : {0}to * by dn.exact=gidNumber=0+uidNumber=0,cn=peercred,
             cn=external,cn=auth manage by * break
olcAccess : {1}to dn.exact="" by * read
olcAccess : {2}to dn.base="cn=Subschema" by * read
```

La toute première ACL est cruciale :

```
olcAccess : {0}to attrs=userPassword,shadowLastChange by self write by anonymous
              auth by dn="cn=admin,dc=example,dc=com" write by * none
```

Ceci peut être représenté différemment pour une digestion plus facile :

```
to attrs=userPassword
by self write
by anonymous auth
by dn="cn=admin,dc=example,dc=com" write
by * none

to attrs=shadowLastChange
by self write
by anonymous auth
by dn="cn=admin,dc=example,dc=com" write
by * none
```

Cette ACL composée (il y en a deux) implique ce qui suit :

- Un accès anonyme « auth » est fourni à l'attribut **userPassword** pour l'établissement de la connexion initiale. Même si cela peut sembler contre-intuitif, une « authentification par anonyme » est nécessaire, même si l'accès anonyme au DIT n'est pas souhaité. Une fois l'extrémité distante connectée, l'authentification peut se faire (voir le point suivant).
- L'authentification peut avoir lieu parce que tous les utilisateurs ont accès en lecture (en raison de « by self write ») à l'attribut **userPassword**.
- L'attribut **Mot_de_passe_utilisateur** est par ailleurs inaccessible aux autres utilisateurs, à l'exception de rootDN, qui a l'accès complet à celui-ci.
- Pour permettre aux utilisateurs de changer leurs mots de passe en utilisant la commande **passwd** ou d'autres utilitaires, l'attribut **shadowLastChange** doit être accessible une fois qu'un utilisateur s'est authentifié.

Cette DIT peut être sujette à des requêtes anonymes du fait du « by * read » dans cette ACL :

```
to *
by self write
by dn="cn=admin,dc=example,dc=com" write
by * read
```

Si ce n'est pas désiré, il vous faut modifier les ACLs. Pour forcer l'authentification lors d'une demande de liaison, vous pouvez alternativement (ou en combinaison avec l'ACL modifiée) utiliser la directive « olcRequire : authc ».

Comme mentionné précédemment, il n'existe pas de compte administrateur créé pour la base de données slapd-config. Il y a cependant une identité SASL accordée pour un accès complet à celle-ci. Il représente le super-utilisateur de l'hôte local (root/sudo). Le voici :

```
dn.exact=gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
```

La commande suivante affichera les ACL (listes de contrôle d'accès) de la base de données slapd-config :

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi :/// -b \
cn=config '(olcDatabase={0}config)' olcAccess
```

```
dn : olcDatabase={0}config,cn=config
olcAccess : {0}to * by dn.exact=gidNumber=0+uidNumber=0,cn=peercred,
             cn=external,cn=auth manage by * break
```

Comme il s'agit d'une identité SASL, nous devons utiliser un **mécanisme** SASL lors de l'appel de l'utilitaire LDAP en question que nous avons vu beaucoup de fois dans ce guide. C'est le mécanisme EXTERNE. Voir la commande précédente pour avoir un exemple. Notez que :

1. Vous devez utiliser **sudo** pour devenir l'identité root afin de faire la correspondance entre les ACL.
2. Le mécanisme EXTERNE fonctionne via **IPC** (sockets de domaine UNIX). Cela signifie que vous devez utiliser le format URI **ldapi**.

Voici une façon rapide d'obtenir toutes les ACL :

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi :/// -b \
cn=config '(olcAccess=*)' olcAccess olcSuffix
```

Il y a beaucoup à dire sur le sujet du contrôle d'accès. Voir la page de manuel sur les **accès.slapd** : http ://manpages.ubuntu.com/manpages/raring/fr/man5/slapd.access.5.html.

7.1.8. TLS

Pour s'authentifier sur un serveur OpenLDAP, il est préférable d'utiliser une session chiffrée. Cela peut être accompli en utilisant le protocole TLS (Transport Layer Security).

Ici, nous serons notre propre **autorité de certification (CA)**, puis nous allons créer et signer notre certificat de serveur LDAP en tant que CA. Puisque **slapd** est compilé avec la bibliothèque **gnutls**, nous utiliserons l'utilitaire **certtool** pour effectuer ces tâches.

1. Installez les paquets **gnutls-bin** et **ssl-cert** :

   ```
   sudo apt install gnutls-bin ssl-cert
   ```

2. Créer une clé privée pour l'autorité de certification :

   ```
   sudo sh -c "certtool --generate-privkey > /etc/ssl/private/cakey.pem"
   ```

3. Créez le modèle ou le fichier /etc/ssl/ca.info pour définir le CA :

   ```
   cn = Entreprise Exemple
   ca
   cert_signing_key
   ```

4. Créer le certificat d'autorité de certification auto-signé :

   ```
   sudo certtool --generate-self-signed \
   --load-privkey /etc/ssl/private/cakey.pem \
   --template /etc/ssl/ca.info \
   --outfile /etc/ssl/certs/cacert.pem
   ```

5. Créer une clef privée pour le serveur :

   ```
   sudo certtool --generate-privkey \
   --bits 1024 \
   --outfile /etc/ssl/private/ldap01_slapd_key.pem
   ```

   Remplacez **ldap01** dans le nom de fichier par le nom d'hôte de votre serveur. Nommer le certificat, la clé pour l'hôte et le service qui les utilisera aidera à garder les choses claires.

6. Créez le fichier d'informations /etc/ssl/ldap01.info contenant :

   ```
   organization = Compagnie Exemple
   cn = ldap01.example.com
   tls_www_server
   encryption_key
   signing_key
   expiration_days = 3650
   ```

   Le certificat ci-dessus est valable pendant 10 ans. Ajustez en conséquence.

7. Créer le certificat du serveur :

```
sudo certtool --generate-certificate \
--load-privkey /etc/ssl/private/ldap01_slapd_key.pem \
--load-ca-certificate /etc/ssl/certs/cacert.pem \
--load-ca-privkey /etc/ssl/private/cakey.pem \
--template /etc/ssl/ldap01.info \
--outfile /etc/ssl/certs/ldap01_slapd_cert.pem
```

Créez le fichier certinfo.ldif avec le contenu suivant (ajustez en conséquence, notre exemple suppose que nous avons créé les certificats en utilisant https ://www.cacert.org) :

```
dn : cn=config
add : olcTLSCACertificateFile
olcTLSCACertificateFile : /etc/ssl/certs/cacert.pem
-
add : olcTLSCertificateFile
olcTLSCertificateFile : /etc/ssl/certs/ldap01_slapd_cert.pem
-
add : olcTLSCertificateKeyFile
olcTLSCertificateKeyFile : /etc/ssl/private/ldap01_slapd_key.pem
```

Utilisez la commande **ldapmodify** pour informer slapd de notre emploi de TLS via la base de données slapd-config :

```
sudo ldapmodify -Y EXTERNAL -H ldapi :/// -f /etc/ssl/certinfo.ldif
```

Contrairement à la croyance populaire, vous n'avez pas besoin de **ldaps ://** dans /etc/default/slapd pour utiliser le chiffrement. Vous devriez avoir seulement :

```
SLAPD_SERVICES="ldap :/// ldapi :///"
```

> LDAP via TLS/SSL (LDAPS :/ /) est déconseillée en faveur de StartTLS . Ce dernier se réfère à une session existante LDAP (écoute sur le port TCP 389) devient protégé par TLS/SSL alors que LDAPS, comme HTTPS, est une distincte crypté-de-la-début protocole qui fonctionne sur le port TCP 636.

Resserrez la propriété et les autorisations :

```
sudo adduser openldap ssl-cert
sudo chgrp ssl-cert /etc/ssl/private/ldap01_slapd_key.pem
sudo chmod g+r /etc/ssl/private/ldap01_slapd_key.pem
sudo chmod o-r /etc/ssl/private/ldap01_slapd_key.pem
```

Redémarrez OpenLDAP :

```
sudo systemctl restart slapd.service
```

Consultez les fichiers de journalisation de votre hôte (/var/log/syslog) pour voir si le serveur a démarré

correctement.

7.1.9. Réplication et TLS

Si vous avez configuré la réplication entre les serveurs, un pratique commune consiste à chiffrer (StartTLS) le trafic de réplication pour se prémunir d'écoutes. Ceci est distinct de l'utilisation du chiffrement pour l'authentification présentée ci-dessus. La présente section s'appuie sur cette présentation de l'authentification TLS.

Partons de l'hypothèse que vous avez mis en place la réplication entre le fournisseur et le consommateur conformément au *Chapitre 7, paragraphe 1. Serveur OpenLDAP.6. Réplication*, et que vous avez configuré TLS pour l'authentification sur le fournisseur conformément au *Chapitre 7, paragraphe 1. Serveur OpenLDAP.8. TLS*.

Comme indiqué précédemment, pour nous, l'objectif de la réplication est d'avoir une haute disponibilité pour le service LDAP. Puisque nous avons TLS pour l'authentification sur le fournisseur, il est nécessaire de l'avoir également sur le consommateur. En plus de cela, il convient de chiffrer le trafic de réplication. Il reste à créer une clé et un certificat pour le consommateur, puis configurer en conséquence. Nous allons générer la clé et le certificat sur le fournisseur, pour ne pas devoir créer un autre certificat CA, puis transférer les éléments nécessaires au consommateur.

1. Sur le fournisseur,

   Créez un répertoire (qui sera utilisé pour le transfert éventuel), puis la clé privée de l'utilisateur :

   ```
   mkdir ldap02-ssl
   cd ldap02-ssl
   sudo certtool --generate-privkey \
   --bits 1024 \
   --outfile ldap02_slapd_key.pem
   ```

   Créez un fichier d'informations, ldap02.info, pour le serveur consommateur, en ajustant ses valeurs en conséquence :

   ```
   organization = Compagnie Exemple
   cn = ldap02.example.com
   tls_www_server
   encryption_key
   signing_key
   expiration_days = 3650
   ```

   Créer le certificat du consommateur :

```
sudo certtool --generate-certificate \
--load-privkey ldap02_slapd_key.pem \
--load-ca-certificate /etc/ssl/certs/cacert.pem \
--load-ca-privkey /etc/ssl/private/cakey.pem \
--template ldap02.info \
--outfile ldap02_slapd_cert.pem
```

Obtenir une copie du certificat CA :

```
cp /etc/ssl/certs/cacert.pem .
```

Nous avons terminé. Maintenant transférez le répertoire ldap02-ssl à l'utilisateur. Ici, nous utilisons scp (ajustez en conséquence) :

```
cd ..
scp -r ldap02-ssl utilisateur@consumer :
```

2. Sur l'utilisateur,

   Configurer l'authentification TLS :

```
sudo apt install ssl-cert
sudo cp ldap02_slapd_cert.pem cacert.pem /etc/ssl/certs
sudo cp ldap02_slapd_key.pem /etc/ssl/private
sudo chgrp ssl-cert /etc/ssl/private/ldap02_slapd_key.pem
sudo chmod g+r /etc/ssl/private/ldap02_slapd_key.pem
sudo chmod o-r /etc/ssl/private/ldap02_slapd_key.pem
```

   Créez le fichier /etc/ssl/certinfo.ldif avec le contenu suivant (ajustez en conséquence) :

```
dn : cn=config
add : olcTLSCACertificateFile
olcTLSCACertificateFile : /etc/ssl/certs/cacert.pem
-
add : olcTLSCertificateFile
olcTLSCertificateFile : /etc/ssl/certs/ldap02_slapd_cert.pem
-
add : olcTLSCertificateKeyFile
olcTLSCertificateKeyFile : /etc/ssl/private/ldap02_slapd_key.pem
```

   Configurer la base de données slapd-config :

```
sudo ldapmodify -Y EXTERNAL -H ldapi :/// -f certinfo.ldif
```

   Configurez /etc/default/slapd comme sur le fournisseur (SLAPD_SERVICES).

3. Sur l'utilisateur,

   Configurez TLS pour la réplication sur le consommateur. Modifiez l'attribut **olcSyncrepl** existant en utilisant des options de TLS. Ce faisant, nous verrons, pour la première fois, comment changer les valeurs d'un attribut.

   Créez le fichier utilisateur_sync_tls.ldif avec le contenu suivant :

   ```
   dn : olcDatabase={1}hdb,cn=config
   replace : olcSyncRepl
   olcSyncRepl : rid=0 provider=ldap ://ldap01.example.com bindmethod=simple
    binddn="cn=admin,dc=example,dc=com" credentials=secret
   searchbase="dc=example,dc=com"
    logbase="cn=accesslog" logfilter="(&amp;(objectClass=auditWriteObject)
   (reqResult=0))"
    schemachecking=on type=refreshAndPersist retry="60 +" syncdata=accesslog
    starttls=critical tls_reqcert=demand
   ```

   Les options supplémentaires indiquent, respectivement, que le consommateur doit utiliser StartTLS et que le certificat CA est tenu de vérifier l'identité du fournisseur. Notez aussi la syntaxe LDIF pour modifier les valeurs d'un attribut (« replace »).

   Mettre en œuvre ces changements :

   ```
   sudo ldapmodify -Y EXTERNAL -H ldapi :/// -f consumer_sync_tls.ldif
   ```

   Et redémarrez slapd :

   ```
   sudo systemctl restart slapd.service
   ```

4. Sur le fournisseur,

   Assurez-vous qu'une session TLS a été ouverte. Dans /var/log/syslog, à condition que la journalisation ait été configurée au niveau « conns », vous devriez voir des messages semblables à :

   ```
   slapd[3620] : conn=1047 fd=20 ACCEPT from IP=10.153.107.229 :57922 (IP=0.0.0.0 :
   389)
   slapd[3620] : conn=1047 op=0 EXT oid=1.3.6.1.4.1.1466.20037
   slapd[3620] : conn=1047 op=0 STARTTLS
   slapd[3620] : conn=1047 op=0 RESULT oid= err=0 text=
   slapd[3620] : conn=1047 fd=20 TLS established tls_ssf=128 ssf=128
   slapd[3620] : conn=1047 op=1 BIND dn="cn=admin,dc=example,dc=com" method=128
   slapd[3620] : conn=1047 op=1 BIND dn="cn=admin,dc=example,dc=com" mech=SIMPLE
   ssf=0
   slapd[3620] : conn=1047 op=1 RESULT tag=97 err=0 text
   ```

7.1.10. Authentification LDAP

Une fois que vous avez un serveur LDAP fonctionnel, vous devrez installer des bibliothèques sur le client qui saura comment et quand les contacter. Sur Ubuntu, ceci a été traditionnellement fait par l'installation du paquet **libnss-ldap**. Ce paquet apportera d'autres outils qui vous assisteront dans l'étape de configuration. Maintenant, installez ce paquet :

```
sudo apt install libnss-ldap
```

Vous serez invité à entrer les détails de votre serveur LDAP. Si vous faites une erreur, vous pouvez essayer à nouveau en utilisant :

```
sudo dpkg-reconfigure ldap-auth-config
```

Le résultat de la configuration est visible dans /etc/ldap.conf. Si votre serveur requiert des options non couvertes par l'assistant, modifiez ce fichier en conséquence.

Maintenant, configurez le profil LDAP pour NSS :

```
sudo auth-client-config -t nss -p lac_ldap
```

Configurez le système pour qu'il utilise LDAP pour l'authentification :

```
sudo pam-auth-update
```

Dans le menu, choisissez LDAP et les autres mécanismes d'authentification dont vous avez besoin.

Vous devriez maintenant être capable de vous connecter en utilisant les informations d'identification basées sur LDAP.

Les clients LDAP devront se référer à plusieurs serveurs si la réplication est en cours d'utilisation. Dans /etc/ldap.conf, vous devriez avoir quelque chose comme :

```
uri ldap ://ldap01.example.com ldap ://ldap02.example.com
```

La demande sera interrompue et le consommateur (ldap02) tentera d'être atteint si le fournisseur (ldap01) ne répond plus.

Si vous envisagez d'utiliser LDAP pour stocker les utilisateurs Samba, vous devrez configurer le serveur Samba pour qu'il s'authentifie en utilisant LDAP. Voir samba-ldap pour plus de détails.

> Une alternative au paquet **libnss-ldap** est **libnss-ldapd**. Cependant, ceci apportera le paquet **nscd** qui est probablement indésirable. Il vous suffit de le retirer par la suite.

7.1.11. Gestion des groupes et utilisateurs

Le paquet **ldap-utils** est livré avec assez d'utilitaires pour gérer le repertoire, mais la longue chaîne d'options nécessaires peuvent le rendre lourd à utiliser. Le paquet **ldapscripts** contient des scripts d'encapsulation pour ces utilitaires que certains trouvent plus facile à utiliser.

Installez le paquet :

```
sudo apt install ldapscripts
```

Puis éditez le fichier /etc/ldapscripts/ldapscripts.conf pour arriver à quelque chose de semblable à ce qui suit :

```
SERVER=localhost
BINDDN='cn=admin,dc=example,dc=com'
```

```
BINDPWDFILE="/etc/ldapscripts/ldapscripts.passwd"
SUFFIX=’dc=example,dc=com’
GSUFFIX=’ou=Groups’
USUFFIX=’ou=People’
MSUFFIX=’ou=Computers’
GIDSTART=10000
UIDSTART=10000
MIDSTART=10000
```

Maintenant, créez le fichier ldapscripts.passwd pour permettre l’accès de rootDN au répertoire :

sudo sh -c "echo -n ’secret’ > /etc/ldapscripts/ldapscripts.passwd"

sudo chmod 400 /etc/ldapscripts/ldapscripts.passwd

R emplacez "secret" par le mot de passe actuel de l’utilisateur rootdn de votre base de données.

Les scripts sont maintenant prêts à vous aider à gérer votre répertoire. Voici quelques exemples de la façon de les utiliser :

- Créez un nouvel utilisateur :

sudo ldapadduser laurence exemple

Ceci créera un utilisateur ayant pour UID **laurence** et pour groupe primaire (GID) **exemple**.

- Modifiez un mot de passe utilisateur :

sudo ldapsetpasswd laurence

```
Modifier le mot de passe de l’utilisateur uid=laurence,ou=People,dc=example,dc=com
```

Nouveau mot de passe :

Nouveau mot de passe (vérification) :

- Supprimer un utilisateur :

sudo ldapdeleteuser laurence

- Ajouter un groupe :

sudo ldapaddgroup qa

- Supprimer un groupe :

sudo ldapdeletegroup qa

- Ajouter un utilisateur à un groupe :

```
sudo ldapaddusertogroup laurence qa
```

Vous devez avoir maintenant un attribut **memberUid** ayant pour valeur **laurence** pour le groupe **qa**.

- Supprimer un utilisateur d'un groupe :

```
sudo ldapdeleteuserfromgroup laurence qa
```

L'attribut **memberUid** ne doit plus apparaître dans le groupe **qa** group.

- Le script **ldapmodifyuser** vous permet d'ajouter, supprimer ou modifier les attributs des utilisateurs. Il utilise la même syntaxe que **ldapmodify**. Par exemple :

```
sudo ldapmodifyuser laurence
```

```
# About to modify the following entry :
dn: uid=george,ou=People,dc=example,dc=com
objectClass: account
objectClass: posixAccount
cn: laurence
uid: laurence
uidNumber: 1001
gidNumber: 1001
homeDirectory: /home/laurence
loginShell: /bin/bash
gecos: laurence
description: User account
userPassword:: e1NTSEF9eXFsTFcyWlhwWkF1eGUybVdFWHZKRontujU!!FTSG9vcHk=

# Enter your modifications here, end with CTRL-D.
dn: uid=laurence,ou=People,dc=example,dc=com
replace : gecos
gecos: Laurence Bibot
```

Le **gecos** de l'utilisateur doit être maintenant "Laurence Bibot".

- L'une des fonctionnalités intéressantes de **ldapscripts** est son système de modèles qui permettent de personnaliser les attributs d'utilisateur, de groupe et des objets machine. Par exemple, pour activer le modèle **utilisateur**, modifiez /etc/ldapscripts/ldapscripts.conf en changeant :

```
UTEMPLATE="/etc/ldapscripts/ldapadduser.template"
```

Il y a des modèles d'**échantillons** dans le répertoire /usr/share/doc/ldapscripts/examples. Copiez ou renommez le fichier ldapadduser.template.sample en /etc/ldapscripts/ldapadduser.template :

```
sudo cp /usr/share/doc/ldapscripts/examples/ldapadduser.template.sample \
/etc/ldapscripts/ldapadduser.template
```

Modifiez le nouveau modèle pour ajouter les attributs désirés. Ce qui suit va créer de nouveaux utilisateurs avec un objectClass de inetOrgPerson :

```
dn : uid=<user>,<usuffix>,<suffix>
objectClass : inetOrgPerson
objectClass : posixAccount
cn : <user>
sn : <ask>
uid : <user>
uidNumber : <uid>
gidNumber : <gid>
homeDirectory : <home>
loginShell : <shell>
gecos : <user>
description : User account
title : Employee
```

Notez l'option **<ask>** utilisée pour l'attribut **sn**. Ceci fera que **ldapadduser** vous demandera sa valeur.

Il existe des utilitaires dans le paquet qui n'ont pas été abordés ici. En voici la liste complète :

ldaprenamemachine http://manpages.ubuntu.com/manpages/en/man1/ldaprenamemachine.1.html
ldapadduser http://manpages.ubuntu.com/manpages/en/man1/ldapadduser.1.html
ldapdeleteuserfromgroup http://manpages.ubuntu.com/manpages/en/man1/ldapdeleteuserfromgroup.1.html
ldapfinger http://manpages.ubuntu.com/manpages/en/man1/ldapfinger.1.html
ldapid http://manpages.ubuntu.com/manpages/en/man1/ldapid.1.html
ldapgid http://manpages.ubuntu.com/manpages/en/man1/ldapgid.1.html
ldapmodifyuser http://manpages.ubuntu.com/manpages/en/man1/ldapmodifyuser.1.html
ldaprenameuser http://manpages.ubuntu.com/manpages/en/man1/ldaprenameuser.1.html
lsldap http://manpages.ubuntu.com/manpages/en/man1/lsldap.1.html
ldapaddusertogroup http://manpages.ubuntu.com/manpages/en/man1/ldapaddusertogroup.1.html
ldapsetpasswd http://manpages.ubuntu.com/manpages/en/man1/ldapsetpasswd.1.html
ldapinit http://manpages.ubuntu.com/manpages/en/man1/ldapinit.1.html
ldapaddgroup http://manpages.ubuntu.com/manpages/en/man1/ldapaddgroup.1.html
ldapdeletegroup http://manpages.ubuntu.com/manpages/en/man1/ldapdeletegroup.1.html
ldapmodifygroup http://manpages.ubuntu.com/manpages/en/man1/ldapmodifygroup.1.html
ldapdeletemachine http://manpages.ubuntu.com/manpages/en/man1/ldapdeletemachine.1.html
ldaprenamegroup http://manpages.ubuntu.com/manpages/en/man1/ldaprenamegroup.1.html
ldapaddmachine http://manpages.ubuntu.com/manpages/en/man1/ldapaddmachine.1.html
ldapmodifymachine http://manpages.ubuntu.com/manpages/en/man1/ldapmodifymachine.1.html
ldapsetprimarygroup http://manpages.ubuntu.com/manpages/en/man1/ldapsetprimarygroup.1.html
ldapdeleteuser http://manpages.ubuntu.com/manpages/en/man1/ldapdeleteuser.1.html

7.1.12. Archivage et restauration

ldap tourne maintenant tout juste comme nous le voulons, il est temps de s'assurer que nous pouvons enregistrer l'ensemble de notre travail et le restaurer si nécessaire.

Ce que nous voulons est un moyen de sauvegarder la ou les bases de données ldap, en particulier le backend (cn=config) et le frontend (dc=exemple, dc=com). Si nous souhaitons sauvegarder ces bases de

données dans, par exemple, /export/backup, nous pourrions utiliser **slapcat** comme indiqué dans le script suivant nommé /usr/local/bin/ldapbackup :

```
#!/bin/bash

BACKUP_PATH=/export/backup
SLAPCAT=/usr/sbin/slapcat

nice ${SLAPCAT} -n 0 > ${BACKUP_PATH}/config.ldif
nice ${SLAPCAT} -n 1 > ${BACKUP_PATH}/example.com.ldif
nice ${SLAPCAT} -n 2 > ${BACKUP_PATH}/access.ldif
chmod 640 ${BACKUP_PATH}/*.ldif
```

> Ces fichiers sont des fichiers texte non compressés qui contiennent tout sur vos bases de données ldap, y compris l'arborescence, les noms d'utilisateurs, et chaque mot de passe. Donc, vous voudrez peut-être faire en sorte que /export/sauvegarde soit une partition chiffrée et aussi avoir le script qui chiffre ces fichiers en les créant. Idéalement, vous devriez faire les deux, mais cela dépend de vos exigences de sécurité.

Ensuite, il s'agit simplement d'avoir un script cron pour exécuter ce programme tant que nous nous sentons à l'aise. Pour beaucoup, une fois par jour suffit. Pour d'autres, le faire plus souvent est nécessaire. Voici un exemple de script cron appelé /etc/cron.d/ldapbackup qui s'exécute tous les soirs à 22h45 :

```
MAILTO=backup-emails@domain.com
45 22 * * * root /usr/local/bin/ldapbackup
```

Les fichiers étant créés, ils doivent être copiés sur un serveur de sauvegarde.

En supposant que nous ayons fait une réinstallation fraîche de ldap, le processus de restauration pourrait être quelque chose comme ceci :

```
sudo systemctl stop slapd.service
sudo mkdir /var/lib/ldap/accesslog
sudo slapadd -F /etc/ldap/slapd.d -n 0 -l /export/backup/config.ldif
sudo slapadd -F /etc/ldap/slapd.d -n 1 -l /export/backup/domain.com.ldif
sudo slapadd -F /etc/ldap/slapd.d -n 2 -l /export/backup/access.ldif
sudo chown -R openldap :openldap /etc/ldap/slapd.d/
sudo chown -R openldap :openldap /var/lib/ldap/
sudo systemctl start slapd.service
```

7.1.13. Ressources

La ressource principale est la documentation amont : **www.openldap.org** : http://www.openldap.org/

Il y a de nombreuses pages de manuel fournies avec le paquet slapd. Voici quelques pages importantes, surtout au vu des documents présentés dans ce guide :

slapd : http://manpages.ubuntu.com/manpages/en/man8/slapd.8.html

slapd-config : *http://manpages.ubuntu.com/manpages/en/man5/slapd-config.5.html*

slapd.access : *http://manpages.ubuntu.com/manpages/en/man5/slapd.access.5.html*

slapo-syncprov : *http://manpages.ubuntu.com/manpages/en/man5/slapo-syncprov.5.html*

Autres pages de manuel :

auth-client-config : *http://manpages.ubuntu.com/manpages/en/man8/auth-client-config.8.html*

pam-auth-update : http://manpages.ubuntu.com/manpages/en/man8/pam-auth-update.8.html

Le site de Zytrax, **LDAP for Rocket Scientists** : un peu magistral mais qui traite complètement de LDAP : http://www.zytrax.com/books/ldap/

Une page **wiki en anglais sur OpenLDAP** de la communauté Ubuntu qui comporte un ensemble de notes sur le sujet : https://help.ubuntu.com/community/OpenLDAPServer

LDAP System Administration sur le site de O'Reilly (manuel ; 2003) : http://www.oreilly.com/catalog/ldapsa/

Maîtriser OpenLDAP (en anglais) sur le site Packt (manuel ; 2007) : http://www.packtpub.com/OpenLDAP-Developers-Server-Open-Source-Linux/book

7.2. Samba et LDAP

Cette section couvre l'intégration de Samba avec LDAP. Le rôle du serveur Samba sera celle d'un serveur « autonome » et l'annuaire LDAP fournira la couche d'authentification en plus de contenir les informations utilisateur, groupe et compte de machine dont Samba a besoin pour fonctionner (dans n'importe lequel de de ses trois rôles possibles). Le pré-requis est un serveur OpenLDAP configuré avec un répertoire qui peut accepter les demandes d'authentification. Voir le *Chapitre 7, paragraphe 1. Serveur OpenLDAP* pour plus de détails sur ce pré-requis. Une fois cette partie terminée, vous devrez décider ce que vous voulez que Samba fasse pour vous et le configurer en conséquence.

7.2.1. Installation de logiciels

Deux paquets sont nécessaires pour intégrer Samba avec LDAP : **samba** et **smbldap-tools**.

Le paquet **smbldap-tools** n'est pas nécessaire à proprement parler, mais si vous n'avez pas d'autre moyen de gérer les diverses entités Samba (utilisateurs, groupes, ordinateurs) dans le contexte LDAP, alors, vous devriez installer le paquet **smbldap-tools**.

Maintenant, installez ces paquets :

```
sudo apt install samba smbldap-tools
```

7.2.2. Configuration LDAP

Nous allons maintenant configurer le serveur LDAP afin qu'il puisse accueillir les données de Samba. Nous allons effectuer trois tâches dans cette section :

1. Importez un schéma
2. Indexez des entrées
3. Ajouter des objets

7.2.2.1. Schéma Samba

Logiquement, pour que OpenLDAP soit utilisé comme backend pour Samba, le DIT devra utiliser des attributs qui peuvent décrire correctement les données de Samba. Ces attributs peuvent être obtenus par l'introduction d'un schéma LDAP Samba. Faisons-le maintenant.

> Pour avoir plus d'informations sur les schémas et leur installation, voir *Chapitre 7, paragraphe 1. Serveur OpenLDAP.4. Modification de la base de données de configuration slapd.*

1. Le schéma se trouve dans le paquet **samba**, à présent installé. Il doit être dézippé et copié dans le répertoire /etc/ldap/schema :

```
sudo cp /usr/share/doc/samba/examples/LDAP/samba.schema.gz /etc/ldap/schema
sudo gzip -d /etc/ldap/schema/samba.schema.gz
```

2. Prenez le fichier de configuration schema_convert.conf qui contient les lignes suivantes :

```
include /etc/ldap/schema/core.schema
include /etc/ldap/schema/collective.schema
include /etc/ldap/schema/corba.schema
include /etc/ldap/schema/cosine.schema
include /etc/ldap/schema/duaconf.schema
include /etc/ldap/schema/dyngroup.schema
include /etc/ldap/schema/inetorgperson.schema
include /etc/ldap/schema/java.schema
include /etc/ldap/schema/misc.schema
include /etc/ldap/schema/nis.schema
include /etc/ldap/schema/openldap.schema
include /etc/ldap/schema/ppolicy.schema
include /etc/ldap/schema/ldapns.schema
include /etc/ldap/schema/pmi.schema
include /etc/ldap/schema/samba.schema
```

3. Prenez le répertoire ldif_output contenant les sorties.
4. Déterminez l'index du schéma :

```
slapcat -f schema_convert.conf -F ldif_output -n 0 | grep samba,cn=schema
```

```
dn : cn={14}samba,cn=schema,cn=config
```

5. Convertissez le schéma au format LDIF :

```
slapcat -f schema_convert.conf -F ldif_output -n0 -H \ ldap
:///cn={14}samba,cn=schema,cn=config -l cn=samba.ldif
```

6. Modifiez le fichier cn=samba.ldif généré en supprimant les informations d'index pour arriver à :

```
dn : cn=samba,cn=schema,cn=config
...
cn : samba
```

Retirez les lignes du bas :

```
structuralObjectClass : olcSchemaConfig
entryUUID : b53b75ca-083f-102d-9fff-2f64fd123c95
creatorsName : cn=config
createTimestamp : 20080827045234Z
entryCSN : 20080827045234.341425Z#000000#000#000000
modifiersName : cn=config
modifyTimestamp : 20080827045234Z
```

Les valeurs des attributs varieront.

7. Ajoutez le nouveau schéma :

```
sudo ldapadd -Q -Y EXTERNAL -H ldapi :/// -f cn\=samba.ldif
```

Pour interroger et voir ce nouveau schéma :

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi :/// -b \
cn=schema,cn=config 'cn=*samba*'
```

7.2.2.2. Indices Samba

Maintenant que slapd connaît les attributs Samba, nous pouvons définir quelques indices basés sur ces attributs. L'indexation des entrées est un moyen d'améliorer les performances lorsqu'un client effectue une recherche filtrée dans le DIT.

Créez le fichier samba_indices.ldif avec le contenu suivant :

```
dn : olcDatabase={1}hdb,cn=config
changetype : modify
add : olcDbIndex
olcDbIndex : uidNumber eq
olcDbIndex : gidNumber eq
olcDbIndex : loginShell eq
olcDbIndex : uid eq,pres,sub
olcDbIndex : memberUid eq,pres,sub
olcDbIndex : uniqueMember eq,pres
olcDbIndex : sambaSID eq
olcDbIndex : sambaPrimaryGroupSID eq
olcDbIndex : sambaGroupType eq
olcDbIndex : sambaSIDList eq
olcDbIndex : sambaDomainName eq
olcDbIndex : default sub
```

Avec l'utilitaire **ldapmodify**, charger les nouveaux indices :

```
sudo ldapmodify -Q -Y EXTERNAL -H ldapi :/// -f samba_indices.ldif
```

Si tout s'est bien passé, vous devriez voir les nouveaux indices en utilisant **ldapsearch** :

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H \
ldapi :/// -b cn=config olcDatabase={1}hdb olcDbIndex
```

7.2.2.3. Ajout d'objets LDAP à Samba

Ensuite, configurez le paquet **smbldap-tools** pour qu'il corresponde à votre environnement. Le paquet est fournit avec un script d'aide à la configuration, smbldap-config.pl, qui pose des questions.

Le script **smbldap-populate** va ensuite ajouter les objets LDAP nécessaires pour Samba. C'est une bonne idée que de commencer par sauvegarder votre DIT avec **slapcat** :

```
sudo slapcat -l backup.ldif
```

Une fois que vous avez une sauvegarde, procédez au remplissage de votre répertoire :

```
sudo smbldap-populate
```

Vous pouvez créer un fichier LDIF contenant les nouveaux objets Samba en exécutant **sudo smbldap-populate -e samba.ldif**. Cela vous permet de consulter les modifications et de s'assurer que tout est correct. Si c'est le cas, relancez le script sans le commutateur « -e ». Alternativement, vous pouvez prendre le fichier LDIF et importer ses données comme d'habitude.

Votre répertoire LDAP a maintenant les informations nécessaires pour authentifier les utilisateurs Samba.

7.2.3. Configuration de Samba

Il ya plusieurs façons de configurer Samba. Pour plus de détails sur certaines configurations communes voir samba. Pour configurer Samba pour qu'il utilise LDAP, éditez son fichier de configuration /etc/samba/smb.conf en mettant en commentaire le paramètre **passdb backend** par défaut et en ajoutant de nouveaux paramètres liés à LDAP :

```
# passdb backend = tdbsam

# LDAP Settings
   passdb backend = ldapsam :ldap ://hostname
   ldap suffix = dc=example,dc=com
   ldap user suffix = ou=People
   ldap group suffix = ou=Groups
   ldap machine suffix = ou=Computers
   ldap idmap suffix = ou=Idmap
   ldap admin dn = cn=admin,dc=example,dc=com
   ldap ssl = start tls
   ldap passwd sync = yes
...
   add machine script = sudo /usr/sbin/smbldap-useradd -t 0 -w "%u"
```

Modifiez les valeurs pour correspondre à votre environnement.

Redémarrez **samba** pour activer les nouveaux paramètres :

```
sudo systemctl restart smbd.service nmbd.service
```

Maintenant, informez Samba à propos du mot de passe de l'utilisateur rootDN (celui défini lors de l'installation du paquet slapd) :

```
sudo smbpasswd -w password
```

Si vous avez déjà des utilisateurs LDAP que vous souhaitez inclure dans votre nouveau Samba soutenu par LDAP, certains des attributs supplémentaires devront bien sûr aussi leur être associés. L'utilitaire

smbpasswd peut faire cela (votre hôte devra être en mesure de voir (énumérer) les utilisateurs via NSS ; installez et configurez soit **libnss-ldapd**, soit **libnss-ldap**) :

```
sudo smbpasswd -a username
```

Vous serez invité à entrer un mot de passe. Il sera considéré comme le nouveau mot de passe pour cet utilisateur. Choisir le même que précédemment est raisonnable.

Pour gérer les utilisateurs, les groupes et les comptes machine, utilisez les utilitaires fournis par le paquet **smbldap-tools**. Voici quelques exemples :

- Pour ajouter un nouvel utilisateur :

  ```
  sudo smbldap-useradd -a -P username
  ```

  L'option **-a** ajoute les attributs Samba, et l'option **-P** appelle l'utilitaire **smbldap-passwd** après que l'utilisateur ait été créé, vous permettant de saisir un mot de passe pour cet utilisateur.

- Pour supprimer un utilisateur :

  ```
  sudo smbldap-userdel username
  ```

  Dans la commande ci-dessus, utilisez l'option **-r** pour supprimer le répertoire personnel de l'utilisateur.

- Pour ajouter un groupe :

  ```
  sudo smbldap-groupadd -a groupname
  ```

  Comme pour **smbldap-useradd**, l'option **-a** ajoute les attributs Samba.

- Pour faire qu'un utilisateur existant devienne membre d'un groupe :

  ```
  sudo smbldap-groupmod -m username groupname
  ```

  L'option **-m** permet d'ajouter plusieurs utilisateurs à la fois en les listant dans un format séparé par des virgules.

- Pour supprimer un utilisateur d'un groupe :

  ```
  sudo smbldap-groupmod -x username groupname
  ```

- Pour ajouter un compte machine Samba :

  ```
  sudo smbldap-useradd -t 0 -w nom_machine
  ```

  Remplacez **username** avec le nom du poste de travail. L'option **-t 0** permet de créer le compte machine sans délai, tandis que l'option **-w** option spécifie l'utilisateur comme un compte machine. En outre, notez que le paramètre **add machine script** dans /etc/samba/smb.conf a été modifié pour utiliser **smbldap-useradd**.

Il y a des utilitaires dans le paquet **smbldap-tools** qui n'ont pas été abordés ici. En voici la liste complète :

~~smbldap-groupadd~~ : http://manpages.ubuntu.com/manpages/en/man8/smbldap-groupadd.8.html (semble rayé

dans la version anglaise, NDT)

smbldap-groupdel : http://manpages.ubuntu.com/manpages/en/man8/smbldap-groupdel.8.html

smbldap-groupmod : http://manpages.ubuntu.com/manpages/en/man8/smbldap-groupmod.8.html

smbldap-groupshow : http://manpages.ubuntu.com/manpages/en/man8/smbldap-groupshow.8.html

smbldap-passwd : http://manpages.ubuntu.com/manpages/en/man8/smbldap-passwd.8.html

smbldap-populate : http://manpages.ubuntu.com/manpages/en/man8/smbldap-populate.8.html

smbldap-useradd : http://manpages.ubuntu.com/manpages/en/man8/smbldap-useradd.8.html

smbldap-userdel : http://manpages.ubuntu.com/manpages/en/man8/smbldap-userdel.8.html

smbldap-userinfo : http://manpages.ubuntu.com/manpages/en/man8/smbldap-userinfo.8.html

smbldap-userlist : http://manpages.ubuntu.com/manpages/en/man8/smbldap-userlist.8.html

smbldap-usermod : http://manpages.ubuntu.com/manpages/en/man8/smbldap-usermod.8.html

smbldap-usershow : http://manpages.ubuntu.com/manpages/en/man8/smbldap-usershow.8.html

7.2.4. Ressources

Pour plus d'informations sur l'installation et la configuration de Samba, voir le *Chapitre 18. Samba* de ce guide du serveur Ubuntu.

LDAP et Samba sont documentés dans plusieurs sections du **guide pratique de Samba** : http://samba.org/samba/docs/man/Samba-HOWTO-Collection/.

Concernant ce qui précède, voir en particulier la **section passdb** : http://samba.org/samba/docs/man/Samba-HOWTO-Collection/passdb.html .

Bien que daté de 2007, le **HOWTO Linux Samba-OpenLDAP** contient de précieuses notes : http://download.gna.org/smbldap-tools/docs/samba-ldap-howto/ .

La page principale de la **documentation communautaire Samba Ubuntu** a une pléthore de liens vers des articles qui peuvent s'avérer utiles : https://help.ubuntu.com/community/Samba#samba-ldap .

7.3. Kerberos

Kerberos est un système d'authentification réseau basé sur le principe d'un tiers de confiance. Les deux autres parties sont l'utilisateur et le service sur lequel l'utilisateur veut s'authentifier. Tous les services et applications ne savent pas utiliser Kerberos, mais pour ceux qui en sont capables, cela rapproche l'environnement réseau d'un système à authentification unique (Single Sign On : SSO).

Cette section couvre l'installation et la configuration d'un serveur Kerberos, et propose quelques exemples de configurations de clients.

7.3.1. Aperçu

Si vous débutez avec Kerberos, il y a quelques termes qu'il est bon de comprendre avant de paramétrer un serveur Kerberos. La plupart des termes sont proches d'éléments qui peuvent vous être familiers dans d'autres environnements.

- **Donneur d'ordre (Principal)** : tous les utilisateurs, ordinateurs et services fournis par des serveurs doivent être définis comme « Donneurs d'ordre » Kerberos.
- **Instances** : sont utilisés pour les donneurs d'ordre de service et les donneurs d'ordre administratifs spéciaux.
- **Domaines (Realms)** : le domaine de contrôle unique proposé par l'installation Kerberos. C'est un peu comme un domaine ou un groupe auquel vos hôtes et utilisateurs appartiendraient tous. Par convention, le domaine est en majuscules. Par défaut, Ubuntu utilise le domaine DNS converti en majuscule (EXAMPLE.COM) comme domaine Kerberos.
- **Centre de distribution de clef (Key Distribution Center : KDC)** : se compose de trois parties, une base de données de tous les clients, le serveur d'authentification, et le serveur accordant les tickets. Pour chaque domaine il doit y avoir au moins un KDC.
- **Ticket d'octroi de ticket (Ticket Granting Ticket : TGT)** : émis par le serveur d'authentification (Authentication Server : AS), le ticket d'octroi du ticket (TGT) est chiffré avec le mot de passe utilisateur qui n'est connu que par l'utilisateur et le KDC.
- **Serveur d'octroi de ticket (Ticket Granting Server : TGS)** : génère sur demande des tickets de service aux clients.
- **Tickets :** confirment l'identité des deux donneurs d'ordre. Un donneur d'ordre étant un utilisateur et l'autre un service demandé par l'utilisateur. Les tickets établissent une clé de chiffrage utilisée pour la communication sécurisée pendant la session authentifiée.
- **Fichiers Keytab :** ce sont des fichiers extraits de la base de données KDC des « principals » et qui contiennent la clé de chiffrement pour un service ou un hôte.

Pour recoller les morceaux, un Domaine a au moins un KDC, de préférence plus par redondance, qui contient une base de données des Donneurs d'ordres. Quand un utilisateur Donneur d'ordres se connecte à un poste de travail qui est configuré pour l'authentification Kerberos, le KDC émet un Ticket d'octroi de ticket (TGT). Si l'utilisateur a fourni des références qui correspondent, l'utilisateur est authentifié et peut ensuite demander des tickets pour les services Kerberos du Serveur d'octroi de tickets (TGS). Les tickets de service permettent à l'utilisateur de s'authentifier auprès du service sans entrer dans un autre et mot de passe.

7.3.2 Serveur Kerberos

7.3.2.1 Installation

Pour cette discussion, nous allons créer un domaine MIT Kerberos avec les caractéristiques suivantes (les modifier en fonction de vos besoins) :

Domaine : EXEMPLE.COM

KDC primaire : kdc01.example.com (192.168.0.1)

KDC secondaire : kdc02.example.com (192.168.0.2)

Utilisateur principal : steve

Administrateur principal : steve/admin

> I est **chaudement** recommandé que les uid de vos utilisateurs authentifiés par le réseau soient dans une gamme différente (par exemple, à partir de 5000) de celle de vos utilisateurs locaux.

Avant d'installer le serveur Kerberos, il faut qu'un serveur DNS soit correctement configuré pour votre domaine. Comme, par convention, le domaine Kerberos correspond au nom de domaine, cette section utilise le domaine **EXAMPLE.COM**, configuré comme dans la documentation DNS *Chapitre 8, paragraphe 2. Configuration.3. Maître primaire*.

En outre, Kerberos est un protocole sensible au temps. Donc, si l'heure du système local entre un ordinateur client et le serveur diffère de plus de cinq minutes (par défaut), le poste de travail ne pourra pas s'authentifier. Pour corriger le problème, tous les hôtes doivent avoir leur temps synchronisé avec le même serveur **Network Time Protocol (NTP)**. Pour plus de détails sur la configuration de NTP, voir chapitre *4, paragraphe 4. Synchronisation temporelle avec NTP* .

La première étape dans la création d'un domaine Kerberos est d'installer les paquets **krb5-kdc** et **krb5-admin-server**. Dans un terminal saisissez :

```
sudo apt install krb5-kdc krb5-admin-server
```

À la fin de l'installation, il vous sera demandé de fournir le nom d'hôte pour les serveurs Kerberos et d'administration, qui peuvent être le même serveur ou non, pour le domaine.

> P ar défaut, le domaine est créé à partir du nom de domaine du KDC.

Ensuite, créez le nouveau domaine à l'aide de l'utilitaire **kdb5_newrealm** :

```
sudo krb5_newrealm
```

7.3.2.2. Configuration

Les questions posées lors de l'installation servent à configurer le fichier /etc/krb5.conf. Si vous avez besoin d'ajuster les paramètres du Centre de distribution de clés (Key Distribution Center, KDC), éditez simplement le fichier et redémarrez le démon **krb5-kdc**. Si vous devez reconfigurer Kerberos à partir de zéro, par exemple pour changer le nom de domaine, vous pouvez le faire en tapant :

```
sudo dpkg-reconfigure krb5-kdc
```

1. Une fois que le KDC est bien en cours d'exécution, un utilisateur admin - le principal **admin** - est nécessaire. Il est recommandé d'utiliser un différent de votre au quotidien. Utilisation de la **kadmin.local** utilitaire dans un terminal saisissez :

```
sudo kadmin.local
```

```
Identification comme root/admin@EXAMPLE.COM avec mot de passe.
kadmin.local : addprinc steve/admin
ATTENTION : pas de règle spécifique pour steve/admin@EXAMPLE.COM; configuration
par défaut sans règles.
Entrez un mot de passe pour "steve/admin@EXAMPLE.COM":
Ré-entrez le mot de passe pour "steve/admin@EXAMPLE.COM":
Donneur d'ordres "steve@EXAMPLE.COM" créé.
kadmin.local: quit

versions originale :
Authenticating as principal root/admin@EXAMPLE.COM with password.
kadmin.local: addprinc steve/admin
WARNING: no policy specified for steve/admin@EXAMPLE.COM; defaulting to no policy
Enter password for principal "steve/admin@EXAMPLE.COM":
Re-enter password for principal "steve/admin@EXAMPLE.COM":
Principal "steve/admin@EXAMPLE.COM" created.
kadmin.local: quit
```

Dans l'exemple ci-dessus **steve** est le principal , **/ admin** est un accent < > Instance, et **@ EXAMPLE.COM** représente le royaume. Le **"tous les jours "** principal, alias le principal d'utilisateur , serait **steve @ EXEMPLE . COM**, et devraient avoir des droits d'utilisateur que la normale.

R emplacez **EXEMPLE.COM** et **steve** par vos noms de domaine et d'administrateur.

2. Ensuite, le nouvel utilisateur admin a besoin des permissions ACL (Access Control List) appropriées. Les permissions sont configurées dans le fichier /etc/krb5kdc/kadm5.acl :

```
steve/admin@EXAMPLE.COM        *
```

Cette entrée assure à **steve/admin** la possibilité d'effectuer toute opération sur tous les Donneurs d'ordres dans le domaine.

Vous pouvez configurer les Donneurs d'ordres avec des privilèges plus restrictifs, ce qui est pratique si vous avez besoin d'un profil d'administrateur Donneur d'ordres, que le personnel subalterne peut utiliser dans les clients Kerberos. Veuillez voir la page de man de **kadm5.acl** pour plus de détails.

3. Redémarrez maintenant **krb5-admin-server** pour que les nouvelles ACL soient prises en compte :

```
sudo systemctl restart krb5-admin-server.service
```

4. Le nouveau « principal » d'utilisateur peut être testé en utilisant **kinit utility** :

kinit steve/admin

```
Mot de passe de steve/admin@EXAMPLE.COM :
```

Après avoir saisi le mot de passe, utilisez **klist** pour afficher les informations du TGT (Ticket Granting Ticket, ticket d'octroi de tickets) :

klist

```
Credentials cache : FILE :/tmp/krb5cc_1000
Principal: steve/admin@EXAMPLE.COM
Issued . .        Expires          Principal
Jul 13 17:53:34   Jul 14 03:53:34   krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

Où le nom du fichier cache krb5cc_1000 est composé du préfixe krb5cc_ et l'ID utilisateur (uid), qui dans ce cas est 1000. Vous devrez peut-être ajouter une entrée dans les /etc/hosts pour le KDC afin que le client puisse trouver le KDC. Par exemple :

```
192.168.0.1 kdc01.example.com kdc01
```

en remplaçant **192.168.0.1** par l'adresse IP de votre KDC. Cela se produit généralement lorsque vous avez un domaine Kerberos englobant différents réseaux séparés par des routeurs.

5. La meilleure façon de permettre aux clients de déterminer automatiquement le KDC pour le domaine est d'utiliser les enregistrements DNS SRV. Ajoutez ce qui suit à /etc/named/db.exemple.com :

```
_kerberos._udp.EXAMPLE.COM. IN SRV 1 0 88 kdc01.example.com.
_kerberos._tcp.EXAMPLE.COM. IN SRV 1 0 88 kdc01.example.com.
_kerberos._udp.EXAMPLE.COM. IN SRV 10 0 88 kdc02.example.com.
_kerberos._tcp.EXAMPLE.COM. IN SRV 10 0 88 kdc02.example.com.
_kerberos-adm._tcp.EXAMPLE.COM. IN SRV 1 0 749 kdc01.example.com.
_kpasswd._udp.EXAMPLE.COM. IN SRV 1 0 464 kdc01.example.com.
```

Remplacez **EXAMPLE.COM**, **kdc01**, et **kdc02** par vos noms de domaine, de serveur KDC primaire et secondaire.

Consultez le *Chapitre 8. Service de nom de domaine (DNS)* pour des instructions détaillées sur le paramétrage des DNS.

Votre nouveau domaine Kerberos est maintenant prêt à authentifier des clients.

7.3.3. KDC secondaire

Une fois que vous avez un centre de distribution de clés (KDC) sur votre réseau, il est conseillé d'avoir un KDC secondaire au cas où le principal deviendrait indisponible. En outre, si vous avez des clients Kerberos dans des réseaux différents (éventuellement séparés par des routeurs utilisant NAT), il est judicieux de placer un KDC secondaire dans chacun de ces réseaux.

1. Tout d'abord, installez les paquets, et lors de la demande des noms de serveurs Kerberos et Administrateur, saisissez le nom du serveur KDC primaire :

```
sudo apt install krb5-kdc krb5-admin-server
```

2. Une fois les paquets installés, créez un « principal » du KDC secondaire. Dans un terminal, saisissez :

```
kadmin -q "addprinc -randkey host/kdc02.example.com"
```

Ensuite, l'exécution de n'importe quelle commande **kadmin** nécessitera l'introduction du mot de passe du Donneur d'ordres **username/admin@EXAMPLE.COM**.

3. Extrayez le fichier **keytab** :

```
kadmin -q "ktadd -norandkey -k keytab.kdc02 host/kdc02.example.com"
```

4. Il devrait y avoir un fichier keytab.kdc02 dans le dossier actuel. Déplacez le vers /etc/krb5.keytab :

```
sudo mv keytab.kdc02 /etc/krb5.keytab
```

S i l'emplacement du fichier keytab.kdc02 est différent, adaptez le en conséquence.

Vous pouvez également lister les « principals » d'un fichier Keytab à l'aide de **klist**, ce qui peut être utile au dépannage :

```
sudo klist -k /etc/krb5.keytab
```

L'option **-k** indique qu'il s'agit d'un fichier keytab.

5. Ensuite, il doit exister un fichier kpropd.acl sur chaque KDC qui liste tous les KDC du domaine. Par exemple, sur les serveurs primaire et secondaire, créez le fichier /etc/krb5kdc/kpropd.acl :

```
host/kdc01.example.com@EXAMPLE.COM
host/kdc02.example.com@EXAMPLE.COM
```

6. Créez une base de données vide sur le **KDC secondaire** :

```
sudo kdb5_util -s create
```

7. Lancez maintenant le démon **kpropd**, qui écoute les connexions depuis l'utilitaire **kprop**. **kprop** est utilisé pour transférer des fichiers de sauvegarde :

```
sudo kpropd -S
```

8. Depuis un terminal sur le **KDC primaire**, créez un fichier de sauvegarde de la base de données des Donneurs d'ordres :

```
sudo kdb5_util dump /var/lib/krb5kdc/dump
```

9. Décompressez le fichier **keytab** du KDC primaire et copiez le dans /etc/krb5.keytab :

```
kadmin -q "ktadd -k keytab.kdc01 host/kdc01.example.com"
sudo mv keytab.kdc01 /etc/krb5.keytab
```

A ssurez-vous qu'il y ait un **hôte** pour **kdc01.example.com** avant d'extraire le Keytab.

10. L'utilitaire **kprop** envoie la base de données vers le serveur KDC secondaire :

```
sudo kprop -r EXAMPLE.COM -f /var/lib/krb5kdc/dump kdc02.example.com
```

I devrait y avoir un message de **succès** si le transfert s'est bien passé. S'il y a un message d'erreur, vérifiez /var/log/syslog sur le KDC secondaire pour plus d'informations.

Vous pouvez également créer une tâche **cron** pour mettre à jour périodiquement la base de données sur le KDC secondaire. Par exemple, ce qui suit va mettre à jour la base de données toutes les heures (notez que la grande ligne a été divisée pour l'adapter au format du document) :

```
# m h dom mon dow command
0 * * * * /usr/sbin/kdb5_util dump /var/lib/krb5kdc/dump &amp;amp;&amp;amp;
/usr/sbin/kprop -r EXAMPLE.COM -f /var/lib/krb5kdc/dump kdc02.example.com
```

11. De retour sur le **KDC secondaire**, créez un fichier **stash** qui contiendra la clé maître de Kerberos :

```
sudo kdb5_util stash
```

12. Finalement, démarrez le service **krb5-kdc** sur le KDC secondaire :

```
sudo systemctl start krb5-kdc.service
```

Le KDC secondaire devrait maintenant être en mesure d'émettre des ticket pour le domaine. Vous pouvez tester cela en arrêtant le démon **krb5-kdc** sur le KDC primaire, puis en utilisant **kinit** pour demander un ticket. Si tout va bien, vous devriez recevoir un ticket du KDC secondaire. Sinon, vérifiez /var/log/syslog et /var/log/auth.log dans le KDC secondaire.

7.3.4. Client Kerberos Linux

Cette section présente la configuration d'un système Linux comme un client **Kerberos**. Ceci va autoriser l'accès à n'importe quel service gérant Kerberos une fois l'utilisateur correctement connecté au système.

7.3.4.1. Installation

Pour pouvoir s'authentifier sur un domaine Kerberos, les paquets **krb5-user** et **libpam-krb5** sont nécessaires, ainsi que quelques autres qui ne sont pas obligatoires mais vous faciliteront la tâche. Pour installer ces paquets tapez la commande suivante dans un terminal :

```
sudo apt install krb5-user libpam-krb5 libpam-ccreds auth-client-config
```

Le paquet **auth-client-config** permet une configuration simple de PAM pour l'authentification depuis

plusieurs sources. **libpam-ccreds** va mettre en cache les références de l'authentification pour vous permettre de vous connecter si le KDC (Key Distribution Center) n'est pas disponible. Ce paquet est également utile pour les portables qui s'identifient via Kerberos sur leur réseau professionnel, mais doivent également rester accessibles en dehors ce réseau.

7.3.4.2. Configuration

Pour configurer le client, tapez dans un terminal :

```
sudo dpkg-reconfigure krb5-config
```

Il vous sera alors demandé de donner le nom du domaine Kerberos. Si vous n'avez pas de DNS configuré avec des enregistrements **SRV** Kerberos, le menu vous demandera le nom de l'hôte KDC et du serveur d'administration du domaine.

dpkg-reconfigure ajoute des entrées au fichier /etc/krb5.conf pour votre domaine. Vous devriez avoir des entrées similaires à :

```
[libdefaults]
        default_realm = EXAMPLE.COM
...
[realms]
        EXAMPLE.COM = {
                kdc = 192.168.0.1
                admin_server = 192.168.0.1
        }
```

Si vous réglez l'uid de chacun de vos utilisateurs authentifiés du réseau pour commencer à 5000, comme l'a suggéré dans la section *3.2.1. Installation*, vous pouvez alors appeller pam (man pam pour info, pas votre voisine) pour seulement essayer de s'authentifier via des profils d'utilisateurs Kerberos avec l'uid> 5000 :

```
# Kerberos ne doit être appliqué qu'à des utilisateurs LDAP/Kerberos, et non à des utilisateurs locaux.
for i in common-auth common-session common-account common-password; do
sudo sed-i-r \ -e 's/pam_krb5.so minimum_uid=1000/pam_krb5.so minimum_uid=5000/' \
/etc/pam.d/$i
```

Cela évitera une demande de mot de passe Kerberos (inexistant) d'un utilisateur authentifié localement lors du changement de son mot de passe à l'aide de la commande **passwd**.

Vous pouvez tester la configuration en demandant un ticket à l'aide de **kinit**. Par exemple :

```
kinit steve@EXAMPLE.COM
```

```
Mot de passe pour steve@EXAMPLE.COM :
```

Lorsqu'un ticket a été accordé, les détails peuvent être affichés avec **klist** :

```
klist
```

```
Ticket cache: FILE:/tmp/krb5cc_1000
Default principal: steve@EXAMPLE.COM
Valid starting
07/24/08 05:18:56
```

```
Expires
07/24/08 15:18:56
Service principal
krbtgt/EXAMPLE.COM@EXAMPLE.COM
renew until 07/25/08 05:18:57
150Network Authentication
Kerberos 4 ticket cache: /tmp/tkt1000
klist: You have no tickets cached
```

Ensuite, utilisez **auth-client-config** pour configurer le module **libpam-krb5** pour demander un ticket lors de l'ouverture de session :

```
sudo auth-client-config -a -p kerberos_example
```

Vous devriez maintenant recevoir un ticket dès qu'une ouverture de session avec authentification est réussie.

7.3.5. Ressources

Pour plus d'informations sur la version Kerberos de MIT, consultez le site **MIT Kerberos** : http://web.mit.edu/Kerberos/ .

La page du **wiki anglophone d'Ubuntu sur Kerberos** comprend des détails complémentaires : https://help.ubuntu.com/community/Kerberos .

Le guide d'O'Reilly **Kerberos : The Definitive Guide** est une bonne référence pour mettre en place Kerberos : http://oreilly.com/catalog/9780596004033/ .

Aussi, n'hésitez pas à passer par les canaux IRC **#ubuntu-server** et **#kerberos** sur **Freenode** si vous avez des questions concernant Kerberos : http://freenode.net/ .

7.4. Kerberos et LDAP

La plupart des gens n'utiliseront pas Kerberos directement, une fois qu'un utilisateur est authentifié (Kerberos), nous avons besoin de comprendre ce que cet utilisateur peut faire (autorisation). Et ce serait la tâche de programmes comme LDAP.

Répliquer une bases de données de Donneurs d'ordres Kerberos entre deux serveurs peut être compliqué, et cela ajoute une base de données supplémentaire d'utilisateurs à votre réseau. Heureusement, MIT Kerberos peut être configuré pour utiliser un annuaire **LDAP** comme base de données de Donneurs d'ordres. Cette section couvre la configuration de serveurs Kerberos primaire et secondaire pour utiliser **OpenLDAP** pour la base de données de Donneurs d'ordres.

> L es exemples présentés ici utilisent **MIT Kerberos** et **OpenLDAP**.

7.4.1. Configuration OpenLDAP

Tout d'abord, le **schéma** nécessaire doit être chargé sur un serveur **OpenLDAP** qui dispose d'une connectivité réseau avec les centres de distribution de clés primaires et secondaires (KDC). La suite de cette section considère que vous disposez aussi d'une réplication LDAP configurée entre au moins deux serveurs. Pour plus de détails concernant la configuration de OpenLDAP, voir le *Chapitre 7, paragraphe 1. Serveur OpenLDAP*.

Il est également nécessaire de configurer OpenLDAP pour les connexions TLS et SSL, de sorte que le trafic entre les serveurs KDC et LDAP soit chiffré. Voir le *Chapitre 7, paragraphe 1. Serveur OpenLDAP.8. TLS* pour plus de détails.

> C n=admin,cn=config est un utilisateur que nous avons créé avec les droits pour éditer la base de données ldap. De nombreuses fois, il est le RootDN. Modifiez sa valeur en fonction de vos réglages.

- Pour charger le schéma dans LDAP, installez le paquet **krb5-kdc-ldap** sur le serveur LDAP. Saisissez dans un terminal :

```
sudo apt install krb5-kdc-ldap
```

- Ensuite, décompressez le fichier kerberos.schema.gz :

```
sudo gzip -d /usr/share/doc/krb5-kdc-ldap/kerberos.schema.gz
sudo cp /usr/share/doc/krb5-kdc-ldap/kerberos.schema /etc/ldap/schema/
```

- Le schéma **Kerberos** doit être ajouté à l'arborescence **cn=config**. La procédure pour ajouter un nouveau schéma à **slapd** est également expliquée dans openldap-configuration.

1. Créez d'abord un fichier de configuration schema_convert.conf, ou tout autre nom vous convenant, avec les données suivantes :

```
include /etc/ldap/schema/core.schema
include /etc/ldap/schema/collective.schema
include /etc/ldap/schema/corba.schema
include /etc/ldap/schema/cosine.schema
```

```
include /etc/ldap/schema/duaconf.schema
include /etc/ldap/schema/dyngroup.schema
include /etc/ldap/schema/inetorgperson.schema
include /etc/ldap/schema/java.schema
include /etc/ldap/schema/misc.schema
include /etc/ldap/schema/nis.schema
include /etc/ldap/schema/openldap.schema
include /etc/ldap/schema/ppolicy.schema
include /etc/ldap/schema/kerberos.schema
```

2. Créez un dossier temporaire pour recevoir les fichiers LDIF :

```
mkdir /tmp/ldif_output
```

3. Maintenant, servez-vous de **slapcat** pour convertir les fichiers de schéma :

```
slapcat -f schema_convert.conf -F /tmp/ldif_output -n0 -s \
"cn={12}kerberos,cn=schema,cn=config" > /tmp/cn=kerberos.ldif
```

Modifiez si nécessaire le nom et l'emplacement du fichier.

4. Modifiez le fichier /tmp/cn\=kerberos.ldif généré, en changeant les attributs suivants :

```
dn : cn=kerberos,cn=schema,cn=config
...
cn : kerberos
```

Et supprimez les lignes suivantes à la fin du fichier :

```
structuralObjectClass : olcSchemaConfig
entryUUID : 18ccd010-746b-102d-9fbe-3760cca765dc
creatorsName : cn=config
createTimestamp : 20090111203515Z
entryCSN : 20090111203515.326445Z#000000#000#000000
modifiersName : cn=config
modifyTimestamp : 20090111203515Z
```

Les valeurs des attributs peuvent varier, assurez-vous simplement qu'ils soient supprimés.

5. Chargez le nouveau schéma avec **ldapadd** :

```
ldapadd -x -D cn=admin,cn=config -W -f /tmp/cn\=kerberos.ldif
```

6. Ajoutez un index pour l'attribut **krb5principalname** :

```
ldapmodify -x -D cn=admin,cn=config -W
```

```
Saisissez le mot de passe LDAP :
dn : olcDatabase={1}hdb,cn=config
add: olcDbIndex
olcDbIndex: krbPrincipalName eq,pres,sub
modifying entry "olcDatabase={1}hdb,cn=config"
```

7. Enfin, mettez à jour la liste de contrôle d'accès (ACL : Access Control Lists) :

```
ldapmodify -x -D cn=admin,cn=config -W
```

```
Saisissez le mot de passe LDAP :
dn : olcDatabase={1}hdb,cn=config
replace: olcAccess
olcAccess: to attrs=userPassword,shadowLastChange,krbPrincipalKey by
dn="cn=admin,dc=example,dc=com" write by anonymous auth by self write by *
none
-
add: olcAccess
olcAccess: to dn.base="" by * read
-
add: olcAccess
olcAccess: to * by dn="cn=admin,dc=example,dc=com" write by * read
modifying entry "olcDatabase={1}hdb,cn=config"
```

Voila, votre annuaire LDAP est maintenant prêt à servir de base de données de Donneur d'ordres Kerberos.

7.4.2. Configuration du KDC primaire

Avec **OpenLDAP** opérationnel, il est temps de configurer le KDC.

- Tout d'abord, installez les paquets nécessaires. Saisissez dans un terminal :

```
sudo apt install krb5-kdc krb5-admin-server krb5-kdc-ldap
```

- Maintenant, modifiez /etc/krb5.conf en ajoutant les options suivantes dans les sections appropriées :

```
[libdefaults]
        default_realm = EXAMPLE.COM

...

[realms]
        EXAMPLE.COM = {
                kdc = kdc01.example.com
                kdc = kdc02.example.com
                admin_server = kdc01.example.com
                admin_server = kdc02.example.com
                default_domain = example.com
                database_module = openldap_ldapconf
        }
```

```
...

[domain_realm]
        .example.com = EXAMPLE.COM


...

[dbdefaults]
        ldap_kerberos_container_dn = dc=example,dc=com

[dbmodules]
        openldap_ldapconf = {
                db_library = kldap
                ldap_kdc_dn = "cn=admin,dc=example,dc=com"

                # this object needs to have read rights on
                # the realm container, principal container and realm sub-trees
                ldap_kadmind_dn = "cn=admin,dc=example,dc=com"

                # this object needs to have read and write rights on
                # the realm container, principal container and realm sub-trees
                ldap_service_password_file = /etc/krb5kdc/service.keyfile
                ldap_servers = ldaps ://ldap01.example.com ldaps
://ldap02.example.com
                ldap_conns_per_server = 5
        }
```

Remplacez **example.com**, **dc=example,dc=com**, **cn=admin,dc=example,dc=com**, et **ldap01.example.com** par votre domaine, objet LDAP et serveur LDAP de votre réseau, respectivement.

- Ensuite, utilisez **kdb5_ldap_util** pour créer le domaine :

```
sudo kdb5_ldap_util -D cn=admin,dc=example,dc=com create -subtrees \
dc=example,dc=com -r EXAMPLE.COM -s -H ldap ://ldap01.example.com
```

- Créez un fichier de dissimulation (stash : mettre de côté) du mot de passe utilisé pour la liaison au serveur LDAP. Ce mot de passe est utilisé par les options **ldap_kdc_dn** et **ldap_kadmin_dn** du fichier /etc/krb5.conf :

```
sudo kdb5_ldap_util -D cn=admin,dc=example,dc=com stashsrvpw -f \
/etc/krb5kdc/service.keyfile cn=admin,dc=example,dc=com
```

- Copiez le certificat de l'AC depuis le serveur LDAP :

```
scp ldap01 :/etc/ssl/certs/cacert.pem .

sudo cp cacert.pem /etc/ssl/certs
```

Et modifiez /etc/ldap/ldap.conf pour utiliser le certificat :

```
TLS_CACERT /etc/ssl/certs/cacert.pem
```

Le certificat devra également être copié vers le KDC secondaire, afin de permettre la connexion aux serveurs LDAP en utilisant LDAPS.

Vous pouvez maintenant ajouter des utilisateurs Kerberos à la base de données LDAP et ils seront copiés aux autres serveurs LDAP configurés pour la réplication. Pour ajouter un utilisateur se servant de l'utilitaire **kadmin.local**, entrez :

```
sudo kadmin.local
```

```
Authenticating as principal root/admin@EXAMPLE.COM with password.
kadmin.local:     addprinc -x dn="uid=steve,ou=people,dc=example,dc=com" steve
WARNING: no policy specified for steve@EXAMPLE.COM; defaulting to no policy
Enter password for principal "steve@EXAMPLE.COM":
Re-enter password for principal "steve@EXAMPLE.COM":
Principal "steve@EXAMPLE.COM" created.
```

Les attributs krbPrincipalName, krbPrincipalKey, krbLastPwdChange, et krbExtraData devraient maintenant être ajoutés à l'objet utilisateur **uid=steve,ou=people,dc=example,dc=com**. Utilisez **kinit** et **klist** pour tester si l'utilisateur reçoit effectivement un ticket.

Si l'objet utilisateur est déjà créé, l'option **-x dn = "..."** est nécessaire pour ajouter les attributs de Kerberos. Autrement, un nouvel objet **utilisateur** sera créé dans les sous-domaines.

7.4.3. Configuration secondaire de KDC

Configurer un KDC secondaire en utilisant le moteur LDAP est semblable à une configuration utilisant la base de données Kerberos normale.

1. Tout d'abord, installez les paquets nécessaires. Saisissez dans un terminal :

```
sudo apt install krb5-kdc krb5-admin-server krb5-kdc-ldap
```

2. Ensuite, modifiez /etc/krb5.conf pour utiliser le moteur LDAP :

```
[libdefaults]
        default_realm = EXAMPLE.COM

...

[realms]
        EXAMPLE.COM = {
                kdc = kdc01.example.com
                kdc = kdc02.example.com
                admin_server = kdc01.example.com
                admin_server = kdc02.example.com
                default_domain = example.com
                database_module = openldap_ldapconf
        }

...
```

```
[domain_realm]
        .example.com = EXAMPLE.COM

...

[dbdefaults]
        ldap_kerberos_container_dn = dc=example,dc=com

[dbmodules]
        openldap_ldapconf = {
                db_library = kldap
                ldap_kdc_dn = "cn=admin,dc=example,dc=com"

                # this object needs to have read rights on
                # the realm container, principal container and realm sub-trees
                ldap_kadmind_dn = "cn=admin,dc=example,dc=com"

                # this object needs to have read and write rights on
                # the realm container, principal container and realm sub-trees
                ldap_service_password_file = /etc/krb5kdc/service.keyfile
                ldap_servers = ldaps ://ldap01.example.com ldaps
://ldap02.example.com
                ldap_conns_per_server = 5
        }
```

3. Créez un fichier de dissimulation (stash) pour y stocker le mot de passe de liaison à LDAP :

```
sudo kdb5_ldap_util -D cn=admin,dc=example,dc=com stashsrvpw -f \
/etc/krb5kdc/service.keyfile cn=admin,dc=example,dc=com
```

4. Maintenant, sur le **KDC principal**, copiez le fichier de dissimulation de la **clé maitresse**/etc/krb5kdc/.k5.EXAMPLE.COM sur le KDC secondaire. Assurez-vous de copier le fichier via une connexion chiffrée telle que **scp**, ou via des supports physiques.

```
sudo scp /etc/krb5kdc/.k5.EXAMPLE.COM steve@kdc02.example.com :~
sudo mv .k5.EXAMPLE.COM /etc/krb5kdc/
```

D e nouveau, remplacez **EXAMPLE.COM** par votre domaine réel.

5. De retour sur le **KDC secondaire**, (re-)démarrez seulement le serveur ldap,

```
sudo systemctl restart slapd.service
```

6. Enfin, démarrez le démon **krb5-kdc** :

```
sudo systemctl start krb5-kdc.service
```

7. Vérifiez que les deux serveurs ldap (et Kerberos par extension) sont synchronisés.

Vous avez maintenant des KDCs redondants sur votre réseau, et avec des serveurs LDAP redondants, vous devriez être en mesure de continuer à authentifier les utilisateurs si un serveur LDAP, un serveur Kerberos, ou un serveur LDAP et un serveur Kerberos deviennent indisponibles.

7.4.4. Ressources

Le Guide d'administration de Kerberos contient des détails supplémentaires : http://web.mit.edu/Kerberos/krb5-1.6/krb5-1.6.3/doc/krb5-admin.html#Configuring-Kerberos-with-OpenLDAP-back_002dend .

Pour plus d'informations sur **kdb5_ldap_util** voyez la **Section 5.6 :** http://web.mit.edu/Kerberos/krb5-1.6/krb5-1.6.3/doc/krb5-admin.html#Global-Operations-on-the-Kerberos-LDAP-Database et la page de man kdb5_ldap_util : http://manpages.ubuntu.com/manpages/xenial/en/man8/kdb5_ldap_util.8.html .

Un autre lien utile est la **page de man de krb5.conf** : http://manpages.ubuntu.com/manpages/xenial/en/man5/krb5.conf.5.html .

Vous pouvez également consulter la page de wiki Ubuntu sur **Kerberos et LDAP** : https://help.ubuntu.com/community/Kerberos#kerberos-ldap .

7.5. SSSD et Active Directory

Cette section décrit l'utilisation de sssd pour authentifier les connexions des utilisateurs sur un Active Directory à l'aide d'un fournisseur "ad" sssd. Dans les versions précédentes de sssd, il était possible de s'authentifier en utilisant le fournisseur "ldap". Cependant, lors de l'authentification sur un Contrôleur de Domaine Microsoft Windows AD, il est généralement nécessaire d'installer les extensions POSIX AD sur le Contrôleur de Domaine. Le fournisseur "ad" simplifie la configuration et ne nécessite aucune modification à la structure AD.

7.5.1. Prérequis, les hypothèses et exigences

- Ce guide n'explique pas Active Directory, ni comment il fonctionne, ni comment le paramétrer, ni comment le maintenir. Il ne fournit pas les « meilleures pratiques » pour votre environnement.
- Ce guide suppose qu'un domaine de travail Active Directory est déjà configuré.
- Le contrôleur de domaine agit comme un serveur DNS faisant autorité pour le domaine.
- Le contrôleur de domaine est le solveur DNS primaire comme spécifié dans /etc/resolv.conf.
- Le cas échéant les entrées **_kerberos**, **_ldap**, **_kpasswd**, etc. sont configurées dans la zone DNS (voir la section Ressources pour les liens externes).
- Le temps du système est synchronisé sur le contrôleur de domaine (nécessaire pour Kerberos).
- Le domaine utilisé dans cet exemple est **myubuntu.example.com**.

7.5.2. Installation

Les paquets suivants sont nécessaires : **krb5-user**, **Samba**, **sssd**, et **NTP**. Samba doit être installé, même si le système n'exporte pas de partages. Le domaine Kerberos et le Nom de Domaine Pleinement Qualifié (Fully Qualified Domain Names : FQDN) ou l'adresse IP des contrôleurs de domaine sont nécessaires pour cette étape.

Installez ces packages maintenant.

```
sudo apt install krb5-user samba sssd ntp
```

Voir la section suivante pour les réponses aux questions posées par le **krb5-user** script de post.

7.5.3. Configuration Kerberos

L'installation de **krb5-user** vous demandera le nom de domaine (en majuscules), le serveur KDC (ie le contrôleur de domaine) et le serveur d'administration (également le contrôleur de domaine dans cet exemple). Ceci écrira les sections [domaine] et [domain_realm] dans /etc/krb5.conf. Ces sections peuvent ne pas être nécessaire si l'option de recherche automatique (autodiscovery) de domaine est activée. Si cela n'est pa le cas, alors les deux sont nécessaires.

Si le domaine est **myubuntu.example.com**, entrez dans le domaine en tant que **MYUBUNTU.EXAMPLE.COM**

Facultativement, modifiez **/etc/krb5.conf** avec quelques paramètres supplémentaires pour spécifier le ticket à vie Kerberos (ces valeurs sont à utiliser comme paramètres par défaut sans risque) :

```
[libdefaults]

default_realm = MYUBUNTU.EXAMPLE.COM
ticket_lifetime = 24h #
renew_lifetime = 7d
```

Si default_realm n'est pas spécifié, il sera peut-être nécessaire de s'identifier avec "@domaine" au lieu de "".

Le temps du système sur l'élément Active Directory doit être cohérent avec celui du contrôleur de domaine, ou l'authentification Kerberos peut échouer. Idéalement, le serveur de contrôleur de domaine lui-même fournir le service NTP. Modifier /etc/ntp.conf :

```
server dc.myubuntu.example.com
```

7.5.4. Configuration de Samba

Samba sera utilisé pour effectuer les services NetBIOS/nmbd liés à l'authentification Active Directory, même si aucun partage de fichiers n'est exporté. Éditez le fichier /etc/samba/smb.conf et ajouter ce qui suit à la section **[global]** :

```
[global]

workgroup = MYUBUNTU
client signing = yes
client use spnego = yes
kerberos method = secrets and keytab
realm = MYUBUNTU.EXAMPLE.COM
security = ads
```

> Certains guides précisent que le "password server " devrait être précisé et souligné au contrôleur de domaine. Cela n'est nécessaire que si le DNS n'est pas correctement mis en place pour trouver la DC. Par défaut, Samba affichera un avertissement si "password server" est spécifié avec "security = ads".

7.5.5. Configuration SSSD

Il n'y a pas d'exemple de fichier de configuration par défaut (default/exemple) pour le fichier /etc/sssd/sssd.conf inclus dans le package de sssd. Il est nécessaire d'en créer un. Ceci est un fichier de configuration minimale de travail :

```
[sssd]
services = nss, pam
config_file_version = 2
domains = MYUBUNTU.EXAMPLE.COM

[domain/MYUBUNTU.EXAMPLE.COM]
id_provider = ad
access_provider = ad

# Use this if users are being logged in at /.
# This example specifies /home/DOMAIN-FQDN/user as $HOME. Use with pam_mkhomedir.so
override_homedir = /home/%d/%u

# Uncomment if the client machine hostname doesn’t match the computer object on the DC.
# ad_hostname = mymachine.myubuntu.example.com

# Uncomment if DNS SRV resolution is not working
# ad_server = dc.mydomain.example.com

# Uncomment if the AD domain is named differently than the Samba domain
# ad_domain = MYUBUNTU.EXAMPLE.COM

# Enumeration is discouraged for performance reasons.
# enumerate = true
```

Après avoir enregistré ce fichier, définir la propriété à root et les permissions de fichier à 600 :

```
sudo chown root :root /etc/sssd/sssd.conf
sudo chmod 600 /etc/sssd/sssd.conf
```

Si la propriété ou les autorisations ne sont pas correctes, sssd refusera de démarrer.

7.5.6. Vérification de la configuration de nsswitch.conf

Le script de post-installation pour le package de sssd fait quelques modifications du fichier /etc/nsswitch.conf automatiquement. Il devrait ressembler à quelque chose comme ceci :

```
passwd : compat sss
group : compat sss
...
netgroup : nis sss
sudoers : files sss
```

7.5.7. Modifier /etc/hosts

Ajouter un alias à l’entrée localhost dans /etc/hosts en précisant le FQDN. Par exemple :

```
192.168.1.10 myserver myserver.myubuntu.example.com
```

Ceci est utile en liaison avec mises à jour DNS dynamiques.

7.5.8. Rejoindre l'Active Directory

Maintenant, redémarrez NTP et samba et démarrer sssd.

```
sudo systemctl restart ntp.service
sudo systemctl start sssd.service
```

Testez la configuration en obtenant un ticket Kerberos :

```
sudo kinit Administrator
```

Vérifiez le ticket avec :

```
sudo klist
```

S'il y a un ticket avec une date d'expiration inscrite, alors il est temps de rejoindre le domaine :

```
sudo net ads join -k
```

Un avertissement sur "Aucun domaine DNS configuré. Impossible d'effectuer de mise à jour DNS." signifie probablement qu'il n'y a pas d'alias (correct) dans /etc/hosts, et le système ne pouvait pas fournir son propre FQDN dans le cadre de la mise à jour d'Active Directory. Ceci est nécessaire pour les mises à jour DNS dynamiques. Vérifiez l'alias dans /etc/hosts décrit dans "Modifier /etc/hosts " ci-dessus.

> Le message "NT_STATUS_UNSUCCESSFUL " indique que la jonction de domaine a échoué et que quelque chose est incorrect. Revoir les étapes préalables avant de continuer.

Voici un couple de contrôles (en option) pour vérifier que la jonction de domaine a été un succès. Notez que si le domaine a été rejoint avec succès, mais une ou deux de ces étapes échouent, il peut être nécessaire d'attendre 1-2 minutes et d'essayer à nouveau. Certains de ces changements semblent être asynchrone.

Vérification l'option # 1 :

Vérifiez l'Unité d'Organisation (Organizational Unit) par défaut des comptes d'ordinateurs dans Active Directory pour vérifier que le compte d'ordinateur a été créé. (les Unités d'organisation dans Active Directory est un sujet en dehors de la portée de ce guide).

Vérification l'option # 2 :

Exécutez cette commande pour un utilisateur spécifique de AD (par exemple, administrateur) :

```
getent passwd username
```

Si **enumerate = true** est configuré dans sssd.conf, **getent passwd** sans argument d' va lister tous les utilisateurs du domaine. Cela peut être utile pour les essais, mais il est lent et n'est pas recommandé pour la production.

7.5.9. Test d'Authentification

Il devrait maintenant être possible de s'authentifier en utilisant les informations d'identification d'un utilisateur Active Directory :

```
su - username
```

Si cela fonctionne, alors d'autres méthodes de connexion (getty, ssh) devraient également travailler.

Si le compte d'ordinateur a été créé, indiquant que le système a été "joint" au domaine, mais que l'authentification échoue, il peut être utile d'examiner /etc/pam.d et nssswitch .conf ainsi que les modifications de fichiers décrits précédemment dans ce guide.

7.5.10. Les répertoires personnels avec pam_mkhomedir (facultatif)

Lorsque vous vous connectez en utilisant un compte utilisateur Active Directory, c'est comme si l'utilisateur n'avait pas de répertoire personnel. Cela peut être résolu en utilisant pam_mkdhomedir.so, qui créera le répertoire personnel associé à la connexion. Éditez le fichier /etc/pam.d/common-session, et ajoutez cette ligne directement après **session required pam_unix.so** :

```
session required pam_mkhomedir.so skel=/etc/skel/ umask=0022
```

Cela nécessite aussi éventuellement d'écrire **override_homedir** dans le fichier sssd.conf pour fonctionner correctement, alors assurez-vous que cela est défini.

7.5.11. Authentification Ubuntu Desktop

Il est possible d'authentifier également les connexions à Ubuntu Desktop en utilisant les comptes Active Directory. Les comptes AD n'apparaîtront pas dans la liste de sélection avec les utilisateurs locaux, de sorte lightdm devra être modifié. Éditez le fichier /etc/lightdm/lightdm.conf.d/50-unity-greeter.conf et ajoutez les deux lignes suivantes :

```
greeter-show-manual-login=true
greeter-hide-users=true
```

Redémarrez pour relancer lightdm. Il devrait maintenant être possible de se connecter en utilisant un compte de domaine en utilisant l'un des deux formats : **username** ou **username/username@domain** .

7.5.12. Ressources

Le projet SSSD : https://fedorahosted.org/sssd

Les Directives de configuration de serveur DNS : http://www.ucs.cam.ac.uk/support/windows-support/winsuptech/activedir/dnsconfig

Zone d'Entrées DNS Active Directory : https://technet.microsoft.com/en-us/library/cc759550%28v=ws.10%29.aspx

Options de configuration Kerberos : http://web.mit.edu/kerberos/krb5-1.12/doc/admin/conf_files/krb5_conf.html

Chapitre 8. Service de nom de domaine (DNS)

Le service de nom de domaine (DNS) est un service Internet qui établit la correspondance entre les adresses IP et les noms de domaines pleinement qualifiés (FQDN : Fully Qualified Domain Name). Ainsi, le DNS évite d'avoir à se rappeler des adresses IP. Les ordinateurs sur lesquels s'exécutent les DNS sont appelés des **serveurs de nom**. Ubuntu est fourni avec **BIND** (Berkley Internet Naming Daemon), le programme le plus couramment utilisé pour gérer un serveur de nom sur Linux.

8.1. Installation

Pour installer le service **dns**, exécutez la commande suivante dans un terminal :

```
sudo apt install bind9
```

Le paquet **dnsutils** est très utile pour tester et dépanner les problèmes de DNS. Très souvent, ces outils seront déjà installés, mais afin de vérifier la présence et/ou d'installer **dnsutils**, saisissez ce qui suit :

```
sudo apt install dnsutils
```

8.2. Configuration

Il y a plusieurs façons de configurer **BIND9**. Certaines configurations les plus courantes sont un serveur cache, maître primaire, et comme un maître secondaire.

- Quand il est configuré en serveur de noms en mode cache, BIND9 effectuera les résolutions de noms et se souviendra de la réponse lorsque qu'un domaine sera demandé une nouvelle fois.
- En tant que serveur maître primaire, BIND9 lit les données d'une zone dans un fichier sur son serveur hôte et il fait autorité pour cette zone.
- En tant que maître secondaire, BIND9 obtient les données de la zone depuis le serveur de noms faisant autorité pour la zone.

8.2.1. Présentation

Les fichiers de configuration DNS sont situés dans le répertoire /etc/bind. Le fichier de configuration de base est /etc/bind/named.conf.

La ligne **include** spécifie le nom du fichier contenant les options DNS. La ligne **directory** dans le fichier /etc/bind/named.conf.options indique au DNS où chercher les fichiers. Tous les fichiers utilisés par BIND seront relatifs à ce répertoire.

Le fichier /etc/bind/db.root décrit les serveurs DNS racines mondiaux. Les serveurs changeant de temps à autre, il est nécessaire de mettre à jour ce fichier de temps en temps. Ceci est généralement effectué par des mises à jour du paquet **bind9**. La section **zone** définit le serveur maître, et est stockée dans le fichier spécifié par l'option **file**.

Il est possible de configurer un unique serveur comme serveur de noms en mode cache, maître primaire et maître secondaire. Un serveur peut faire autorité sur une zone (Start of Authority, SOA), tout en fournissant un service secondaire pour une autre zone, et en fournissant des services de cache pour les hôtes sur le LAN local.

8.2.2. Serveur de noms de cache

La configuration par défaut alloue un rôle de serveur cache. Il vous suffit d'ajouter les adresses IP des DNS de votre FAI. Dé-commentez simplement et modifiez ce qui suit dans /etc/bind/named.conf.options :

```
forwarders {
               1.2.3.4;
               5.6.7.8;
          };
```

R emplacez **1.2.3.4** et **5.6.7.8** par les adresses IP des véritables serveurs de noms.

Redémarrez à présent le serveur DNS pour appliquer les changements. Saisissez dans un terminal :

```
sudo systemctl restart bind9.service
```

Consultez le *Chapitre 8, paragraphe 3. Résolution des pannes.1.2. dig* pour plus d'informations à propos d'un serveur DNS cache.

8.2.3. Maître primaire

Dans cette section, **BIND9** sera configuré comme serveur primaire du domaine **example.com**. Remplacez **example.com** par votre FQDN (Fully Qualified Domain Name).

8.2.3.1. Fichier zone de recherche directe (Forward zone)

Pour ajouter une zone DNS à BIND9 afin de le transformer en serveur maître primaire, il faut tout d'abord modifier /etc/bind/named.conf.local :

```
zone "example.com" {
type master;
        file "/etc/bind/db.example.com";
};
```

Notez que si bind recevrait les mises à jour automatiques dans le fichier comme avec DDNS, alors utilisez /var/lib/bind/db.example.com au lieu de /etc/bind/db. example.com, à la fois ici et dans la commande de copie ci-dessous.

Nous utiliserons un fichier zone existant comme modèle pour la création du fichier /etc/bind/db.example.com :

```
sudo cp /etc/bind/db.local /etc/bind/db.example.com
```

Modifiez le nouveau fichier de zone /etc/bind/db.example.com Changez **localhost.** pour le FQDN de votre serveur, en laissant le "." supplémentaire" à la fin . Changez **127.0.0.1** pour l'adresse IP du serveur de noms et **root.localhost** pour une adresse de courriel valide, mais avec un "." au lieu de l'habituel symbole "@", ce qui laisse à nouveau le "." à la fin. Modifier le commentaire pour indiquer à quel domaine ce fichier est destiné.

Créer un **enregistrement A** pour le domaine de base, **exemple.com**. Également, créer un **enregistrement A** pour **ns.exemple.com**, avec le serveur de noms dans cet exemple :

```
;
; BIND data file for example.com
;
$TTL 604800
@ IN SOA example.com. root.example.com. (
                              2 ; Serial
                         604800 ; Refresh
                          86400 ; Retry
                        2419200 ; Expire
                         604800 ) ; Negative Cache TTL
```

```
        IN A 192.168.1.10
;
@ IN NS ns.example.com.
@ IN A 192.168.1.10
@ IN AAAA ::1
ns IN A 192.168.1.10
```

Vous devez incrémenter le **numéro de série (Serial Number)** à chaque fois que vous modifiez le fichier de zone. Si vous faites de multiples modifications avant de redémarrer BIND9, n'incrémentez le numéro qu'une seule fois.

Vous pouvez ajouter maintenant les enregistrements DNS à la fin du fichier de zone. Consultez le *Chapitre 8, paragraphe 4. Références.1. Types d'enregistrement communs* pour plus de détails.

De nombreux administrateurs aiment utiliser la date de dernière modification que le numéro de série d'une zone, comme **2012010100** qui est yyyymmddss (où **ss** est le numéro de série)

Une fois les modifications apportées au fichier de zone, **BIND9** doit être redémarré pour que les changements soient pris en compte :

```
sudo systemctl restart bind9.service
```

8.2.3.2. Fichier zone de recherche inverse(Reverse zone)

Maintenant que la zone est configurée pour résoudre les noms en adresses IP, il est nécessaire de paramétrer la **zone de recherche inverse**. Celle-ci permet de résoudre les adresses IP en noms.

Éditez le fichier /etc/bind/named.conf.local et ajoutez ce qui suit :

```
zone "1.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/db.192";
};
```

Remplacez **1.168.192** par les trois premiers octets du réseau que vous utilisez. Nommez également le fichier de zone /etc/bind/db.192 en conséquence. Il devrait correspondre au premier octet de votre réseau.

Créez maintenant le fichier /etc/bind/db.192 :

```
sudo cp /etc/bind/db.127 /etc/bind/db.192
```

Éditez ensuite /etc/bind/db.192 en changeant les mêmes options que dans /etc/bind/db.example.com :

```
;
; BIND reverse data file for local 192.168.1.XXX net
;
$TTL 604800
@    IN    SOA    ns.example.com.   root.example.com. (
```

```
                              2     ; Serial
                         604800     ; Refresh
                          86400     ; Retry
                        2419200     ; Expire
                         604800 )   ; Negative Cache TTL
;
@    IN    NS     ns.
10   IN    PTR    ns.example.com.
```

Le **numéro de série** dans la Zone Inverse (Reverse zone) doit être incrémenté à chaque changement aussi. Pour chaque Enregistrement A (**A record)** que vous configurez dans /etc/bind/db.example.com, c'est pour une adresse différente, vous devez créer un Enregistrement PTR dans / etc/bind/db.192.

Après avoir créé le fichier de zone de recherche inverse, redémarrez **BIND9** :

```
sudo systemctl restart bind9.service
```

8.2.4. Maître secondaire

Une fois que le **maître primaire** est paramétré il faut configurer un **maître secondaire** afin de maintenir la disponibilité du domaine en cas d'indisponibilité du serveur primaire.

Nous devons tout d'abord autoriser le transfert de zone sur le serveur maître primaire. Ajoutez l'option **allow-transfer** dans les exemples de définitions de zone de recherche directe et inverse du fichier /etc/bind/named.conf.local :

```
zone "example.com" {
        type master;
file "/etc/bind/db.example.com";
        allow-transfer { 192.168.1.11; };
};

zone "1.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/db.192";
allow-transfer { 192.168.1.11; };
};
```

R emplacez **192.168.1.11** par l'adresse IP de votre serveur de noms secondaire.

Redémarrez BIND9 sur le Primary Master:

```
sudo systemctl restart bind9.service
```

Installez ensuite le paquet **bind9** sur votre serveur maître secondaire de la même manière que pour le serveur primaire. Puis éditez le fichier /etc/bind/named.conf.local et ajoutez les déclarations suivantes pour les zones de recherche directe et inverse :

```
zone "example.com" {
type slave;
        file "db.example.com";
        masters { 192.168.1.10; };
```

```
};

zone "1.168.192.in-addr.arpa" {
type slave;
        file "db.192";
        masters { 192.168.1.10; };
};
```

R emplacez **192.168.1.10** par l'adresse IP de votre serveur de noms primaire.

Redémarrez **BIND9** sur votre serveur maître secondaire :

```
sudo systemctl restart bind9.service
```

Dans /var/log/syslog, vous devriez voir quelque chose de semblable à (certaines lignes ont été scindées afin de les adapter au format du document) :

```
client 192.168.1.10 # 39448: reçu notification pour la zone '1 .168.192 in-addr.arpa
'Nzone 1.168.192.in-addr.arpa/IN:... Transfert commencé
transfer de '100 .18.172 en- addr.arpa / IN 'à partir de 192.168.1.10 # 53:
raccordé à l'aide 192.168.1.11 # 37531
zone 1.168.192.in-addr.arpa/IN:. transféré série 5
transfer de '100 .18.172 en adr .arpa / IN 'à partir de 192.168.1.10 # 53:
Transfert terminé: 1 messages,
6 dossiers, 212 octets, 0,002 s (106000 bytes / sec)
zone 1.168.192.in-addr.arpa/IN: envoi notifie (série 5)

client 192.168.1.10 # 20329: reçu notification pour la zone 'example.com'
zone example.com / EN: Transfert commencé
transfer de 'example.com / IN' à partir de 192.168.1.10 #. 53: connecté à l'aide
192.168.1.11 # 38577
zone example.com / IN: transféré série 5
transfer de 'example.com / IN' à partir de 192.168.1.10 # 53: Transfert terminé: 1
messages,
8 dossiers, 225 octets, 0.002 secs (112500 bytes / sec)
```

Remarque: Une zone est seulement transféré si le numéro de série sur le primaire est plus grand que celui de la secondaire. Si vous voulez avoir votre serveur DNS maître primaire notifiant les changements de zone aux serveurs DNS secondaires, vous pouvez ajouter **also-notify {ipaddress;} ;** dans /etc/bind/named.conf.local comme indiqué dans l'exemple ci-dessous:

```
zone "example.com" {
type master;
file "/etc/bind/db.example.com";
allow-transfer { 192.168.1.11; };
also-notify { 192.168.1.11; };
};

zone "1.168.192.in-addr.arpa" {
type master;
file "/etc/bind/db.192";
allow-transfer { 192.168.1.11; };
```

```
also-notify { 192.168.1.11; };
};
```

Le répertoire par défaut pour les fichiers de zone non-autorisées est /var/cache/bind/ . Ce répertoire est également configuré dans **AppArmor** pour permettre au démon nommé d'y écrire. Pour plus d'informations sur AppArmor voir le *Chapitre 9, paragraphe 4. AppArmor*.

8.3. Résolution des pannes

Cette section aide à trouver la cause d'éventuels problèmes liés au DNS et à **BIND9**.

8.3.1. Essai

8.3.1.1. resolv.conf

La première étape de l'essai **BIND9** est d'ajouter l'adresse IP du serveur de noms à un solveur hôtes. Les serveurs de noms primaires doivent être configurés ainsi qu'un autre hôte pour doubler la vérification des paramètres. Reportez-vous au *Chapitre 4, paragraphe 1. Configuration du réseau.3.1. Configuration de client DNS* pour plus de détails sur l'ajout d'adresses de serveurs de noms pour les clients du réseau, et ensuite vérifier que le fichier /etc/resolv.conf contient (pour cet exemple) :

```
nameserver192.168.1.10
nameserver192.168.1.11
```

Les serveurs de noms qui écoutent l'adresse 127.* sont chargés d'ajouter leurs propres adresses IP pour resolv.conf (en utilisant resolvconf). Cela se fait via le fichier /etc/default/bind9 en changeant la ligne RESOLVCONF=no à RESOLVCONF=yes.

> Vous devriez ajouter aussi l'adresse IP du serveur de noms secondaire en cas d'indisponibilité du serveur primaire.

8.3.1.2. dig

Si vous avez installé le paquet **dnsutils**, vous pouvez tester votre configuration avec l'utilitaire de recherche DNS **dig** :

- Après avoir installé **BIND9**, utilisez **dig** sur l'interface loopback pour vous assurer qu'il écoute bien le port 53. Saisissez dans un terminal :

  ```
  dig -x 127.0.0.1
  ```

  Vous devriez obtenir un résultat similaire à ce qui suit :

  ```
  ;; Query time: 1 msec
  ;; SERVER: 192.168.1.10#53(192.168.1.10)
  ```

- Si vous avez configuré **BIND9** en tant que serveur de noms de **cache**, exécutez « dig » sur un domaine extérieur pour vérifier le temps de requête :

  ```
  dig ubuntu.com
  ```

  Notez le temps de réponse en fin de résultat :

  ```
  ;; Query time: 49 msec
  ```

Ce temps devrait être plus court après un deuxième « dig » :

```
;; Query time: 1 msec
```

8.3.1.3. ping

Maintenant, pour démontrer comment des applications se servent d'un DNS pour résoudre un nom d'hôte, utilisez **ping** pour envoyez une requête écho ICMP. Depuis un terminal, saisissez :

```
ping example.com
```

Ceci teste si le serveur de nom peut résoudre le nom **ns.example.com** en une adresse IP. Le retour de la commande output ressemble à ceci :

```
PING ns.exemple.com (192.168.1.10) 56(84) bytes of data.
64 bytes from 192.168.1.10: icmp_seq=1 ttl=64 time=0.800 ms
64 bytes from 192.168.1.10: icmp_seq=2 ttl=64 time=0.813 ms
```

8.3.1.4. named-checkzone

Un excellent moyen pour tester vos fichiers de zone est d'employer l'utilitaire **named-checkzone** installé avec le paquet **bind9**. Cet utilitaire vous permet de vous assurer que la configuration est correcte avant de redémarrer **BIND9** et d'appliquer les changements de façon permanente.

- Afin de vérifier notre fichier exemple de zone directe, entrez ce qui suit en ligne de commande :

```
named-checkzone example.com /etc/bind/db.example.com
```

Si tout est configuré correctement, vous devriez voir une sortie similaire à :

```
zone example.com/IN: loaded serial 6
OK
```

- De la même façon, afin de vérifier le fichier de Zone Inverse, entrez la commande :

```
named-checkzone 1.168.192.in-addr.arpa /etc/bind/db.192
```

La sortie devrait être semblable à :

```
zone 1.168.192.in-addr.arpa/IN: loaded serial 3
OK
```

L e **numéro de série** de votre fichier de zone sera probablement différent.

8.3.2. Journalisation

BIND9 dispose d'un large panel d'options de configuration de journalisation. Voici les deux principales. L'option **channel** définit où les journaux sont enregistrés, et l'option **category** détermine quelles informations y sont consignées.

Si aucune option de journalisation n'est configurée l'option par défaut est :

```
logging {
     category default { default_syslog; default_debug; };
     category unmatched { null; };
};
```

Cette section décrit comment paramétrer **BIND9** pour envoyer les messages de **débogage** concernant les requêtes DNS vers un fichier distinct.

- Premièrement, nous avons besoin de configurer un canal pour spécifier vers quel fichier envoyer les messages. Editez /etc/bind/named.conf.local et ajoutez ce qui suit :

  ```
  logging {
      channel query.log {
          file "/var/log/query.log";
          severity debug 3;
      };
  };
  ```

- Ensuite, configurez une catégorie pour envoyer toutes les requêtes DNS au fichier de requêtes :

  ```
  logging {
      channel query.log {
          file "/var/log/query.log";
    severity debug 3;
      };
      category queries { query.log; };
  };
  ```

  À noter : l'option **debug** peut prendre les valeurs 1 à 3. Si aucune valeur n'est spécifiée alors le niveau 1 est le niveau par défaut.

- Puisque le **démon nommé** est exécuté en tant qu'utilisateur **bind** le fichier /var/log/query.log doit être créé et le propriétaire changé :

  ```
  sudo touch /var/log/query.log
  sudo chown bind /var/log/query.log
  ```

- Il faut mettre à jour le profil **AppArmor** pour que le démon **named** puisse écrire dans le nouveau fichier journal. En premier, Editez /etc/apparmor.d/usr.sbin.named en ajoutant :

  ```
  /var/log/query.log w,
  ```

  Rechargez ensuite le profil :

  ```
  cat /etc/apparmor.d/usr.sbin.named | sudo apparmor_parser -r
  ```

  Pour plus d'informations sur **AppArmor** , référez-vous au *Chapitre 9, paragraphe 4. AppArmor*

- Redémarrez maintenant **BIND9** pour que les changements prennent effet :

```
sudo systemctl restart bind9.service
```

Vous devriez voir le fichier /var/log/query.log rempli d'informations de requêtes. Ceci est un exemple simple des options de journalisation de **BIND9**. Consultez le *Chapitre 8, paragraphe 4. Références.2 Informations supplémentaires* pour plus d'informations sur les options avancées.

8.4. Références

8.4.1. Types d'enregistrement communs

Cette section couvre les types d'enregistrement DNS les plus communs.

- Enregistrement **A** : cet enregistrement fait correspondre un nom d'hôte à une adresse IP.

  ```
  www IN A 192.168.1.12
  ```

- Enregistrement **CNAME** : utilisé pour créer un alias d'un enregistrement A. Il n'est pas possible de créer un enregistrement CNAME pointant vers un autre enregistrement CNAME.

  ```
  web IN CNAME www
  ```

- Enregistrement **MX** : utilisé pour définir où les courriels doivent être envoyés. Il doit pointer vers un enregistrement A, et non vers un CNAME.

  ```
          IN MX 1  mail.example.com.
  mail    IN A     192.168.1.13
  ```

- Enregistrement **NS** : utilisé pour définir les serveurs fournissant des copies d'une zone. Il doit pointer vers un enregistrement A, et non vers un CNAME. C'est ici que les serveurs Primaires et Secondaires sont définis.

  ```
          IN NS  ns.example.com.
          IN NS  ns2.example.com.
  ns      IN A   192.168.1.10
  ns2     IN A   192.168.1.11
  ```

8.4.2. Informations supplémentaires

La partie **BIND9 serveur HOWTO** dans le Wiki Ubuntu a beaucoup d'informations utiles : https://help.ubuntu.com/community/BIND9ServerHowto .

La partie **DNS HOWTO** du Projet de Documentation Linux a aussi beaucoup d'informations sur la configuration de Bind9 : http://www.tldp.org/HOWTO/DNS-HOWTO.html .

Le site **Bind9.net** a des liens avec une grande collection de ressources DNS et BIND9 : http://www.bind9.net/ .

Le livre **DNS et BIND** est un livre populaire maintenant dans sa cinquième édition : http://shop.oreilly.com/product/9780596100575.do . Il y a maintenant aussi un sujet sur **DNS BIND** du livre **IPv6** : http://shop.oreilly.com/product/0636920020158.do .

Un bon endroit pour demander de l'assistance pour **BIND9**, et être impliqué dans la communauté Ubuntu Serveur, est le canal IRC **#ubuntu-server** sur **freenode** : http://freenode.net .

Chapitre 9. Sécurité

La sécurité devrait toujours être considérée lors de l’installation, le déploiement et l’utilisation de différents types de système d’ordinateur, bien qu’une fraîche installation d’Ubuntu soit relativement sécurisée pour une utilisation immédiate d’internet. Il est important d’avoir une compréhension équilibrée de l’attitude de sécurité de votre système, basée sur comment il sera utilisé après le déploiement.

Ce chapitre fournit une vue d’ensemble des sujets liés à la sécurité concernant Ubuntu 16.04 LTS Server Edition, et suggère des mesures simples pour protéger votre serveur et votre réseau d’un certain nombre de possibles menaces de sécurité.

9.1. Gestion des utilisateurs

La gestion des utilisateurs est une partie cruciale de la sécurisation du système. Une gestion inefficace des utilisateurs et de leurs droits conduit souvent de nombreux systèmes a être corrompus. Il est donc fondamental de comprendre comment vous pouvez protéger votre serveur aux travers de techniques simples de gestion des comptes utilisateurs.

9.1.1. Où est la racine ?

Les développeurs Ubuntu ont choisi en conscience de désactiver par défaut le compte root pour toutes les versions d'Ubuntu. Ce qui ne signifie pas que le compte root ait été supprimé, ou qu'il ne soit pas accessible. Il lui a simplement été attribué un mot de passe qui ne correspond à aucune valeur chiffrée possible, on ne peut donc se connecter directement avec ce compte.

À la place, les utilisateurs sont invités à se servir d'un outil nommé **sudo** pour effectuer les tâches d'administration du système. **Sudo** permet à un utilisateur qui y est autorisé, d'étendre temporairement ses privilèges en saisissant son propre mot de passe plutôt que d'avoir à connaître celui du compte root. Cette méthode simple mais efficace permet de responsabiliser l'utilisateur pour toutes ses actions et permet à l'administrateur de contrôler finement les actions qu'un utilisateur peut effectuer avec lesdits privilèges.

- Si pour une raison quelconque vous voulez activer le compte root, donnez-lui tout simplement un mot de passe :

  L es configurations avec mot de passe racine ne sont pas prises en charge.

  sudo passwd

  Sudo vous demandera votre mot de passe, puis de fournir un nouveau mot de passe pour root, tel que présenté ci-dessous :

  ```
  [sudo] mot de passe pour l'utilisateur : (saisissez votre propre mot de passe)
  Saisissez un nouveau mot de passe UNIX : (saisissez un nouveau mot de passe pour root)
  Ressaisissez un nouveau mot de passe UNIX : (répétez le nouveau mot de passe pour root)
  passwd : mise à jour du mot de passe réussie
  ```

- Pour désactiver le mot de passe du compte root, utilisez la syntaxe de mot de passe suivante :

  sudo passwd -l root

- Enfin, pour désactiver le compte root en lui-même, utilisez la commande suivante :

  usermod --expiredate 1

- Vous trouverez plus d'information sur s**udo** dans le manuel manuel :

```
man sudo
```

Par défaut, l'utilisateur initial créé par l'installateur Ubuntu est un membre du groupe « **sudo** » qui est ajouté au fichier /etc/sudoers en tant qu'utilisateur sudo autorisé. Si vous souhaitez donner l'accès root complet à d'autres comptes par le biais de **sudo**, il suffit de les ajouter au groupe **sudo**.

9.1.2. Ajout et suppression d'utilisateurs

Le processus de gestion des utilisateurs et groupes locaux est direct et diffère très peu de la plupart des systèmes d'exploitation GNU/Linux. Ubuntu et les autres distributions fondées sur Debian encouragent l'utilisation du paquet « adduser » pour la gestion de comptes.

- Pour ajouter un compte utilisateur, utilisez la syntaxe ci-après, et suivez les instructions pour attribuer au compte un mot de passe et des caractéristiques identifiables, telles qu'un nom complet, un numéro de téléphone, etc.

```
sudo adduser username
```

- Pour supprimer un compte utilisateur et son groupe primaire, utilisez la syntaxe suivante :

```
sudo deluser username
```

La suppression d'un compte n'entraîne pas la suppression de son répertoire personnel. C'est à vous de décider si vous voulez ou non, supprimer ce dossier manuellement, en accord avec votre politique de conservation des données.

Notez bien que n'importe quel utilisateur ajouté par la suite avec le même UID/GID que le précédent propriétaire aura alors accès à ce dossier, si vous n'avez pas pris les précautions nécessaires.

Vous voudrez sans doute modifier ces valeurs des UID/GID pour quelque chose de plus approprié, telles que celles du compte root, et peut-être déplacer le dossier pour éviter de futurs conflits :

```
sudo chown -R root:root /home/username/
sudo mkdir /home/archives_utilisateurs/
sudo mv /home/username /home/archives_utilisateurs/
```

- Pour verrouiller ou déverrouiller temporairement un compte utilisateur, utilisez la syntaxe suivante, respectivement :

```
sudo passwd -l username
sudo passwd -u username
```

- Pour ajouter ou supprimer un groupe personnalisé, utilisez la syntaxe suivante, soit respectivement :

```
sudo addgroup nomgroupe
sudo delgroup nomgroupe
```

- Pour ajouter un utilisateur à un groupe, utilisez la syntaxe suivante :

```
sudo adduser username nomgroupe
```

9.1.3. Sécurité du profil utilisateur

Lorsqu'un utilisateur est créé, l'utilitaire adduser crée un tout nouveau répertoire appelé /home/username. Le profil par défaut prend pour modèle le contenu du répertoire /etc/skel, qui inclut tous les éléments de base du profil.

Si votre serveur héberge de multiples utilisateurs, vous devrez être particulièrement attentif aux droits d'accès des répertoires personnels pour assurer la confidentialité des données. Par défaut, les répertoires personnels sur Ubuntu sont créés avec des droits de lecture et d'exécution pour tout le monde. Ce qui signifie que tous les utilisateurs peuvent parcourir et lire les contenus des dossiers personnels des autres utilisateurs. Cela ne convient peut-être pas à votre configuration.

- Pour vérifier les droits d'accès dans le répertoire home en cours d'utilisation, utilisez la syntaxe suivante :

```
ls -ld /home/username
```

- L'ordinateur affiche alors que le répertoire /home/username contient des droits d'accès « lisible par tous » :

```
drwxr-xr-x 2 username username 4096 2007-10-02 20:03 /home/username
```

- Vous pouvez supprimer les droits d'accès « lisible par tous » en utilisant la syntaxe suivante :

```
sudo chmod 0750 /home/username
```

Certaines personnes ont tendance à utiliser aveuglément l'option de récursion (-R) qui modifie tous les sous-répertoires et fichiers. Ceci n'est pas nécessaires et peut conduire à des résultats indésirables. Agir sur le répertoire principal est suffisant pour empêcher les accès non autorisés à tout ce qui peut se trouver dedans.

- Une approche bien plus efficace pour ce problème serait de modifier globalement les droits d'accès établis par défaut par **adduser** lors de la création des répertoires personnels. Ouvrez simplement le fichier /etc/adduser.conf et changez la valeur de la variable **DIR_MODE** pour quelque chose d'approprié, ainsi les nouveaux dossiers utilisateurs auront les bons droits d'accès lors de leur création.

```
DIR_MODE=0750
```

- Après avoir corrigé les droits d'accès avec l'une des méthodes mentionnée précédemment, effectuez-en un contrôle avec la commande suivante :

ls -ld /home/username

Les résultats ci-dessous montrent que les droits d'accès « lisible par tous » ont été supprimés :

```
drwxr-x--- 2 username username 4096 2007-10-02 20:03 username
```

9.1.4. Politique des mots de passe

Avoir une politique rigoureuse des mots de passe est l'un des aspect les plus important de votre stratégie de sécurité. Des attaques de type force brute ou par dictionnaire contre des mots de passe faibles sont à l'origine de nombreuses intrusions. Si vous désirez ouvrir un accès distant (quel que soit son type) à votre système en utilisant votre mot de passe local, vous devez vous assurer que vous respectez des exigences minimales de complexité des mots de passe, des durées de vie des mots de passe limitées, et que vous effectuez des audits fréquents de vos systèmes d'authentification.

9.1.4.1. Longueur minimale du mot de passe

Par défaut, Ubuntu exige des mots de passe d'une longueur minimum de 6 caractères, ainsi que quelques contrôles d'entropie de base. Ces valeurs sont contrôlées dans le fichier /etc/pam.d/common-password, qui est expliqué ci-après.

```
password    [success=1 default=ignore]    pam_unix.so obscure sha512
```

Si vous souhaitez ajuster la longueur minimum à 8 caractères, vous pouvez changer la variable associée à min=8. La modification est expliquée ci-après.

```
password    [success=1 default=ignore]    pam_unix.so obscure sha512 minlen=8
```

Les contrôles basiques d'entropie du mot de passe et les règles de longueur minimales ne s'appliquent pas à l'administrateur lorsqu'il utilise des commandes de niveau sudo pour configurer un nouvel utilisateur.

9.1.4.2. Expiration du mot de passe

Lorsque vous créez des comptes utilisateurs, vous devriez vous fixer comme règle de définir une durée de vie minimale et maximale pour les mots de passe. Cela obligera les utilisateurs à changer leur mot de passe lorsqu'il arrive à expiration.

- Pour afficher facilement l'état actuel d'un compte utilisateur, utilisez la syntaxe suivante :

sudo chage -l username

La sortie ci-dessous montre des choses intéressantes sur le compte utilisateur, en fait aucune règle n'est appliquée :

```
Dernière modification du mot de passe : 20 Jan 2015
Expiration du mot de passe : jamais
Inactivation du mot de passe : jamais
Expiration du compte : jamais
Nombre minimum de jours entre deux modifications du mot de passe : 0
```

```
Nombre maximum de jours entre deux modifications du mot de passe : 99999
Nombre de jours d'avertissement avant expiration du mot de passe : 7
```

- Pour définir une de ces valeurs, utilisez simplement la syntaxe suivante et suivez les indications :

```
sudo chage username
```

En suivant, c'est aussi un exemple de comment vous pouvez changer manuellement la date d'expiration (-E) à 01/31/2015, l'âge minimum du mot de passe (-m) de 5 jours, l'âge maximum de mot de passe (-M) de 90 jours, la période d'inactivité (-I) de 5 jours après l'expiration du mot de passe, et une periode de temps d'alerte (-W) de 14 jours avant l'expiration du mot de passe :

```
sudo chage -E 01/31/2015 -m 5 -M 90 -I 30 -W 14 username
```

- Pour vérifier les modifications, utilisez la même syntaxe que celle mentionnée précédemment :

```
sudo chage -l username
```

La sortie ci-dessous indique les nouvelles règles qui ont été établies pour le compte :

```
Last password change                                    : Jan 20, 2015
Password expires                                        : Apr 19, 2015
Password inactive                                       : May 19, 2015
Account expires                                         : Jan 31, 2015
Minimum number of days between password change          : 5
Maximum number of days between password change          : 90
Number of days of warning before password expires       : 14
```

9.1.5. Autres considérations de sécurité

Un grand nombre d'applications utilisent d'autres mécanismes d'authentification qui peuvent facilement être négligés, même par des administrateurs système expérimentés. Par conséquent, il est important de comprendre et de contrôler la manière dont les utilisateurs s'authentifient et ont accès aux services et aux applications sur votre serveur.

9.1.5.1. Accès SSH par des utilisateurs désactivés

Le simple fait de désactiver/bloquer un compte utilisateur n'empêche pas un utilisateur de se connecter à distance à votre serveur s'ils ont auparavant configuré une authentification par clef publique RSA. Ils seront en mesure d'accéder au shell du serveur, sans avoir à saisir de mot de passe. Pensez à vérifier si les répertoires home des utilisateurs contiennent des fichiers qui permettraient ce type d'accès SSH authentifié, par exemple /home/username/.ssh/authorized_keys.

Supprimez ou renommez le dossier .ssh/ du répertoire personnel de l'utilisateur pour l'empêcher d'utiliser les capacités d'authentification SSH à l'avenir.

Vérifiez bien qu'aucune connexion SSH n'est établie par l'utilisateur désactivé, en effet il peut avoir une connexion entrante ou sortante active. Mettez fin à toutes celles que vous trouvez.

```
who | grep username (pour obtenir le terminal pts/#)
sudo pkill -f pts/#
```

Restreignez l'accès en SSH aux seuls comptes utilisateurs qui devrait l'avoir. Vous pouvez par exemple, créer un groupe nommé « sshlogin » et ajouter ce nom de groupe comme valeur à la variable **AllowGroups** située dans le fichier /etc/ssh/sshd_config.

```
AllowGroups sshlogin
```

Puis ajoutez vos utilisateurs SSH autorisés au groupe « sshlogin », et redémarrez le service SSH.

```
sudo adduser username sshlogin
sudo systemctl restart sshd.service
```

9.1.5.2. Authentification via une base de données utilisateurs externe

La plupart des réseaux d'entreprise exigent une authentification centralisée et des contrôles d'accès pour toutes les ressources système. Si vous avez configuré votre serveur pour authentifier les utilisateurs à travers des bases de données externes, assurez-vous de désactiver les comptes utilisateurs tant en externe que localement. Ainsi, vous vous assurez que toute authentification locale soit impossible.

9.2. Sécurité de la console

Comme avec n'importe quel autre barrière de sécurité que vous mettez en place pour protéger votre serveur, il est assez difficile de se défendre contre des dégâts inconnus causés par une personne ayant un accès physique à votre environnement, par exemple, le vol de disques durs, la perturbation de l'alimentation électrique ou de services, et ainsi de suite . Par conséquent, la sécurité de la console doit être envisagée comme une simple composante de votre stratégie globale de sécurité physique. Une « porte d'écran » verrouillée peut dissuader un criminel occasionnel ou à tout le moins en ralentir un plus déterminé, il est donc toujours conseillé de prendre des précautions de base en matière de sécurité de console.

Les instructions suivantes vous aideront à prémunir votre serveur contre des problèmes qui pourraient, le cas échéant, avoir de très graves conséquences.

9.2.1. Désactiver Ctrl+Alt+Suppr

N'importe qui ayant l'accès physique au clavier peut simplement utiliser la combinaison de touches **Ctrl+Alt+Delete** pour redémarrer le serveur sans avoir à se connecter. Tandis que quelqu'un pourrait simplement débrancher la prise de courant, vous devriez toujours éviter l'utilisation de cette combinaison de touches sur un serveur de production. Cela oblige un pirate à prendre des mesures plus radicales pour redémarrer le serveur, et permettra d'éviter des redémarrages accidentels dans le même temps.

Pour désactiver un reboot initié en appuyant sur **Ctrl+Alt+Delete**, exécutez les deux commandes suivantes :

```
sudo systemctl mask ctrl-alt-del.target
sudo systemctl daemon-reload
```

9.3. Pare-feu

9.3.1. Introduction

Le noyau Linux intègre le sous-système **Netfilter**, qui est utilisé pour manipuler ou décider du destin du trafic réseau arrivant, sortant ou passant par votre serveur. Tous les pare-feu modernes pour Linux utilisent ce système pour le filtrage des paquets.

Le système de filtrage de paquets du noyau serait peu utile aux administrateur sans une interface *userspace* pour le gérer. C'est l'objet d'**iptables** : quand un paquet atteint votre serveur, il est confié au sous-système Netfilter pour acceptation, manipulation ou rejet, sur la base de règles qui lui sont fournies par userspace via iptables. Ainsi, si vous êtes familiers avec iptables, vous n'avez besoin de rien d'autre pour gérer votre pare-feu, mais de nombreuses interfaces utilisateur sont disponibles pour simplifier cette tâche.

9.3.2. ufw - pare-feu simplifié

Sous Ubuntu, l'outil de configuration du pare-feu par défaut est **ufw**. Développé pour faciliter la configuration du pare-feu par iptables, **ufw** propose des manières conviviales de créer un pare-feu basé sur les hôtes IPv4 ou IPv6.

ufw est désactivé par défaut. D'après la page manuel de **ufw** :

> Ufw n'est pas conçu pour fournir une solution pare-feu complète via son interfaces de commandes, mais il propose d'ajouter ou de supprimer facilement des règles simples. Il est actuellement principalement utilisé pour des machines servant de pare-feu.

Voici quelques exemples d'utilisation de **ufw** :

- D'abord, **ufw** doit être activé. Depuis un terminal saisissez :

```
sudo ufw enable
```

- Pour ouvrir un port (SSH dans cet exemple) :

```
sudo ufw allow 22
```

- Les règles peuvent également être ajoutées en utilisant un format **numéroté** :

```
sudo ufw insert 1 allow 80
```

- De même, pour fermer un port ouvert :

```
sudo ufw deny 22
```

- Pour supprimer une règle, utilisez « delete » suivi de la règle :

```
sudo ufw delete deny 22
```

- Il est également possible d'autoriser l'accès à un port depuis des hôtes ou des réseaux spécifiques. L'exemple ci-après autorise l'accès SSH depuis l'hôte 192.168.0.2 à n'importe quelle adresse IP sur cet hôte :

```
sudo ufw allow proto tcp from 192.168.0.2 to any port 22
```

  Remplacez 192.168.0.2 par 192.168.0.0/24 pour accorder l'accès SSH à l'ensemble du sous-réseau.

- L'ajout de l'option **--dry-run** à la commande **ufw** affichera les règles sans les appliquer. Par exemple, voici ce qu'il faudrait faire pour ouvrir le port HTTP :

```
sudo ufw --dry-run allow http
```

```
*filter
:ufw-user-input - [0:0]
:ufw-user-output - [0:0]
:ufw-user-forward - [0:0]
:ufw-user-limit - [0:0]
:ufw-user-limit-accept - [0:0]
### RULES ###
### tuple ### allow tcp 80 0.0.0.0/0 any 0.0.0.0/0
-A ufw-user-input -p tcp --dport 80 -j ACCEPT
### END RULES ###
-A ufw-user-input -j RETURN
-A ufw-user-output -j RETURN
-A ufw-user-forward -j RETURN
-A ufw-user-limit -m limit --limit 3/minute -j LOG --log-prefix "[UFW LIMIT]: "
-A ufw-user-limit -j REJECT
-A ufw-user-limit-accept -j ACCEPT
COMMIT
Rules updated
```

- **ufw** peut être désactivé par :

```
sudo ufw disable
```

- Pour voir le statut du pare-feu, saisissez :

```
sudo ufw status
```

- Et pour des informations plus détaillées sur son statut, utilisez :

```
sudo ufw status verbose
```

- Pour voir le format **numéroté** :

```
sudo ufw status numbered
```

Si le port que vous voulez ouvrir ou fermer est défini dans /etc/services, vous pouvez utiliser le nom du port au lieu de son numéro. Dans les exemples ci-dessus, remplacez **22** par **ssh**.

Ceci est une introduction rapide à l'utilisation de **ufw**. Veuillez vous référer à la page de manuel de **ufw** pour plus d'informations.

9.3.2.1. Intégration du programme ufw

Les applications ouvrant des ports peuvent inclure un profil pour **ufw** qui renseigne les ports utilisés par ce programme pour fonctionner correctement. Les profils se conservés dans le répertoire /etc/ufw/applications.d et peuvent être modifiés si les ports par défaut ont été changés.

Pour voir quelles applications ont installé un profil, saisissez la commande suivante dans un terminal :

```
sudo ufw app list
```

De même que pour autoriser l'utilisation d'un port, on peut utiliser un profil pour un programme en écrivant :

```
sudo ufw allow Samba
```

Une syntaxe étendue est également disponible :

```
ufw allow from 192.168.0.0/24 to any app Samba
```

Remplacez **Samba** et **192.168.0.0/24** par le profil d'application que vous utilisez et la plage d'adresses IP de votre réseau.

> Il n'est pas utile de spécifier le **protocole** car cette information est renseignée dans le profil. Notez également que le nom **app** remplace le numéro de **port**.

- Pour voir des détails sur quels ports, protocoles, etc., sont définis pour une application, entrez :

```
sudo ufw app info Samba
```

Les applications nécessitant l'ouverture d'un port réseau ne sont pas forcément fournies avec des profils **ufw**, mais si vous avez profilé une application et voulez que le fichier soit inclut dans le paquet, veuillez signaler un bogue sur ce paquet dans Launchpad.

```
ubuntu-bug nomdupaquet
```

9.3.3. Masquage IP

Le but du masquage IP (forme de translation d'adresses) est de permettre à des machines d'un réseau doté d'adresses IP privées non traçables d'accéder à l'Internet en passant par une autre machine effectuant la translation. Le trafic sortant du réseau privé pour aller vers Internet doit être manipulé pour que les réponses

puissent être acheminées vers la machine qui a fait la requête correspondante. Pour cela, le noyau doit modifier l'adresse IP **source** de chaque paquet pour que les réponses lui soient renvoyées à lui plutôt qu'à l'adresse privée qui a fait la requête, ce qui est impossible sur l'Internet. Linux utilise **Connection Tracking** (conntrack) pour savoir à chaque instant quelle connexion appartient à quelle machine, et renvoyer par le même chemin ensuite les paquets vers la bonne machine. Le trafic sortant du réseau privé apparaît donc « masqué », comme s'il provenait de la passerelle Ubuntu. Ce procédé est appelé « Partage de connexion Internet » dans la documentation de Microsoft.

9.3.3.1. Masquage IP avec ufw

Le masquage IP peut être accompli en utilisant des règles **ufw** spécifiques. Ceci est possible car **ufw** se base actuellement sur **iptables-restore** avec des fichiers de règles situés dans /etc/ufw/*.rules. Ces fichiers sont le meilleur endroit pour ajouter des anciennes règles iptables sans passer par **ufw**, ainsi que des règles qui touchent au routage et aux ponts réseau.

Les règles sont scindées en deux fichiers différents, celles qui doivent être exécutées avant les règles en ligne de commande de **ufw** et celles qui doivent être exécutées après les règles en ligne de commande de **ufw**.

- Tout d'abord, la retransmission (forwarding) des paquets doit être activée dans **ufw**. Deux fichiers de configuration doivent être modifiés. Dans /etc/default/ufw ajustez la valeur de **DEFAULT_FORWARD_POLICY** à "ACCEPT" :

  ```
  DEFAULT_FORWARD_POLICY="ACCEPT"
  ```

  Éditez ensuite /etc/ufw/sysctl.conf et dé-commentez :

  ```
  net/ipv4/ip_forward=1
  ```

  De manière similaire, pour IPV6 dé-commentez :

  ```
  net/ipv6/conf/default/forwarding=1
  ```

- Maintenant, ajoutez des règles au fichier /etc/ufw/before.rules. Les règles par défaut configurent uniquement la table **filter**. Pour activer le camouflage des connexion, il faut configurer la table **nat**. Ajoutez les éléments suivants au début du fichier, juste après les commentaires d'en-tête :

  ```
  # règles pour le NAT
  *nat
  :POSTROUTING ACCEPT [0:0]

  # Retransmet le trafic de eth1 vers eth0.
  -A POSTROUTING -s 192.168.0.0/24 -o eth0 -j MASQUERADE

  # ne pas effacer « COMMIT » sinon les nouvelles règles ne seront pas prises en
  compte
  COMMIT
  ```

  Les commentaires ne sont pas strictement nécessaires, mais c'est une bonne habitude à prendre de documenter votre configuration. Vérifiez bien également, que lorsque vous modifiez l'un des fichiers **rules** dans /etc/ufw, ces lignes soient bien présentes à la fin de chaque table modifiée :

  ```
  # n'effacez pas « COMMIT » sinon ces règles ne seront pas traitées
  COMMIT
  ```

  Pour chaque **table** il est nécessaire de faire correspondre une déclaration **COMMIT**. Dans ces exemples seules les tables **nat** et **filter** sont décrites mais vous pouvez aussi ajouter des règles aux

tables **raw** et **mangle**.

Remplacez dans l'exemple ci-dessus **eth0**, **eth1** et **192.168.0.0/24** par vos propres interfaces et la plage d'IP pour votre réseau.

- Enfin, désactivez et réactivez **ufw** pour appliquer les modifications :

```
sudo ufw disable &amp;amp;&amp;amp; sudo ufw enable
```

Le masquage IP doit maintenant être activé. Vous pouvez également ajouter des règles FORWARD supplémentaires au fichier /etc/ufw/before.rules. Il est recommandé d'ajouter ces règles supplémentaires à la chaîne **ufw-before-forward**.

9.3.3.2. Masquage IP avec iptables

iptables peut aussi être utilisé pour activer le masquage.

- De même qu'avec **ufw**, la première étape consiste à activer la transmission de paquets IPv4 en éditant /etc/sysctl.conf et d'annuler le commentaire de la ligne :

  ```
  net.ipv4.ip_forward=1
  ```

- Si vous souhaitez activer la retransmission IPv6, décommentez également :

  ```
  net.ipv6.conf.default.forwarding=1
  ```

- Ensuite, exécutez la commande **sysctl** pour activer les nouveaux paramètres dans le fichier de configuration :
- sudo sysctl -p
- Le masquage IP peut maintenant être effectué avec une seule règle iptable, pouvant être légèrement différente 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 supposent que votre plage d'adresses privées 192.168.0.0/16 et que votre interface de connexion à l'Internet est ppp0. La syntaxe se décompose ainsi :

  - -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 spécifiée
  - -o ppp0 -- la règle s'applique au trafic devant être routé à travers l'interface réseau spécifiée
  - -j MASQUERADE -- le trafic correspondant à cette règle est « rejeté » (-j) vers la cible MASQUERADE pour être manipulé comme décrit ci-dessus

- Chaque chaîne de la table « filter » (la table par défaut où le filtrage des paquets a principalement lieu) a pour **règle** par défaut ACCEPT (accepter), mais si vous créez une machine pare-feu et routeur, vous avez peut-être défini les règles sur DROP (ignorer) ou REJECT (rejeter), dans ce cas le trafic masqué doit être autorisé avec la chaîne FORWARD pour que la règle ci-dessus fonctionne :

  ```
  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 ACCEPT
  ```

Les commandes ci-dessus autoriseront toutes les connexions depuis votre réseau local vers l'Internet et tout le trafic lié à ces connexions sera redirigé vers la machine qui l'a initié.

- Si vous souhaitez que le masquage IP soit activé au démarrage du serveur, modifiez /etc/rc.local et ajoutez les commandes utilisez ci-dessus. Par exemple, ajoutez la première commande sans filtrage :

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

9.3.4. Journaux

Les journaux du pare-feu sont essentiels pour identifier les attaques, résoudre les problèmes des règles du pare-feu, et remarquer une activité inhabituelle sur votre réseau. Vous devez inclure des règles d'écriture des journaux dans votre pare-feu pour qu'ils soient générés. Ces règles doivent être placées avant toute règle applicable de terminaison (une règle qui décide du sort des paquets, comme ACCEPT, DROP ou REJECT).

Si vous utilisez **ufw**, vous pouvez activer la journalisation en saisissant ce qui suit dans un terminal :

```
sudo ufw logging on
```

Pour désactiver la journalisation de **ufw**, remplacez simplement **on** par **off** dans la commande ci-dessus.

Si vous utilisez **iptables** au lieu de **ufw**, saisissez :

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

Une requête sur le port 80 de la machine locale, à ce moment là, générera un journal dans dmesg qui ressemble à ceci (une ligne unique divisée en 3 pour s'adapter à ce document) :

```
[4304885.870000] NEW_HTTP_CONN: IN=lo OUT=
MAC=00:00:00:00:00:00:00:00:00:00:00:00:08:00
SRC=127.0.0.1 DST=127.0.0.1 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=58288 DF PROTO=TCP
SPT=53981 DPT=80 WINDOW=32767 RES=0x00 SYN URGP=0
```

Le journal ci-dessus apparaîtra également dans /var/log/messages, /var/log/syslog, et /var/log/kern.log. Ce comportement peut être modifié en éditant /etc/syslog.conf de façon appropriée ou en installant et configurant **ulogd** en utilisant la cible ULOG au lieu de LOG. Le démon **ulogd** est un serveur d'espace utilisateur qui écoute les instructions de journalisation du noyau spécialement pour les pare-feu, et peut se connecter à n'importe quel fichier, ou base de données **PostgreSQL** ou encore **MySQL**. Donner du sens à vos journaux de pare-feu peut être simplifié en utilisant un analyseur de journalisation tel que **logwatch**, **fwanalog**, **fwlogwatch**, ou **lire**.

9.3.5. Autres outils

Il existe de nombreux outils pour vous aider à constituer un pare-feu complet sans connaissances particulières de iptables. Les outils en mode graphique :

fwbuilder est très puissant et semblera familier à un administrateur ayant déjà utilisé un pare-feu commercial comme Checkpoint FireWall-1 : http://www.fwbuilder.org/ .

Si vous préférez un outil en ligne de commande avec des fichiers de configuration en mode texte :

Shorewall est une solution très puissante pour vous aider à configurer un pare-feu avancé pour n'importe quel réseau : http://www.shorewall.net/ .

9.3.6. Références

La page de wiki **Pare-feu Ubuntu** contient des informations sur le développement de ufw : https://wiki.ubuntu.com/UncomplicatedFirewall .

La page de manuel **ufw** contient des informations très utiles : **man ufw**.

Voir **IPtables HOWTO en français** pour plus d'informations sur l'utilisation de iptables : http://www.nbs-system.com/dossiers/howto-iptables.html .

Le **guide pratique du NAT** contient plus de renseignements sur le masquage IP : http://www.linux-france.org/prj/inetdoc/guides/NAT-HOWTO/ .

La page du Wiki Ubuntu (en anglais) **IPTables HowTo** est également une très bonne source d'informations : https://help.ubuntu.com/community/IptablesHowTo .

9.4. AppArmor

AppArmor est une implémentation de contrôles d'accès obligatoires basée sur l'infrastructure LSM (Linux Security Module). AppArmor restreint les programmes individuels à un ensemble de fichiers répertoriés et de capacités définies dans l'ébauche POSIX 1003.1e.

AppArmor est installé et chargé en mémoire par défaut. Il utilise des **profils** d'une application afin de déterminer quels fichiers et quelles permissions l'application nécessite. Certains paquets installent leurs propres profils, et des profils additionnels se trouvent dans le paquet **apparmor-profiles**.

Pour installer le paquet **apparmor-profiles** depuis un terminal :

```
sudo apt install apparmor-profiles
```

Les profils d'AppArmor ont deux modes d'exécution :

- Réclamation/apprentissage : les infractions au profil sont autorisées et journalisées. C'est utile pour tester et développer de nouveaux profils.
- Imposé/restreint : la politique du profil est imposée et les infractions sont journalisées.

9.4.1. Utilisation d'AppArmor

Cette section souffre d'un bogue (**LP #1304134**) et les instructions ne fonctionneront pas comme annoncées : https://bugs.launchpad.net/ubuntu/+source/apparmor/+bug/1304134 .

Le paquet **apparmor-utils** contient des utilitaires en ligne de commande que vous pouvez utiliser pour changer le mode d'exécution d'**AppArmor**, trouver l'état d'un profil, créer de nouveaux profils, etc.

- **apparmor_status** est utilisé pour voir l'état actuel des profils d'AppArmor.

  ```
  sudo apparmor_status
  ```

- **aa-complain** place un profil en mode **complain** (réclamation).

  ```
  sudo aa-complain /chemin/vers/application
  ```

- **aa-enforce** place un profil en mode **enforce** (imposé).

  ```
  sudo aa-enforce /chemin/vers/application
  ```

- Le répertoire /etc/apparmor.d est l'endroit où se situent les profils d'AppArmor. Il peut être utilisé pour manipuler le **mode** de l'ensemble des profils.

  Saisissez ce qui suit pour placer tous les profils en mode complain (recommandation) :

```
sudo aa-complain /etc/apparmor.d/*
```

Pour placer tous les profils en mode enforce (imposé) :

```
sudo aa-enforce /etc/apparmor.d/*
```

- **apparmor_parser** est utilisé pour charger un profil dans le noyau. Il peut aussi être utilisé pour recharger un profil déjà chargé en utilisant l'option **-r**. Pour charger un profil :

```
cat /etc/apparmor.d/profile.name | sudo apparmor_parser -a
```

Pour recharger un profil :

```
cat /etc/apparmor.d/profile.name | sudo apparmor_parser -r
```

- systemctl peut être utilisé pour **actualiser** tous les profils :

```
sudo systemctl reload apparmor.service
```

- Le répertoire /etc/apparmor.d/disable peut être utilisé en même temps que l'option **apparmor_parser -R** pour **désactiver** un profil.

```
sudo ln -s /etc/apparmor.d/profile.name /etc/apparmor.d/disable/
sudo apparmor_parser -R /etc/apparmor.d/profile.name
```

Afin de **ré-activer** un profil désactivé, supprimez le lien symbolique vers le profil dans /etc/apparmor.d/disable/. Puis chargez le profil en utilisant l'option **-a**.

```
sudo rm /etc/apparmor.d/disable/profile.name
cat /etc/apparmor.d/profile.name | sudo apparmor_parser -a
```

- **AppArmor** peut être désactivé, et le module déchargé du noyau en entrant les lignes suivantes :

```
sudo systemctl stop apparmor.service
sudo update-rc.d -f apparmor remove
```

- Pour réactiver **AppArmor** saisissez :

```
sudo systemctl start apparmor.service
sudo update-rc.d apparmor defaults
```

Remplacez **profile.name** avec le nom du profil que vous souhaitez manipuler. Remplacez aussi /chemin/vers/application avec le chemin d'accès de l'exécutable en cours. Par exemple, pour la commande **ping** utilisez /bin/ping.

9.4.2. Les Profils

Les profils **AppArmor** sont de simples fichiers texte qui se trouvent dans /etc/apparmor.d/. Les fichiers portent le nom du chemin d'accès entier de l'exécutable dont ils sont les profils en remplaçant "/" par ".". Par exemple /etc/apparmor.d/bin.ping est le profil AppArmor de la commande /bin/ping.

Il existe deux grands types de règles utilisées dans les profils :

- **Path entries:** donne le détail de quels fichiers et quelles applications peuvent accéder au système de fichier.
- **Capability entries :** détermine les privilèges qu'un processus restreint est autoriser à utiliser.

Pour voir un exemple, consultez /etc/apparmor.d/bin.ping :

```
#include <tunables/global>
/bin/ping flags=(complain) {
#include <abstractions/base>
#include <abstractions/consoles>
#include <abstractions/nameservice>

capability net_raw,
capability setuid,
network inet raw,

/bin/ping mixr,
/etc/modules.conf r,
}
```

- **#include <tunables/global>:** directives d'inclusion d'autres fichiers. Ceci permet de placer dans un fichier commun les directives dépendant de plusieurs applications.
- **/bin/ping flags=(complain):** chemin de l'exécutable et réglage du mode sur **complain** (réclamation).
- **capability net_raw,:** autorise l'application à accéder à la fonctionnalité Posix 1e CAP_NET_RAW.
- **/bin/ping mixr,:** donne à l'application les droits de lecture et d'exécution sur le fichier.

Après modification d'un fichier de profil, le profil doit être rechargé. Consultez le *Chapitre 9, paragraphe 4. AppArmor.1. Utilisation d'AppArmor* pour plus de renseignements.

9.4.2.1. Création d'un profil

- **Conception d'un plan de test :** Réfléchissez à la manière dont l'application doit être examinée. Le plan de test devrait être divisé en test unitaires. Chaque test unitaire devrait avoir une courte description et énumérer les étapes à suivre.

  Quelques tests unitaires standard sont :

  - Démarrage du programme.
  - Arrêt du programme.
  - Rechargement du programme.
  - Test de toutes les commandes prises en charge par le script init.

- **Générer le nouveau profil :** Utilisez **aa-genprof** pour générer un nouveau profil. Depuis un terminal :

```
sudo aa-genprof executable
```

  Par exemple :

```
sudo aa-genprof slapd
```

- Pour que votre nouveau profil soit inclus dans le paquet **apparmor-profiles**, remplissez un rapport de bogue (en anglais) sur **Launchpad** concernant le paquet **AppArmor** : https://bugs.launchpad.net/ubuntu/+source/apparmor/+filebug :
  - Inclure votre plan de test et vos cas de test.
  - Joignez votre nouveau profil au rapport de bogue.

9.4.2.2. Mise à jour des profils

Lorsque le programme ne se comporte pas correctement, des messages d'audit sont journalisés. L'application **aa-logprof** peut être utilisée pour analyser les massages d'audit **AppArmor** dans les fichiers journaux. Examinez-les puis mettez à jour le profil. Dans un terminal :

```
sudo aa-logprof
```

9.4.3. Références

Voir **AppArmor Administration Guide** (en anglais) pour les options de configuration avancées : http://www.novell.com/documentation/apparmor/apparmor201_sp10_admin/index.html?page=/documentation/apparmor/apparmor201_sp10_admin/data/book_apparmor_admin.html .

Pour plus de détails sur l'utilisation d'AppArmor avec les autres versions d'Ubuntu, voir la page **AppArmor Community Wiki** (en anglais) http://doc.ubuntu-fr.org/apparmor ou la page AppArmor du Wiki francophone : https://help.ubuntu.com/community/AppArmor .

La page **Apparmor dans OpenSUSE** est une autre introduction à AppArmor : http://en.opensuse.org/SDB:AppArmor_geeks .

Un endroit fantastique pour demander de l'assistance sur **AppArmor**, et s'impliquer dans la communauté Ubuntu Server, est le canal IRC anglophone **#ubuntu-server** sur **le serveur freenode** : http://freenode.net .

9.5. Certificats

L'une des formes de cryptographie les plus répandues de nos jours est la cryptographie par **clé publique**. La cryptographie par clé publique utilise une **clé publique** et une **clé privée**. Ce système **chiffre** une information en utilisant une clé publique. L'information ne peut alors être **déchiffrée** qu'en utilisant la clé privée.

L'utilisation courante de clé publique de chiffrement est le camouflage du trafic d'application en utilisant une couche de prise sécurisée (SSL : Secure Socket Layer) ou une connexion par sécurité de couche de transport (TLS : Transport Layer Security). Un exemple : configurer Apache pour fournir **HTTPS**, le protocole HTTP par SSL. Cela permet de camoufler

Un **Certificat** est une méthode utilisée pour distribuer une **clé publique** ainsi que d'autres informations à propos d'un serveur et de l'organisation qui en est responsable. Les Certificats peuvent être signés numériquement par une **Autorité de Certification**, ou CA (Certification Authority). Une CA est une partie tiers de confiance qui a confirmé que l'information contenue dans le certificat est exacte.

9.5.1. Types de Certificats

Dans la plupart des cas, pour configurer un serveur sécurisé utilisant le chiffrement par clé publique, vous envoyez votre demande de certificat (avec votre clé publique) à l'autorité de certification, accompagnée d'une preuve de votre identité et de votre paiement. La CA vérifie votre identité et la demande de certificat, puis vous renvoie un certificat pour votre serveur sécurisé. Une alternative consiste a créer votre propre certificat **auto-signé**.

> Veuillez noter qu'un certificat auto-signé ne devrait pas être utilisé dans la plupart des environnements de production.

Pour continuer sur l'exemple de HTTPS, un certificat signé par une autorité de certification (CA) fournit deux fonctionnalités importantes absentes dans un certificat auto-signé :

- Les navigateurs reconnaissent (généralement) automatiquement le certificat et permettent l'établissement d'une connexion sécurisée sans intervention de l'utilisateur.
- Lorsqu'une autorité de certification (CA) émet un certificat, cela garantit l'identité de l'organisation qui fournit les pages Web au navigateur.

La plupart des navigateurs web et des ordinateurs, qui prennent en charge SSL ont une liste d'autorités de certification (CA) qu'ils acceptent automatiquement. Si un navigateur rencontre un certificat dont l'autorité de certification n'est pas dans la liste, le navigateur demande à l'utilisateur d'accepter ou de refuser la connexion. De plus, d'autres applications peuvent générer un message d'erreur lors de l'utilisation d'un certificat auto-signé.

Le processus d'acquisition d'un certificat signé par un CA est relativement simple et facile. En voici un survol rapide :

1. Créez une paire de clefs privé et publique.
2. Créez une demande de certificat basée sur la clé publique. La demande de certificat contient les informations concernant votre serveur et la société qui l'héberge.
3. Envoyez votre demande de certificat, avec les documents prouvant votre identité, à l'autorité de certification (CA). Nous ne pouvons pas vous dire quelle autorité de certification choisir. Votre décision peut être basée sur votre expériences passée, ou sur l'expérience de vos amis ou collègues, ou simplement sur des considérations financières.

Une fois l'autorité de certification choisie, vous devez suivre les instructions qu'ils vous ont indiquées pour obtenir un certificat de leur part.

4. Quand l'autorité de certification est sûre que vous êtes celui que vous prétendez être, elle vous envoie un certificat numérique.
5. Installez ce certificat sur votre serveur sécurisé, et configurez les applications appropriées pour utiliser le certificat.

9.5.2. Génération d'une demande de signature de certificat (Certificate Signing Request : CSR)

Que vous ayez obtenu votre certificat d'une autorité de certification, ou qu'il s'agisse d'un certificat auto-signé, la première étape consiste à générer une clé.

Si le certificat est destiné à être utilisé par des services, comme par exemple Apache, Postfix, Dovecot, etc., une clef sans phrase de passe est souvent appropriée. Le fait de ne pas avoir de phrase de passe permet aux services de se lancer sans intervention manuelle, ce qu'on attend généralement un service.

Cette section décrit la mise en place d'une clé avec et sans phrase de passe. La clé sans phrase de passe sera ensuite utilisée pour générer un certificat pouvant servir pour divers services ou démons.

> ! L'utilisation de votre service de sécurisé sans phrase de passe est utile car ces services peuvent démarrer sans que vous ayez à saisir cette phrase à chaque fois. Mais cela peut constituer une faille de sécurité pouvant mettre en danger tout le serveur.

Pour générer les **clés** pour une demande de signature de certificat (CSR), exécutez la commande suivante dans un terminal :

```
openssl genrsa -des3 -out server.key 2048
```

```
Generating RSA private key, 2048 bit long modulus
.........................++++++
.......++++++
e is 65537 (0x10001)
Enter pass phrase for server.key:
```

Vous pouvez maintenant saisir votre mot de passe. Pour une meilleure sécurité, il doit contenir au minimum huit caractères. La longueur minimum lorsque vous spécifiez -des3 (algorithme de cryptographie) est de quatre caractères. Il devrait contenir des chiffres et/ou des signes de ponctuation et ne pas se trouver dans un dictionnaire de mots. Rappelez vous également que votre mot de passe est sensible à la casse (NdT : au sens typographique majuscules/minuscules).

Ressaisissez le mot de passe pour vérification. Lorsque vous l'avez retapé correctement, la clé du serveur est générée et stockée dans le fichier server.key.

Créez maintenant le clef non sécurisée (celle sans phrase de passe) et échangez le nom des clés :

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

La clé non sécurisée se nomme maintenant server.key et vous pouvez utiliser ce fichier pour générer le CSR sans saisir de mot de passe.

Pour créer la CSR, lancer la commande suivante dans un terminal :

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

Il vous sera alors demandé d'entrer la phrase de passe. Si elle est correcte, il vous sera alors demandé d'entrer le nom de l'entreprise, le nom du site, courriel, etc. Une fois toutes ces informations renseignées, votre CSR sera créé et conservé dans le fichier server.csr.

Vous pouvez maintenant soumettre ce fichier CSR à une autorité de certification (CA) pour traitement. La CA utilisera ce fichier CSR et émettra le certificat. D'un autre côté, vous pouvez créer un certificat auto-signé en utilisant ce CSR.

9.5.3. Création d'un certificat auto-signé (Self-Signed Certificate : SSC)

Pour créer le certificat auto-signé, utilisez la commande suivante dans un terminal :

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

La commande ci-dessus vous demandera de saisir votre mot de passe. Une fois le mot de passe correct saisi, votre certificat sera créé et stocké dans le fichier server.crt.

> ! Si votre serveur sécurisé doit être utilisé dans un environnement de production, vous avez probablement besoin d'un certificat signé par une autorité de certification. Il n'est pas recommandé d'utiliser un certificat auto-signé.

9.5.4. Installation du certificat

Vous pouvez installer le fichier de clé server.key et le fichier de certificat server.crt, ou le fichier de certificat émis par votre autorité de certification, en exécutant les commandes suivantes dans un terminal :

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

Vous devez maintenant simplement configurer les applications ayant la capacité d'utiliser le chiffrement par clé publique, pour qu'elles utilisent les fichiers de **certificat** et de **clé**. Par exemple, **Apache** peut servir les documents en HTTPS, **Dovecot** peut servir le courrier en IMAPS et POP3S, etc.

9.5.5. Autorité de certification

Si les services de votre réseau nécessitent plusieurs certificats, il peut être intéressant de mettre en place votre propre **autorité de certification (AC)** interne. En effet, cela permet aux différents services utilisant des certificats de faire confiance aisément aux autres services utilisant des certificats émis par la même AC.

1. Créez d'abord les répertoires qui hébergeront le certificat de l'AC et ses divers fichiers :

```
sudo mkdir /etc/ssl/CA
sudo mkdir /etc/ssl/newcerts
```

2. L'AC a besoin de quelques fichiers supplémentaires pour être opérationnelle. Un pour garder trace du dernier numéro de série utilisé par l'AC (chaque certificat doit avoir un numéro de série distinct) et un autre pour garder trace des certificats générés :

```
sudo sh -c "echo '01' > /etc/ssl/CA/serial"
sudo touch /etc/ssl/CA/index.txt
```

3. Le troisième fichier est celui des paramètres de l'AC. Bien qu'il ne soit pas strictement nécessaire, il est utile lors de la génération de plusieurs certificats. Modifiez /etc/ssl/openssl.cnf et changez la déclaration **[CA_default]** :

```
dir             = /etc/ssl                  # Where everything is kept
database        = $dir/CA/index.txt         # database index file.
certificate     = $dir/certs/cacert.pem     # The CA certificate
serial          = $dir/CA/serial            # The current serial number
private_key     = $dir/private/cakey.pem    # The private key
```

4. Ensuite, créez le certificat racine auto-signé :

```
openssl req -new -x509 -extensions v3_ca -keyout cakey.pem -out cacert.pem
-days 3650
```

   Il vous sera demandé de donner les renseignements concernant le certificat.

5. Installez maintenant le certificat racine et la clef :

```
sudo mv cakey.pem /etc/ssl/private/
sudo mv cacert.pem /etc/ssl/certs/
```

6. Vous êtes maintenant prêts à signer des certificats. Le premier élément nécessaire est un Certificate Signing Request (CSR) (plus de détails sont disponibles au *Chapitre 9, paragraphe 5. Certificats.2. Génération d'une demande de signature de certificat*). Une fois que vous avez un CSR, entrez ce qui suit pour générer un certificat signé par le CA :

```
sudo openssl ca -in server.csr -config /etc/ssl/openssl.cnf
```

   Après avoir saisi un mot de passe pour la clé de l'AC, il vous sera demandé de signer le certificat. Une somme importante de données défileront ensuite à l'écran durant la création du certificat.

7. Il devrait maintenant y avoir un nouveau fichier, /etc/ssl/newcerts/01.pem, contenant la même sortie. Copiez et collez toutes les lignes à partir de : **-----BEGIN CERTIFICATE-----** jusqu'à la ligne : **-----END CERTIFICATE-----** dans un fichier nommé selon le nom d'hôte du serveur ou le certificat sera installé. Par exemple courriel.exemple.com.crt est un nom suffisamment précis.

   Les certificats suivants seront nommés 02.pem, 03.pem etc.

R emplacez **mail.exemple.com.crt** par le nom correspondant à votre nom d'hôte.

8. Pour finir, copier le nouveau certificat vers son hôte et paramétrez les programmes devant l'utiliser. L'endroit par défaut pour installer les certificats est directory /etc/ssl/certs. Cela permet à de multiples services d'utiliser le même certificat sans compliquer de trop la gestion des droits d'accès aux fichiers.

   Pour les applications pouvant être paramétrés pour utiliser un certificat issu d'une AC, vous devriez copier aussi le fichier /etc/ssl/certs/cacert.pem vers le répertoire /etc/ssl/certs/ de chaque serveur.

9.5.6. Références

Pour des instructions plus détaillées sur l'utilisation de la cryptographie, voir le **guide pratique SSL Certificates** de tldp.org : http://tldp.org/HOWTO/SSL-Certificates-HOWTO/index.html

La page **HTTPS** de Wikipedia présente davantage d'informations sur HTTPS : http://en.wikipedia.org/wiki/HTTPS .

Pour plus d'informations sur **OpenSSL** consultez le **site Web de OpenSSL** : http://www.openssl.org/ .

La page **Network Security with OpenSSL** d'O'Reilly est une bonne référence détaillée : http://oreilly.com/catalog/9780596002701/ .

9.6. eCryptfs

eCryptfs système de fichiers chiffré empilés « entreprise de classe compatible » POSIX pour Linux. Positionner la couche **eCryptfs** au plus haut des couches du système de fichiers protège les fichiers, peu importe le système de fichiers sous-jacent, le type de partition, etc...

Lors de l'installation, il y a une option pour chiffrer la partition /home. Cela configurera automatiquement tout ce qu'il faut pour chiffrer la partition mais aussi pour la monter.

A titre d'exemple, cette section traitera de la configuration de /srv afin qu'il soit crypté en utilisant **eCryptfs**.

9.6.1. Utilisation de eCryptfs

Installez d'abord les paquets nécessaires. Saisissez dans un terminal :

```
sudo apt install ecryptfs-utils
```

Montez la partition à chiffrer :

```
sudo mount -t ecryptfs /srv /srv
```

Des renseignements sur la manière dont **ecryptfs** doit chiffrer des données vont vous être demandés.

Pour vérifier que les données de /srv sont effectivement chiffrées, copiez le répertoire /etc/default vers /srv :

```
sudo cp -r /etc/default /srv
```

Démontez /srv et essayez de lire un fichier :

```
sudo umount /srv
cat /srv/default/cron
```

Vous pourrez lire à nouveau les données une fois que vous aurez remonté /srv en utilisant **ecryptfs**.

9.6.2. Monter automatiquement les partitions chiffrées

Plusieurs méthodes sont disponibles pour monter automatiquement au démarrage un système de fichiers chiffré avec **ecryptfs.**

- Créez d'abord /root/.ecryptfsrc contenant les informations suivantes :

```
key=passphrase:passphrase_passwd_file=/mnt/usb/fichier_avec_phrase_de_passe.txt
ecryptfs_sig=5826dd62cf81c615
ecryptfs_cipher=aes
ecryptfs_key_bytes=16
ecryptfs_passthrough=n
```

```
ecryptfs_enable_filename_crypto=n
```

F aites correspondre **ecryptfs_sig** avec la signature se trouvant dans /root/.ecryptfs/sig-cache.txt.

- Créez ensuite le fichier de phrase de passe /mnt/usb/fichier_avec_mot_de_passe.txt :

  ```
  passphrase_passwd=[secrets]
  ```

- Ajouter les lignes nécessaires dans /etc/fstab :

  ```
  /dev/sdb1 /mnt/usb ext3 ro 0 0
  /srv /srv ecryptfs defaults 0 0
  ```

  Assurez-vous que le périphérique USB est monté avant la partition chiffrée.

- Enfin, redémarrez et /srv devrait être monté à l'aide de **eCryptfs**.

9.6.3. Autres utilitaires

Le paquet **ecryptfs-utils** contient d'autres utilitaires :

- **ecryptfs-setup-private :** crée un répertoire ~/Private recevant les informations chiffrées. Cet utilitaire peut être lancé par de simples utilisateurs (sans privilèges) pour chiffrer leur données.
- **ecryptfs-mount-private** et **ecryptfs-umount-private** monteront et démonteront un répertoire d'utilisateur ~/Private.
- **ecryptfs-add-passphrase :** ajoute une nouvelle phrase de passe au trousseau de clés du noyau.
- **ecryptfs-manager :** gère les objets **eCryptfs** tels que les clés.
- **ecryptfs-stat :** vous permet de voir les méta-informations **ecryptfs** d'un fichier.

9.6.4. Références

Pour plus d'informations sur **eCryptfs**, voir la **page du projet Launchpad** : https://launchpad.net/ecryptfs .

Il y a aussi un article de **Linux Journal** traitant de eCryptfs : http://www.linuxjournal.com/article/9400 .

Également, pour plus d'options **ecryptfs** et des détails, consultez la **page de man ecryptfs** : http://manpages.ubuntu.com/manpages/xenial/en/man7/ecryptfs.7.html .

Chapitre 10. Surveillance

10.1. Vue d’ensemble

La supervision des serveurs et services primordiaux est une part importante de l’administration système. La plupart des services réseaux sont sous surveillance pour leurs performances, leur disponibilité, voire les deux. Cette section couvre l’installation et la configuration de **Nagios** pour la surveillance de la disponibilité et **Munin** pour les performances.

Les exemples dans cette section utilisent deux serveurs nommés **server01** et **server02**. **Server01** sera configuré avec **Nagios** pour superviser les services des deux serveurs. Le service **Munin** sera également installé et configuré sur **server01** afin de récolter des informations depuis le réseau. On installera et configurera alors le paquet **munin-node** sur **server02** pour envoyer ces informations au **server01**.

Espérons que ces exemples simples vous permettront de superviser des serveurs et services supplémentaires sur votre réseau.

10.2. Nagios

10.2.1. Installation

Tout d'abord, installez le paquet **nagios** sur **serveur01**. Dans un terminal, saisissez :

```
sudo apt install nagios3 nagios-nrpe-plugin
```

Il vous sera alors demandé d'entrer un mot de passe pour l'utilisateur **nagiosadmin**. Les droits d'accès des utilisateurs sont conservés dans le fichier /etc/nagios3/htpasswd.users. Pour changer le mot de passe de **nagiosadmin**, ou ajouter d'autres utilisateurs aux scripts CGI de Nagios, utilisez **htpasswd**, qui fait partie du paquet **apache2-utils**.

Par exemple, pour changer le mot de passe de l'utilisateur **nagiosadmin**, entrez :

```
sudo htpasswd /etc/nagios3/htpasswd.users nagiosadmin
```

Pour ajouter un utilisateur :

```
sudo htpasswd /etc/nagios3/htpasswd.users steve
```

Ensuite, sur **serveur02**, installez le paquet **nagios-nrpe-server**. Depuis un terminal sur serveur02, entrez :

```
sudo apt install nagios-nrpe-server
```

N **RPE** vous permet d'exécuter des vérifications locales sur des hôtes distants. Il existe d'autres façons d'accomplir ces vérifications, ainsi que d'autres, grâce à d'autres greffons de Nagios.

10.2.2. Vue d'ensemble de la configuration

Il y a plusieurs répertoires contenant les fichiers de configuration et de tests de **Nagios**.

- /etc/nagios3 : contient les fichiers de configuration pour l'exécution du démon **nagios**, des fichiers CGI, des hôtes, etc.
- /etc/nagios-plugins : héberge les fichiers de configuration pour les vérifications du service.
- /etc/nagios : sur l'hôte distant, contient les fichiers de configuration de **nagios-nrpe-server**.
- /usr/lib/nagios/plugins/ : où les fichiers binaires vérifiés sont conservés. Pour consulter les options de vérification, utilisez l'option **-h**.

Par exemple: **/usr/lib/nagios/plugins/check_dhcp -h**

Nagios peut être configuré pour exécuter une pléthore de vérifications pour n'importe quel hôte donné. Pour cet exemple Nagios sera configuré pour vérifier l'espace disque, les DNS, et un groupe d'hôtes MySQL. Le contrôle des DNS sera fait sur **server02**, et le groupe d'hôtes MySQL contiendra **server01** et **server02**.

Voir le Chapitre *11, paragraphe 1. HTTPD - serveur web Apache2* pour les détails concernant la préparation d'Apache, le *Chapitre 8. Service de nom de domaine (DNS)* pour DNS, et le *Chapitre 12, paragraphe 1. MySQL* pour MySQL.

En complément, voici quelques termes qui, une fois expliqués, faciliteront la compréhension de la configuration de Nagios :

- **Hôte** : un serveur, une station de travail, un périphérique réseau, etc., qui est en train d'être contrôlé.
- **Groupe d'hôtes** : un groupe d'hôtes similaires. Par exemple, vous pourriez grouper tous les serveurs web, les serveurs de fichiers, etc.
- **Service** : le service qui est en train d'être contrôlé sur l'hôte. Comme HTTP, DNS, NFS, etc.
- **Groupe de services** : vous permet de grouper plusieurs services ensemble. Ceci est utile pour regrouper plusieurs HTTP.
- **Contact** : personne à prévenir quand un événement se produit. Nagios peut être configuré pour envoyer des courriels, des SMS, etc.

Par défaut, Nagios est configuré pour vérifier HTTP, l'espace disque, SSH, les utilisateurs actuels, les processus, et la charge de **l'hôte local**. Nagios lancera aussi un **ping** de vérification sur la **passerelle**.

Les grosses installations de Nagios peuvent s'avérer compliquées à configurer. Il est généralement plus sage de commencer par une petite installation d'un ou deux hôtes, et de la configurer comme vous l'entendez avant de l'agrandir.

10.2.3. Configuration

1. Tout d'abord, créez un fichier de configuration **hôte** pour **serveur02**. Sauf indication contraire, exécuter toutes ces commandes sur **serveur01**. Dans un terminal saisissez :

```
sudo cp /etc/nagios3/conf.d/localhost_nagios2.cfg \
/etc/nagios3/conf.d/server02.cfg
```

Dans les exemples de commandes ci-dessus et ci-dessous, remplacez **« serveur01 »**, **« serveur02 »** **172.18.100.100** et **172.18.100.101** par les noms et les adresses IP de vos serveurs.

2. Ensuite, éditez /etc/nagios3/conf.d/serveur02.cfg:

```
define host{
        use                     generic-host     ; Name of host template to use
        host_name               server02
        alias                   Server 02
        address                 172.18.100.101
}

# check DNS service.
define service {
        use                     generic-service
        host_name               server02
        service_description     DNS
        check_command           check_dns!172.18.100.101
}
```

3. Relancez le démon **nagios** pour activer la nouvelle configuration :

```
sudo systemctl restart nagio3.service
```

1. Maintenant, définissez un nouveau service pour la vérification de MySQL, en ajoutant ceci au fichier /etc/nagios3/conf.d/services_nagios2.cfg :

```
# check MySQL servers.
define service {
        hostgroup_name       mysql-servers
        service_description  MySQL
        check_command        check_mysql_cmdlinecred!nagios!secret!$HOSTADDRESS
        use                  generic-service
        notification_interval 0 ; set > 0 if you want to be renotified
}
```

2. Maintenant, Il faut définir un groupe d'hôtes **mysql-servers**. Modifiez /etc/nagios3/conf.d/hostgroups_nagios2.cfg en y ajoutant :

```
# Groupe d'hôtes MySQL.
define hostgroup {
        hostgroup_name       mysql-servers
                alias              MySQL serveurs
                members            localhost, serveur02
        }
```

3. La vérification de Nagios a besoin de s'authentifier auprès de MySQL. Pour ajouter **nagios** en tant qu'utilisateur de MySQL, entrez :

```
mysql -u root -p -e "create user nagios identified by 'secret';"
```

L 'utilisateur **nagios** devra être ajouté pour tous les hôtes du groupe **mysql-servers**.

4. Redémarrez **nagios** pour commencer à vérifier les serveurs MySQL.

```
sudo systemctl restart nagios3.service
```

1. Enfin, configurez NRPE pour vérifier l'espace disque sur **serveur02**.

   Sur **serveur01** ajoutez le service de vérification dans /etc/nagios3/conf.d/serveur02.cfg :

```
# NRPE disk check.
define service {
        use                         generic-service
        host_name                   server02
        service_description         nrpe-disk
        check_command               check_nrpe_1arg!check_all_disks!172.18.100.101
}
```

2. Maintenant sur **serveur02**, modifiez /etc/nagios/nrpe.cfg en y changeant :

```
allowed_hosts=172.18.100.100
```

Et dessous, dans la zone de définition de commande, ajoutez :

```
command[check_all_disks]=/usr/lib/nagios/plugins/check_disk -w 20% -c 10% -e
```

3. Pour finir, redémarrez **nagios-nrpe-server** :

```
sudo systemctl restart nagios-nrpe-server.service
```

4. De plus, sur **serveur01**, redémarrez **nagios** :

```
sudo systemctl restart nagios3.service
```

Vous devriez maintenant être capable de voir l'hôte et les services de vérification dans les fichiers CGI de Nagios. Pour y accéder, rendez-vous sur http://server01/nagios3 avec votre navigateur. Il vous sera demandé le nom d'utilisateur et le mot de passe de **nagiosadmin**.

10.2.4 Références

Cette partie n'a fait qu'effleurer le potentiel des fonctionnalités de Nagios. **nagios-plugins-extra** et **nagios-snmp-plugins** contiennent bien plus de services de vérification.

Pour plus d'informations, voir le site internet de **Nagios** : http://www.nagios.org/ .

Plus précisément, le site de **documentation en ligne** (en anglais) : http://nagios.sourceforge.net/docs/3_0/

Ci-dessous, une liste de **livres** traitant de Nagios et de la supervision réseau : http://www.nagios.org/propaganda/books/

La page du **wiki Ubuntu sur Nagios (en anglais)** contient plus de détails : https://help.ubuntu.com/community/Nagios3 .

10.3. Munin

10.3.1. Installation

Avant d'installer **Munin** sur **serveur01** il faut d'abord avoir installé **apache2**. La configuration par défaut est satisfaisante pour faire fonctionner un serveur **munin**. Pour plus d'information, voir le *Chapitre 11, paragraphe 1. HTTPD - serveur web Apache2* .

Tout d'abord, installez **munin** sur **serveur01**. Saisissez dans un terminal :

```
sudo apt install munin
```

Ensuite, installez le paquet **munin-node** sur **serveur02** :

```
sudo apt install munin-node
```

10.3.2. Configuration

Sur **serveur01**, éditez le fichier /etc/munin/munin.conf pour ajouter l'adresse IP de **serveur02** :

```
## Premièrement, notre hôte "normal".
[serveur02]
       Address 172.18.100.101
```

R emplacez **serveur02** et **172.18.100.101** par le véritable nom d'hôte et adresse IP de votre serveur.

Ensuite, configurez **munin-node** sur **serveur02**. Modifiez le fichier /etc/munin/munin-node.conf pour permettre l'accès au **serveur01** :

```
Allow ^172\.18\.100\.100$
```

R emplacez **^172\.18\.100\.100$** par l'adresse IP de votre serveur **munin**.

Maintenant, redémarrez **munin-node** sur **serveur02** pour que les changements prennent effet :

```
sudo systemctl restart munini-node.service
```

Pour finir, dans un navigateur, allez sur **http://serveur01/munin**, et vous devriez voir des liens vers des graphiques clairs affichant les informations standard tirées de **munin-plugins** à propos des disques, du réseau, des processus et du système.

Puisque c'est une nouvelle installation, il faudra peut-être attendre un peu avant de pouvoir voir des choses utiles sur ces graphiques.

10.3.3. Plugins supplémentaires

Le paquet **munin-plugins-extra** contient des vérifications de performances de services supplémentaires tel que DNS, DHCP, Samba, etc. Pour installer ce paquet, entrez dans un terminal :

```
sudo apt install munin-plugins-extra
```

Assurez vous d'installer ce paquet à la fois sur le serveur et sur les machines nœud.

10.3.4. Références

Vous pouvez consulter le site de **Munin** pour plus de détails : http://munin.projects.linpro.no/ .

Les pages de **Documentation Munin**, en particulier, contiennent des informations sur les plugins supplémentaires, comment écrire des plugins, etc : http://munin.projects.linpro.no/wiki/Documentation .

De plus, il existe un livre en allemand par Open Source Press: **Munin Graphisches Netzwerk- und System-Monitoring** : https://www.opensourcepress.de/index.php?26&backPID=178&tt_products=152 .

Chapitre 11. Serveurs web

Un serveur web est un logiciel chargé d’accepter les requêtes HTTP de clients, appelés navigateurs Web, et de leur envoyer des réponses HTTP en même temps que des contenus, qui sont habituellement des pages web, c’est à dire des documents HTML et des objets liés (images, etc.).

11.1. HTTPD - serveur web Apache2

Apache est le serveur Web le plus couramment utilisé sur les systèmes Linux. Les serveurs Web sont utilisés pour remettre des pages Web demandées par des ordinateurs clients. Les clients demandent et affichent habituellement des pages Web en utilisant des applications de navigation Web telles que Firefox, Opera, Chromium, ou Internet Explorer.

Les utilisateurs saisissent une URL (adresse internet) pour pointer vers un serveur web au moyen de son nom de domaine complet (FQDN) et un chemin d'accès à la ressource requise. Par exemple, pour afficher la page d'accueil du site web Ubuntu un utilisateur entrera seulement le FQDN :

```
www.ubuntu.com
```

Pour voir la sous-page sur la communauté http://www.ubuntu.com/community, un utilisateur entrera le nom complet suivi d'un chemin :

```
www.ubuntu.com/community
```

La méthode la plus communément utilisée pour le transfert de pages web est le protocole de transfert hypertexte (HTTP). Le protocole de transfert hypertexte sur sockets sécurisées (HTTPS) et le protocole de transfert de fichiers (FTP), qui permet d'envoyer et de télécharger des fichiers, sont également pris en charge.

Les serveurs web Apache sont fréquemment utilisés en combinaison avec le moteur de base de données MySQL, le langage de script de pré-traitement hypertexte (PHP), et d'autres langages de scripts prisés tels que Python et Perl. Cette configuration, connue sous le nom de LAMP (Linux, Apache, MySQL et Perl/Python/PHP), constitue une puissante et robuste plate-forme de développement et de déploiement d'applications web.

11.1.1. Installation

Le serveur web Apache2 est disponible dans Ubuntu Linux. Pour installer Apache2 :

Saisissez la commande suivante dans un terminal :

```
sudo apt install apache2
```

11.1.2. Configuration

Apache2 est configuré en plaçant des **directives** en texte gras dans des fichiers de configuration. Ces **directives** sont réparties entre les fichiers et dossiers suivants :

- **apache2.conf** : le fichier principal de configuration d'Apache2. Il contient des paramètres **globaux** d'Apache2.
- **httpd.conf** : historiquement le principal fichier de configuration d'Apache2, nommé d'après le démon httpd. Maintenant, le fichier n'existe plus. Dans les anciennes versions d'Ubuntu, le fichier peut être

présent mais vide, toutes les options de configurations ayant été déplacées dans les répertoires référencés ci-dessous.

- **conf-available :** ce répertoire contient les fichiers de configuration disponibles. Tous les fichiers qui étaient auparavant dans /etc/apache2/conf.d peuvent être déplacés dans /etc/apache2/conf-available.
- **conf-enabled** : conserve les **liens symboliques** dans /etc/apache2/conf-available. Quand un fichier de configuration est pointé, il sera activé au prochain démarrage de apache2.
- **envvars** : fichier où les variables d'**environnement** d'Apache2 sont définies.
- **mods-available** : ce répertoire contient les fichiers de configuration qui permettent de charger les modules et de les paramétrer. Certains **modules** peuvent ne pas avoir de fichier de configuration.
- **mods-enabled** : contient les **liens symboliques (symlinks)** vers les fichiers de /etc/apache2/mods-available. Lorsqu'un lien symbolique vers un module de configuration est créé, il sera activé au prochain redémarrage d'Apache2.
- **ports.conf** : héberge les directives déterminant les ports TCP sur lesquels Apache2 est en écoute.
- **sites-available** : ce dossier contient des fichiers de configuration pour les **serveurs virtuels** d'Apache2. Les serveurs virtuels permettent de configurer Apache2 pour plusieurs sites ayant différentes configurations.
- **sites-enabled** : comme mods-enabled, sites-enabled contient des liens symboliques vers le dossier /etc/apache2/sites-available. De la même manière que lorsqu'un lien symbolique vers un fichier de configuration de sites-available est créé, le site ainsi configuré sera activé au prochain redémarrage d'Apache2.
- **magic** : instructions pour déterminer le type MIME à partir des premiers octets d'un fichier.

Enfin, d'autres paramétrages peuvent être ajoutés en utilisant la directive **Include** et des caractères jokers peuvent être utilisés pour inclure de multiples fichiers de configuration. Ces **directives** peuvent être placées dans n'importe lequel de ces fichiers de configuration. Les changements effectués dans les fichiers de configuration principaux ne sont pris en compte par Apache2 lorsque qu'il est démarré ou redémarré.

Le serveur lit également un fichier contenant les documents de type MIME, le nom du fichier est défini par la commande **TypesConfig**, généralement par l'intermédiaire de /etc/apache2/mods-available/mime.conf, qui peut également inclure des ajouts ou des remplacements, et est /etc/mime.types par défaut.

11.1.2.1. Réglages de base

Cette section explique les paramètres de configuration essentiels pour Apache2. Referez vous à la documentation Apache2 pour plus de détails : http://httpd.apache.org/docs/2.4/

- Apache2 transporte les données avec une configuration compatible par défaut avec un hôte virtuel. C'est-à-dire qu'il est configuré avec un hôte virtuel par défaut (utilisant la directive **VirtualHost**) qui peut être modifiée ou utilisée tel quel si vous avez un site unique ou utilisée comme un gabarit pour les hôtes virtuels supplémentaires si vous avez plusieurs sites. Pour un site unique, l'hôte virtuel par défaut exercera les fonctions de votre site par défaut, ou les utilisateurs du site verront si l'URL dans laquelle ils entrent ne correspond pas à la directive **ServerName** d'aucun de vos sites personnalisés. Pour modifier l'hôte virtuel par défaut, éditez le dossier /etc/apache2/sites-available/000-default.conf.

  Le jeu de **directives** pour un hôte virtuel ne s'applique qu'à cet hôte virtuel en particulier. Si une directive est définie globalement pour le serveur et n'est pas définie dans les paramètres de l'hôte virtuel, les paramètres par défaut s'appliquent. Par exemple, vous pouvez définir l'adresse électronique du webmaster globalement, et ne pas définir d'adresses individuelles pour chaque hôte virtuel.

  Si vous souhaitez configurer un nouvel hôte virtuel ou site, copiez ce fichier dans le même répertoire avec un nom de votre choix. Par exemple :

```
sudo cp /etc/apache2/sites-available/000-default.conf_ \
/etc/apache2/sites-available/mynewsite.conf
```

Editez le nouveau fichier pour configurer le nouveau site en utilisant certaines des commandes décrites ci-dessous.

- La directive **ServerAdmin** spécifie l'adresse électronique qui figurera comme adresse de l'administrateur du serveur. La valeur par défaut est webmaster@localhost. Cette valeur devrait être remplacée par une adresse dont vous êtes destinataire (dans le cas où vous êtes l'administrateur du serveur). Si votre site rencontre un problème, Apache2 affichera un message d'erreur contenant cette adresse mail afin de signaler le problème. Cette directive est à placer dans les fichiers de configuration de vos sites situés dans /etc/apache2/sites-available.
- La directive **Listen** précise le port, et de manière optionnelle l'adresse IP, sur lesquels Apache2 écoute. Si l'adresse IP n'est pas spécifiée, Apache écoutera sur toutes les adresses IP assignées à la machine. La valeur par défaut de la directive **Listen** est 80. Modifiez la en 127.0.0.1:80 afin qu'Apache2 n'écoute que sur l'interface locale et ne soit pas accessible depuis l'Internet, en 81 (par exemple) afin de modifier le port sur lequel Apache2 écoute, ou laissez la valeur par défaut dans la majorité des cas. Cette directive se situe dans le fichier /etc/apache2/ports.conf .
- La directive **ServerName** est optionnelle et spécifie à quel FQDN votre site devrait répondre. L'hôte virtuel par défaut n'a aucune directive **ServerName** spécifiée, donc il répondra à toutes les requêtes qui ne correspondent pas à une directive **ServerName** dans un autre hôte virtuel. Si vous venez d'acquérir le nom de domaine ubunturocks.com et voulez l'héberger sur votre serveur Ubuntu, la valeur de la directive **ServerName** dans votre fichier de configuration d'hôte virtuel devrait être ubunturocks.com. Ajoutez cette directive au nouveau fichier d'hôte virtuel précédemment créé (/etc/apache2/sites-available/mynewsite.conf).

  Comme beaucoup de visiteurs pensent que le préfixe www est utile, il est souhaitable que vous configuriez votre hôte virtuel pour qu'il réponde à ce nom. Utilisez la directive **ServerAlias**. Il est possible d'utiliser des caractères jokers dans la directive **ServerAlias**.

  Par exemple, votre site répondra à n'importe quelle requête de domaine finissant par **.ubunturocks.com** en utilisant la configuration suivante :

  ```
  ServerAlias *.ubunturocks.com
  ```

- La directive **DocumentRoot** spécifie où Apache2 doit rechercher les fichiers qui composent le site. La valeur par défaut est /var/www/html, comme indiqué dans le fichier /etc/apache2/sites-available/000-default.conf. Si vous le souhaitez, modifiez cette valeur dans le fichier de l'hôte virtuel de votre site, et n'oubliez pas de créer ce répertoire si nécessaire !

Activer le nouveau **VirtualHost** grâce à l'utilitaire **a2ensite** puis redémarrez Apache2 :

```
sudo a2ensite mon_nouveau_site
sudo systemctl restart apache2.service
```

> I est préférable d'utiliser un nom plus explicite que **mon_nouveau_site**. Par exemple nommez le fichier en utilisant la valeur de la directive **ServerName** de l'hôte virtuel.

De manière analogue l'utilitaire **a2dissite** permet de désactiver les sites. Cela peut être utile lors du dépannage de problèmes de configuration avec plusieurs hôtes virtuels :

```
sudo a2dissite mon_nouveau_site
sudo systemctl restart apache2.service
```

11.1.2.2. Réglages par défaut

Cette section explique la configuration par défaut du serveur Apache2. Par exemple, si vous ajoutez un hôte virtuel, les paramètres que vous définissez pour celui-ci deviennent prioritaires. Pour une directive qui n'est pas définie à l'intérieur de l'hôte virtuel, la valeur par défaut est utilisée.

- La directive **DirectoryIndex** stipule la page par défaut qui doit être servie lorsqu'un utilisateur demande l'index d'un répertoire en spécifiant une barre oblique (/) à la fin du nom d'un répertoire.

  Par exemple, lorsqu'un utilisateur demande la page http://www.exemple.com/ce_repertoire/, il obtiendra soit la page **DirectoryIndex** si elle existe, soit un listing du répertoire généré par le serveur si Option Indexes est spécifiée, soit encore une page « Autorisation refusée » si aucune de ces deux conditions n'est remplie. Le serveur essaiera de trouver un fichier parmi ceux listés dans la directive **DirectoryIndex** et renverra le premier d'entre eux. S'il ne trouve aucun des fichiers stipulés et si **Options Indexes** est configurée pour ce répertoire, le serveur en renverra alors la liste des sous-répertoires et fichiers, au format HTML. La valeur par défaut, spécifiée dans /etc/apache2/mods-available/dir.conf, est « index.html index.cgi index.pl index.php index.xhtml index.htm ». Ainsi, si Apache2 trouve un fichier portant l'un de ces noms, il l'affichera.

- La directive **ErrorDocument** vous permet de spécifier un fichier à utiliser par Apache2 pour les événements d'erreurs spécifiques. Par exemple, si un utilisateur demande une ressource qui n'existe pas, une erreur 404 se produira. Par défaut, Apache2 renverra simplement un code de retour HTTP 404. Lisez /etc/apache2/conf-available/localized-error-pages.conf pour obtenir des instructions détaillées et des lieux de fichiers d'exemples sur l'utilisation de la directive **ErrorDocument**.

- Par défaut, le serveur écrit un journal des transferts dans le fichier /var/log/apache2/access.log. Vous pouvez le changer pour chaque site individuellement dans vos fichiers de configuration d'hôte virtuel avec la directive **CustomLog** ou l'omettre pour accepter les valeurs par défaut, spécifiées dans le fichier /etc/apache2/conf-available/other-vhosts-access-log.conf. Vous pouvez aussi spécifier le fichier dans lequel les erreurs de transfert sont écrites au journal, via la directive **ErrorLog**, dont le nom par défaut est /var/log/apache2/error.log. Les erreurs sont gardées séparées des transferts pour faciliter le diagnostic des pannes de votre serveur Apache2. Vous pouvez aussi spécifier le niveau d'alerte avec les directives **LogLevel** (la valeur par défaut est " prévenir ") et **LogFormat** (voir /etc/apache2/apache2.conf pour la valeur par défaut).

- Certaines options sont définies par répertoire plutôt que par serveur. **Options** est l'une de ces **directives**. Une strophe Directory est entourée d'étiquettes de type XML, comme ceci :

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

  La directive **Options** à l'intérieur d'une déclaration **Directory** peut avoir avoir une ou plusieurs valeurs séparées par des espaces :

  - **ExecCGI** - Autorise l'exécution des scripts CGI. Les scripts CGI ne sont pas exécutés si cette option n'est pas choisie.

La plupart des fichiers ne devraient pas être exécutés comme des scripts CGI. Ce serait très dangereux. Les scripts CGI doivent être dans un répertoire distinct et en dehors de votre dossier racine de serveur, et seul ce répertoire aura l'option ExecCGI active. Le répertoire par défaut où se trouvent les scripts CGI est /usr/lib/cgi-bin.

- **Includes** - Autorise les inclusions côté serveur. Les inclusions côté serveur permettent à un fichier HTML d' inclure d'autres fichiers. Voir Apache SSI documentation (Ubuntu community) pour plus d'informations : https://help.ubuntu.com/community/ServerSideIncludes
- **IncludesNOEXEC** - Autorise les inclusions côté serveur, mais désactive les commandes **#exec** et **#include** dans les scripts CGI.
- **Indexes** - affiche une liste des fichiers et dossiers du répertoire s'il n'existe aucun

  « **DirectoryIndex** » (tel que index.html) dans le répertoire demandé.

! Pour des raisons de sécurité, ceci ne devrait habituellement pas être activé, et cela ne devrait certainement pas être activé dans votre répertoire racine de documents (**DocumentRoot**). Si vous êtes certain de vouloir que les utilisateurs voient le contenu complet d'un répertoire, activez cette option avec prudence dans une section pour ce répertoire.

- **Multiview** - Autorise les vues multiples à contenu négocié ; cette option est désactivée par défaut pour des raisons de sécurité. Voir la documentation Apache2 de cette option : http://httpd.apache.org/docs/2.4/mod/mod_negotiation.html#multiviews
- **SymLinksIfOwnerMatch** - Ne suit les liens symboliques que si le fichier ou répertoire cible a le même propriétaire que le lien.

11.1.2.3. Paramètres httpd

Cette section explique certains paramétrages basiques du démon **httpd**.

- **LockFile** - La directive **LockFile** définit le chemin vers le fichier **LockFile** utilisé lorsque le serveur est compilé soit avec USE_FCNTL_SERIALIZED_ACCEPT, soit USE_FLOCK_SERIALIZED_ACCEPT. Ce fichier doit être enregistré sur le disque local. On doit laisser la valeur par défaut à moins que le répertoire des journaux se situe sur un partage NFS. Dans ce cas, la valeur par défaut doit être modifiée pour un emplacement, sur le disque local, lisible uniquement par le super-utilisateur (root).
- **PidFile** - La directive **PidFile** définit le fichier dans lequel le serveur enregistre son ID de processus (pid : process ID). Ce fichier ne doit être accessible en lecture que par le super-utilisateur (root). Dans la plupart des cas, la valeur par défaut peut être conservée.
- **User** - La commande **User** définit l'identité de l'utilisateur utilisée par le serveur pour répondre aux demandes. Ce paramètre détermine l'accès au serveur. Tous les fichiers inaccessibles à cet utilisateur seront également inaccessibles aux visiteurs de votre site web. La valeur par défaut pour l'utilisateur est "www-data".

  ! À moins que vous ne sachiez exactement ce que vous faites, ne définissez jamais la directive **User** à root. Utiliser root (super-utilisateur) comme valeur pour User créera des failles de sécurité béantes dans votre serveur Web.

- **Group** - La commande **Group** est similaire à la commande **User**. Group définit le groupe sous lequel le serveur répond aux requêtes. Le groupe par défaut est également "www-data".

11.1.2.4. Modules Apache2

Apache2 est un serveur modulaire. Cela signifie que seules les fonctionnalités les plus basiques sont incluses dans le cœur même du serveur. Les fonctionnalités étendues sont disponibles grâce aux modules qui peuvent être chargés dans Apache2. Par défaut, un ensemble de modules de base est inclus dans le serveur au moment de la compilation. Si le serveur est compilé pour utiliser les modules chargés dynamiquement, alors ces derniers peuvent être compilés séparément et ajouté à tout moment en utilisant la directive **LoadModule**. Sinon, Apache2 doit être recompilé pour ajouter ou supprimer des modules.

Ubuntu compile Apache2 pour permettre le chargement dynamique de modules. Les **directives** de configuration peuvent être incluses dans un module particulier en les délimitant par un bloc **<IfModule>**.

Vous pouvez installer des modules Apache2 additionnels et les utiliser avec votre serveur Web. Par exemple, lancez la commande suivante, à l'invite de commande du terminal, pour installer le module **MySQL Authentication** :

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

Consultez le répertoire /etc/apache2/mods-available pour voir les modules supplémentaires.

L'utilitaire **a2enmod** permet d'activer un module :

```
sudo a2enmod auth_mysql
sudo systemctl restart apache2.service
```

De même, a2dismod désactivera un module :

```
sudo a2dismod auth_mysql
sudo systemctl restart apache2.service
```

11.1.3. Configuration HTTPS

Le module **mod_ssl** ajoute d'importantes caractéristiques au serveur Apache2 - la capacité de chiffrer les communications. De plus, lorsque votre navigateur Web communique en utilisant SSL, le préfixe https:// est utilisé au début de l'adresse Web (URL) dans la barre d'adresse du navigateur.

Le module **mod_ssl** est disponible dans le paquet apache2-common. Exécutez la commande suivante à l'invite du terminal pour activer le module mod_ssl :

```
sudo a2enmod ssl
```

Il y a un fichier par défaut de configuration du mode HTTPS qui est /etc/apache2/sites-available/default-ssl.conf. Pour qu'Apache2 fournisse le mode HTTPS, les fichiers **certificat** et **clé** sont également nécessaires. La configuration par défaut du mode HTTPS utilisera un **certificat** et une **clé** générés par le paquet **ssl-cert**. Ils seront suffisants pour essayer le mode HTTPS, mais le **certificat** et la **clé** automatiquement générés devraient être remplacés par un certificat spécifique du site ou du serveur.

Pour configurer Apache2 pour HTTPS, saisissez les informations suivantes :

```
sudo a2ensite default-ssl
```

Les répertoires par défaut sont /etc/ssl/certs et /etc/ssl/private. Si vous installez le certificat et la clé dans un autre répertoire, assurez-vous de modifier **SSLCertificateFile** et **SSLCertificateKeyFile** en conséquence.

Avec Apache2 maintenant configuré pour HTTPS, redémarrez le service pour activer les nouveaux paramètres :

```
sudo systemctl restart apache2.service
```

Selon comment vous avez obtenu votre certificat, vous devrez entrer un mot de passe lors du redémarrage d'Apache2.

Vous pouvez accéder aux pages du serveur sécurisé en tapant https://votre_nom_d_hote/url/ dans la barre d'adresse de votre navigateur.

11.1.4. Permission d'écriture sur le partage

Pour que plusieurs utilisateurs soient en mesure d'écrire dans le même répertoire, il sera nécessaire d'accorder la permission d'écriture à un groupe qu'ils partagent en commun. Les exemples suivants accordent l'autorisation partagée d'écriture dans /var/www/html pour le groupe «webmasters».

```
sudo chgrp -R webmasters /var/www/html
sudo find /var/www/html -type d -exec chmod g=rwxs "{}" \;
sudo find /var/www/html -type f -exec chmod g=rw "{}" \;
```

Ces commandes paramètrent récursivement la permission du groupe en lecture-écriture sur tous les fichiers et dossiers dans /var/www/html ainsi que de fixer l'identifiant de l'utilisateur. Cela permet aux fichiers et dossiers d'hériter de leur parents, l'appartenance à un groupe et la permission d'accès et de modification. De nombreux administrateurs trouvent cela utile pour autoriser différents utilisateurs à éditer des fichiers dans une arborescence de répertoire.

Si l'accès doit être accordé à plus d'un groupe par répertoire, activez **Access Control Lists** (ACLs).

11.1.5. Références

- La *Documentation Apache2* contient des informations détaillées sur les **directives** de configuration Apache2 : http://httpd.apache.org/docs/2.4/.

  Également, consultez le paquet apache2-doc pour les documents officiels Apache2.
- Consultez le site Mod SSL Documentation (en anglais) pour plus d'informations concernant SSL : http://www.modssl.org/docs/
- Apache Cookbook éditions O'Reilly (en anglais) est une bonne ressource pour réaliser des configurations spécifiques d'Apache2 : http://oreilly.com/catalog/9780596001919/
- Pour les questions concernant Apache2 mais spécifiques à Ubuntu, consultez le canal anglophone IRC **#ubuntu-server** sur http://freenode.net, ou le canal généraliste francophone **#ubuntu-fr**.
- Étant habituellement couplé avec PHP et MySQL, le Wiki Ubuntu consacrée à Apache MySQL PHP est également une très bonne source d'information : https://help.ubuntu.com/community/ApacheMySQLPHP

11.2. PHP - Langage de script

PHP est un langage de script générique adapté au développement Web. Des scripts PHP peuvent être intégrés dans des pages HTML. Cette section explique comment installer et configurer PHP dans un système Ubuntu avec Apache2 et MySQL.

Cette section présuppose que vous ayez installé et configuré le serveur Web Apache2 ainsi que la base de données MySQL. Vous pouvez vous référer aux sections Apache2 et MySQL de ce document pour installer et configurer ceux-ci.

11.2.1. Installation

PHP est disponible pour Ubuntu Linux. Contrairement à Python et Perl, qui sont installés avec le système de base, PHP doit être ajouté.

- Pour installer PHP et le module Apache PHP, vous pouvez saisir la commande suivante à l'invite d'un terminal :

```
sudo apt install php libapache2-mod-php
```

Vous pouvez lancer des scripts PHP à l'invite d'un terminal. Pour le faire, vous devez installer le paquet php-cli en saisissant la commande suivante à l'invite du terminal :

```
sudo apt install php-cli
```

Vous pouvez aussi exécuter des scripts PHP sans installer le module Apache PHP. Pour le faire, vous devez installer le paquet php-cgi en saisissant la commande suivante à l'invite du terminal :

```
sudo apt install php-cgi
```

Pour utiliser MySQL avec PHP, vous devez installer le paquet php-mysql. Pour le faire, vous pouvez saisir la commande suivante à l'invite d'un terminal :

```
sudo apt install php-mysql
```

De la même manière, pour utiliser PostgreSQL avec PHP, vous devez installer le paquet php-pgsql. Pour ce faire, vous pouvez saisir la commande suivante à l'invite d'un terminal :

```
sudo apt install php-pgsql
```

11.2.2. Configuration

Si vous avez installé les paquets libapache2-mod-php ou php-cgi, vous pouvez lancer des scripts PHP depuis votre navigateur internet. Si vous avez installé le paquet php-cli, vous pouvez lancer des scripts PHP

à l'invite d'un terminal.

Par défaut, lorsque libapache2-mod-php est installé, le serveur web Apache 2 est configuré pour lancer des scripts PHP. En d'autres termes, le module PHP est activé dans le serveur Web Apache lorsque vous installez le module. Veuillez vérifier l'existence des fichiers /etc/apache2/mods-enabled/php7.0.conf et /etc/apache2/mods-enabled/php7.0.load. S'ils ne sont pas présents, vous pouvez activer le module en utilisant la commande **a2enmod**.

Une fois les paquets concernant PHP installés et le module Apache PHP activé, vous devez redémarrer le serveur web Apache2 pour lancer des scripts PHP. Vous pouvez saisir la commande suivante à l'invite d'un terminal pour redémarrer votre serveur web :

```
sudo systemctl restart apache2.service
```

11.2.3. Tests

Pour vérifier votre installation, vous pouvez lancer le script PHP phpinfo suivant :

```
<?php
  phpinfo();
?>
```

Vous pouvez enregistrer le contenu dans un fichier phpinfo.php et le placer dans le dossier **DocumentRoot** du serveur web Apache2. En dirigeant votre navigateur vers http://hostname/phpinfo.php, il affichera les valeurs de différents paramètres de configuration PHP.

11.2.4. Références

- Pour plus d'informations détaillées, consultez la documentation php.net : http://www.php.net/docs.php
- Il y a une multitude de livres sur PHP. *Learning PHP* de O'Reilly en est un bon : http://oreilly.com/catalog/0636920043034/. Tout comme *PHP Cook Book*, mais il n'a pas été mis à jour pour PHP7 : http://oreilly.com/catalog/9781565926813/
- Pour plus d'information, consultez également la page du Wiki Ubuntu consacrée à Apache MySQL PHP : https://help.ubuntu.com/community/ApacheMySQLPHP

11.3. Squid - Serveur mandataire (proxy)

Squid est est une application de cache web proxy qui fournit des services de proxy et de cache pour les protocoles de transport de texte (HTTP), le protocole de transfert de fichiers (FTP) et autres protocoles réseau courants. Squid supporte la mémoire cache et peut gérer un proxy via des requêtes Secure Sockets Layer (SSL), la recherche dans la mémoire cache des serveurs de noms de domaine (DNS) et effectuer une mise en cache transparente. Squid prend également en charge une grande variété de protocoles de mise en cache, tel que l'Internet Cache Protocol (ICP), l'Hyper Text Caching Protocol (HTCP), le Cache Array Routing Protocol (CARP) et le Web Cache Coordination Protocol (WCCP).

Le serveur de cache proxy Squid est une excellente solution pour une variété de nécessités de cache et de proxy, de l'échelle de la succursale aux réseaux d'entreprise, tout en offrant des mécanismes de contrôle d'accès granulaires et complets, et une supervision de paramètres critiques via le protocole Simple Network Manager Protocol (SNMP). Lors de la sélection d'un système informatique pour une utilisation de serveur proxy cache Squid avec de nombreux utilisateurs, assurez vous de le configurer avec une large quantité de mémoire vive, étant donné que Squid utilise un cache mémoire pour des performances optimales.

11.3.1. Installation

Pour installer le serveur Squid, utilisez la commande suivante dans un terminal :

```
sudo apt install squid
```

11.3.2. Configuration

Squid se configure en modifiant les **directives** contenues dans le fichier de configuration /etc/squid/squid.conf. Les exemples suivants illustrent certaines modifications de **directives** qui peuvent affecter le comportement du serveur Squid. Pour une configuration plus avancée de Squid, voyez la section *3.3. Références*.

Avant de modifier le fichier de configuration, vous devriez faire une copie du fichier original et le protéger en écriture, vous aurez alors les paramètres par défaut en référence à utiliser si besoin. Faites cette copie et protégez la de l'écriture en utilisant la commande suivante :

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

- Pour que votre serveur Squid écoute sur le port TCP 8888 à la place du port par défaut 3128, modifiez la directive **http_port** comme ceci :

  ```
  http_port 8888
  ```

- Pour donner un nom d'hôte spécifique à votre serveur Squid, changez la directive **visible_hostname**. Ce nom d'hôte n'a pas forcément besoin d'être le même que le nom d'hôte de la machine. Dans cet exemple il est défini comme étant **weezie**.

  ```
  visible_hostname weezie
  ```

- En utilisant le contrôle d'accès de Squid, vous pouvez configurer l'accès aux services Internet gérés par le proxy Squid de telle sorte qu'ils ne soient disponibles que pour les utilisateurs ayant certaines adresses IP. À titre d'exemple, nous allons détailler le cas d'un accès uniquement aux utilisateurs du sous-réseau 192.168.42.0/24 :

  Ajoutez ce qui suit en **bas** de la section ACL de votre fichier /etc/squid/squid.conf :

  ```
  acl fortytwo_network src 192.168.42.0/24
  ```

  Ajoutez ensuite ce qui suit, en **haut** de la section http_access de votre fichier /etc/squid/squid.conf :

  ```
  http_access allow fortytwo_network
  ```

- En utilisant les excellentes fonctionnalités de contrôle d'accès de Squid, vous pouvez configurer l'utilisation des services Internet par proxy Squid pour n'être disponibles que pendant les heures normales de bureau. Par exemple, nous allons illustrer l'accès par les employés d'une entreprise qui opère entre 09h00 et 17h00, du lundi au vendredi, et qui utilise le sous-réseau 10.1.42.0/24 :

  Ajoutez ce qui suit en **bas** de la section ACL de votre fichier /etc/squid/squid.conf :

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

  Ajoutez ensuite ce qui suit, en **haut** de la section http_access de votre fichier /etc/squid/squid.conf :

  ```
  http_access allow biz_network biz_hours
  ```

Après avoir effectué les changements dans le fichier /etc/squid/squid.conf, enregistrez le fichier et redémarrez le serveur squid afin que les modifications soient prises en compte, en utilisant la commande suivante dans une console :

```
sudo systemctl restart squid.service
```

Si une version personnalisée de squid3 a déjà été utilisée, et si elle a établi le dossier spool /var/log/squid3 comme point de montage mais a par ailleurs conservé la configuration par défaut, la mise à jour va échouer. La mise à jour tente de renommer/déplacer les fichiers en tant que de besoin, mais elle ne peut pas le faire pour un point de montage actif. Dans ce cas, adaptez soit le point de montage soit la configuration dans /etc/squid/squid.conf, de manière à ce qu'il y ait correspondance entre les deux.

Cela vaut également si l'instruction de configuration **include** a été utilisée pour récupérer d'autres fichiers depuis l'ancien chemin /etc/squid3/. Dans ce cas, vous devez déplacer et adapter la configuration en conséquence.

11.3.3. Références

Site web de Squid : http://www.squid-cache.org/

La page du Wiki Ubuntu consacrée à Squid : https://help.ubuntu.com/community/Squid

11.4. Ruby on Rails

Ruby on Rails est une infrastructure Web libre pour développer des applications Web liées à des bases de données. Elle optimise durablement la productivité du programmeur, car elle lui permet d'écrire le code en favorisant la convention plutôt que la configuration.

11.4.1. Installation

Avant d'installer Rails, vous devez installer Apache et MySQL. Pour installer Apache, veuillez consulter le *Chapitre 11, paragraphe 1. HTTPD - serveur web Apache2* . Pour les instructions d'installation MySQL, consultez le *Chapitre 12, paragraphe 1. MySQL*.

Une fois que vous avez installé les paquets Apache et MySQL, vous êtes prêt pour installer le paquet de Ruby on Rails.

Pour installer les paquets de base Ruby et Ruby on Rails, vous pouvez saisir la commande suivante dans un terminal :

```
sudo apt install rails
```

11.4.2. Configuration

Modifiez le fichier de configuration /etc/apache2/sites-available/000-default.conf pour paramétrer vos domaines.

La première chose à changer est la directive **DocumentRoot** :

```
DocumentRoot /path/to/rails/application/public
```

Puis, modifiez la directive **<Directory "/path/to/rails/application/public">** :

```
<Directory "/path/to/rails/application/public">
        Options Indexes FollowSymLinks MultiViews ExecCGI
        AllowOverride All
        Order allow,deny
        allow from all
        AddHandler cgi-script .cgi
</Directory>
```

Vous pouvez également activer le module **mod_rewrite** pour Apache. Pour ce faire, veuillez saisir la commande suivante dans un terminal :

```
sudo a2enmod rewrite
```

Enfin, vous devrez remplacer le propriétaire des répertoires /path/to/rails/application/public et /path/to/rails/application/tmp par l'utilisateur exécutant habituellement le processus Apache :

```
sudo chown -R www-data:www-data /path/to/rails/application/public
sudo chown -R www-data:www-data /path/to/rails/application/tmp
```

C’est tout ! Maintenant votre serveur est prêt pour vos applications Ruby on Rails.

11.4.3. Références

- Consultez le site Ruby on Rails (en anglais) pour de plus amples informations : http://rubyonrails.org/
- Agile Development with Rails (en anglais) est aussi une mine d’informations : http://pragprog.com/titles/rails3/agile-web-development-with-rails-third-edition
- Vous trouverez également des informations sur la page du Wiki Ubuntu consacrée à Ruby on Rails : https://help.ubuntu.com/community/RubyOnRails

11.5. Apache Tomcat

Apache Tomcat est un conteneur vous permettant de fournir des Servlets Java et des applications Web JSP (Java Server Pages).

Ubuntu possède des paquets pour Tomcat 6 et 7. Tomcat 6 est la version historique et Tomcat 7 la version courante où les nouvelles fonctions sont implémentées. Les deux sont considérées comme stables. Ce guide va se concentrer sur Tomcat 7 mais la plupart des détails de configurations sont valides pour les deux versions.

Les paquets Tomcat d'Ubuntu permettent deux types de fonctionnement pour tomcat. Vous pouvez les installer comme une instance unique pour l'ensemble du système, qui sera lancée au démarrage du système et fonctionnera avec les droits de l'utilisateur sans privilèges tomcat7 (ou tomcat6). Mais vous pouvez aussi déployer des instances privées, exécutées avec vos propres droits d'utilisateur, et que vous devrez démarrer et arrêter par vous-même. Cette deuxième possibilité est particulièrement utile dans un contexte de serveur de développement où plusieurs utilisateurs peuvent réaliser des tests sur leurs propres instances privées de Tomcat.

11.5.1 Installation pour tout le système

Pour installer le serveur Tomcat, vous pouvez entrer la commande suivante dans l'invite de terminal:

```
sudo apt install tomcat7
```

Cela installera un serveur Tomcat avec par défaut une application Web ROOT par défaut qui affichera la page minimale "it works" par défaut.

11.5.2. Configuration

Les fichiers de configuration de Tomcat se trouvent dans /etc/tomcat7. Seulement quelques ajustements courants de configuration seront décrits ici, veuillez voir la documentation Tomcat 7.0 pour plus de détails : http://tomcat.apache.org/tomcat-7.0-doc/index.html

11.5.2.1 Modification des ports par défaut

Par défaut, Tomcat exécute un connecteur HTTP sur le port 8080 et un connecteur AJP (protocole Apache Jserv) sur le port 8009. Vous devrez peut-être changer ces ports par défaut pour éviter des conflits avec d'autres applications du système. Ceci est effectué en changeant les lignes suivantes dans /etc/tomcat7/server.xml :

```
<Connector port="8080" protocol="HTTP/1.1"
               connectionTimeout="20000"
               redirectPort="8443" />
...
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
```

11.5.2.2. Modification de la machine virtuelle Java utilisée

Par défaut, Tomcat se lancera de préférence avec les JVMs OpenJDK, puis essayera les JVMs Sun, et enfin d'autres JVMs. Vous pouvez forcer Tomcat à utiliser une JVM spécifique en définissant JAVA_HOME dans /etc/default/tomcat7 :

```
JAVA_HOME=/usr/lib/jvm/java-6-sun
```

11.5.2.3. Déclaration des utilisateurs et des rôles

Les noms d'utilisateurs, mots de passes et rôles (groupes) peuvent être définis dans un conteneur Servlet. Ceci est accompli dans le fichier /etc/tomcat7/tomcat-users.xml :

```
<role rolename="admin"/>
<user username="tomcat" password="s3cret" roles="admin"/>
```

11.5.3. Utilisations des applications Web standard de Tomcat

Tomcat est fourni avec des applications Web que vous pouvez installer pour la documentation, l'administration ou pour des démonstrations.

11.5.3.1 Documentation Tomcat

Le paquet tomcat7-docs contient la documentation Tomcat qui est empaquetée comme une application web dans laquelle vous pouvez accéder par défaut à l'adresse http://VotreServeur:8080/docs . Vous pouvez l'installer en saisissant la commande suivante dans un terminal :

```
sudo apt install tomcat7-docs
```

11.5.3.2 Les applications Web d'administration pour Tomcat

Le paquet tomcat7-admin contient deux applications web qui peuvent être utilisées pour administrer le serveur Tomcat à l'aide d'une interface web. Vous pouvez installer ces applications web en saisissant la commande suivante dans un terminal :

```
sudo apt install tomcat7-admin
```

La première est l'application Web **manager**. Vous pouvez y accéder par défaut sur http://yourserver:8080/manager/html. Elle est principalement utilisée pour obtenir les statuts du serveur et redémarrer les applications Web.

> L'accès à l'application de **gestion** est protégé par défaut : vous devez définir un utilisateur avec le rôle « manager-gui » dans /etc/tomcat7/tomcat-users.xml avant de pouvoir y accéder.

La seconde est l'application Web **host-manager**. Vous pouvez y accéder par défaut sur http://yourserver:8080/host-manager/html. Elle peut être utilisée pour créer dynamiquement des hôtes virtuels.

> L'accès à l'application de **host-manager** est également protégé par défaut : vous devez définir un utilisateur avec le rôle « admin-gui » dans /etc/tomcat7/tomcat-users.xml avant de pouvoir y accéder.

Pour des raisons de sécurité, par défaut l'utilisateur tomcat7 ne peut pas écrire dans le répertoire /etc/tomcat7. Certaines fonctionnalités dans l'administration des applications web (déploiement d'application, création d'hôte virtuel) ont besoin d'avoir accès en écriture à ce répertoire. Si vous voulez utiliser ces fonctionnalités, exécutez la commande suivante pour donner les droits nécessaires aux utilisateurs du groupe tomcat7 :

```
sudo chgrp -R tomcat7 /etc/tomcat7
sudo chmod -R g+w /etc/tomcat7
```

11.5.3.3. Exemples d'applications Web Tomcat

Le paquet tomcat7-examples contient deux applications web qui peuvent être utilisées pour tester ou présenter les fonctionnalités de Servlet et de JSP, et accessibles à l'adresse par défaut http://yourserver:8080/examples. Vous pouvez les installer en entrant la commande suivante dans un terminal :

```
sudo apt install tomcat7-examples
```

11.5.4. Utilisation des instances privées

Tomcat est largement utilisé pour des besoins de développement et de test où utiliser une seule instance accessible par tout le système ne peux pas répondre aux exigences de plusieurs utilisateurs sur un seul système. Les paquets de Tomcat dans Ubuntu fournissent des outils pour vous aider à déployer vos propres instances utilisateur, et permettent à chaque utilisateur d'un système de lancer (sans les droits root) des instances privées distinctes tout en utilisant les bibliothèques installées sur le système.

> I est possible de lancer les instances système et privée en parallèle, du moment qu'elles n'utilisent pas les mêmes ports TCP.

11.5.4.1. Installation de la gestion des instances privées

Vous pouvez installer tout ce qui est nécessaire pour lancer une instance privée en saisissant la commande suivante dans un terminal :

```
sudo apt install tomcat7-user
```

11.5.4.2 Création d'une instance privée

Vous pouvez créer un répertoire d'instance privée en saisissant la commande suivant dans un terminal :

```
tomcat7-instance-create my-instance
```

Cela créera un nouveau dossier my-instance avec les sous-dossiers et scripts nécessaires. Vous pouvez par exemple installer vos bibliothèques communes dans le sous-dossier lib/ et déployer votre application dans le sous-dossier webapps/. Par défaut, aucune application Web n'est déployée.

11.5.4.3. Configuration de votre instance privée

Vous trouverez les fichiers de configuration de Tomcat pour votre instance privée dans le sous-dossier conf/. Vous devrez certainement par exemple modifier le fichier conf/server.xml pour changer les ports par défaut utilisés par votre instance privée Tomcat pour éviter les conflits avec d'autres instances actives.

11.5.4.4. Démarrage/arrêt de votre instance privée

Vous pouvez lancer votre instance privée en saisissant la commande suivante dans un terminal (en supposant qu'elle se trouve dans le répertoire my-instance) :

```
my-instance/bin/startup.sh
```

Vous devez vérifier si il y a des erreurs dans le sous-dossier logs/. Si vous avez l'erreur **java.net.BindException: Address already in use<null>:8080**, cela veut dire que le port que vous utilisez est déjà pris et que vous devez le changer.

Vous pouvez arrêter votre instance en saisissant la commande suivante dans le terminal (en supposant qu'elle se trouve dans le répertoire my-instance) :

```
my-instance/bin/shutdown.sh
```

11.5.5. Références

- Consultez le site Web Apache Tomcat (en anglais) pour plus d'informations : http://tomcat.apache.org/
- *Tomcat : The Definitive Guide* est une bonne ressource pour construire des applications web avec Tomcat : http://shop.oreilly.com/product/9780596003180.do
- Pour les livres de référence consultez la liste sur la page : http://wiki.apache.org/tomcat/Tomcat/Books (en anglais).

Chapitre 12. Bases de données

Ubuntu fournit deux serveurs de bases de données populaires. Ce sont :

- MySQL
- PostgreSQL

Ils sont disponibles dans le dépôt principal. Cette section explique comment installer et paramétrer ces serveurs de bases de données.

12.1. MySQL

MySQL est un rapide, multi-unité d'exécution, multi-utilisateur et robuste serveur de base de données SQL. Il est destiné aux missions stratégiques et aux systèmes de production à forte charge, ainsi qu'à l'intégration dans des logiciels déployés en masse.

12.1.1. Installation

Pour installer MySQL, exécutez la commande suivante dans un terminal :

```
sudo apt install mysql-server
```

Lors du processus d'installation, vous serez invité à entrer un mot de passe pour l'utilisateur root MySQL.

Une fois l'installation terminée, le serveur MySQL devrait démarrer automatiquement. Vous pouvez utiliser la commande suivante à l'invite d'un terminal pour vérifier si le serveur MySQL fonctionne :

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

Quand vous exécutez cette commande, vous devriez voir apparaître la ligne suivante ou quelque chose de similaire :

```
tcp       0       0 localhost:mysql       *:*   LISTEN      2556/mysqld
```

Si le serveur ne fonctionne pas correctement, saisissez la commande suivante pour le démarrer :

```
sudo systemctl restart mysql.service
```

12.1.2. Configuration

Vous pouvez éditer le fichier /etc/mysql/my.cnf pour configurer les paramètres de base - fichier journal, numéro de port, etc Par exemple, pour configurer MySQL pour écouter les connexions provenant d'hôtes du réseau, les changements l'**bind-address** de directive à l'adresse IP du serveur:

```
Bind-address = 192.168.0.5
```

R emplacez 192.168.0.5 par l'adresse appropriée.

Après tout changement dans /etc/mysql/my.cnf, le démon MySQL devra être redémarré :

```
sudo systemctl restart mysql.service
```

Si vous souhaitez changer le mot de passe **root** MySQL, saisissez dans un terminal :

```
sudo dpkg-reconfigure mysql-server-5.5
```

Le démon MySQL sera arrêté et vous serez invité à saisir un nouveau mot de passe.

12.1.3. Moteurs de bases de données

Bien que la configuration par défaut de MySQL fournie par les paquets Ubuntu soit parfaitement fonctionnelle et performante, il y a des choses que vous devez prendre en compte avant de poursuivre.

MySQL est conçu pour permettre aux données d'être stockées dans différentes manières. Ces méthodes sont appelées moteurs de bases de données ou de stockage soit. Il existe deux principaux moteurs que vous serez intéressé par: InnoDB et MyISAM. Les moteurs de stockages sont transparentes pour l'utilisateur final. MySQL va gérer les choses différemment sous la surface, mais quel que soit le moteur de stockage est en cours d'utilisation, vous pourrez interagir avec la base de données de la même manière.

Chaque moteur a des avantages et des inconvénients.

Bien qu'il soit possible, et peut être avantageux de mélanger et assortir les moteurs de bases de données sur un niveau de la table, ce qui réduirait l'efficacité de l'optimisation des performances, vous pouvez faire ce que vous serez en divisant les ressources entre les deux moteurs au lieu de les consacrer à un.

- MyISAM est le plus âgé des deux. Il peut être plus rapide que InnoDB dans certaines circonstances et favorise une charge de travail en lecture seule. Certaines applications Web ont été réglés autour des tables MyISAM (mais cela ne veut pas dire que ils vont ralentir sous InnoDB). MyISAM supporte aussi le type de données FULLTEXT, ce qui permet des recherches très rapides de grandes quantités de données textuelles. Cependant MyISAM est seulement capable de verrouiller une table entière pour l'écriture. Cela signifie qu'un seul processus peut mettre à jour une table à la fois. Comme toute application qui utilise les échelles de table ce qui peut se révéler être un obstacle. Il manque également la journalisation, ce qui rend plus difficile pour les données à récupérer après un crash. Le lien suivant fournit quelques éléments de réflexion sur l'utilisation de **MyISAM sur une base de données de production** : http://www.mysqlperformanceblog.com/2006/06/17/using-myisam-in-production/ .
- InnoDB est un moteur de base de données plus moderne, conçu pour être conforme à ACIDE qui garantit que les transactions de base de données sont traitées de manière fiable : http://en.wikipedia.org/wiki/ACID . Le verrouillage d'écriture peut se produire sur une base au niveau des lignes dans une table. Cela signifie que plusieurs mises à jour peuvent se produire simultanément sur une seule table. La mise en cache de données est également gérée en mémoire dans le moteur de base de données, ce qui permet la mise en cache sur une base plus efficace au niveau des lignes plutôt que bloc de fichier. Pour répondre à la compatibilité ACID toutes les transactions sont journalisées de façon indépendamment des principaux tableaux. Cela permet beaucoup plus de récupérations de données fiables parce que la cohérence des données peut être vérifiée.

En conséquence, MySQL 5.5 InnoDB est le moteur par défaut, et est hautement recommandé plutôt que MyISAM sauf si vous avez besoin spécifique de fonctionnalités uniques pour le moteur.

12.1.4. Configuration avancée

12.1.4.1. Création d'un fichier my.cnf personnalisé

Il y a un certain nombre de paramètres qui peuvent être ajustés dans le fichier de configuration de MySQL qui vous permettra d'améliorer les performances du serveur au fil du temps. Pour la configuration initiale,

vous pouvez trouver utile l'outil **Percona's my.cnf generating tool** : http://tools.percona.com/members/wizard . Cet outil permettra de générer un fichier my.cnf qui sera beaucoup plus optimisé pour vos capacités de serveur spécifiques et pour vos exigences.

Ne remplacez pas votre fichier my.cnf existant avec celui de Percona si vous avez déjà chargé les données dans la base de données. Certains des changements qui seront dans le fichier seront incompatibles car elles modifient la façon dont les données sont stockées sur le disque dur et vous serez incapable de démarrer MySQL. Si vous souhaitez vraiment l'utiliser et que vous avez des données existantes, vous devrez générer un fichier de sauvegarde de MySQL avec mysqldump (dump : décharge de la mémoire) et le recharger :

```
mysqldump --all-databases --routines -u root -p > ~/fulldump.sql
```

Cela vous demandera alors le mot de passe root avant de créer une copie des données. Il est conseillé de s'assurer qu'il n'y a pas d'autres utilisateurs ou processus utilisant la base de données pendant que tout cela se déroule. Selon la quantité de données que vous avez dans votre base de données, cela peut prendre un certain temps. Vous ne verrez rien sur l'écran au cours de ce processus.

Une fois la décharge achevé, fermez MySQL :

```
sudo systemctl stop mysql.service
```

Puis sauvegardez le fichier my.cnf original et remplacez-le par le nouveau :

```
sudo cp /etc/mysql/my.cnf /etc/mysql/my.cnf.backup
sudo cp /path/to/new/my.cnf /etc/mysql/my.cnf
```

Ensuite, effacez et réinitialisez l'espace de base de données et assurez-vous que les attributs de propriété soient corrects avant de redémarer MySQL :

```
sudo rm -rf /var/lib/mysql/*
sudo mysql_install_db
sudo chown -R mysql: /var/lib/mysql
sudo systemctl start mysql.service
```

Enfin, il reste à ré-importer vos données. Pour avoir une idée du niveau d'avancement du processus d'importation, vous trouverez l'utilitaire « Pipe Viewer », pv, utile. Il est indiqué ci-après comment installer et utiliser pv dans ce cas, mais si vous préférez ne pas l'utiliser, remplacez simplement pv par cat dans la commande suivante. Ignorez tout les temps ETA généré par pv, ils se fondent sur le temps moyen nécessaire à gérer chaque ligne du fichier, mais la rapidité d'insertion peut varier grandement d'une ligne à l'autre avec mysqldumps :

```
sudo apt install pv
pv ~/fulldump.sql | mysql
```

Une fois ces commandes achevées, c'est bon pour y aller !

Ce n'est pas nécessaire pour tous les changements de my.cnf. La plupart des variables que vous pouvez changer pour améliorer les performances sont réglables même pendant que le serveur fonctionne. Comme avec n'importe quoi, assurez-vous d'avoir une bonne copie de sauvegarde des fichiers de configuration et des données avant toute modification.

12.1.4.2. MySQL Tuner

MySQL Tuner est un outil utile qui se connectera à une instance MySQL active et offre des suggestions sur comment elle peut être configurée au mieux pour votre charge de travail. Plus la durée d'activité du serveur pour cette charge de travail est importante, meilleurs sont les conseils fournis par mysqltuner. Dans un environnement de production, considérez qu'il faut attendre au moins 24 heures avant de lancer cet outil. Vous pouvez obtenir l'installation de mysqltuner depuis les dépôts Ubuntu :

```
sudo apt install mysqltuner
```

Donc, lorsqu'il est installé, lancez le :

```
mysqltuner
```

et attendez son rapport final. La section supérieure fournit de l'information générale à propos du serveur de base de données et la partie inférieure fournit des suggestions de personnalisation à changer dans votre fichier my.cnf. La plupart de celles-ci peuvent être changées en temps réel sur le serveur sans redémarrer ; référez-vous à la documentation officielle de MySQL (le lien est dans la section Ressources) pour les variables pertinentes à changer en production. Ce qui suit est une partie d'un exemple de rapport venant d'une base de donnée de production qui montre qu'il y aurait quelques intérêts à augmenter le volume de cache de requêtes :

```
-------- Recommendations -----------------------------------------------------
General recommendations:
Run OPTIMIZE TABLE to defragment tables for better performance
Increase table_cache gradually to avoid file descriptor limits
Variables to adjust:
key_buffer_size (> 1.4G)
query_cache_size (> 32M)
table_cache (> 64)
innodb_buffer_pool_size (>= 22G)
```

Un dernier commentaire sur les réglages de bases de données : tandis que nous pouvons dire globalement que certains paramètres sont les meilleurs, les performances peuvent varier d'une application à l'autre. Par exemple, ce qui fonctionne le mieux pour Wordpress pourrait ne pas être le meilleur pour Drupal, Joomla ou des applications propriétaires. La performance est tributaire des types de requêtes, de l'utilisation d'indices, de l'efficacité de la conception de la base de données, et ainsi de suite.

Vous trouverez peut-être utile de passer un peu de temps à chercher les conseils de réglage de la base de données en fonction des applications pour lesquelles vous l'utilisez. Une fois que vous avez passé un certain point, tout réglage que vous effectuerez ne permettra d'obtenir que des améliorations mineures, et vous ferez pire plutôt que d'améliorer l'application, sinon en envisageant un redimensionnement de votre environnement de base de données, soit par l'utilisation de matériel plus puissant ou en ajoutant des serveurs esclaves.

12.1.5 Ressources

Consultez **la page d'accueil de MySQL** pour plus d'informations : http://www.mysql.com/ .

Une documentation complète est disponible dans les deux formats en ligne et hors ligne du **portail MySQL pour développeurs** : http://dev.mysql.com/doc/

Pour des informations générales SQL voir **l'Édition Spéciale : Utilisation de SQL** par Rafe Colburn :

http://www.informit.com/store/product.aspx?isbn=0768664128 .

La **page du wiki anglophone d'Ubuntu sur Apache MySQL PHP** contient également des informations utiles : https://help.ubuntu.com/community/ApacheMySQLPHP .

12.2. PostgreSQL

PostgreSQL est un système de base de données relationnel-objet qui a les caractéristiques des systèmes de bases de données commerciales traditionnelles avec les améliorations que l'on trouve dans les systèmes SGBD de nouvelle génération.

12.2.1. Installation

Pour installer **PostgreSQL**, exécutez la commande suivante dans l'invite de commande :

```
sudo apt install postgresql
```

Une fois l'installation terminée, vous devez configurer les serveur PostgreSQL en fonction de vos besoins, bien que la configuration par défaut est viable.

12.2.2. Configuration

PostgreSQL prend en charge plusieures méthodes d'authentification du client. La méthode d'authentification IDENT est utilisée pour **postgres** et les utilisateurs locaux, sauf configuration contraire. Veuillez vous référer au **Guide de l'administrateur de PostgreSQL** si vous souhaitez configurer des solutions de rechange comme Kerberos : http://www.postgresql.org/docs/9.1/static/admin.html .

La discussion qui suit suppose que vous souhaitez activer les connexions TCP/IP et utiliser la méthode MD5 pour l'authentification du client. Les fichiers de configuration de PostgreSQL sont stockés dans le répertoire /etc/postgresql/<version>/main . Par exemple, si vous installez **PostgreSQL 9.1** , les fichiers de configuration sont stockés dans le répertoire /etc/postgresql/9.1/main .

> Pour configurer l'authentification **ident**, ajoutez des entrées au fichier /etc/postgresql/9.1/main/pg_ident.conf. Il y a des commentaires détaillés dans le fichier pour vous guider.

Pour permettre à d'autres ordinateurs de se connecter à votre serveur **PostgreSQL**, éditez le fichier /etc/postgresql/9.1/main/postgresql.conf .

Localisez la ligne **#listen_addresses = 'localhost'** et changez-la en :

```
listen_addresses = '*'
```

> Pour permettre les connexions IPv4 et IPv6 remplacer 'localhost' par '::'

Vous pouvez également modifier tous les autres paramètres, si vous savez ce que vous faites ! Pour plus de détails, référez-vous au fichier de configuration ou à la documentation PostgreSQL.

Maintenant que nous pouvons nous connecter à notre serveur PostgreSQL, l'étape suivante consiste à définir un mot de passe pour l'utilisateur **postgres**. Exécutez la commande suivante à l'invite de commande d'un terminal, pour se connecter à la base de données modèle PostgreSQL par défaut :

```
sudo -u postgres psql template1
```

La commande ci-dessus se connecte à la base de données **PostgreSQL template1** en tant qu'utilisateur

postgres . Une fois que vous vous connectez au serveur PostgreSQL, vous serez à l'invite SQL. Vous pouvez exécuter la commande SQL suivante à l'invite **psql** pour configurer le mot de passe pour l'utilisateur **postgres** :

```
ALTER USER postgres with encrypted password 'votre_mot_de_passe';
```

Après avoir configuré le mot de passe, modifiez le fichier / etc/postgresql/9.1/main/pg_hba.conf pour utiliser l'authentification **MD5** avec l'utilisateur **postgres** :

```
local       all         postgres                          md5
```

Enfin, vous devez redémarrer le service **PostgreSQL** pour initialiser la nouvelle configuration. À partir d'un terminal, tapez ceci pour redémarrer **PostgreSQL** :

```
sudo systemctl restart postgresql.service
```

! La configuration ci-dessus n'est pas complète en tout sens. Veuillez vous référer au **Guide de l'administrateur de PostgreSQL** pour configurer plusieurs paramètres : http://www.postgresql.org/docs/9.1/static/admin.html .

Vous pouvez tester les connexions au serveur à partir d'autres machines en utilisant le client **PostgreSQL**.

```
sudo apt install postgresql-client
psql -h postgres.example.com -U postgres -W
```

R emplacez le nom de domaine par votre nom de domaine de serveur actuel.

12.2.3. Sauvegardes

Les bases de données **PostgreSQL** doivent être sauvegardées régulièrement. Reportez-vous au **Guide de l'administrateur de PostgreSQL** pour différentes approches : http://www.postgresql.org/docs/9.1/static/backup.html .

12.2.4. Ressources

Comme mentionné ci-dessus le **Guide de l'administrateur de PostgreSQL** est une excellente ressource : http://www.postgresql.org/docs/9.1/static/admin.html . Le guide est également disponible dans le paquet **postgresql-doc-9.1**. Exécutez la commande suivante dans un terminal pour installer le paquet :

```
sudo apt install postgresql-doc-9.1
```

Pour consulter le guide, saisissez **file:///usr/share/doc/postgresql-doc-9.1/html/index.html** dans la barre d'adresse de votre navigateur internet.

Pour des informations générales sur SQL, consultez l'**Édition Spéciale : Using SQL** (en anglais) par Rafe Colburn : http://www.informit.com/store/product.aspx?isbn=0768664128

La **page du wiki anglophone d'Ubuntu sur PostgreSQL** contient également des informations utiles : https://help.ubuntu.com/community/PostgreSQL .

Chapitre 13. Les programmes LAMP

13.1. Vue d'ensemble

Les installations LAMP (Linux + Apache + MySQL + PHP/Perl/Python) sont des configurations populaires pour les serveurs Ubuntu. Il existe une pléthore d'applications Open Source écrites en utilisant le jeu d'applications LAMP. Certaines applications LAMP populaires sont les Wikis, les systèmes de gestion de contenu et les logiciel de gestion comme phpMyAdmin.

L'un des avantages de LAMP est sa grande flexibilité, notamment pour les base de données, les serveurs web et les langages de script. Les substituts populaires pour MySQL incluent PostgreSQL et SQLite. Python, Perl et Ruby sont également fréquemment utilisé à la place de PHP. Tandis que Nginx, Cherokee et Lighttpd peuvent remplacer Apache.

Le moyen le plus rapide pour commencer est d'installer LAMP en utilisant **tasksel**. Tasksel est un outil Debian/Ubuntu qui installe plusieurs paquets liés en tant que « tâches » coordonnées sur votre système. Pour installer un serveur LAMP :

- A l'invite de commande, entrez les commandes suivantes :

```
sudo tasksel install lamp-server
```

- Après l'avoir installé, vous serez en mesure d'installer la plupart des applications **LAMP** de cette façon :
- Téléchargez une archive contenant les fichiers sources du programme.
- Décompressez l'archive, généralement dans un répertoire accessible par le serveur Web.
- Selon l'endroit où la source a été extraite, configurez un serveur web pour servir les fichiers.
- Configurez le programme pour qu'il se connecte à la base de données.
- Lancez un script ou allez sur une page de ce programme pour installer la base de données dont il a besoin.
- Vous pourrez vous servir du programme une fois que toutes ces étapes ont été achevées.

Un des inconvénients de cette méthode est que les fichiers des programmes ne se trouvent pas dans les endroits standard du système de fichiers, ce qui peut entraîner des confusions quant à leur emplacement. Un autre plus important apparaît lors de la mise à jour du programme. Lorsqu'une nouvelle version est distribuée, il vous faudra repasser par toutes ces étapes.

Heureusement, grand nombre de ces applications **LAMP** sont disponibles dans les dépôts Ubuntu. Cependant, selon le type de programme, vous devrez éventuellement les configurer après-coup.

Cette section explique comment installer des applications **LAMP**.

13.2. Moin Moin

MoinMoin est un moteur pour wiki développé en Python, basé sur le moteur PikiPiki Wiki, et distribué sous la liscence GNU GPL.

13.2.1. Installation

Pour installer **MoinMoin**, lancez la commande suivante dans un terminal :

```
sudo apt install python-moinmoin
```

Vous devriez installer aussi Serveur web **apache2**. Pour cette installation, référez-vous au *Chapitre 11, paragraphe 1. HTTPD - serveur web Apache2 .1, Installation*.

13.2.2. Configuration

Pour configurer votre première application wiki, veuillez lancer les commandes suivantes. Supposons que vous créiez un wiki appelé **mywiki** :

```
cd /usr/share/moin
sudo mkdir mywiki
sudo cp -R data mywiki
sudo cp -R underlay mywiki
sudo cp server/moin.cgi mywiki
sudo chown -R www-data:www-data mywiki
sudo chmod -R ug+rwX mywiki
sudo chmod -R o-rwx mywiki
```

Maintenant, vous devez configurer **MoinMoin** pour trouver votre nouveau wiki mywiki. Pour configurer **MoinMoin**, ouvrez le fichier /etc/moin/mywiki.py et changez la ligne suivante :

```
data_dir = '/org/mywiki/data'
```

en

```
data_dir = '/usr/share/moin/mywiki/data'
```

Ajoutez aussi **data_underlay_dir** sous l'option **data_dir** :

```
data_underlay_dir='/usr/share/moin/mywiki/underlay'
```

Si le fichier /etc/moin/mywiki.py n'existe pas, vous devriez copier le fichier /usr/share/moin/config/wikifarm/mywiki.py sur le fichier /etc/moin/mywiki.py et faire la modification ci-dessus.

Si vous avez nommé votre wiki **my_wiki_name** vous devriez insérer une ligne « ("my_wiki_name", r".*")" » dans le fichier /etc/moin/farmconfig.py après la ligne « ("mywiki", r".*")" ».

Lorsque vous avez configuré **MoinMoin** pour trouver votre première application wiki, **mywiki**, vous devriez configurer **apache2** et le préparer pour votre wiki.

Vous devriez ajouter les lignes suivante dans le fichier /etc/apache2/sites-available/000-default.conf dans le tag "<VirtualHost *>" :

```
### moin
  ScriptAlias /mywiki "/usr/share/moin/mywiki/moin.cgi"
  alias /moin_static<version> "/usr/share/moin/htdocs"
  <Directory /usr/share/moin/htdocs>
  Order allow,deny
  allow from all
  </Directory>
### end moin
```

La version, dans l'exemple ci-dessus, est déterminée en lançant :

```
$ moin –version
```

Si la réponse est version 1.9.7, votre seconde ligne devrait être :

```
alias /moin_static197 "/usr/share/moin/htdocs"
```

Lorsque vous avez configuré votre serveur web **apache2** et l'avez préparé pour votre application wiki, vous devriez le relancer. Vous pouvez lancer la commande suivante pour redémarrer le serveur web **apache2** :

```
Sudo systemctl restart apache2.service
```

13.2.3. Vérification

Vous pouvez vérifier le bon fonctionnement de votre application Wiki en saisissant l'URL suivante dans votre navigateur Web :

```
http://localhost/mywiki
```

Référez-vous au site web **MoinMoin** pour de plus amples informations : http://moinmo.in/ .

13.2.4. Références

Consultez le **Wiki de moinmoin** pour de plus amples informations : http://moinmo.in .

Vous pouvez également consulter la page **du wiki Ubuntu pour MoinMoin** (en anglais) : https://help.ubuntu.com/community/MoinMoin .

13.3. phpMyAdmin

phpMyAdmin est un programme LAMP écrit spécifiquement pour administrer les serveurs **MySQL**. Écrit en PHP et accessible à l'aide d'un navigateur Web, phpMyAdmin fournit une interface graphique pour l'administration des bases de données.

13.3.1. Installation

Avant d'installer **phpMyAdmin**, il est préférable de pouvoir accéder à une base de données **MySQL** soit sur le même hôte soit sur un hôte accessible par le réseau. Voir le *Chapitre 12, paragraphe 1. MySQL* pour de plus amples informations. Saisissez :

```
sudo apt install phpmyadmin
```

À l'invite de commandes, choisissez quel serveur Web vous souhaitez configurer pour **phpMyAdmin**. Nous utiliserons le serveur **Apache2** par la suite.

Dans un navigateur aller à **http://servername/phpmyadmin** , en remplaçant **servername** avec nom d'hôte du serveur. A la connexion, la page entrez **root** pour le **nom d'utilisateur**, ou d'une autre **MySQL** utilisateur, si vous avez ne importe quelle configuration, et entrez dans la **MySQL** mot de passe de l'utilisateur.

Une fois identifié et si vous avez les droits nécessaires, vous pouvez changez le mot de passe **root**, gérer les utilisateurs, les tables, etc.

13.3.2. Configuration

Les fichiers de configuration de **phpMyAdmin** sont situés dans /etc/phpmyadmin. Le fichier principal de configuration est /etc/phpmyadmin/config.inc.php. Il contient les options qui s'appliquent globalement à **phpMyAdmin**.

Afin d'utiliser **phpMyAdmin** pour administrer une base de données MySQL d'un autre serveur, modifiez /etc/phpmyadmin/config.inc.phpen conséquence :

```
$cfg['Servers'][$i]['host'] = 'db_server';
```

Remplacez **db_server** par le nom du serveur distant ou par son adresse IP. Assurez-vous que l'hôte de **phpMyAdmin** a les droits nécessaires pour accéder à cette base de données distante.

Une fois **phpMyAdmin** configuré, déconnectez-vous et connectez-vous à nouveau. Vous devriez accéder au nouveau serveur.

Les fichiers config.header.inc.php et config.footer.inc.php sont utilisés pour ajouter un en-tête et un pied de page HTML à **phpMyAdmin**.

/etc/phpmyadmin/apache.conf est un autre fichier de configuration important. Ce fichier est lié par symlink au fichier /etc/apache2/conf-available/phpmyadmin.conf, et, une fois activé, est utilisé pour configurer **Apache2** pour servir le site **phpMyAdmin**. Ce fichier contient des directives pour charger **PHP**, les permissions de répertoire, etc.... Depuis un terminal, entrez[nbsp] :

```
sudo ln -s /etc/phpmyadmin/apache.conf \
/etc/apache2/conf-available/phpmyadmin.conf
sudo a2enconf phpmyadmin.conf
sudo systemctl reload apache2.service
```

Pour plus d'informations sur la configuration d'**Apache2**, voir *Chapitre 11, paragraphe 1. HTTPD - serveur web Apache2* .

13.3.3. Références

- La documentation de **phpMyAdmin** est fournie avec le paquet phpmyadmin et peut être affichée en cliquant sur le lien **Documentation de phpMyAdmin** (point d'interrogation dans une bulle) se trouvant juste en dessous du logo phpMyAdmin. La documentation officielle est aussi accessible en ligne à **phpMyAdmin** : http://www.phpmyadmin.net/home_page/docs.php .
- **Mastering phpMyAdmin** est aussi une bonne source d'informations : http://www.packtpub.com/phpmyadmin-3rd-edition/book .
- Une troisième ressource est la page du **wiki Ubuntu sur phpMyAdmin** (en anglais) : https://help.ubuntu.com/community/phpMyAdmin .

13.4. WordPress

Wordpress est un outil blog, une plate-forme de publication et de mise en œuvre avec CMS en PHP et distribué sous license GNU GPLv2.

13.4.1. Installation

Pour installer **WordPress**, exécutez la commande suivante dans l'invite :

```
sudo apt install wordpress
```

Vous devriez également installer le serveur web **apache2** et le serveur **mysql**. Pour l'installation du serveur web **apache2**, veuillez vous référer au *Chapitre 11, paragraphe 1. HTTPD - serveur web Apache2 , 1.1. Installation*. Pour l'installation du serveur **mysql**, referez vous au *Chapitre 12, paragraphe 1. MySQL.*

13.4.2. Configuration

Pour configurer votre première application **WordPress**, configurez un site apache. Ouvrir /etc/apache2/sites-available/wordpress.conf et écrire les lignes suivantes :

```
Alias /blog /usr/share/wordpress
<Directory /usr/share/wordpress>
    Options FollowSymLinks
    AllowOverride Limit Options FileInfo
    DirectoryIndex index.php
    Order allow,deny
    Allow from all
</Directory>
<Directory /usr/share/wordpress/wp-content>
    Options FollowSymLinks
    Order allow,deny
    Allow from all
</Directory>
```

Activez ce nouveau site **WordPress**

```
sudo a2ensite wordpress
```

Dès que le serveur web **apache2** est configuré et prêt pour votre application **WordPress**, vous devriez le redémarrer en exécutant la commande suivante :

```
sudo systemctl restart apache2.service
```

Pour faciliter des installations multiples de **WordPress**, le nom de ce fichier de configuration est basée sur l'en-tête de l'hôte de la requête HTTP. Cela signifie que vous pouvez avoir une configuration par VirtualHost par simple correspondance à la partie hôte de cette configuration avec votre hôte virtuel Apache. eg

/etc/wordpress/config-10.211.55.50.php, /etc/wordpress/config-hostalias1.php, etc... Ces instructions supposent que vous pouvez accéder à Apache via le nom d'hôte localhost (peut-être en utilisant un tunnel ssh) sinon, remplacer /etc/wordpress/config-localhost.php par /etc/wordpress/config-NAME_OF_YOUR_VIRTUAL_HOST.php.

Une fois le fichier de configuration est écrit, c'est à vous de choisir une convention de nom d'utilisateur et mot de passe mysql pour chaque **WordPress** instance de base de données. Cette documentation montre qu'un seul exemple localhost.

Maintenant, configurez **WordPress** pour utiliser une base de données mysql. Ouvrez le fichier /etc/wordpress/config-localhost.php et écrivez les lignes suivantes :

```
<?php
define('DB_NAME', 'wordpress');
define('DB_USER', 'wordpress');
define('DB_PASSWORD', 'yourpasswordhere');
define('DB_HOST', 'localhost');
define('WP_CONTENT_DIR', '/usr/share/wordpress/wp-content');
?>
```

Maintenant, créez cette base de données mysql. Ouvrez un fichier temporaire avec la commande mysql wordpress.sql et écrivez les lignes suivantes :

```
CREATE DATABASE wordpress;
GRANT SELECT,INSERT,UPDATE,DELETE,CREATE,DROP,ALTER
ON wordpress.*
TO wordpress@localhost
IDENTIFIED BY 'yourpasswordhere';
FLUSH PRIVILEGES;
```

Exécutez ces commande.

```
cat wordpress.sql | sudo mysql --defaults-extra-file=/etc/mysql/debian.cnf
```

Votre nouveau **WordPress** peut maintenant être configuré en visitant http://localhost/blog/wp-admin/install.php . Ou, si votre serveur possède pas d'interface graphique, un autre site : http://NAME_OF_YOUR_VIRTUAL_HOST/blog/wp-admin/install.php ; vous remplissez la configuration **WordPress** via un navigateur Web s'exécutant sur un autre ordinateur. Remplir le titre du site, le nom d'utilisateur, le mot de passe, le courriel et cliquez sur **Installer WordPress**.

Notez le mot de passe généré (le cas échéant) et cliquez sur le mot de passe de connexion. Votre **WordPress** est maintenant prêt à être utilisé.

13.4.3. Références

Le Codex WordPress.org : https://codex.wordpress.org/

Le Wiki Ubuntu WordPress : https://help.ubuntu.com/community/WordPress

Chapitre 14. Serveurs de fichier

Si vous avez plus d’un seul ordinateur sur un réseau, vous aurez probablement besoin un jour de partager des fichiers entre les machines. Dans cette section nous allons traiter de l’installation et du paramétrage de FTP, NFS et CUPS.

14.1. Serveur FTP

Le protocole de transfert de fichiers (FTP) est un protocole TCP fait pour télécharger des fichiers entre des ordinateurs. Dans le passé, il a également été utilisé pour l'envoi de données, mais, comme cette méthode n'utilise pas le chiffrage, les informations d'identification des utilisateurs et les données sont transmises en clair et sont donc facilement interceptées. Alors, si vous cherchez un moyen de transférer des fichiers en toute sécurité, consultez à la place la section **OpenSSH** dans le *Chapitre 6. Administration à distance*.

Le FTP fonctionne sur un modèle client/serveur. L'élément serveur est appelé **démon FTP**. Il écoute en permanence les requêtes FTP des clients distants. Lorsqu'une demande est reçue, il gère l'ouverture de session et établit la connexion. Pendant la durée de la session, il exécute toutes les commandes envoyées par le client FTP.

L'accès à un serveur FTP peut être pris en charge de deux façons :

- Anonyme
- Authentifié

Dans le mode anonyme, les clients distants peuvent accéder au serveur FTP en utilisant le compte d'utilisateur par défaut appelé anonyme" ou"ftp" et en envoyant une adresse e-mail comme mot de passe. En mode authentifié un utilisateur doit avoir un compte et un mot de passe. Ce dernier choix est très précaire et ne doit pas être utilisé, sauf dans des circonstances particulières. Si vous êtes à la recherche de transférer des fichiers en toute sécurité SFTP voir dans la section sur OpenSSH-Server. L'accès des utilisateurs aux répertoires du serveur FTP et les fichiers dépend des permissions définies pour le compte utilisé lors de la connexion. En règle générale, le démon FTP permet de masquer le répertoire racine du serveur FTP et allez dans le répertoire d'accueil FTP. Cela masque le reste du système de fichiers de sessions à distance.

14.1.1. vsftpd - Installation du serveur FTP

vsftpd est un démon FTP disponible dans Ubuntu. Il est facile à installer, à configurer et à entretenir. Pour installer **vsftpd** vous pouvez exécuter la commande suivante :

```
sudo apt install vsftpd
```

14.1.2. Configuration d'un FTP anonyme

Par défaut, **vsftpd** n'est **pas** configuré pour permettre le téléchargement anonyme. Si vous souhaitez activer le téléchargement anonyme, modifiez le fichier de configuration /etc/vsftpd.conf en changeant :

```
anonymous_enable=Yes
```

Lors de l'installation, un utilisateur **ftp** est créé avec un répertoire personnel nommé /srv/ftp. Il s'agit du répertoire FTP par défaut.

Si vous souhaitez modifier cet emplacement en /srv/files/ftp par exemple, il suffit de créer un répertoire dans un autre emplacement et de changer le répertoire personnel de l'utilisateur :

```
sudo mkdir /srv/files/ftp
sudo usermod -d /srv/files/ftp ftp
```

Les changements effectués, redémarrez **vsftpd** :

```
sudo restart vsftpd
```

Enfin, copiez les fichiers et répertoires que vous voulez rendre disponibles via le serveur FTP anonyme dans /srv/files/ftp, ou alors /srv/ftp si vous souhaitez utiliser le dossier par défaut.

14.1.3. Configuration d'un serveur FTP avec authentification des utilisateurs

Par défaut, **vsftpd** est configuré pour authentifier les utilisateurs système et leur permettre de télécharger des fichiers. Si vous voulez que les utilisateurs puissent envoyer des fichiers sur le serveur, modifiez /etc/vsftpd.conf :

```
write_enable=YES
```

Redémarrez maintenant **vsftpd** :

```
sudo restart vsftpd
```

Maintenant lorsque des utilisateurs de votre système se connectent au FTP, leur répertoire racine sera leur répertoire **personnel (/home/utilisateur)** dans lequel ils pourront télécharger (download/upload), créer des répertoires etc…

De même, par défaut, les utilisateurs anonymes ne sont pas autorisés à envoyer des fichiers vers le serveur FTP. Pour modifier ce paramètre, vous pouvez supprimer le commentaire de la ligne suivante puis redémarrer **vsftpd** :

```
anon_upload_enable=YES
```

> ! Autoriser des téléchargements (upload) anonymes d'Internet vers le serveur est une faille de sécurité majeure. Il est préférable de ne pas l'autoriser pour des serveurs branchés directement sur Internet.

Le fichier de configuration est composé de plusieurs paramètres de configuration. Les informations à propos de chaque paramètre sont disponibles dans le fichier de configuration. Vous pouvez aussi vous référer à la page du manuel (man page), **man 5 vsftpd.conf** pour les détails de chaque paramètre.

14.1.4. Sécuriser le serveur FTP

Des options de /etc/vsftpd.conf permettent de sécuriser un tant soit peu **vsftpd**. Par exemple, les utilisateurs peuvent être confinés dans leur répertoire personnel en dé-commentant :

```
chroot_local_user=YES
```

Vous pouvez aussi définir les utilisateurs qui seront confinés dans leur répertoire personnel (home) :

```
chroot_list_enable=YES
```

```
chroot_list_file=/etc/vsftpd.chroot_list
```

Après avoir dé-commenté l'option ci-dessus, créez le fichier /etc/vsftpd.chroot_list contenant la liste des utilisateurs à restreindre. Mettez un utilisateur par ligne. Redémarrez ensuite **vsftpd** :

```
sudo restart vsftpd
```

De manière similaire, le fichier /etc/ftpusers contient les utilisateurs qui ne sont pas autorisés à se connecter au serveur FTP. la liste par défaut inclut root, daemon, nobody, etc. Écrivez dans cette liste les utilisateurs que vous ne souhaitez pas voir connectés au FTP.

FTP peut également être cryptées en utilisant FTPS . Différente de **SFTP**, **FTPS** est FTP via Secure Socket Layer (SSL). **SFTP** est un FTP comme sur une session de SSH cryptée de connexion. Une différence majeure est que les utilisateurs de SFTP besoin d'avoir un shell compte sur le système, au lieu d'un **nologin** shell. Offrir à tous les utilisateurs un shell peut ne pas être idéal pour certains environnements, tels que un hébergeur partagé. Cependant, il est possible de limiter de tels comptes SFTP uniquement et désactiver l'interaction coquille. Voir la section sur OpenSSH-Server pour plus d'informations.

Pour configurer **FTPS**, modifiez /etc/vsftpd.conf et ajoutez en fin de fichier :

```
ssl_enable=Yes
```

Prenez garde aux options certificat et clef :

```
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
```

Par défaut, ces options sont définies dans le certificat et la clé fournie par le paquet **ssl-cert**. Dans un environnement de production, ceux-ci doivent être remplacés par un certificat et une clé générés pour l'hôte spécifique. Pour plus d'informations sur les certificats, voir le *Chapitre 9, paragraphe 5. Certificats*.

Redémarrez maintenant **vsftpd**, et les utilisateurs non-anonymes seront désormais forcés d'utiliser **FTPS** :

```
sudo restart vsftpd
```

Pour permettre aux utilisateurs avec un shell /usr/sbin/nologin de se connecter au FTP, mais sans accès shell, il est nécessaire d'ajouter le shell **nologin** au fichier /etc/shells :

```
# /etc/shells: shells de connexion valides
/bin/csh
/bin/sh
/usr/bin/es
/usr/bin/ksh
/bin/ksh
/usr/bin/rc
/usr/bin/tcsh
/bin/tcsh
/usr/bin/esh
/bin/dash
/bin/bash
/bin/rbash
/usr/bin/screen
/usr/sbin/nologin
```

En effet, par défaut, **vsftpd** utilise PAM pour l'identification et le fichier de configuration /etc/pam.d/vsftpd stipule :

```
auth     required       pam_shells.so
```

Le module PAM **shells** a pour effet de n'autoriser que les shells listés dans le fichier /etc/shells.

Les clients FTP les plus populaires peuvent être configurés pour se connecter en utilisant FTPS. Le client FTP en ligne de commande **lftp** a aussi la possibilité d'utiliser FTPS.

14.1.5. Références

Consultez le **site internet de vsftpd** pour de plus amples informations : http://vsftpd.beasts.org/vsftpd_conf.html .

Pour les options détaillées de /etc/vsftpd.conf référez-vous à la **page de man de vsftpd.conf** : http://manpages.ubuntu.com/manpages/xenial/en/man5/vsftpd.conf.5.html .

14.2. 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.

Parmi les avantages les plus remarquables de NFS, on peut mentionner :

- Les stations de travail locales utilisent moins d'espace disque parce que les données fréquemment utilisées peuvent être stockées sur une seule machine centrale tout en restant accessibles à d'autres par le réseau.
- Il n'est pas nécessaire que les utilisateurs disposent d'un répertoire personnel sur chaque machine du réseau. Les répertoires personnels peuvent être centralisés sur le serveur NFS afin d'être accessibles par tout le réseau.
- Les périphériques de stockage, comme les lecteurs disquettes, les lecteurs de CD-ROM ou les clefs USB, peuvent être utilisés par d'autres machines du réseau. Ceci permet de réduire le nombre de lecteurs de supports amovibles sur un réseau.

14.2.1. Installation

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

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

14.2.2. 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)
```

Vous pouvez remplacer * par l'un des formats de nom d'hôte. La formulation du nom d'hôte devrait être la plus précise possible pour éviter que des systèmes indésirables puissent accéder aux points de montage NFS.

Pour démarrer le serveur NFS, saisissez la commande suivante dans un terminal :

```
sudo systemctl start nfs-kernel-server.service
```

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

Une autre façon de monter un partage NFS à partir d'une autre machine est d'ajouter une ligne au fichier /etc/fstab. La ligne doit comporter le nom d'hôte du serveur NFS, le répertoire du serveur qui doit être partagé, et le répertoire de la machine locale où le partage NFS doit être monté.

La syntaxe générale de la ligne dans le fichier /etc/fstab est celle-ci :

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

Si vous rencontrez des ennuis pour monter un partage NFS, assurez-vous que le paquet **nfs-common** est installé chez votre client. Pour installer **nfs-common**, entrer la commande suivante à l'invite de commande d'un terminal :

```
sudo apt install nfs-common
```

14.2.4. Références

QFD Linux NFS : http://nfs.sourceforge.net/

Le wiki Guide de NFS d'Ubuntu : https://help.ubuntu.com/community/NFSv4Howto

14.3. Initiateur iSCSI

iSCSI (Internet Small Computer System Interface) est un protocole qui permet à des commandes SCSI d'être transmises sur un réseau. Typiquement iSCSI est mise en œuvre dans un réseau SAN (Storage Area Network) pour permettre aux serveurs d'accéder à un grand magasin d'espace disque dur. Le protocole iSCSI se réfère à des clients comme initiateurs et les serveurs iSCSI en tant que cibles .

Ubuntu Server peut être configuré à la fois comme un initiateur iSCSI et une cible. Ce guide fournit des commandes et options de configuration pour configurer un initiateur iSCSI. Il est supposé que vous avez déjà une cible iSCSI sur votre réseau local et disposer des droits appropriés pour s'y connecter. Les instructions pour configurer une cible varient grandement entre les fournisseurs de matériel, afin de consulter la documentation de votre fournisseur pour configurer votre cible iSCSI spécifique.

14.3.1. Installation de l'initiateur iSCSI

Pour configurer un serveur Ubuntu en tant qu'initiateur iSCSI, installez le paquet **open-iscsi**. Dans un terminal tapez :

```
sudo apt install open-iscsi
```

14.3.2. Configuration de l'initiateur iSCSI

Une fois le paquet **open-iscsi** installé, modifiez /etc/iscsi/iscsid.conf en changeant ce qui suit :

```
node.startup = automatic
```

Vous pouvez vérifier quelles cibles sont disponibles en utilisant l'utilitaire **iscsiadm**. Entrez la commande suivante dans un terminal :

```
sudo iscsiadm -m discovery -t st -p 192.168.0.10
```

- **-m :** détermine le mode dans lequel iscsiadm s'exécute.
- **-t :** spécifie le type de détection.
- L'option **-p :** indique l'adresse IP cible.

R emplacez l'exemple **192.168.0.10** par l'adresse IP cible sur votre réseau.

Si la cible est disponible, vous devriez voir une sortie semblable à ce qui suit :

```
192.168.0.10:3260,1 iqn.1992-05.com.emc:sl7b92030000520000-2
```

L e numero **iqn** et l'adresse IP ci-dessus varieront en fonction de votre matériel.

Vous devriez maintenant être en mesure de vous connecter à la cible iSCSI, et en fonction de la configuration de votre cible, vous devrez saisir les informations d'identification de l'utilisateur. Connectez-vous au nœud iSCSI :

```
sudo iscsiadm -m node --login
```

Assurez-vous que le nouveau disque a été détecté à l'aide de **dmesg** :

```
dmesg | grep sd
```

```
[4.322384] sd 2:0:0:0: Attached SCSI générique sg1 tapez 0
[4.322797] sd 2:0:0:0: [sda] 41943040 blocs de 512 octets logiques: (21,4 GB/20.0 GiB )
[4.322843] sd 2:0:0:0: [sda] Write Protect est désactivé
[4.322846] sd 2:0:0:0: [sda] Mode Sense: 03 00 00 00
[4,322896 ] sd 2:0:0:0: [sda] Cache de données disponible
[4.322899] sd 2:0:0:0: [sda] En supposant cache du disque: écrire par
[4.323230] sd 02:00:00 : 0: [sda] Les données de cache disponible
[4.323233] sd 2:0:0:0: [sda] En supposant cache du disque: écrire par
[4,325312] sda: sda1 sda2 <sda5>
[4,325729 ] sd 2:0:0:0: [sda] Cache de données disponible
[4.325732] sd 2:0:0:0: [sda] En supposant cache du disque: écrire par
[4.325735] sd 02:00:00 : 0: [sda] Attached SCSI disque
[2486.941805] sd 4:0:0:3: Attached SCSI générique sg3 type 0
[2486.952093] sd 4:0:0:3: [sdb] 1126400000 512 octets blocs logiques: (576 GB/537 Gio)
[2486.954195] sd 4:0:0:3: [sdb] Write Protect est désactivé
[2486.954200] sd 4:0:0:3: [sdb] Mode Sense : 00 00 08 8f
[2486.954692] sd 4:0:0:3: [sdb] Write cache: désactivé, cache de lecture: activé, ne
support DPO ou FUA
[2486.960577] sdb: sdb1
[2486.964862] sd 4:0:0:3: [sdb] Attached SCSI disque
```

Dans la sortie ci-dessus **sdb** est le nouveau disque iSCSI. Rappelez-vous que ceci est un exemple, la sortie que vous aurez sur votre écran sera différente.

Ensuite, créez une partition, formatez le système de fichiers et montez le nouveau disque iSCSI. Dans un terminal saisissez :

```
sudo fdisk /dev/sdb
n
p
enter
w
```

Les commandes ci-dessus proviennent de l'intérieur de la commande utilitaire fdisk, voir fdisk <commande> pour des instructions plus détaillées. En outre, le cfdisk utilitaire est parfois plus facile à utiliser.

Maintenant, formatez le système de fichiers montez le dans /srv à titre d'exemple :

```
sudo mkfs.ext4 /dev/sdb1
sudo mount /dev/sdb1 /srv
```

Enfin, ajoutez une entrée dans /etc/fstab pour monter le disque iSCSI lors du démarrage :

```
/dev/sdb1         /srv        ext4        defaults,auto,_netdev 0 0
```

C’est une bonne idée de s’assurer que tout fonctionne comme prévu en redémarrant le serveur.

14.3.3. Références

Site web de Open-iSCSI : http://www.open-iscsi.com/

Page Debian Open-iSCSI : http://wiki.debian.org/SAN/iSCSI/open-iscsi

14.4. CUPS - Serveur d'impression

Le système principal d'impression sous Ubuntu est le **Common UNIX Printing System** (CUPS). Ce système d'impression, qui est librement disponible et portable, est devenu le nouveau standard pour imprimer dans la plupart des distributions Linux.

CUPS organise les tâches d'impression, les met en file d'attente, et rend possible l'impression en réseau en utilisant le standard d'impression Internet Printing Protocol (IPP). Il offre un large support pour un très grand nombre d'imprimantes, allant des imprimantes matricielles aux imprimantes laser, en passant par de nombreux autres types. CUPS offre également le support PostScript Printer Description (PPD - description d'imprimante PostScript) et l'auto-détection des imprimantes réseaux, sans oublier une interface de configuration Web simple et des outils d'administration.

14.4.1. Installation

Pour installer CUPS sur votre ordinateur Ubuntu, utilisez simplement **sudo** avec la commande **apt** et saisissez le paquet à installer comme premier paramètre. Une installation complète de CUPS a beaucoup de dépendances de paquet, mais elles pourraient être toutes spécifiées sur la même ligne de commande. Entrez ce qui suit à l'invite de commande d'un terminal pour installer CUPS :

```
sudo apt install cups
```

Une fois identifié avec votre mot de passe utilisateur, les paquets devraient être téléchargés et installés sans problème. Dès la fin de l'installation, le serveur CUPS sera démarré automatiquement.

À des fins de dépannage, vous pouvez consulter le fichier journal des erreurs de CUPS à l'emplacement suivant : /var/log/cups/error_log . Si le journal des erreurs n'affiche pas suffisamment d'informations pour identifier les problèmes que vous rencontrez, la quantité d'information enregistrée peut être accrue en modifiant dans le fichier de configuration, le paramètre **LogLevel** de la valeur par défaut « info » vers « debug » ou même « debug2 », ce qui enregistrera tous les événements. Si vous faites cette modification, n'oubliez pas de remettre ce paramètre à sa valeur d'origine une fois votre problème réglé afin d'éviter que le fichier journal ne devienne trop important.

14.4.2 Configuration

Le comportement du système commun d'impression sous Linux est configuré par les directives contenues dans le fichier /etc/cups/cupsd.conf. La syntaxe du fichier de configuration de CUPS est identique au fichier principal de configuration du serveur HTTP Apache, les utilisateurs déjà habitués à éditer les fichiers Apache devraient donc se sentir à l'aise. Quelques exemples de modifications que vous pourriez souhaiter apporter vont être présentés ici.

> Avant de modifier le fichier de configuration, vous devriez faire une copie de la configuration originale et la protéger en écriture. Vous disposerez ainsi des paramètres par défaut en guise de référence que vous pourrez réutiliser au besoin.

Copiez le fichier /etc/cups/cupsd.conf et protégez-le en écriture en exécutant dans un terminal la commande suivante :

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

- **ServerAdmin** : Pour configurer l'adresse courriel de l'administrateur du serveur CUPS, éditez simplement le fichier de configuration /etc/cups/cupsd.conf à l'aide de votre éditeur de texte préféré, et ajoutez ou modifiez la ligne **ServerAdmin** conformément. Par exemple, si vous êtes l'administrateur du serveur CUPS, et que votre adresse courriel est « bjoy@somebigco.com », vous devriez donc modifier la ligne ServerAdmin comme ceci :

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

- **Listen** : Par défaut sur Ubuntu, le serveur CUPS n'est en écoute que sur l'interface de bouclage à l'adresse IP **127.0.0.1**. Pour indiquer au serveur CUPS qu'il doit être en écoute sur l'adresse IP d'une véritable interface réseau, vous devez spécifier un nom d'hôte, une adresse IP, ou en option un couple adresse IP/port, en ajoutant une directive « Listen ». Par exemple, si votre serveur CUPS se trouve sur un réseau local à l'adresse IP **192.168.10.250** et que vous vouliez le rendre accessible aux autres systèmes de ce réseau, vous devrez modifier /etc/cups/cupsd.conf pour y ajouter une directive « Listen » comme ceci :

  ```
  Listen 127.0.0.1:631 # Directive d'écoute existante sur l'interface loopback
  Listen /var/run/cups/cups.sock # Directive d'écoute existante sur un socket
  Listen 192.168.10.250:631 # Directive d'écoute sur l'interface réseau local, port 631 (IPP)
  ```

  Dans l'exemple ci-dessus, vous pouvez commenter ou supprimer la référence à l'adresse loopback (127.0.0.1) si vous ne voulez pas que **cupsd** écoute sur cette interface, mais préférez qu'il n'écoute que sur les interfaces Ethernet du réseau local. Pour activer l'écoute sur toutes les interfaces réseau auxquelles un nom d'hôte donné est lié, y compris l'interface loopback, vous pourriez créer une entrée Listen pour le nom d'hôte **socrates** comme cela :

  ```
  Listen socrates:631 # Directive d'écoute sur toutes les interfaces du nom d'hôte 'socrates'
  ```

  ou en omettant la directive Listen et en utilisant **Port**, comme cela :

  ```
  Port 631 # Écouter sur le port 631 de toutes les interfaces
  ```

Pour des exemples supplémentaires de directives de configuration du serveur CUPS, consultez le manuel associé en tapant la commande suivante dans un terminal :

```
man cupsd.conf
```

À chaque modification du fichier de configuration /etc/cups/cupsd.conf, vous devrez redémarrer le serveur CUPS en tapant dans un terminal la commande suivante :

```
sudo systemctl restart cups.service
```

14.4.3. Interface Web

CUPS peut être configuré et contrôlé en utilisant un interface web, qui est par défaut accessible à : http://localhost:631/admin . L'interface web peut être utilisée pour réaliser toutes les opérations de gestion d'imprimante.

Dans le but de réaliser des opérations administratives à l'aide de l'interface web, vous devrez soit avoir le compte super-utilisateur (root) activé sur votre serveur, soit vous authentifier comme utilisateur du groupe **lpadmin**. Pour des raisons de sécurité, CUPS n'acceptera pas d'inclure un utilisateur qui n'a pas de mot de passe.

Pour ajouter un utilisateur au groupe **lpadmin**,lancez dans un terminal la commande :

```
sudo usermod -aG lpadmin username
```

Plus d'informations sont disponibles dans l'onglet **Documentation/Aide** de l'interface web.

14.4.4. Références

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

Page Debian Open-iSCSI : http://wiki.debian.org/SAN/iSCSI/open-iscsi

Chapitre 15. Services de courriel

La transmission d'un courriel d'une personne à une autre au travers d'un réseau ou par Internet nécessite la mise en œuvre de nombreux systèmes travaillant ensemble. Chacun de ces systèmes doit être correctement configuré pour que cette tâche soit réalisée. L'expéditeur utilise un agent de courrier utilisateur (**Mail User Agent :** MUA), ou client courriel, afin d'envoyer le message au travers d'un ou plusieurs agents de transport de courriel (**Mail Transport Agent :** MTA), le dernier d'entre eux le remettant à un agent de livraison de courriel (**Mail Delivery Agent :** MDA), ou serveur de réception, qui le déposera dans la boite à lettres du destinataire, d'où il sera retiré par le client courriel du destinataire, généralement par l'intermédiaire d'un serveur POP3 ou IMAP(**Internet Message Access Protocol**, protocole d'accès de message internet).

15.1. Postfix

Postfix est le Service de Transfert de Courriel (MTA) par défaut d'Ubuntu. Il est conçu pour être sûr autant que facile et rapide à configurer. Il est compatible avec le MTA **sendmail**. Cette section détaille l'installation et la configuration de **postfix**. Elle explique aussi comment en faire un serveur SMTP utilisant une connexion sécurisée (afin d'assurer la sécurité des courriels envoyés).

Ce guide n'explique cependant pas comment mettre en place des **Domaines Virtuels** Postfix. Pour obtenir des informations sur les Domaines Virtuels et d'autres configurations avancées, voir le *Chapitre 15, paragraphe 1. Postfix.7.4. Références*.

15.1.1. Installation

Pour installer **postfix**, exécutez la commande suivante :

```
sudo apt install postfix
```

Appuyez simplement sur la touche « entrée » lorsque le processus d'installation pose des questions, la configuration se fera plus en détail dans la prochaine étape.

15.1.2. Configuration de base

Pour configurer **postfix**, exécutez la commande suivante :

```
sudo dpkg-reconfigure postfix
```

L'interface utilisateur sera affichée. Sur chaque écran, sélectionnez les valeurs suivantes :

- Site Web
- mail.example.fr
- steve
- mail.example.fr, localhost.localdomain, localhost
- Non
- 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128 192.168.0.0/24
- 0
- +
- tous

Remplacer **mail.example.com** avec le domaine pour lequel vous accepterez des courriels, **192.168.0.0/24** avec le réseau réel et la gamme de classe de votre serveur de messagerie, et **steve** avec le nom d'utilisateur approprié.

C'est maintenant le bon moment pour choisir le format de boite courriel que vous souhaitez utiliser. Par

défaut, Postfix utilisera le format **mbox**. Plutôt que d'éditer directement le fichier de configuration, vous pouvez utiliser la commande **postconf** pour configurer tous les paramètres de **postfix**. Les paramètres de configuration seront conservés dans le fichier /etc/postfix/main.cf. Plus tard, si vous souhaitez reconfigurer un paramètre en particulier, vous pourrez soit réutiliser cette commande, soit éditer manuellement ce fichier.

Pour utiliser le format de boîte aux lettres **Maildir**, lancez cette commande :

```
sudo postconf -e 'home_mailbox = Maildir/'
```

Cela placera les nouveaux courriels dans /home/**nom_utilisateur**/Maildir, vous aurez donc besoin de configurer votre agent de distribution du courrier (MDA) de façon à utiliser le même chemin.

15.1.3. Authentification SMTP

SMTP-AUTH permet à un client de s'identifier par un mécanisme d'authentification (SASL). Transport Layer Security (TLS) devrait être utilisée afin de chiffrer le processus d'authentification. Une fois authentifié, le serveur SMTP autorisera le client à relayer les courriels.

1. configurez Postfix pour SMTP-AUTH en utilisant SASL (Dovecot SASL):

```
sudo postconf -e 'smtpd_sasl_type = dovecot'
sudo postconf -e 'smtpd_sasl_path = private/auth'
sudo postconf -e 'smtpd_sasl_local_domain ='
sudo postconf -e 'smtpd_sasl_security_options = noanonymous'
sudo postconf -e 'broken_sasl_auth_clients = yes'
sudo postconf -e 'smtpd_sasl_auth_enable = yes'
sudo postconf -e 'smtpd_recipient_restrictions = \
permit_sasl_authenticated,permit_mynetworks,reject_unauth_destination'
```

Le chemin **smtpd_sasl_path** est un chemin relatif au répertoire de la file d'attente (queue) de Postfix.

2. Ensuite, générez ou obtenez un certificat numérique pour TLS. Voir le *Chapitre 9, paragraphe 5. Certificats* pour plus de détails. Cet exemple utilise également une autorité de certification (CA). Pour plus d'informations sur la génération d'un certificat, voir le *Chapitre 9, paragraphe 5. Certificats.5. Autorité de certification*.

   Les clients courriels (MUA) se connectant à votre serveur de messagerie via TLS devront reconnaître le certificat utilisé pour l'authentification TLS. Cela peut être fait en utilisant un certificat à partir d'une autorité de certification commerciale ou d'un certificat auto-signé que les utilisateurs installent/acceptent manuellement. Pour MTA à MTA TLS, à moins que la politique locale l'exige, il n'y a aucune raison de ne pas utiliser un certificat auto-signé. Reportez-vous à *5.3. Création d'un certificat auto-signé* pour plus de détails.

3. Une fois que vous avez un certificat, configurez Postfix pour fournir le chiffrement à l'aide du protocole TLS des e-mails entrants et sortants :

```
sudo postconf -e 'smtp_tls_security_level = may'
sudo postconf -e 'smtpd_tls_security_level = may'
sudo postconf -e 'smtp_tls_note_starttls_offer = yes'
sudo postconf -e 'smtpd_tls_key_file = /etc/ssl/private/server.key'
sudo postconf -e 'smtpd_tls_cert_file = /etc/ssl/certs/server.crt'
sudo postconf -e 'smtpd_tls_loglevel = 1'
sudo postconf -e 'smtpd_tls_received_header = yes'
sudo postconf -e 'myhostname = mail.example.com'
```

4. Si vous utilisez votre propre **autorité de certification**, saisissez ce qui suit pour signer le certificat :

   sudo postconf -e 'smtpd_tls_CAfile = /etc/ssl/certs/cacert.pem'

   De nouveau, pour plus de détails sur les certificats, consultez le *Chapitre 9, paragraphe 5. Certificats*

Après avoir exécuté toutes les commandes, **Postfix** est configuré pour SMTP-AUTH et un certificat auto-signé a été créé pour le chiffrement TLS.

Maintenant, le fichier /etc/postfix/main.cf devrait ressembler à ceci :

```
# See /usr/share/postfix/main.cf.dist for a commented, more complete
# version

smtpd_banner = $myhostname ESMTP $mail_name (Ubuntu)
biff = no

# appending .domain is the MUA's job.
append_dot_mydomain = no

# Uncomment the next line to generate "delayed mail" warnings
#delay_warning_time = 4h

myhostname = server1.example.com
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = server1.example.com, localhost.example.com, localhost
relayhost =
mynetworks = 127.0.0.0/8
mailbox_command = procmail -a "$EXTENSION"
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
smtpd_sasl_local_domain =
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
broken_sasl_auth_clients = yes
smtpd_recipient_restrictions =
permit_sasl_authenticated,permit_mynetworks,reject _unauth_destination
smtpd_tls_auth_only = no
smtp_tls_security_level = may
smtpd_tls_security_level = may
smtp_tls_note_starttls_offer = yes
smtpd_tls_key_file = /etc/ssl/private/smtpd.key
smtpd_tls_cert_file = /etc/ssl/certs/smtpd.crt
smtpd_tls_CAfile = /etc/ssl/certs/cacert.pem
smtpd_tls_loglevel = 1
smtpd_tls_received_header = yes
smtpd_tls_session_cache_timeout = 3600s
tls_random_source = dev:/dev/urandom
```

La configuration initiale de Postfix est terminée. Tapez la commande suivante pour redémarrer le démon Postfix :

```
sudo systemctl restart postfix.service
```

Postfix prend en charge le protocole SMTP-AUTH tel que défini dans la **RFC2554** : http://www.ietf.org/rfc/rfc2554.txt . Il est basé sur SASL : http://www.ietf.org/rfc/rfc2222.txt . Toutefois, il est encore nécessaire de mettre en place l'authentification SASL avant de pouvoir utiliser SMTP-AUTH.

15.1.4. Configuration de SASL

Postfix supporte deux implémentations SASL, Cyrus SASL et Dovecot SASL. Pour activer Dovecot SASL, le paquet **dovecot-core** devra être installé. Á l'invite d'un terminal, entrez la commande suivante :

```
sudo apt install dovecot-core
```

Ensuite, vous devrez modifier /etc/dovecot/conf.d/10-master.conf. Changez ce qui suit :

```
service auth {
  # auth_socket_path points to this userdb socket by default. It's typically
  # used by dovecot-lda, doveadm, possibly imap process, etc. Its default
  # permissions make it readable only by root, but you may need to relax these
  # permissions. Users that have access to this socket are able to get a list
  # of all usernames and get results of everyone's userdb lookups.
  unix_listener auth-userdb {
    #mode = 0600
    #user =
    #group =
  }

  # Postfix smtp-auth
  unix_listener /var/spool/postfix/private/auth {
    mode = 0660
    user = postfix
    group = postfix
  }
```

Afin de permettre aux clients **Outlook** d'utiliser le protocole SMTP-AUTH, dans la section **authentication mechanisms** de /etc/dovecot/conf.d/10-auth.conf, changez cette ligne :

```
auth_mechanisms = plain
```

En ceci :

```
auth_mechanisms = plain login
```

Une fois que vous avez configuré **Dovecot**, faites le redémarrer avec :

```
sudo systemctl restart dovecot.service
```

15.1.5. Mail-Stack Delivery

Une autre option de configuration de **Postfix** pour SMTP-AUTH est l'utilisation du paquet **mail-stack-delivery** (nommé auparavant dovecot-postfix). Ce paquet installera **Dovecot** et configurera **Postfix** afin d'utiliser **Dovecot** pour l'authentification SASL et en tant qu'agent distributeur de courriel. Le paquet configure également **Dovecot** pour les protocoles IMAP, IMAPS, POP3, et POP3S.

> Vous pouvez ou ne voulez pas exécuter IMAP, IMAPS, POP3 ou POP3S sur votre serveur de messagerie. Par exemple, si vous configurez votre serveur pour être une passerelle de messagerie, le filtre spam/virus, etc... Si c'est le cas, il peut être plus facile d'utiliser les commandes ci-dessus pour configurer Postfix pour SMTP-AUTH.

Pour installer le paquet, saisissez dans un terminal :

```
sudo apt install mail-stack-delivery
```

Votre serveur de courriel devrait être opérationnel, mais vous voudrez sans doute configurer certaines options. Par exemple, le paquet utilise le certificat et la clé du paquet **ssl-cert**, mais dans un environnement de production, vous devriez utiliser un certificat et une clef créée pour l'hôte. Consultez le *Chapitre 9, paragraphe 5. Certificats* pour de plus amples informations.

Changez les options suivantes dans /etc/postfix/main.cf une fois que vous avez personnalisé un certificat et une clé pour l'hôte :

```
smtpd_tls_cert_file = /etc/ssl/certs/ssl-mail.pem
smtpd_tls_key_file = /etc/ssl/private/ssl-mail.key
```

Redémarrez ensuite Postfix :

```
sudo systemctl restart postfix.service
```

15.1.6. Procédure de test

La configuration de SMTP-AUTH est terminée. Il est maintenant temps de tester la configuration.

Pour vérifier que SMTP-AUTH et TLS fonctionnent correctement, exécutez la commande suivante :

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

Après avoir établi la connexion au serveur Postfix, tapez :

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

Si vous voyez, entre autres, les lignes suivantes :

```
250-STARTTLS
```

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

alors tout fonctionne parfaitement. Tapez **quit** pour sortir.

15.1.7. Dépannage

Cette section introduit les méthodes de base pour déterminer les causes d'un éventuel problème.

15.1.7.1. Échappement du chroot

Le paquet **postfix** d'Ubuntu s'installera par défaut dans un environnement **chroot** par mesure de sécurité. Ceci peut accroître la complexité de la résolution de problèmes.

Pour désactiver l'opération chroot essayez de trouver la ligne suivante dans le fichier de configuration /etc/postfix/master.cf :

```
smtp      inet  n       -       -       -       -       smtpd
```

et la modifier ainsi :

```
smtp      inet  n       -       n       -       -       smtpd
```

Vous devrez ensuite redémarrer Postfix pour utiliser la nouvelle configuration. A parti d'un terminal, saisissez :

```
sudo systemctl restart postfix.service
```

15.1.7.2. Smtps

Si vous avez besoin de smtps, modifiez /etc/postfix/master.cf et dé-commentez la ligne suivante :

```
smtps inet n - - - - smtpd
  -o smtpd_tls_wrappermode=yes
  -o smtpd_sasl_auth_enable=yes
  -o smtpd_client_restrictions=permit_sasl_authenticated,reject
  -o milter_macro_daemon_name=ORIGINATING
```

15.1.7.3. Fichiers journaux

Postfix inscrit tous les messages de journalisation dans /var/log/mail.log. Cependant, les erreurs et les alertes peuvent quelquefois disparaître dans les messages normaux, ils sont donc également inscrits dans /var/log/mail.err et /var/log/mail.warn respectivement.

Pour voir en temps réel les messages inscrits dans les journaux, vous pouvez utiliser la commande **tail -f** :

```
tail -f /var/log/mail.err
```

La quantité de renseignements enregistrés dans les journaux peut être augmenté. Voici quelques options de configuration afin d'augmenter le niveau de journalisation pour certains des domaines visés ci-dessus.

- Afin d'accroître l'activité de log de **TLS**, configurez l'option **smtpd_tls_loglevel** sur une valeur entre 1 et 4.

```
sudo postconf -e 'smtpd_tls_loglevel = 4'
```

- Si vous avez des problèmes d'envoi ou de réception de courriers électroniques en provenance d'un domaine spécifique vous pouvez ajouter ce domaine à la directive **debug_peer_list**.

```
sudo postconf -e 'debug_peer_list = problem.domain'
```

- Vous pouvez accroître la verbosité de n'importe quel démon **Postfix** en modifiant /etc/postfix/master.cf et en ajoutant **-v** après l'entrée. Par exemple, modifiez l'entrée **smtp** :

```
smtp      unix      -      -      -      -      -      smtp -v
```

Il est important de noter qu'après avoir fait un des changements de connexion ci-dessus, le processus **Postfix** nécessitera d'être rechargé dans l'ordre pour prendre connaissance de la nouvelle configuration : **sudo systemctl reload postfix.service**

- Pour augmenter la quantité d'informations journalisées lors du dépannage de problèmes avec **SASL**, vous pouvez définir les options suivantes dans /etc/dovecot/conf.d/10-logging.conf

```
auth_debug=yes
auth_debug_passwords=yes
```

Comme pour **Postfix**, si vous changez une configuration **Dovecot**, le processus nécessitera d'être rechargé : **sudo systemctl reload dovecot.service**.

Certaines options ci-dessous peuvent dramatiquement augmenter la quantité d'informations inscrites dans les fichiers journaux. Pensez à ramener le niveau de journalisation à la normale une fois que vous aurez détecté et corrigé le problème. Ensuite redémarrez le démon afin que la nouvelle configuration soit prise en compte.

15.1.7.4. Références

Administrer un serveur **Postfix** peut être une tâche très complexe. À un certain moment, vous devrez peut-être vous tourner vers la communauté Ubuntu pour être aidé par des utilisateurs plus expérimentés.

Un endroit génial pour demander de l'assistance pour **Postfix** et s'impliquer dans la communauté Ubuntu Server, est le canal IRC (anglophone) **#ubuntu-server** sur **freenode** : http://freenode.net. Vous pouvez aussi poster un message sur les forums Ubuntu francophones : http://forum.ubuntu-fr.org/

Pour des informations plus complètes sur **Postfix**, les développeurs Ubuntu recommandent vivement : **The Book of Postfix** : http://www.postfix-book.com/ .

Enfin, le site web Postfix http://www.postfix.org/documentation.html possède également une grande documentation sur toutes les différentes options de configuration disponibles.

De plus, la page du **wiki Ubuntu sur Postfix** (en anglais) contient plus d'informations : https://help.ubuntu.com/community/Postfix .

15.2. Exim4

Exim4 est un autre agent de transfert de courrier (MTA) développé à l'université de Cambridge pour une utilisation sur des systèmes Unix connectés à l'internet. Exim peut être installé à la place de sendmail, bien que la configuration d'exim soit assez différente de celle de sendmail.

15.2.1. Installation

Pour installer exim4, lancez la commande suivante :

```
sudo apt install exim4
```

15.2.2. Configuration

Pour configurer Exim4, utilisez la commande suivante :

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

L'interface utilisateur sera affichée. Celle-ci vous permet de modifiez plusieurs paramètres. Par exemple, les options de configuration d'Exim4 sont réparties dans plusieurs fichiers. Grâce à cette interface vous pouvez les réunir en seul fichier.

Tous les paramètres que vous configurez dans l'interface utilisateur sont conservés dans le fichier /etc/exim4/update-exim4.conf.conf. Si vous souhaitez les modifier, vous pouvez soit relancer l'assistant de configuration, ou éditer manuellement ce fichier à l'aide de votre éditeur préféré. Une fois la configuration terminée, vous pouvez effectuer la commande suivant pour générer le fichier maître de configuration :

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

Le fichier de configuration maître, est généré et est stocké dans /var/lib/exim4/config.autogenerated.

> ! À aucun moment, vous ne devez pas éditer manuellement le fichier de configuration principal /var/lib/exim4/config.autogenerated, car il est mis à jour automatiquement chaque fois que vous exécutez **update-exim4.conf**.

Utilisez la commande suivante pour lancer le démon Exim4.

```
sudo systemctl start exim4.service
```

15.2.3. Authentification SMTP

Cette section couvre la configuration de SMTP-AUTH avec TLS et SASL pour Exim4.

La première étape consiste à créer un certificat numérique pour TLS. Entez les commandes suivantes dans un terminal:

```
sudo /usr/share/doc/exim4-base/examples/exim-gencert
```

Maintenant, Exim doit être configuré pour utiliser TLS en éditant /etc/exim4/conf.d/main/03_exim4-config_tlsoptions. Ajoutez comme suit:

```
MAIN_TLS_ENABLE = yes
```

Ensuite, vous aurez besoin de configurer Exim4 pour utiliser saslauthd pour l'authentication. Modifiez /etc/exim4/conf.d/auth/30_exim4-config_examples et dé-commentez les sections **plain_saslauthd_server** et **login_saslauthd_server** :

```
 plain_saslauthd_server:
   driver = plaintext
   public_name = PLAIN
   server_condition = ${if saslauthd{{$auth2}{$auth3}}{1}{0}}
   server_set_id = $auth2
   server_prompts = :
   .ifndef AUTH_SERVER_ALLOW_NOTLS_PASSWORDS
   server_advertise_condition = ${if eq{$tls_cipher}{}{}{*}}
   .endif
#
 login_saslauthd_server:
   driver = plaintext
   public_name = LOGIN
   server_prompts = "Username:: : Password::" :
   # don't send system passwords over unencrypted connections
   server_condition = ${if saslauthd{{$auth1}{$auth2}}{1}{0}}
   server_set_id = $auth1
   .ifndef AUTH_SERVER_ALLOW_NOTLS_PASSWORDS
   server_advertise_condition = ${if eq{$tls_cipher}{}{}{*}}
   .endif
```

De plus, afin que les clients de messagerie extérieurs soient en mesure de se connecter au nouveau serveur exim, le nouvel utilisateur doit être ajouté dans exim à l'aide de la commande suivante :

```
sudo /usr/share/doc/exim4-base/examples/exim-adduser
```

Les utilisateurs devraient protéger les nouveaux fichiers de mots de passes exim avec les commandes suivantes :

```
sudo chown root:Debian-exim /etc/exim4/passwd
sudo chmod 640 /etc/exim4/passwd
```

Enfin, mettez à jour la configuration d'Exim5 et redémarrez le service :

```
sudo update-exim4.conf
sudo systemctl restart exim4.service
```

15.2.4. Configurer SASL

Cette section mets à votre disposition des détails sur la configuration du saslauthd afin de fournir un mécanisme d'authentification pour **Exim4**.

La première étape consiste à installer le paquet sasl2-bin. A partir d'un terminal, saisissez ce qui suit :

```
sudo apt install sasl2-bin
```

Pour configurer saslauthd ouvrez le fichier de configuration /etc/default/saslauthd et changez START=no en :

```
START=yes
```

Ensuite, l'utilisateur **Debian-exim** devra faire partie du groupe **sasl** afin que Exim4 puisse utiliser le service saslauthd :

```
sudo adduser Debian-exim sasl
```

Maintenant démarrez le service **saslauthd**:

```
sudo systemctl start saslauthd.service
```

Exim4 est maintenant configuré avec SMTP-AUTH utilisant l'authentification TLS et SASL.

15.2.5. Références

Consultez **exim.org** pour de plus amples informations : http://www.exim.org/ .

Vous pouvez aussi lire ce livre : Exim4 Book : http://www.uit.co.uk/content/exim-smtp-mail-server .

Une autre ressource est la page du **wiki Ubuntu pour Exim4** (en anglais) : https://help.ubuntu.com/community/Exim4 .

15.3. Serveur Dovecot

Dovecot est un serveur de réception de courriel (MDA : Mail Delivery Agent), conçu avec la sécurité comme souci principal. Il prend en charge la majorité des formats de boites à lettres : mbox ou Maildir. Cette section explique comment le paramétrer pour en faire un serveur IMAP ou POP3.

15.3.1. Installation

Pour installer dovecot, exécutez la commande suivante dans l'invité de commande :

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

15.3.2. Configuration

Pour configurer dovecot, vous pouvez modifier /etc/dovecot/dovecot.conf. Choisissez le protocole à utiliser si nécessaire (pop3, pop3s - pop3 sécurisé, imap et imaps - imap sécurisé). La description de ces protocoles ne relève pas de ce guide. Pour de plus amples informations, référez-vous aux articles de Wikipédia : POP3 : http://fr.wikipedia.org/wiki/POP3 et IMAP : http://fr.wikipedia.org/wiki/Internet_Message_Access_Protocol .

IMAPS et POP3S sont plus sûrs que les simples IMAP et POP3 parce qu'ils utilisent le chiffrage SSL pour la connexion. Une fois que vous avez choisi le protocole, ajoutez la ligne suivante dans le fichier /etc/dovecot/dovecot.conf :

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

Ensuite, choisissez la boîte de courriel que vous souhaitez utiliser. **Dovecot** prend en charge les formats **maildir** et **mbox**. Ce sont les formats de boîtes courriel les plus couramment utilisés. Ils ont tous deux leurs propres avantages et sont comparés sur **le site web Dovecot** : http://wiki2.dovecot.org/MailboxFormat.

Une fois le type de boîte à lettre choisie, modifiez le fichier /etc/dovecot/conf.d/10-mail.conf en changeant la ligne suivante :

```
mail_location = maildir:~/Maildir # (for maildir)
or
mail_location = mbox:~/mail:INBOX=/var/spool/mail/%u # (for mbox)
```

> Vous devez configurer votre agent de transfert de courriel (MTA : Mail Transport Agent) pour transférer les courriels entrants vers ce type de boite aux lettres s'il est différent de celui que vous avez configuré.

Une fois que vous aurez configuré dovecot, redémarrez le démon dovecot afin de tester votre configuration :

```
sudo systemctl restart dovecot.service
```

Si vous avez activé imap ou pop3, vous pouvez aussi essayer de vous connecter avec les commandes **telnet localhost pop3** ou **telnet localhost imap2**. Votre installation est un succès si vous voyez quelque chose ressemblant à :

```
bhuvan@rainbow:~$ telnet localhost pop3
```

```
Trying 127.0.0.1...
Connected to localhost.localdomain.
Escape character is '^]'.
+OK Dovecot ready.
```

15.3.3. Configuration SSL de Dovecot

Pour configurer **dovecot** afin qu'il utilise SSL, vous pouvez modifier le fichier /etc/dovecot/conf.d/10-ssl.conf en changeant les lignes suivantes :

```
ssl = yes
ssl_cert = </etc/ssl/certs/dovecot.pem
ssl_key = </etc/ssl/private/dovecot.pem
```

Vous pouvez obtenir le certificat SSL d'une Autorité de Délivrance de Certificat (CIA : Certificate Issuing Authority) ou vous pouvez créer un certificat auto-signé SSL. Celle-ci est une bonne option pour le courrier électronique, car les clients SMTP se plaignent rarement de "certificats auto-signés". Veuillez vous référer au *Chapitre 9, paragraphe 5. Certificats* pour plus de détails sur la façon de créer un certificat auto-signé SSL. Une fois que vous créez le certificat, vous aurez un fichier de clés et un fichier de certificat. Veuillez les copier à l'endroit indiqué dans le fichier de configuration /etc/dovecot/conf.d/10-ssl.conf.

15.3.4. Configuration du pare-feu pour un Serveur de courrier électronique

Pour accéder à votre serveur de courriel depuis un autre ordinateur, vous devez configurer votre pare-feu pour qu'il autorise les connexions au serveur sur les ports requis.

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

15.3.5. Références

Consultez le **site Web Dovecot** pour de plus amples informations : http://www.dovecot.org/ .

En outre, la page du **wiki Ubuntu pour Dovecot** (en anglais) comporte plus de détails : https://help.ubuntu.com/community/Dovecot .

15.4. Mailman

Mailman est un logiciel libre permettant la gestion de discussions par courrier électronique et de listes de bulletins d'information électroniques. De nombreuses listes de discussions sur le libre (dont toutes les **listes de discussions de Ubuntu**) utilisent Mailman comme logiciel de gestion de liste de diffusion : http://lists.ubuntu.com . Il est puissant, facile à installer et à gérer.

15.4.1. Installation

Mailman fournit une interface Web aux administrateurs et utilisateurs en s'appuyant sur un serveur de courriel externe pour envoyer et recevoir les courriels. Il fonctionne parfaitement avec les serveur de courriel suivants :

- Postfix
- Exim
- Sendmail
- Qmail

Nous allons découvrir comment installer et configurer Mailman avec le serveur Apache, et le serveur de courriel Postfix ou bien Exim. Si vous désirez installer Mailman avec un serveur de courriel différent, veuillez visitez la section des références.

> Vous avez seulement besoin d'un serveur de courrier et Postfix est l'agent de transport de courrier (MTA) par défaut d'Ubuntu.

15.4.1.1. Apache2

Pour installer apache2, reportez-vous au *Chapitre 11, paragraphe 1. HTTPD - serveur web Apache2 .1 Installation* pour plus de détails.

15.4.1.2. Postfix

Pour les instructions sur l'installation et la configuration de Postfix, référez vous au *Chapitre 15, paragraphe 1. Postfix.*

15.4.1.3. Exim4

Pour installer Exim4, référez vous au *Chapitre 15, paragraphe 2. Exim4*.

Une fois que exim4 est installé, les fichiers de configuration sont stockés dans le répertoire /etc/exim4. Dans Ubuntu, par défaut, les fichiers de configuration exim4 sont répartis dans différents fichiers. Vous pouvez changer ce comportement en modifiant la variable suivante dans le fichier /etc/exim4/update-exim4.conf :

```
dc_use_split_config='true'
```

15.4.1.4. Mailman

Pour installer **Mailman**, lancez la commande suivante dans un terminal :

```
sudo apt install mailman
```

Il copie les fichiers d'installation dans le répertoire /var/lib/mailman. Il installe les scripts CGI dans le répertoire /usr/lib/cgi-bin/mailman. Il crée l'utilisateur Linux **list** et le groupe Linux **list**. Le processus mailman appartiendra à cet utilisateur.

15.4.2. Configuration

Cette section suppose que vous avez installé **mailman**, **apache2**, and **postfix** or **exim4** avec succès. Maintenant vous devez juste les configurer.

15.4.2.1. Apache2

Un exemple de fichier de configuration pour Apache est livré avec **Mailman** et placé dans /etc/mailman/apache.conf. Pour qu'Apache utilise le fichier de configuration, il devra être copié vers /etc/apache2/sites-available :

```
sudo cp /etc/mailman/apache.conf /etc/apache2/sites-available/mailman.conf
```

Ceci configurera un nouvel **VirtualHost** d'Apache pour le site d'administration de Mailman. À présent, activez la nouvelle configuration et redémarrez Apache :

```
sudo a2ensite mailman.conf
sudo systemctl restart apache2.service
```

Mailman utilise apache2 pour exécuter ses scripts CGI. Les scripts CGI de Mailman sont installés dans le répertoire /usr/lib/cgi-bin/mailman. Donc, l'url de mailman sera http://hostname/cgi-bin/mailman/ . Vous pouvez modifier le fichier de configuration /etc/apache2/sites-available/mailman.conf si vous souhaitez changer ce comportement.

15.4.2.2. Postfix

Pour l'intégration de **Postfix**, nous associerons le domaine **lists.example.com** avec les listes de diffusion. Veuillez remplacer **lists.example.com** par le domaine de votre choix.

Vous pouvez utiliser la commande **postconf** pour ajouter les configurations nécessaires à /etc/postfix/main.cf :

```
sudo postconf -e 'relay_domains = lists.example.com'
sudo postconf -e 'transport_maps = hash:/etc/postfix/transport'
sudo postconf -e 'mailman_destination_recipient_limit = 1'
```

Dans /etc/postfix/master.cf, vérifiez bien que vous avez le transport suivant :

```
mailman  unix     -     n     n     -     -     pipe
  flags=FR user=list argv=/usr/lib/mailman/bin/postfix-to-mailman.py
  ${nexthop} ${user}
```

Il appelle le script **postfix-to-mailman.py** quand un courriel est destiné à une liste de diffusion.

Associez le nom de domaine **lists.example.com** au transport Mailman grâce au transport map. Modifiez le fichier /etc/postfix/transport :

```
lists.example.com       mailman:
```

À présent, faites construire la carte de transport par **Postfix** en saisissant ceci dans un terminal :

```
sudo postmap -v /etc/postfix/transport
```

Ensuite redémarrez Postfix pour activer les nouvelles configurations :

```
sudo systemctl restart postfix.service
```

15.4.2.3. Exim4

Une fois Exim4 installé, vous pouvez démarrez le serveur Exim en utilisant la commande suivante dans un terminal :

```
sudo systemctl start exim4.service
```

Afin que Mailman puisse fonctionner avec Exim4, vous devez configurer ce dernier. Comme dit précédemment, par défaut, Exim4 utilise plusieurs fichiers pour son paramétrage. Référez-vous au site Web d' **Exim** : http://www.exim.org . Pour utiliser Mailman, il vous faudra ajouter à nouveau un fichier de configuration à ces types de configuration :

- Principal
- Transport
- Routeur

Exim crée ensuite un fichier de configuration maître en triant tous ces petits fichiers de paramètres. L'ordre dans lequel se trouvent ces fichiers est donc très important.

15.4.2.4. Principal

Tous les fichiers de configuration appartenant à la catégorie Principal sont stockés dans le répertoire /etc/exim4/conf.d/main/. Vous pouvez ajouter le contenu suivant dans un nouveau fichier, nommé 04_exim4-config_mailman :

```
# start
# Home dir for your Mailman installation -- aka Mailman's prefix
# directory.
# On Ubuntu this should be "/var/lib/mailman" :  Pour utiliser Mailman, il vous faudra ajouter un fichier de configuration à : . Exim crée ensuite un fichier de configuration maître en triant tous ces petits fichiers de paramètres. L'ordre dans lequel se trouvent ces fichiers est donc très important.

# start
```

```
# Home dir for your Mailman installation -- aka Mailman's prefix
# directory.
# On Ubuntu this should be
# 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
```

15.4.2.5. Transport

Tous les fichiers de configuration appartenant à la catégorie Transport sont stockés dans le répertoire /etc/exim4/conf.d/transport/. Vous pouvez ajouter le contenu suivant dans un nouveau fichier, nommé 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
```

15.4.2.6. Routeur

Tous les fichiers de configuration appartenant à la catégorie Routeur sont stockés dans le répertoire /etc/exim4/conf.d/router/. Vous pouvez ajouter le contenu suivant dans un nouveau fichier, nommé 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
```

> ! L'ordre des fichiers de configuration des catégories Principal et Transport n'est pas important. Mais l'ordre des fichiers de configuration de la catégorie Routeur doit être respecté. Ce fichier particulier doit se trouver avant le fichier **200_exim4-config_primary**. Ces deux fichiers de configuration contiennent le même type d'information, le premier fichier étant prioritaire. Pour plus de détails, veuillez vous reporter à la section « Références ».

15.4.2.7. Mailman

Une fois mailman installé, vous pouvez le lancer avec la commande suivante :

```
sudo systemctl start mailman.service
```

Une fois mailman installé, vous devez créer la liste de diffusion par défaut. Exécutez la commande suivante pour créer la liste de diffusion :

```
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...

#
```

Nous avons configuré soit Postfix soit Exim4 pour reconnaître les messages de mailman. Ainsi, il n'est pas

obligatoire de créer de nouvelles entrées dans /etc/aliases. Si vous avez apporté des modifications aux fichiers de configuration, assurez-vous de redémarrer les services concernés avant de continuer dans la prochaine section.

> Exim4 n'utilise pas les alias ci-dessus pour faire suivre les courriers à Mailman car il utilise une approche **découverte**. Afin de supprimer les alias à la création de la liste, vous pouvez ajouter la ligne **MTA=None** dans le fichier de configuration de Mailman, /etc/mailman/mm_cfg.py .

15.4.3. Administration

Nous supposons que vous avez fait une installation par défaut. Les scripts cgi de mailman se trouvent toujours dans le répertoire /usr/lib/cgi-bin/mailman/. Mailman fournit un outil d'administration par internet. Pour accéder à cette page, ouvrez l'adresse suivante dans votre navigateur :

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

La liste de diffusion par défaut, **mailman**, apparaîtra sur cet écran. Si vous cliquez sur le nom de la liste, il vous sera demandé de vous authentifier avec votre mot de passe. Si vous saisissez le bon mot de passe, alors vous pourrez modifier les paramètres d'administration de cette liste de diffusion. Vous pouvez créer une nouvelle liste de diffusion, en ligne de commande, avec l'utilitaire **/usr/sbin/newlist**. Sinon, vous pouvez aussi créer une nouvelle liste de diffusion en utilisant l'interface Web.

15.4.4. Utilisateurs

Mailman fournit aux utilisateurs une interface Web. Pour accéder à cette page, ouvrez votre navigateur à l'adresse suivante :

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

La liste de diffusion par défaut, **mailman**, apparaîtrasur cet écran. Si vous cliquez sur le nom de la liste, vous verrez apparaître le formulaire d'inscription. Vous pourrez alors saisir votre adresse électronique, votre nom (facultatif) et votre mot de passe afin de vous y inscrire. Un courriel d'invitation vous sera adressé. Vous pourrez alors suivre les instructions de ce courriel pour vous inscrire.

15.4.5. 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

Vous pouvez également consulter la page du **wiki Ubuntu pour Mailman** (en anglais) : https://help.ubuntu.com/community/Mailman .

15.5. Filtrage du courrier électronique

L'un des plus gros problèmes avec le courrier électronique à l'heure actuelle sont les courriers électroniques non sollicités envoyés en masse (ou UBE en anglais). Également connus sous le nom de SPAM, ces messages peuvent également transmettre des virus et d'autres formes de logiciels malveillants. Selon certains rapports, ces messages constituent l'essentiel de l'ensemble du trafic e-mail sur Internet.

Cette section portera sur l'intégration amavisd-new, Spamassassin, et ClamAV avec l'agent Postfix (Mail Transport Agent : MTA). Postfix peut aussi vérifier la validité de messagerie en passant à travers des filtres de contenu externe. Ces filtres peuvent parfois déterminer si un message est un spam sans avoir besoin de le traiter avec des applications à plus forte intensité de ressources. Deux filtres courants sont opendkim et python-policyd-spf.

- Amavisd-new est un programme enveloppe qui peut appeler différents programmes de filtrage de contenu pour la détection de courrier indésirable (spam), anti-virus, etc.
- Spamassassin utilise divers mécanismes pour filtrer les courriers en se basant sur leur contenu.
- ClamAV est anti-virus libre.
- opendkim met en œuvre un filtre de messagerie Sendmail (Milter) pour les DomainKeys Identified Mail (DKIM) standard.
- python-policyd-spf active la vérification Sender Policy Framework (SPF) avec Postfix.

Voici comment ces applications collaborent :

- Un courriel est accepté par Postfix.
- Dans ce cas, le message passe via les filtres externes opendkim et python-policyd-spf.
- Amavisd-new traite ensuite le message.
- ClamAV est utilisé pour analyser le message. Si le message contient un virus alors Postfix le rejettera.
- Les messages propres seront ensuite analysés par Spamassassin pour savoir si le courrier est indésirable (spam). Spamassassin ajoutera alors des lignes X-Header permettant à Amavisd-new de manipuler le message par la suite.

Par exemple, si un message a un score Spam de plus de cinquante, le message pourrait être automatiquement sorti de la file sans que le destinataire ne soit jamais embêté. Un autre moyen de traiter les messages signalés est de les remettre au client de messagerie électronique (MUA) autorisant l'utilisateur à gérer le message comme il le souhaite.

15.5.1. Installation

Consultez le *Chapitre 15, paragraphe 1. Postfix* pour les instructions d'installation et de configuration de Postfix.

Pour installer le reste des applications saisissez ce qui suit dans un terminal :

```
sudo apt install amavisd-new spamassassin clamav-daemon
sudo apt install opendkim postfix-policyd-spf-python
```

Il existe des paquets facultatifs qui s'intègrent avec **Spamassassin** pour une meilleure détection des spams :

```
sudo apt install pyzor razor
```

Avec les principales applications de filtrage, des utilitaires de compression sont nécessaires pour traiter certaines pièces jointes :

```
sudo apt install arj cabextract cpio lha nomarch pax rar unrar unzip zip
```

S i certains paquets sont introuvables, vérifiez que le dépôt **multiverse** est activé dans /etc/apt/sources.list

S i vous faites des changements du fichier, assurez-vous de lancer la commande **sudo apt update** avant d'essayer d''installer encore.

15.5.2. Configuration

Configurez maintenant cela pour que tout fonctionne ensemble et filtre les courriers.

15.5.2.1 ClamAV

L'installation par défaut de **ClamAV** nous conviendra. Regardez son fichier de configuration dans /etc/clamav pour avoir accès à plus d'options.

Ajoutez l'utilisateur **clamav** au groupe **amavis** de manière à ce que **Amavisd-new** ait les droits suffisants pour lire les fichiers :

```
sudo adduser clamav amavis
sudo adduser amavis clamav
```

15.5.2.2. Spamassassin

Spamassassin détecte automatiquement les composants supplémentaires et les utilisera s'ils sont présents. Ceci veut donc dire qu'il n'est pas nécessaire de configurer **pyzor** et **razor**.

Editez /etc/default/spamassassin pour activer le démon **Spamassassin**. Changez **ENABLED=0** par :

```
ENABLED=1
```

Lancez maintenant le démon :

```
sudo systemctl start spamassassin.service
```

15.5.2.3. Amavisd-new

D'abord, activez la détection de spam et de virus dans **Amavisd-new** en éditant /etc/amavis/conf.d/15-content_filter_mode :

```
use strict;

# You can modify this file to re-enable SPAM checking through spamassassin
# and to re-enable antivirus checking.

#
# Default antivirus checking mode
# Uncomment the two lines below to enable it
#

@bypass_virus_checks_maps = (
   \%bypass_virus_checks, \@bypass_virus_checks_acl, \$bypass_virus_checks_re);



#
# Default SPAM checking mode
# Uncomment the two lines below to enable it
#

@bypass_spam_checks_maps = (
   \%bypass_spam_checks, \@bypass_spam_checks_acl, \$bypass_spam_checks_re);

1; # insure a defined return
```

Faire rebondir (Bounce) le spam peut être une mauvaise idée parce que l'adresse de retour est souvent truquée. Le comportement par défaut est de le jeter à la place. Ceci est configuré dans /etc/amavis/conf.d/21-debian_defaults où **final_spam_destiny $** est réglé sur D_DISCARD plutôt que D_BOUNCE.

De plus, vous devriez peut-être ajuster les options suivantes afin d'étiqueter plus de messages comme indésirables :

```
$sa_tag_level_deflt = -999; # ajoute les entêtes d'informations de courrier indésirable si supérieur ou égal à ce niveau
$sa_tag2_level_deflt = 6.0; # ajoute l'entête 'courrier indésirable détecté' à ce niveau
$sa_kill_level_deflt = 21.0; # déclenche les actions d'évitement de de courrier indésirable
$sa_dsn_cutoff_level = 4; # le niveau de courrier indésirable en dessous duquel un DSN n'est pas envoyé
```

Si le **nom d'hôte (hostname)** du serveur est différent de l'enregistrement MX du domaine vous devrez fixer vous-même l'option **$myhostname**. De même, si le serveur sert de multiples domaines, l'option **@local_domains_acl** devra être personnalisée. Modifiez le fichier /etc/amavis/conf.d/50-user :

```
$myhostname = 'mail.example.com';
```

```
@local_domains_acl = ( "example.com", "example.org" );
```

Si vous voulez couvrir plusieurs domaines, vous pouvez utiliser ce qui suit dans le fichier /etc/amavis/conf.d/50-user :

```
@local_domains_acl = qw(.);
```

Après sa configuration, **Amavisd-new** doit être redémarré :

```
sudo systemctl restart amavis.service
```

15.5.2.3.1. Liste blanche DKIM

Amavisd-new peut être configuré pour mettre automatiquement les adresses des domaines ayant des clés correctes en **liste blanche**. Des domaines pré configurés se trouvent dans /etc/amavis/conf.d/40-policy_banks.

Il existent plusieurs manières de configurer la liste blanche d'un domaine :

- **'example.com' => 'WHITELIST',** : ajoute toutes les adresses du domaine « example.com » à la liste blanche .
- **'.example.com' => 'WHITELIST',** : ajoute n'importe quelle adresse de n'importe quel **sous-domaine** de « example.com » s'ils ont une signature valable.
- **'.example.com/@example.com' => 'WHITELIST',** : ajoute les sous-domaines de « example.com » qui utilisent la signature du domaine parent **example.com**.
- **'./@ example.com'=> 'WHITELIST',** : ajoute des adresses qui ont une signature valable à partir de "example.com ". Ceci est habituellement utilisé pour les groupes de discussion qui signent leurs messages.

Un domaine peut aussi avoir plusieurs configurations de liste blanche. Après avoir modifié le fichier, redémarrez **amavisd-new** :

```
sudo systemctl restart amavis.service
```

Dans ce contexte, une fois qu'un domaine a été ajouté à la liste blanche, le message ne sera pas filtré par un anti-virus quelconque ou un anti-spam. Ceci peut ne pas vous convenir.

15.5.2.4. Postfix

Pour l'intégration dans **Postfix**, saisissez la commande suivant dans un terminal :

```
sudo postconf -e 'content_filter = smtp-amavis:[127.0.0.1]:10024'
```

Ouvrez ensuite le fichier /etc/postfix/master.cf et ajoutez ce qui suit tout à la fin :

```
smtp-amavis unix - - - - 2 smtp
        -o smtp_data_done_timeout=1200
        -o smtp_send_xforward_command=yes
        -o disable_dns_lookups=yes
        -o max_use=20

127.0.0.1:10025 inet n - - - - smtpd
```

```
        -o content_filter=
        -o local_recipient_maps=
        -o relay_recipient_maps=
        -o smtpd_restriction_classes=
        -o smtpd_delay_reject=no
        -o smtpd_client_restrictions=permit_mynetworks,reject
        -o smtpd_helo_restrictions=
        -o smtpd_sender_restrictions=
        -o smtpd_recipient_restrictions=permit_mynetworks,reject
        -o smtpd_data_restrictions=reject_unauth_pipelining
        -o smtpd_end_of_data_restrictions=
        -o mynetworks=127.0.0.0/8
        -o smtpd_error_sleep_time=0
        -o smtpd_soft_error_limit=1001
        -o smtpd_hard_error_limit=1000
        -o smtpd_client_connection_count_limit=0
        -o smtpd_client_connection_rate_limit=0
        -o
receive_override_options=no_header_body_checks,no_unknown_recipient_checks,no_milters
```

Ajoutez aussi les deux lignes suivantes immédiatement en dessous du service de transport **"pickup" :**

```
         -o content_filter=
         -o receive_override_options=no_header_body_checks
```

Ceci empêchera la classification en tant que pourriel des messages de rapport de pourriels.

Maintenant, redémarrez **Postfix** :

```
sudo systemctl restart postfix.service
```

Le filtrage anti-spam et anti-virus est maintenant activé.

15.5.2.5. Amavisd-new et Spamassassin

Lors de l'intégration de **amavisd-new** avec **Spamassassin**, si vous choisissez de désactiver le filtrage bayésien en éditant /etc/spamassassin/local.cf et utilisez **cron** pour actualiser les règles chaque soir, le résultat peut entraîner une situation où une grande quantité de messages d'erreur sont envoyés à l'utilisateur **amavis** via le travail de cron amavisd-new.

Il y a plusieurs façons de traiter cette situation :

- Configurez votre MDA (agent serveur de réception) pour filtrer les messages que vous ne souhaitez pas voir.
- Changez /usr/sbin/amavisd-new-cronjob pour vérifier **use_bayes 0**. Par exemple, modifiez /usr/sbin/amavisd-new-cronjob et ajoutez ce qui suit en haut, avant les instructions **test** :

  ```
  egrep -q "^[ \t]*use_bayes[ \t]*0" /etc/spamassassin/local.cf &amp;&amp; exit 0
  ```

15.5.3. Procédure de test

D'abord, testez que l'application **Amavisd-new** écoute bien sur le port 10024 :

```
telnet localhost 10024
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 [127.0.0.1] ESMTP amavisd-new service ready
^]
```

Dans l'en-tête des messages qui passent par le filtre de contenu, vous devriez lire :

```
X-Spam-Level:
X-Virus-Scanned: Debian amavisd-new at example.com
X-Spam-Status: No, hits=-2.3 tagged_above=-1000.0 required=5.0 tests=AWL, BAYES_00
X-Spam-Level:
```

V otre sortie variera, mais l'important c'est qu'il existe des entrées **X-Virus-Scanned** et **X-Spam-Status**.

15.5.4. Dépannage

La meilleure façon de savoir pourquoi quelque chose ne fonctionne pas est de vérifier les fichiers journaux.

- Pour les instructions sur la journalisation dans **Postfix**, voyez la section *15.1.7 Dépannage*.
- **Amavisd-new** utilise **Syslog** pour envoyer des messages dans /var/log/mail.log. Le niveau de détails peut être augmenté en ajoutant l'option **$log_level** dans /etc/amavis/conf.d/50-user, et en réglant la valeur de 1 à 5.

  ```
  $log_level = 2;
  ```

  L orsque le niveau de journalisation de **Amavisd-new** est augmenté, celui de **Spamassassin** l'est aussi.

- Pour **ClamAV**, la quantité d'informations enregistrée dans le journal peut être augmentée en modifiant /etc/clamav/clamd.conf et en réglant l'option suivante :

  ```
  LogVerbose true
  ```

  Par défaut, **ClamAV** enverra les messages de journalisation (logs) dans /var/log/clamav/clamav.log.
- Après avoir modifié les paramètres de journal d'une application, n'oubliez pas de redémarrer le service pour que les changements soient pris en compte. De plus, une fois le problème résolu, il est judicieux de revenir aux paramètres initiaux.

15.5.5. Références

Pour plus d'informations sur le filtrage des emails, voyez les liens suivants :

La documentation **Amavisd-new** : http://www.ijs.si/software/amavisd/amavisd-new-docs.html

La documentation **ClamAV** : http://www.clamav.net/doc/latest/html/ et le Wiki ClamAV : http://wiki.clamav.net/Main/WebHome

Le **Wiki de spammassassin** : http://wiki.apache.org/spamassassin/

La page d'accueil de **Pyzor** : http://sourceforge.net/apps/trac/pyzor/

Page d'accueil de **Razor** : http://razor.sourceforge.net/

DKIM.org : http://dkim.org/

Postfix Amavis New : https://help.ubuntu.com/community/PostfixAmavisNew

De plus, n'hésitez pas à poser vos questions sur le canal IRC **#ubuntu-server** (en anglais) du réseau freenode : http://freenode.net

Chapitre 16. Applications de Chat

16.1. Vue d’ensemble

Dans cette section, nous allons voir comment installer et configurer un serveur IRC, **ircd-irc2**. Nous allons aussi voir comment installer et configurer Jabber, un serveur de messagerie instantanée.

16.2. Serveur IRC

Le dépôt Ubuntu vous propose de nombreux serveurs Internet Relay Chat. Cette section explique comment installer et configurer le serveur IRC original **ircd-irc2**.

16.2.1. Installation

Pour installer **ircd-irc2**, exécutez la commande suivante dans un terminal :

```
sudo apt install ircd-irc2
```

Les fichiers de configuration sont enregistrés dans le répertoire /etc/ircd. Les documents sont disponible dans le répertoire /usr/share/doc/ircd-irc2.

16.2.2. Configuration

Le paramétrage d'IRC peut être fait dans le fichier de configuration /etc/ircd/ircd.conf. Vous pouvez définir le nom d'hôte IRC dans ce fichier en modifiant la ligne suivante :

```
M:irc.localhost::Debian ircd default configuration::000A
```

Assurez-vous d'ajouter un alias DNS pour votre nom d'hôte IRC. Par exemple, si vous définissez **irc.livecipher.com** comme nom d'hôte IRC, assurez-vous que **irc.livecipher.com** puisse être résolu par votre serveur de nom de domaine. Le nom d'hôte IRC doit être différent de votre nom d'hôte local.

Les détails de l'administrateur IRC peuvent être configurés en modifiant la ligne suivante :

```
A:Organization, IRC dept.:Daemon <ircd@example.irc.org>:Client Server::IRCnet:
```

Vous pouvez ajouter des lignes spécifiques pour configurer la liste des ports d'écoute IRC, les droits Opérateur, l'authentification client, etc. Pour plus d'informations, voir l'exemple de fichier de configuration /usr/share/doc/ircd-irc2/ircd.conf.example.gz.

La bannière IRC à afficher dans le client IRC, quand l'utilisateur se connecte au serveur, peut être modifiée dans le fichier /etc/ircd/ircd.motd.

Après les modifications nécessaires du fichier de configuration, vous pouvez redémarrer le serveur IRC avec la commande suivante :

```
sudo systemctl restart ircd-irc2.service
```

16.2.3. Références

Les autres serveurs IRC disponibles dans les dépôts Ubuntu pourront également vous intéresser. Parmi ceux-ci, on notera **ircd-ircu** et **ircd-hybrid**.

Voir la **FAQ IRCD** pour plus d'informations sur le serveur IRC : http://www.irc.org/tech_docs/ircnet/faq.html .

16.3. Serveur de messagerie instantanée Jabber

Jabber, un protocol de messagerie instantanée populaire, est basé sur XMPP, un standard ouvert pour les messageries instantanées et utilisé par beaucoup d'applications populaires. Cette section traite de la mise en place d'un serveur Jabberd 2 sur un réseau local LAN. Cette configuration peut aussi être adaptée pour fournir des services de messagerie instantanée à des utilisateurs sur internet.

16.3.1. Installation

Pour installer jabberd2, saisissez dans un terminal :

```
sudo apt install jabberd2
```

16.3.2. Configuration

Un couple de fichiers de configuration XML sera utilisé pour configurer jabberd2 pour Berkeley DB d'authentification des utilisateurs. Il s'agit d'une forme très simple d'authentification. Cependant, jabberd2 peut être configuré pour utiliser le protocole LDAP, MySQL, PostgreSQL, etc pour l'authentification des utilisateurs.

Editez tout d'abord /etc/jabberd2/sm.xml en y changeant :

```
<id>jabber.example.com</id>
```

R emplacez jabber.example.com par le nom d'hôte, ou un autre identifiant de votre serveur.

Maintenant, dans la section <storage> changez <driver> en:

```
<driver>db</driver>
```

Ensuite, modifiez /etc/jabberd2/c2s.xml, et dans la section <local>, modifiez :

```
<id>jabber.example.com</id>
```

Et dans la section <authreg>, ajustez la section <module> en:

```
<module>db</module>
```

Finalement, redémarrez jabberd2 pour activer les nouveaux paramètres :

```
sudo systemctl restart jabberd2.service
```

Vous devriez maintenant être capable de vous connecter au serveur en utilisant un client Jabber comme Pidgin par exemple.

L'avantage d'utiliser Berkeley DB pour les données utilisateur est qu'après avoir été configuré, aucune maintenance supplémentaire n'est nécessaire. Si vous avez besoin de plus de contrôle sur les comptes et les informations des utilisateurs, une autre méthode d'authentification est conseillée.

16.3.3. Références

Le **Site web de Jabberd2** contient plus de détails concernant la configuration de Jabberd2 : http://codex.xiaoka.com/wiki/jabberd2:start

Pour plus d'options d'authentification, consultez le **Guide d'Installation de Jabberd2** : http://www.jabberdoc.org/ .

Référez-vous également à la page du **Wiki anglophone d'Ubuntu** pour plus d'informations : https://help.ubuntu.com/community/SettingUpJabberServer .

Chapitre 17. Système de contrôle de version

Le contrôle de version est l’art de gérer les modifications dans l’information. Cela a longtemps été un outil crucial pour les développeurs, qui passent leur temps à effectuer de petites modifications sur leurs logiciels et à les retirer le lendemain. Mais l’utilité d’un logiciel de contrôle de version s’étend largement au-delà du monde du développement de logiciels. Partout où vous pourrez trouver des personnes qui utilisent l’informatique pour gérer une information qui est régulièrement modifiée, le contrôle de version trouvera sa place.

17.1. Bazaar

Bazaar est un nouveau système de contrôle de version sponsorisé par Canonical, l'entreprise commerciale à l'origine d'Ubuntu. À la différence de Subversion et CVS qui ne gèrent qu'un modèle centralisé, Bazaar prend aussi en charge **un contrôle de version décentralisé**, donnant aux gens la capacité de collaborer plus efficacement. En particulier, Bazar est conçu pour maximiser le niveau de participation de la communauté sur des projets libres.

17.1.1. Installation

A l'invite d'un terminal, entrez la commande suivante pour installer **bzr** :

```
sudo apt install bzr
```

17.1.2. Configuration

Pour vous présenter à **bzr**, utilisez la commande **whoami** comme suit :

```
$ bzr whoami 'Joe Doe <joe.doe@gmail.com>'
```

17.1.3. Apprentissage de Bazaar

Bazaar et fourni avec une documentation intégrée. Par défaut, elle se situe dans /usr/share/doc/bzr/html. Il est judicieux de commencer par le tutoriel. La commande **bzr** est également fournie avec une aide intégrée :

```
$ bzr help
```

Pour en savoir plus sur une commande **foo** :

```
$ bzr help foo
```

17.1.4. Intégration avec Launchpad

Tout en étant très utile en tant que système autonome, Bazaar offre en option une bonne intégration avec **Launchpad** : https://launchpad.net/ , le système de développement collaboratif utilisé par Canonical et la vaste communauté du libre pour gérer et améliorer Ubuntu lui-même. Pour savoir comment Bazaar peut être utilisé pour collaborer sur des projets libres, consultez l'adresse : http://bazaar-vcs.org/LaunchpadIntegration/ .

17.2. Git

Git est un système open source de contrôle de version distribuée développé à l'origine par **Linus Torvalds** pour soutenir le développement du noyau Linux. Chaque répertoire de travail Git est un dépôt à part entière avec l'historique complet et la traçabilité des fonctionnalités de toutes les versions, indépendant de l'accès au réseau ou d'un serveur central.

17.2.1. Installation

Le système de contrôle de version **git** est installé avec la commande suivante :

```
sudo apt install git
```

17.2.2. Configuration

Chaque utilisateur de git devrait d'abord se présenter à git, en exécutant ces deux commandes :

```
git config --global user.email "vous@example.com"
git config --global user.name "votre nom d'utilisateur"
```

17.2.3. Usage basique

Ce qui précède est en soit suffisant pour utiliser git d'une manière répartie et sûre, à condition que les utilisateurs aient accès à la machine qui assume le rôle de serveur via SSH. Sur la machine serveur, un nouveau dépôt peut être créé avec :

```
git init --bare /path/to/repository
```

Cela crée un dépôt nu, qui ne peut pas être utilisé pour éditer directement des fichiers. Si vous préférez avoir une copie viable du contenu du dépôt sur le serveur, n'utilisez pas l'option **--bare**.

Tout client avec accès SSH à la machine peut alors cloner le dépôt avec :

```
git clone username@hostname:/path/to/repository
```

Une fois cloné à la machine du client, le client peut modifier les fichiers, puis les engager et les partager avec :

```
cd /path/to/repository
#(modifier des fichiers
git commit -a              # Engage tous les changements dans la version
                           locale du dépôt
git push origin master     # Induit les changements sur la version serveur
                           du dépôt
```

17.2.4. Installation d'un serveur gitolite

Alors que ce qui précède est suffisant pour créer, cloner et modifier les dépôts, les utilisateurs désirant installer git sur un serveur, préféreront davantage un fonctionnement comme un serveur de gestion de contrôle de source plus traditionnel, avec des multi-utilisateurs et l'accès à la gestion des droits. La solution suggérée est d'installer **gitolite** avec la commande suivante :

```
sudo apt install gitolite
```

17.2.5. Configuration de gitolite

La configuration de **gitolite** est un peu différente que celle de la plupart des serveurs sur les systèmes basés sur Unix. À la place du fichier de configuration habituel dans /etc/, gitolite place sa configuration dans un dépôt git. La première étape pour configurer une nouvelle installation est donc de permettre l'accès au dépôt de configuration.

Tout d'abord, créons un utilisateur pour gitolite afin d'y accéder :

```
sudo adduser --system --shell /bin/bash --group \
--disabled-password --home /home/git git
```

Maintenant, nous voulons laisser gitolite connaître la clé SSH publique de l'administrateur du dépôt. Cela suppose que l'utilisateur actuel est l'administrateur de ce dépôt. Si vous n'avez pas encore configuré de clé SSH, reportez-vous au Chapitre *6, paragraphe 1. Serveur OpenSSH.4. Clés SSH* :

```
cp ~/.ssh/id_rsa.pub /tmp/$(whoami).pub
```

Passons sur l'utilisateur de git et importons la clé de l'administrateur dans gitolite :

```
sudo su - git
gl-setup /tmp/*.pub
```

Gitolite vous permettra de faire les changements initiaux à son fichier de configuration au cours du processus d'installation. Vous pouvez maintenant cloner et modifier la configuration de votre dépôt gitolite depuis votre utilisateur administrateur (l'utilisateur duquel vous avez importé la clé publique SSH). Revenez à cet utilisateur, puis cloner le dépôt de configuration :

```
exit
git clone git@$IP_ADDRESS:gitolite-admin.git
cd gitolite-admin
```

L'administrateur gitolite contient deux sous-répertoires, **conf** et **keydir**. Les fichiers de configuration sont dans le répertoire **conf**, et le répertoire **keydir** contient la liste des clés publiques SSH utilisateur.

17.2.6. Gestion des utilisateurs et des dépôts gitolite

Ajouter de nouveaux utilisateurs à gitolite est simple : il suffit d'obtenir la clé SSH publique et l'ajouter à l'annuaire keydir comme **$DESIRED_USER_NAME.pub**. Notez que les noms d'utilisateur gitolite n'ont pas à correspondre aux noms d'utilisateurs du système - ils ne sont utilisés que dans le fichier de configuration gitolite pour gérer le contrôle d'accès. De même, les utilisateurs sont supprimés en supprimant leur fichier de clé publique. Après chaque changement, n'oubliez pas transmettre les modifications à git, et de remonter les modifications sur le serveur avec :

```
git commit -a
git push origin master
```

Les dépôts sont gérés en modifiant le fichier conf/gitolite.conf. La syntaxe est séparée par des espaces et spécifie simplement la liste des dépôts suivie par des règles d'accès. Ce qui suit est un exemple par défaut :

```
repo gitolite-admin
        RW+       =     admin
        R         =     alice

repo project1
        RW+       =     alice
        RW        =     bob
        R         =     denise
```

17.2.7. Utilisation de votre serveur

Pour utiliser le serveur nouvellement créé, l'administrateur gitolite doit importer la clé publique de chaque utilisateurs dans le dépôt de configuration gitolite, ils peuvent ensuite accéder à n'importe quel projet où l'accès leur est autorisé avec la commande suivante :

```
git clone git@$SERVER_IP:$NOM_DU_PROJET.git
```

Ou ajouter le projet du serveur comme une télécommande pour un dépôt git existant:

```
git remote add gitolite git@$SERVER_IP:$NOM_DU_PROJET.git
```

17.3. Subversion

Subversion est un système de contrôle de version libre. En utilisant Subversion, vous pourrez enregistrer l'historique des fichiers sources et des documents. Il gère les fichiers et les répertoires dans le temps. Une arborescence des fichiers est placée dans un dépôt centralisé. Ce dépôt est à peu près identique à un serveur de fichier ordinaire, sauf qu'il conserve une trace de chaque changement effectué sur les fichiers et les répertoires.

17.3.1. Installation

Pour fournir l'accès à un dépôt Subversion en utilisant le protocole HTTP, vous devez installer et configurer un serveur Web. Il s'avère qu'Apache2 fonctionne avec Subversion. Reportez vous à la section HTTP de la rubrique Apache2 pour installer et configurer Apache2. Pour fournir l'accès à un dépôt Subversion en utilisant le protocole HTTPS, vous devez installer et configurer un certificat numérique sur votre serveur Web Apache2. Reportez vous à la section HTTPS de la rubrique Apache2 pour installer et configurer un certificat numérique.

Pour installer Subversion, utilisez la commande suivante dans un terminal :

```
sudo apt install subversion apache2 libapache2-svn
```

17.3.2. Configuration du serveur

Ces étapes supposent que vous ayez installé sur votre système les paquets mentionnés ci-dessus. Cette section explique comment créer un dépôt Subversion et accéder au projet.

17.3.2.1. Créer un dépôt Subversion

Le dépôt Subversion peut être créé en utilisant la commande suivante dans un terminal :

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

17.3.2.2. Importation des fichiers

Dès que vous avez créé le dépôt vous pouvez **importer** des fichiers dans le dépôt. Pour importer un dossier, saisissez dans un terminal :

```
svn import /path/to/import/directory file:///path/to/repos/project
```

17.3.3. Méthodes d'accès

Les dépôts Subversion sont accessibles (vérifiés) via de nombreuses méthodes différentes (sur un disque local ou au travers de protocoles réseaux divers). L'emplacement d'un dépôt est cependant toujours une URL. Le tableau indique comment les différents types d'URL sont reliés aux méthodes d'accès disponibles.

Tableau 17.1 Méthodes d'accès

Schéma	Méthode d'accès
file://	Accès direct au dépôt (sur disque local)
http://	Accès via le protocole WebDAV au serveur Web Apache2 fournissant Subversion
https://	Identique à http://, mais avec chiffrement SSL
svn://	Accès via un protocole personnalisé à un serveur svnserve
svn+ssh://	Identique à svn://, mais au travers d'un tunnel SSH

Dans cette section, nous verrons comment configurer Subversion pour toutes ces méthodes d'accès. Nous voyons ici les bases. Pour une utilisation plus avancée, référez-vous au **svn book** (NdT : livre non traduit en français pour l'heure) : http://svnbook.red-bean.com/ .

17.3.3.1. Accès direct au dépôt (file://)

C'est la plus simple des méthodes d'accès. Elle ne nécessite aucun serveur Subversion pour être exécutée. Cette méthode d'accès est utilisée lors d'un accès Subversion depuis la même machine. La syntaxe de la commande, saisie dans un terminal, est la suivante :

```
svn co file:///path/to/repos/project
```

ou

```
svn co file://localhost/path/to/repos/project
```

Si vous ne spécifiez pas le nom d'hôte, il y a trois barres obliques (///), deux pour le protocole (file, dans ce cas) plus la première barre oblique de l'arborescence des fichiers. Si vous spécifiez le nom d'hôte, vous devez utiliser deux barres obliques (//).

Les droits d'accès au dépôt dépendent de ceux du système de fichiers. Si l'utilisateur a les droits d'accès en lecture et écriture, alors il peut extraire et déposer des fichiers sur le serveur.

17.3.3.2. Accès par le protocole WebDAV (http://)

Pour accéder au dépôt Subversion via le protocole WebDAV, vous devez configurer votre serveur web Apache 2. Ajouter l'extrait suivant entre les balises < VirtualHost > et </VirtualHost > dans /etc/apache2/sites-available/000-default.conf , ou un autre fichier VirtualHost :

```
<Location /svn>
```

```
  DAV svn
  SVNParentPath /path/to/repos
  AuthType Basic
  AuthName "Votre nom de dépôt"
  AuthUserFile /etc/subversion/passwd
  Require valid-user
</Location>
```

Le fragment de configuration ci-dessus suppose que les dépôts Subversion sont créés dans le répertoire /chemin/vers/dépôt en utilisant la commande **svnadmin** et que l'utilisateur HTTP a les droits d'accès à ces fichiers (voir ci-dessous). Ils peuvent être accessibles en utilisant l'url : **http://hostname/svn/nom_du_dépôt**.

Changer la configuration apache comme ci-dessus nécessite le rechargement du service avec la commande suivante :

```
sudo systemctl reload apache2.service
```

Pour importer ou envoyer des fichiers sur votre dépôt Subversion via HTTP, le dépôt doit être possédé (₪!) par l'utilisateur HTTP. Dans les systèmes Ubuntu, l'utilisateur HTTP est **www-data**. Pour changer le propriétaire des fichiers du dépôt, entrez la commande suivante depuis un terminal :

```
sudo chown -R www-data:www-data /path/to/repos
```

Si vous modifiez le propriétaire du dépôt en **www-data** vous ne pourrez plus importer ou renvoyer des fichiers dans le dépôt en exécutant la commande **svn import file:///** comme tout utilisateur différent de **www-data**.

Ensuite, vous devez créer le fichier /etc/subversion/passwd qui contiendra les détails d'authentification des utilisateurs. Pour cela, saisissez la commande suivante dans une invite de terminal (ce qui créera le fichier et ajoutera le premier utilisateur) :

```
sudo htpasswd -c /etc/subversion/passwd nom_utilisateur
```

Pour ajouter d'autres utilisateurs, omettez l'option **« -c »** car celle-ci remplace l'ancien fichier. Utilisez à la place cette formulation :

```
sudo htpasswd /etc/subversion/passwd user_name
```

Cette commande vous demande de saisir le mot de passe. Une fois le mot de passe saisi, l'utilisateur est ajouté. Dès lors, pour accéder au dépôt, vous pouvez utiliser la commande suivante :

```
svn co http://servername/svn
```

! Le mot de passe est transmis en clair, comme texte simple. Si vous craignez que des fouineurs récupèrent votre mot de passe, nous vous conseillons d'utiliser un chiffrement par SSL. Pour plus d'information, veuillez consulter la section suivante.

17.3.3.3. Accès par le protocole WebDAV avec un chiffrement SSL (https://)

L'accès au dépôt subversion via le protocole WebDAV avec cryptage SSL (https: //) est similaire à http://

sauf que vous devez installer et configurer le certificat numérique dans votre serveur web Apache 2. Pour utiliser SSL avec Subversion ajoutez la configuration Apache2 ci-dessus à /etc/apache2/sites-available/default-ssl.conf. Pour plus d'informations sur la configuration Apache2 avec SSL voir le *Chapitre 11, paragraphe 1. HTTPD - serveur web Apache2 .3. Configuration HTTPS*.

Vous pouvez installer un certificat numérique signé par une autorité de certification. Sinon, vous pouvez installer votre propre certificat auto-signé.

Cette étape suppose que vous avez installé et configuré un certificat numérique sur votre serveur Web Apache2. Maintenant, pour accéder au dépôt Subversion, veuillez vous référer à la section ci-dessus ! Les méthodes d'accès sont exactement les mêmes, hormis le protocole. Vous devez utiliser https:// pour accéder au dépôt Subversion.

17.3.3.4. Accès via un protocole personnalisé (svn://)

Une fois le dépôt Subversion créé, vous pouvez configurer le contrôle d'accès. Vous pouvez modifier le fichier /path/to/repos/project/conf/svnserve.conf pour cela. Par exemple, pour activer l'authentification, vous pouvez dé-commenter les lignes suivantes dans le fichier de configuration :

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

Après avoir dé-commenté ces lignes, vous pouvez gérer la liste des utilisateurs dans le fichier passwd. Modifiez donc le fichier passwd dans le même répertoire et ajoutez le nouvel utilisateur. La syntaxe se présente ainsi :

```
username = password
```

Pour plus de renseignements, référez-vous au fichier.

Maintenant, pour accéder à Subversion via le protocole personnalisé svn://, soit de la même machine, soit d'une autre, vous pouvez exécuter svnserver en utilisant la commande svnserve. La syntaxe se présente ainsi :

```
$ 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
```

Une fois la commande exécutée, Subversion démarre en écoutant le port par défaut (3690). Pour accéder au dépôt du projet, vous devez exécuter la commande suivante dans un terminal :

```
svn co svn://hostname/project project --username user_name
```

Suivant la configuration du serveur, il vous demande un mot de passe. Une fois que vous vous êtes authentifié, il vérifie le code sur le dépôt Subversion. Pour synchroniser le dépôt du projet avec votre copie locale, vous pouvez exécuter la sous-commande **update**. La syntaxe de cette commande, saisie dans un terminal, est la suivante :

```
cd project_dir ; svn update
```

Pour plus d'informations sur l'utilisation de chaque sous-commande de Subversion, vous pouvez vous

référer au manuel. Par exemple, pour en savoir plus sur la commande **co** (checkout), exécutez la commande suivante dans un terminal :

```
svn co help
```

17.3.3.5. Accès par protocole personnalisé avec chiffrement SSH (svn+ssh://)

La configuration et le processus du serveur est le même que pour la méthode svn://. Pour plus de détails, veuillez vous référer au chapitre précédent. Dans cette étape, nous supposons que vous avez suivi l'étape précédente et que vous avez démarré le serveur Subversion en utilisant la commande **svnserve**.

De même, nous supposons que le serveur ssh s'exécute sur cette machine et que les connexions entrantes y sont autorisées. Pour vous en assurer, essayez de vous connecter à la machine en utilisant ssh. Si vous pouvez vous identifier, alors tout est parfait. Si vous ne pouvez pas vous identifier, résolvez le problème avant de continuer.

Le protocole svn+ssh:// est utilisé pour accéder au dépôt Subversion en utilisant un chiffrement SSL. Le transfert de données est chiffré en utilisant cette méthode. Pour accéder au dépôt du projet (pour une vérification par exemple), vous devez utiliser la syntaxe suivante :

```
svn co svn+ssh://ssh_utilisateur@hôte/path/to/repos/project
```

Vous devez utiliser le chemin complet (/chemin/vers/dépôt/projet) pour accéder au dépôt Subversion en utilisant cette méthode d'accès.

Suivant la configuration du serveur, il vous demande un mot de passe. Vous devez saisir le mot de passe que vous utilisez pour vous identifier via ssh. Une fois que vous vous êtes authentifié, il vérifie le code sur le dépôt Subversion.

17.4. Références

Site Web de Bazaar : http://bazaar.canonical.com/en/

Launchpad : https://launchpad.net/

Page d'accueil git : http://git-scm.com

Gitolite : https://github.com/sitaramc/gitolite

Site Web de Subversion : http://subversion.apache.org/

Livre sur Subversion : http://svnbook.red-bean.com/

Page du Wiki Ubuntu consacrée à Easy Bazaar : https://help.ubuntu.com/community/EasyBazaar

Page du Wiki Ubuntu consacrée à Subversion : https://help.ubuntu.com/community/Subversion

Chapitre 18. Samba

Les réseaux informatiques sont souvent composés de systèmes divers et même si opérer un réseau constitué exclusivement de stations de travail et de serveurs Ubuntu serait assurément plaisant, certains environnements réseau sont constitués à la fois de systèmes Ubuntu et de systèmes **Microsoft Windows** travaillant ensemble en harmonie. Cette section du guide du serveur **Ubuntu** présente les principes et les outils utilisés pour configurer votre serveur Ubuntu afin de partager des ressources réseau avec des ordinateurs Windows.

18.1. Introduction

Pour réussir la mise en réseau de votre système Ubuntu avec des clients Windows, vous devez fournir et intégrer les services fréquemment utilisés dans les environnements Windows. Ces services permettent le partage des données et des informations sur les ordinateurs et les utilisateurs présents sur le réseau. Ils peuvent être classés selon trois catégories principales suivant leur rôle :

- **Les Services de partage de fichiers et d'imprimantes**. L'utilisation du protocole Server Message Block (SMB) facilite le partage de fichiers, de dossiers, de volumes et le partage des imprimantes sur le réseau.
- **Les Services d'annuaire**. Partage des informations vitales sur les ordinateurs et les utilisateurs du réseau avec des technologies telles que LDAP (Lightweight Directory Access Protocol) et l' **Active Directory** de Microsoft (services d'annuaire).
- **L'Authentification et l'Accès**. Établir l'identité d'un ordinateur ou d'un utilisateur du réseau et déterminer les informations auxquelles l'ordinateur ou l'utilisateur est autorisé à accéder à l'aide de ces principes et des technologies comme les permissions de fichiers, des politiques de groupe et le service d'authentification Kerberos.

Heureusement, votre système Ubuntu peut fournir toutes ces fonctionnalités des clients Windows et partager les ressources du réseau avec eux. L'un des principaux logiciels inclus dans votre système Ubuntu permettant la mise en réseau avec Windows est la suite Samba composée des applications et outils pour serveur SMB.

Cette partie du guide serveur **Ubuntu** vous présentera quelques cas d'utilisation de Samba et comment installer et configurer les paquets nécessaires. Vous trouverez de plus amples informations et une documentation complète sur Samba sur le site de **Samba** : http://www.samba.org .

18.2. Serveur de fichiers

Une des méthodes les plus courantes pour mettre Ubuntu et Windows en réseau est de configurer Samba en serveur de fichiers. Cette section décrit l'installation d'un serveur **Samba** afin de partager des fichiers avec des clients Windows.

Le serveur sera configuré pour partager des fichiers avec n 'importe quel client sur le réseau sans avoir à saisir de mot de passe. Si votre environnement nécessite des contrôles d'accès (Access Controls) plus stricts, voyez samba-fileprint-security Section 4, "Sécurisation du serveur de fichiers et d'impression"

18.2.1. Installation

La première étape consiste à installer le paquet **samba**. Dans un terminal saisissez :

```
sudo apt install samba
```

C'est tout ce que vous avez à faire. Vous êtes maintenant prêt à configurer Samba pour partager des fichiers.

18.2.2. Configuration

Le principal fichier de configuration de Samba est situé dans /etc/samba/smb.conf. Le fichier de configuration par défaut a un nombre important de commentaires afin de documenter des directives de configuration différentes.

> Le fichier de configuration ne contient pas toutes les options disponibles. Consultez la page **man** de smb.conf ou le **Samba HOWTO Collection** (en anglais) pour plus de détails : http://samba.org/samba/docs/man/Samba-HOWTO-Collection/ .

1. Tout d'abord, modifiez les couples clé/valeur suivantes dans la section **[global]** de /etc/samba/smb.conf :

   ```
   workgroup = EXAMPLE
   …
   security = user
   ```

   Le paramètre **security** situé plus bas dans la section [global] est commenté par défaut. Modifiez également **EXEMPLE** afin de l'adapter à votre environnement.

2. Créez une nouvelle section à la fin du fichier (ou dé-commentez un des exemples) pour le dossier à partager :

   ```
   [share]
       comment = Dossier partagé sur le serveur Ubuntu
       path = /srv/samba/share
       browsable = yes
       guest ok = yes
       read only = no
       create mask = 0755
   ```

- **comment :** une brève description du partage. Adaptez-le à vos besoins.
- **path :** l'emplacement du dossier à partager.

  Cet exemple utilise /srv/samba/nom_partage car selon la norme de la hiérarchie des systèmes de fichiers (**Filesystem Hierarchy Standard : FHS**), **/srv** (http://www.pathname.com/fhs/pub/fhs-2.3.html#SRVDATAFORSERVICESPROVIDEDBYSYSTEM) est l'emplacement où doivent se trouver les données à servir sur le réseau. Techniquement, les partages Samba peuvent être placés n'importe où sur le système de fichiers tant que les permissions sont correctes, mais le respect des standards est recommandé.
- **browsable :** autorise les clients Windows à parcourir le répertoire partagé en utilisant l'**explorateur de fichiers de Windows**.
- **guest ok :** permet aux clients de se connecter au répertoire partagé sans fournir de mot de passe.
- **read only :** détermine si le partage est en lecture seule ou si les privilèges en écriture sont accordés. Les droits d'écriture sont accordés seulement si la valeur est **no**. Comme on le voit dans cet exemple, si la valeur est **yes**, alors l'accès au partage est en lecture seule.
- **create mask :** détermine les permissions des fichiers nouvellement créés.

3. Maintenant que **Samba** est configuré, le répertoire doit être créé et les permissions modifiées. Depuis un terminal, tapez :

```
sudo mkdir -p /srv/samba/share
sudo chown nobody:nogroup /srv/samba/share/
```

L 'argument **-p** indique à mkdir de créer l'entière arborescence du répertoires si elle n'existe pas.

4. Pour finir, redémarrez les services **samba** pour activer la nouvelle configuration :

```
sudo systemctl restart smbd.service nmbd.service
```

! Notez bien que la configuration ci-dessus donne un accès complet à n'importe quel client sur le réseau local. Pour une configuration plus sécurisée, consultez le *Chapitre 18, paragraphe 4. Sécurisation du serveur de fichiers et d'impression*.

À partir d'un client Windows, vous devriez maintenant être en mesure d'accéder au serveur de fichiers Ubuntu et de voir le répertoire partagé. Si votre client n'affiche pas votre partage automatiquement, essayez d'accéder à votre serveur par son adresse IP, par exemple, \ \ 192.168.1.1, dans une fenêtre de l'Explorateur Windows. Pour vérifier que tout fonctionne essayez de créer un répertoire à partir de Windows.

Pour créer d'autres partages, ajoutez de nouvelles sections **[dir]** dans /etc/samba/smb.conf et redémarrez **Samba**. Assurez-vous seulement que le répertoire que vous souhaitez partager existe et qu'il possède les permissions idoines.

Le partage de fichier nommé **"[partage]"** et le chemin /srv/samba/share ne sont que des exemples. Adaptez le nom des partages et des chemins à votre environnement. C'est une bonne idée de nommer un partage d'après le nom d'un répertoire sur le système de fichiers. Un autre exemple pourrait être un nom de partage **[qa]** avec un chemin /srv/samba/qa.

18.2.3. Ressources

Pour des configurations plus élaborées de Samba, consultez les **guides pratiques Samba** (en anglais) : http://samba.org/samba/docs/man/Samba-HOWTO-Collection/ .

Ce guide est également disponible en **format papier** : http://www.amazon.com/exec/obidos/tg/detail/-/0131882228 .

Le livre **Using Samba** d'O'Reilly est une autre bonne source d'informations : http://www.oreilly.com/catalog/9780596007690/ .

La page du **Wiki Ubuntu consacrée à Samba** : https://help.ubuntu.com/community/Samba .

18.3. Serveur d'impression

Une autre utilisation classique de Samba est de le configurer pour partager les imprimantes installées sur un serveur Ubuntu, que ce soit localement ou sur le réseau. De même que dans le *Chapitre 18, paragraphe 2. Serveur de fichiers*, cette section permet de configurer Samba pour permettre à n'importe quel client sur le réseau d'utiliser les imprimantes sans demande de mot de passe.

Pour une configuration plus sécurisée, voir le *Chapitre 18, paragraphe 4. Sécurisation du serveur de fichiers et d'impression*.

18.3.1. Installation

Avant d'installer et de configurer Samba, il est préférable de disposer d'une installation fonctionnelle de **CUPS**. Voir le *Chapitre 14, paragraphe 4. CUPS - Serveur d'impression* pour plus de détails.

Pour installer le paquet **samba**, entrez la commande suivante depuis un terminal :

```
sudo apt install samba
```

18.3.2. Configuration

Après avoir installé Samba éditez le fichier /etc/samba/smb.conf. Changez le **workgroup** (groupe de travail) pour l'adapter à votre réseau et passez **security** (sécurité) à **user** (utilisateur) :

```
workgroup = EXAMPLE
...
security = user
```

Dans la section **[printers]**, mettez l'option **guest ok** à **yes** :

```
browsable = yes
guest ok = yes
```

Redémarrez Samba avoir modifié smb.conf :

```
sudo systemctl restart smbd.service nmbd.service
```

La configuration par défaut de Samba partagera automatiquement toute imprimante installée. Installez simplement l'imprimante localement sur vos clients Windows.

18.3.3. Ressources

Pour des configurations plus élaborées de Samba, consultez les **guides pratiques Samba** (en anglais) : http://samba.org/samba/docs/man/Samba-HOWTO-Collection/ .

Ce guide est également disponible en **format papier** :
http://www.amazon.com/exec/obidos/tg/detail/-/0131882228 .

Le livre **Using Samba** d'O'Reilly est une autre bonne source d'informations : http://www.oreilly.com/catalog/9780596007690/ .

Voir également le **site Web de CUPS** pour plus d'informations sur la manière de configurer CUPS : http://www.cups.org/ .

La page du **Wiki Ubuntu consacrée à Samba** : https://help.ubuntu.com/community/Samba .

18.4. Sécurisation du serveur de fichiers et d'impression

18.4.1. Profils de sécurité de Samba

Les deux niveaux de sécurité disponibles pour le protocole réseau CIFS (Common Internet Filesystem) sont **user-level** et **share-level**. La mise en œuvre des **options de sécurité** de Samba permet plus de flexibilité en fournissant quatre possibilités de sécurité au niveau de l'utilisateur plus une au niveau du partage :

- **security = user :** requiert des clients qu'ils fournissent un nom d'utilisateur et un mot de passe pour se connecter aux partages. Les comptes d'utilisateurs Samba sont séparés des comptes système, mais le paquet **libpam-winbind** synchronisera les utilisateurs et mots de passe système avec la base de données des utilisateurs Samba.
- **security = domain :** permet au serveur Samba d'apparaître aux clients Windows comme un contrôleur principal de domaine (PDC : Primary Domain Controller), un contrôleur de domaines de sauvegarde (BDC : Backup Domain Controller) ou un serveur membre du domaine (DMS : Domain Member Server). Consultez le *Chapitre 18, paragraphe 5. En tant que contrôleur de domaine* pour plus d'informations.
- **security = ADS :** permet au serveur Samba de joindre un domaine Active Directory. Consultez le *Chapitre 18, paragraphe 6. Integration Active Directory* pour plus de détails.
- **security = server :** est une option qui date de l'époque où Samba ne pouvait pas devenir un serveur membre et ne devait pas être utilisé en raison de plusieurs problèmes de sécurité. Consultez la section **sécurité du serveur** (en) du guide Samba pour plus de détails : http://samba.org/samba/docs/man/Samba-HOWTO-Collection/ServerType.html#id349531 .
- **security= share :** permet aux clients de se connecter aux partages sans fournir de nom d'utilisateur ni de mot de passe.

Le choix du mode de sécurité dépendra de votre environnement et de ce que vous attendez de votre serveur Samba.

18.4.2. Security = User

Cette section permet de reconfigurer le serveur de fichiers et d'impression Samba défini dans le *Chapitre 18, paragraphe 2. Serveur de fichiers* et dans le *Chapitre 18, paragraphe 3. Serveur d'impression* de façon à imposer une identification.

Tout d'abord, installez le paquet **libpam-winbind**, qui va synchroniser les utilisateurs du système avec la base de données d'utilisateurs de Samba :

```
sudo apt install libpam-winbind
```

S i vous choisissez la tâche **Serveur Samba** pendant l'installation **libpam-winbind** est déjà installé.

Modifiez la section **[share]** du fichier /etc/samba/smb.conf :

```
guest ok = no
```

Pour terminer, redémarrez Samba afin que les nouveaux paramètres soient pris en compte :

```
sudo systemctl restart smbd.service nmbd.service
```

Vous devrez désormais fournir un nom d'utilisateur et un mot de passe quand vous vous connecterez à un dossier ou une imprimante partagée.

Si vous connectez un lecteur réseau au dossier partagé, vous pouvez cocher la case "Reconnecter au démarrage". Vous n'aurez alors à saisir le nom d'utilisateur et le mot de passe qu'une seule fois, du moins jusqu'au changement de mot de passe.

18.4.3. Sécurité des Partages

Plusieurs options sont disponibles pour accroître la sécurité de chaque dossier partagé. En utilisant l'exemple **[share]**, cette section couvre les options les plus fréquentes.

18.4.3.1. Les 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 les ressources réseau configurées pour autoriser l'accès au groupe **qa** seront accessibles à freda, danika et rob, mais pas à jeremy ou à vincent. Comme l'utilisateur **danika** appartient aux deux groupes **qa** et **support**, elle aura accès 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.

Par défaut, Samba inspecte les groupes système locaux définis dans /etc/group pour déterminer quels utilisateurs appartiennent à quels groupes. Pour de plus amples informations sur l'ajout et la suppression des utilisateurs dans les groupes, consultez le *Chapitre 9, paragraphe 1. Gestion des utilisateurs.2. Ajout et suppression d'utilisateurs*.

Pour définir un groupe dans le fichier de configuration de Samba, /etc/samba/smb.conf, vous devez le préfacer avec le symbole « @ ». Par exemple, si vous souhaitez définir un groupe nommé **sysadmin** dans une section spécifique de /etc/samba/smb.conf, vous devrez saisir **@sysadmin**.

18.4.3.2. Droits d'accès aux fichiers

Les permissions sur les fichiers définissent précisément les droits d'un ordinateur ou d'un utilisateur sur un dossier particulier, un fichier ou un groupe de fichiers. De telles permissions peuvent être définies en modifiant le fichier /etc/samba/smb.conf et en précisant les permissions sur un dossier partagé.

Par exemple, si vous avez défini un partage Samba appelé **share** et que vous souhaitez donner des droits en **lecture seule** à un groupe appelé **qa**, ainsi que des droits en écriture au groupe **sysadmin** et à l'utilisateur **vincent**, vous devez modifier le fichier /etc/samba/smb.conf et ajouter les lignes suivantes dans la section **[share]** :

```
read list = @qa
write list = @sysadmin, vincent
```

Un autre type de permissions dans Samba consiste à donner des permissions **administratives** sur une ressource partagée spécifique. Les utilisateurs ayant des permissions administratives sur une ressource peuvent lire, écrire ou modifier toutes les informations contenues dans celle-ci.

Par exemple, si vous voulez donner à l'utilisateur **melissa** des permissions administratives sur le partage **share**, vous devez modifier le fichier /etc/samba/smb.conf et ajouter les lignes suivantes à la section **[share]** :

```
admin users = melissa
```

Après avoir modifié/etc/samba/smb.conf, redémarrez Samba pour que les nouveaux paramètres soient pris en compte :

```
sudo systemctl restart smbd.service nmbd.service
```

Pour que **read list** et **write list** fonctionnent, le mode de sécurité de Samba **ne doit pas** être réglé sur **security = share**

Maintenant que Samba a été configuré pour définir quels groupes ont accès au répertoire partagé, les permissions du système de fichier doivent être mises à jour.

Les permissions de fichiers traditionnelles de Linux ne correspondent pas exactement aux listes de contrôle d'accès (ACL) de Windows NT. Heureusement, les ACL POSIX sont disponibles sur les serveurs Ubuntu, permettant un contrôle plus fin des droits. Par exemple, pour activer les ACL sur un système de fichiers EXT3 /srv, il faut éditer le fichier /etc/fstab et ajouter l'option **acl** :

```
UUID=66bcdd2e-8861-4fb0-b7e4-e61c569fe17d /srv ext3  noatime,relatime,acl 0  1
```

Puis remontez la partition :

```
sudo mount -v -o remount /srv
```

L'exemple ci-dessus suppose que /srv est monté sur une partition dédiée. Si /srv, ou tout autre endroit où vous auriez configuré votre répertoire partagé, appartient à la partition /, un redémarrage de la machine pourrait être nécessaire.

Conformément à la configuration Samba ci-dessus, le groupe **sysadmin** aura les droits en lecture, écriture et exécution sur /srv/samba/share, le groupe **qa** aura les droits en lecture et exécution, et les fichiers auront pour propriétaire l'utilisateur **melissa**. Saisissez dans un terminal :

```
sudo chown -R melissa /srv/samba/share/
sudo chgrp -R sysadmin /srv/samba/share/
sudo setfacl -R -m g:qa:rx /srv/samba/share/
```

La commande **setfacl** ci-dessus donne les droits **execute** à tous les fichiers du répertoire /srv/samba/share, que vous pouvez désirer ou non.

Maintenant, à partir d'un client Windows, vous devriez remarquer la mise en œuvre des nouvelles permissions sur les fichiers. Consultez les pages de manuel **acl** et **setfacl** pour plus d'informations sur la gestion des ACLs POSIX.

18.4.4. Profil AppArmor pour Samba

Ubuntu est fourni avec le module de sécurité **AppArmor**, qui prévoit des contrôles d'accès obligatoires. Le profil par défaut d'AppArmor pour Samba doit être adapté à votre configuration. Pour plus de détails sur AppArmor, voir le *Chapitre 9, paragraphe 4. AppArmor*.

Il existe des profils par défaut pour les démons Samba /usr/sbin/smbd et /usr/sbin/nmbd. Ces profils font partie du paquet **apparmor-profiles**. Pour installer ce paquet, saisissez ceci dans un terminal :

```
sudo apt install apparmor-profiles apparmor-utils
```

C e paquet contient des profils pour plusieurs autres exécutables.

Par défaut les profils pour **smbd** et **nmbd** sont dans le mode **complain** pour permettre à Samba de travailler sans modifier le profil et de journaliser les erreurs seulement. Pour placer le profil **smbd** dans le mode **enforce** et ainsi faire fonctionner Samba comme prévu, le profil doit être modifié de façon à tenir compte de tous les répertoires partagés.

Editez /etc/apparmor.d/usr.sbin.smbd en ajoutant les informations dans **[share]** à partir de l'exemple du serveur de fichiers :

```
/srv/samba/share/ r,
/srv/samba/share/** rwkix,
```

Maintenant, placez le profil dans **enforce** et rechargez-le :

```
sudo aa-enforce /usr/sbin/smbd
cat /etc/apparmor.d/usr.sbin.smbd | sudo apparmor_parser -r
```

Vous devriez pouvoir lire, écrire et exécuter les fichiers dans le dossier partagé et l'exécutable **smbd** n'aura accès qu'aux fichiers et dossiers configurés. Assurez vous d'avoir ajouté une entrée pour chaque dossier que vous voulez partager avec Samba. Quoi qu'il en soit, toutes les erreurs seront écrites dans le fichier journal /var/log/syslog.

18.4.5 Ressources

Pour des configurations plus élaborées de Samba, consultez les **guides pratiques Samba** (en anglais) : http://samba.org/samba/docs/man/Samba-HOWTO-Collection/ .

Ce guide est également disponible en **format papier** : http://www.amazon.com/exec/obidos/tg/detail/-/0131882228 .

Le manuel O'Reilly **Using Samba** (en anglais) est aussi une bonne référence : http://www.oreilly.com/catalog/9780596007690/ .

Le **chapitre 18** (en anglais) de la collection HOWTO de Samba est dédié à la sécurité : http://samba.org/samba/docs/man/Samba-HOWTO-Collection/securing-samba.html .

Pour plus d'informations sur Samba et sur les ACLs, consultez la page **Samba ACLs** : http://samba.org/samba/docs/man/Samba-HOWTO-Collection/AccessControls.html#id397568 .

La page du **Wiki Ubuntu consacrée à Samba** : https://help.ubuntu.com/community/Samba .

18.5. En tant que contrôleur de domaine

Bien qu'il ne puisse pas agir comme un contrôleur de domaine principal Active Directory , un serveur Samba peut être configuré pour apparaître comme contrôleur de domaine de type Windows NT4. Un des avantages majeurs de cette configuration est la centralisation des informations d'identification pour les machines et les utilisateurs. Samba peut également stocker les informations utilisateurs de différentes manières.

18.5.1. Contrôleur de domaine principal

Cette section aborde la configuration de Samba en contrôleur de domaine principal (PDC) en utilisant le gestionnaire de mot de passe par défaut smbpasswd.

1. Commencez par installer Samba et **libpam-winbind** pour synchroniser les comptes d'utilisateurs, en saisissant dans un terminal :

```
sudo apt install samba libpam-winbind
```

2. Ensuite, configurez Samba en éditant /etc/samba/smb.conf. Le mode **security** doit être réglé sur **user**, et le **workgroup** doit correspondre à votre organisation :

```
workgroup = EXAMPLE
...
security = user
```

3. Dans la section commentée "Domains" (Domaines) ajoutez ou supprimez les éléments suivants (la dernière ligne a été divisée pour s'adapter au format de ce document) :

```
domain logons = yes
logon path = \\%N\%U\profile
logon drive = H:
logon home = \\%N\%U
logon script = logon.cmd
add machine script = sudo /usr/sbin/useradd -N -g machines -c Machine -d
     /var/lib/samba -s /bin/false %u
```

Si vous ne voulez pas utiliser les **profils itinérants** laissez *en commentaire* les options **logon home** et **logon path**.

- **domain logons :** permet à Samba d'agir comme un contrôleur de domaine
- **logon path :** place le profil des utilisateurs Windows dans leur répertoire personnel. Il est également possible de configurer un partage **[profiles]** pour placer tous les profils dans un seul et même répertoire.
- **logon drive :** spécifie l'emplacement du répertoire personnel local.
- **logon home :** spécifie l'emplacement du répertoire personnel.
- **logon script :** indique le script à exécuter localement une fois l'utilisateur connecté. Le script doit être placé dans le partage **[netlogon]**.

- **add machine script :** un script qui créera automatiquement un **compte de machine approuvé**, requis pour qu'une station de travail puisse joindre le domaine.

Dans cet exemple le groupe **machines** devra être créé en utilisant la commande **addgroup**, consultez *9.1.2. Ajout et suppression d'utilisateurs* pour plus de détails.

4. Dé-commentez le partage **[homes]** pour permettre au **logon home** d'être monté en lecteur réseau :

```
[homes]
    comment = Home Directories
    browseable = no
    read only = no
    create mask = 0700
    directory mask = 0700
    valid users = %S
```

5. Dans le cas d'une configuration en contrôleur de domaine, un partage **[netlogon]** doit être configuré. Pour activer le partage, dé-commenter :

```
[netlogon]
    comment = Network Logon Service
    path = /srv/samba/netlogon
    guest ok = yes
    read only = yes
    share modes = no
```

Le chemin par défaut du partage **netlogon** est /home/samba/netlogon. Cependant, d'après le standard FHS (Filesystem Hierarchy Standard), **/srv** (http://www.pathname.com/fhs/pub/fhs-2.3.html#SRVDATAFORSERVICESPROVIDEDBYSYSTEM) est l'emplacement correct pour des données spécifiques à un site fournies par le système.

6. Créez maintenant le dossier directory netlogon et le fichier de script logon.cmd vide (pour l'instant) :

```
sudo mkdir -p /srv/samba/netlogon
sudo touch /srv/samba/netlogon/logon.cmd
```

Vous pouvez utiliser les commandes de script de connexion normales Windows dans logon.cmd pour personnaliser l'environnement du client.

7. Redémarrez Samba pour activer le nouveau contrôleur de domaine:

```
sudo systemctl restart smbd.service nmbd.service
```

8. Enfin, il y a quelques commandes supplémentaires nécessaires pour configurer les droits d'accès appropriés.

Comme **root** est désactivé par défaut, il est nécessaire de faire correspondre un groupe système au groupe Windows **Domain Admins** pour pouvoir joindre une machine au domaine. Saisissez la commande suivante dans un terminal (utilisation de **net**) :

```
sudo net groupmap add ntgroup="Domain Admins" unixgroup=sysadmin \
rid=512 type=d
```

Remplacez **sysadmin** par le groupe que vous préférez. De même, l'utilisateur qui joindra les machines au domaine doit être membre du groupe **sysadmin** mais aussi du groupe **admin**. Le groupe **admin** permet l'utilisation de **sudo**.

Si l'utilisateur ne dispose pas encore d'identifiants Samba, vous pouvez les ajouter avec l'utilitaire **smbpasswd**, changer l'identifiant **sysadmin** de manière appropriée :

```
sudo smbpasswd -a sysadmin
```

De plus, les droits d'accès doivent être fournis explicitement au groupe des **Administrateurs domaine** pour permettre l'exécution du script **ajouter une machine** (et autres fonctions administrateur). Ceci peut être accompli en exécutant :

```
net rpc rights grant -U sysadmin "EXAMPLE\Domain Admins" \
SeMachineAccountPrivilege SePrintOperatorPrivilege SeAddUsersPrivilege \
SeDiskOperatorPrivilege SeRemoteShutdownPrivilege
```

9. Vous devriez maintenant être capable de connecter les clients Windows au domaine de la même manière que vous les connectez à un domaine NT4 fonctionnant sur un Serveur Windows.

18.5.2. Contrôleur de domaine de sauvegarde

Avec un contrôleur de domaine principal (PDC) opérationnel, il est préférable d'avoir également un contrôleur de domaine de sauvegarde (BDC). Cela permettra aux clients de pouvoir toujours s'authentifier en cas d'indisponibilité du contrôleur principal de domaine.

Lorsque vous paramétrez Samba en tant que BDC, vous avez besoin de synchroniser les informations de comptes avec le PDC. Ceci peut être fait avec divers outils tels que **scp**, **rsync** ou en utilisant **LDAP** en tant que **passdb backend**.

L'utilisation de LDAP est la façon la plus efficace de synchroniser des informations relatives aux comptes, car les deux contrôleurs de domaine peuvent utiliser les mêmes informations en temps réel. Cependant, configurer un serveur LDAP peut s'avérer trop complexe pour un petit nombre d'utilisateurs et de comptes d'ordinateurs. Voir le *Chapitre 7, paragraphe 2. Samba et LDAP* pour plus de détails.

1. Commencez par installer **samba** et **libpam-winbind**. Dans un terminal, saissisez :

```
sudo apt install samba libpam-winbind
```

2. Modifiez maintenant /etc/samba/smb.conf et dé-commentez ce qui suit dans la section **[global]** :

```
workgroup = EXAMPLE
...
security = user
```

3. Dans la section commentée **Domains** dé-commentez ou ajoutez :

```
domain logons = yes
domain master = no
```

4. Assurez-vous qu'un utilisateur a le droit de lire les fichiers dans /var/lib/samba. Ainsi, pour permettre à un utilisateur du groupe **admin** d'effectuer un **scp** sur les fichiers, saisissez :

```
sudo chgrp -R admin /var/lib/samba
```

5. Il faut ensuite synchroniser les comptes utilisateurs en se servant de **scp** pour copier le répertoire /var/lib/samba depuis le PDC :

```
sudo scp -r identifiant@pdc:/var/lib/samba /var/lib
```

R emplacez **username** par un identifiant correct et **pdc** par le nom d'hôte ou par l'adresse IP du PDC.

6. Pour finir, redémarrez **samba** :

```
sudo systemctl restart smbd.service nmbd.service
```

Vous pouvez tester le bon fonctionnement de votre BDC en arrêtant le démon Samba du PDC puis en essayant de vous identifier sur le domaine à partir d'un client Windows préalablement joint au domaine.

Une autre chose à conserver à l'esprit est que si vous avez configuré l'option **logon home** comme répertoire sur le PDC, et que le PDC devient indisponible, l'accès pour l'utilisateur au lecteur **Home** sera également impossible. Pour cette raison, il est préférable de configurer le **logon home** afin qu'il réside sur un serveur de fichiers séparé du PDC et du BDC.

18.5.3. Ressources

Pour des configurations plus élaborées de Samba, consultez les **guides pratiques Samba** (en anglais) : http://samba.org/samba/docs/man/Samba-HOWTO-Collection/ .

Ce guide est également disponible en **format papier** : http://www.amazon.com/exec/obidos/tg/detail/-/0131882228 .

Le manuel O'Reilly **Using Samba** (en anglais) est aussi une bonne référence : http://www.oreilly.com/catalog/9780596007690/ .

Le **chapitre 4** de la collection des guides Samba décrit la mise en place d'un contrôleur de domaine primaire (PDC) : http://samba.org/samba/docs/man/Samba-HOWTO-Collection/samba-pdc.html .

Le **chapitre 5** de la collection des guide Samba décrit la mise en place d'un contrôleur de domaine de sauvegarde (BDC) : http://us3.samba.org/samba/docs/man/Samba-HOWTO-Collection/samba-bdc.html .

18.6. Integration Active Directory

18.6.1. Accéder à un partage Samba

On peut aussi intégrer Samba dans un réseau Windows existant, puis, une fois qu'il fait partie du domaine Active Directory, l'utiliser pour fournir des services de fichiers et d'impressions aux utilisateurs AD.

Le plus simple pour joindre un domaine AD est d'utiliser **Likewise-open**. Pour obtenir des instructions détaillées, voir **la documentation Likewise-open** (en Anglais) : http://www.beyondtrust.com/Technical-Support/Downloads/files/pbiso/Manuals/ubuntu-active-directory.html .

Une fois partie du domaine Active Directory, entrez la commande suivante dans un terminal :

```
sudo apt install samba cifs-utils smbclient
```

Modifiez ensuite /etc/samba/smb.conf en changeant :

```
workgroup = EXEMPLE
...
security = ads
realm = EXEMPLE.COM
...
idmap backend = lwopen
idmap uid = 50-9999999999
idmap gid = 50-9999999999
```

Redémarrez **samba** pour appliquer les nouveaux paramètres :

```
sudo systemctl restart smbd.service nmbd.service
```

Vous devriez accéder maintenant à n'importe quel partage **Samba** depuis un client Windows. Assurez-vous tout de même que les utilisateurs ou groupes AD ont les autorisations nécessaires sur le partage. Se référer au *Chapitre 18, paragraphe 4. Sécurisation du serveur de fichiers et d'impression* pour de plus amples informations.

18.6.2. Accéder à un partage Windows

Maintenant que le serveur Samba fait partie du domaine Active Directory, vous pouvez accéder à n'importe quel partage Windows :

- Pour monter un partage Windows, tapez la ligne de commande :

```
mount.cifs //fs01.example.com/share mount_point
```

  Il est possible d'accéder aux partages d'ordinateurs ne faisant pas partie d'un domaine AD en fournissant un nom d'utilisateur et un mot de passe.

- Pour monter le partage au démarrage, insérez dans /etc/fstab une entrée du type :

```
//192.168.0.5/share /mnt/windows cifs auto,username=martin,password=secret,rw 0 0
```

- Se servir de l'utilitaire **smbclient** est une autre méthode pour copier des fichiers depuis un serveur Windows. Pour lister les fichiers d'un partage Windows :

```
smbclient //fs01.example.com/share -k -c "ls"
```

- Pour copier un fichier d'un partage, saisissez :

```
smbclient //fs01.example.com/share -k -c "get file.txt"
```

  Le fichier file.txt sera copié depuis le partage dans le répertoire actuel.

- Pour copier un fichier vers le partage :

```
smbclient //fs01.example.com/share -k -c "put /etc/hosts hosts"
```

  Ceci copiera le fichier /etc/hosts vers //fs01.exemple.com/share/hosts.

- L'option **-c** utilisée ci-dessus vous permet d'exécuter la commande **smbclient** en une seule fois. Ceci est utile pour des opérations mineures ainsi qu'à l'intérieur d'un script. Pour accéder à l'invite de commandes **smb: \>** (analogue à une invite de commande FTP) à partir duquel vous pouvez lancer des commandes sur les fichiers et répertoires, servez-vous de :

```
smbclient //fs01.example.com/share -k
```

Remplace toutes les instances **fs01.example.com/share**, **//192.168.0.5/share**, **username=martin,password=secret** et **file.txt** par vos propres adresses IP, nom d'hôte, nom de partage, nom de fichier ainsi que l'identifiant réel (et son mot de passe) ayant les droits sur le partage.

18.6.3. Ressources

Davantage d'options sont disponibles pour **smbclient**. Consultez le manuel : **man smbclient,** également disponible **en ligne :** http://manpages.ubuntu.com/manpages/xenial/en/man1/smbclient.1.html .

Le **manuel** de **mount.cifs** fournit des informations plus détaillées, également utiles : http://manpages.ubuntu.com/manpages/xenial/en/man8/mount.cifs.8.html .

La page **Ubuntu Wiki Samba** : https://help.ubuntu.com/community/Samba .

Chapitre 19. Sauvegardes

Il y a de nombreuses manières de sauvegarder une installation Ubuntu. La chose la plus importante à propos des sauvegardes est de développer un **plan de sauvegarde** détaillant ce qu'il faut sauvegarder, où le sauvegarder et comment le restaurer.

Les sections suivantes proposent diverses manières d'accomplir ces tâches.

19.1. Scripts shell

Une des manières les plus simples pour sauvegarder un système est l'utilisation d'un **script shell**. Par exemple, un script peut être utilisé pour configurer quels répertoires sauvegarder, et passer ces répertoires comme arguments à l'utilitaire **tar**, qui crée un fichier d'archive. Celui-ci peut ensuite être déplacé ou copié vers un autre emplacement. L'archive peut aussi être créée sur un système de fichier distant tel qu'un montage **NFS**.

L'utilitaire **tar** crée un fichier d'archive de plusieurs fichiers ou répertoires. **tar** peut également filtrer les fichiers par le biais des utilitaires de compression, réduisant ainsi la taille du fichier d'archive.

19.1.1. Script shell simple

Le script shell suivant se sert de **tar** pour créer une archive sur un montage NFS. Le nom de l'archive est défini en se servant de divers utilitaires en ligne de commande.

```
#!/bin/bash
####################################
#
# Script de sauvegarde vers NFS monté.
#
####################################

# Ce qu'il faut sauvegarder.
backup_files="/home /var/spool/mail /etc /root /boot /opt"

# Où sauvegarder.
dest="/mnt/backup"

# Créer le nom de fichier de l'archive.
day=$(date +%A)
hostname=$(hostname -s)
archive_file="$hostname-$day.tgz"

# Afficher un message de début.
echo "Backing up $backup_files to $dest/$archive_file"
date
echo

# Sauvegarde des fichiers en utilisant tar.
tar czf $dest/$archive_file $backup_files

# Afficher un message de fin.
echo
echo "Backup finished"
date

# Liste longue des fichiers dans $dest pour vérifier les tailles de fichier.
```

```
ls -lh $dest
```

- **$backup_files :** variable listant les répertoires que vous souhaitez sauvegarder. La liste doit être adaptée à vos besoins.
- **$day :** une variable contenant le jour de la semaine (lundi, mardi, mercredi, etc.) Cette fonction est utilisée pour créer un fichier d'archive pour chaque jour de la semaine, ce qui donne un historique de sauvegarde de sept jours. Il y a d'autres façons d'accomplir cela, par exemple en utilisant l'utilitaire **date**.
- **$hostname :** variable contenant le nom d'hôte de votre système en format **court**. Vous pourrez ainsi placer les archives quotidiennes de plusieurs hôtes dans un même répertoire.
- **$archive_file :** le nom complet de l'archive.
- **$dest :** destination du fichier d'archive. Le répertoire doit être créé et, dans ce cas **monté** avant d'exécuter le script de sauvegarde. Voir le *Chapitre 14, paragraphe 2. Network File System (NFS)* pour des détails sur l'utilisation de **NFS**.
- **status messages :** messages optionnels affichés dans la console lors de l'utilisation de la commande **echo**.
- **tar czf $dest/$archive_file $backup_files :** la commande **tar** utilisée pour créer le fichier d'archive.
  - **c :** crée une archive.
  - **z :** compresser l'archive avec **gzip**.
  - **f :** sortie vers un fichier d'archive. Sinon, la sortie **tar** est envoyée vers STDOUT.
- **ls -lh $dest :** instruction optionnelle affichant une liste du répertoire de destination détaillée **-l** et au format lisible par facilement **-h**. Ceci est utile pour vérifier rapidement la taille du fichier archive, mais ne devrait pas remplacer le test de celui-ci.

Voici un exemple simple de script shell de sauvegarde. Cependant, il y a beaucoup d'options qui peuvent être inclues dans un tel script. Voir le *Chapitre 19, paragraphe 1. Scripts shell.4. Références* pour avoir des liens vers des ressources fournissant des informations plus approfondies sur les scripts shell.

19.1.2. Exécution du script

19.1.2.1. Exécution à partir d'un terminal

Le moyen le plus simple d'exécuter le script ci-dessus est de copier et coller son contenu dans un fichier. backup.sh par exemple. Le fichier doit être rendu exécutable :

```
chmod u+x backup.sh
```

Ensuite, depuis l'invite d'un terminal :

```
sudo ./backup.sh
```

C'est une excellente manière de tester le script pour s'assurer que tout fonctionne comme prévu.

19.1.2.2. Exécution avec cron

L'exécution du script peut être automatisée avec l'utilitaire **cron**. Le démon **cron** permet d'exécuter des scripts ou des commandes, à une date et une heure déterminées.

cron est configuré au travers d'entrées dans un fichier crontab. Les fichiers crontab sont séparés en champs :

```
# m h dom mon dow       command
```

- **m :** minute de l'exécution de la commande, entre 0 et 59.
- **h :** heure de l'exécution de la commande, entre 0 et 23.
- **dom :** jour du mois durant lequel la commande s'exécute.
- **mon :** mois de l'exécution de la commande, entre 1 et 12.
- **dow :** le jour de la semaine ("day of week") où la commande s'exécute (entre 0 et 7). Dimanche peut être spécifié à l'aide de 0 ou 7, les deux valeurs sont valides.
- **command :** la commande à exécuter.

La commande **crontab -e** doit être utilisée pour ajouter ou modifier les entrées d'un fichier crontab. Le contenu d'un fichier crontab peut être affiché avec la commande **crontab -l**.

Afin d'exécuter le script **backup.sh** précédent en utilisant **cron**, saisissez dans une invite de terminal :

```
sudo crontab -e
```

L'utilisation de **sudo** avec la commande **crontab -e** modifie le fichier crontab de l'utilisateur **root**. Cela est nécessaire si vous sauvegardez des répertoires accessibles uniquement par l'utilisateur root.

Ajoutez l'entrée suivante au fichier crontab :

```
# m h dom mon dow       command
0 0 * * * bash /usr/local/bin/backup.sh
```

Le script **backup.sh** sera maintenant lancé tous les jours à 12h00.

Le script **backup.sh** devra être copié dans le répertoire /usr/local/bin/ pour que cette entrée s'exécute correctement. Le script peut se trouver n'importe où sur le système de fichiers, il suffira de changer le chemin d'accès du script en conséquence.

Pour des options **crontab** plus détaillées, consultez le *Chapitre 19, paragraphe 1. Scripts shell.4. Références*.

19.1.3. Restauration à partir d'une archive

Il est important de vérifier une archive après sa création. Une archive peut être testée en listant les fichiers qu'elle contient, mais le mieux est de **restaurer** un fichier depuis cette archive.

- Pour voir une liste du contenu de l'archive. Saisissez à partir d'un terminal :

```
tar -tzvf /mnt/backup/host-Monday.tgz
```

- Pour restaurer un fichier à partir de l'archive dans un répertoire différent, tapez :

```
tar -xzvf /mnt/backup/host-Monday.tgz -C /tmp etc/hosts
```

- L'option **-C** pour **tar** redirige les fichiers extraits vers le répertoire spécifié. L'exemple ci-dessus va extraire le fichier /etc/hosts vers /tmp/etc/hosts. **tar** recrée l'arborescence des dossiers qu'il contient.

  Notez également que le premier **« / »** est enlevé du chemin du fichier à restaurer.

- Pour restaurer tous les fichiers de l'archive saisissez ceci :

```
cd /
sudo tar -xzvf /mnt/backup/host-Monday.tgz
```

C ela écrasera les fichiers actuellement sur le système de fichiers.

19.1.4. Références

Voir **Advanced Bash-Scripting Guide** pour de plus amples informations à propos de l'écriture de scripts shell : http://tldp.org/LDP/abs/html/ .

Le livre **Teach Yourself Shell Programming in 24 Hours** est disponible en ligne et est une mine d'or pour l'écriture de scripts shell : http://safari.samspublishing.com/0672323583 .

La **Page Wiki CronHowto** contient des détails sur l'utilisation des options avancées de **cron** : https://help.ubuntu.com/community/CronHowto .

Voir le **Manuel GNU tar** pour plus d'informations concernant les options de **tar** : http://www.gnu.org/software/tar/manual/index.html .

L'article anglais de Wikipédia **Backup Rotation Scheme** contient des informations à propos d'autres méthodes de sauvegarde : http://en.wikipedia.org/wiki/Backup_rotation_scheme .

Le script shell utilise la commande **tar** pour la création de l'archive, mais il existe bien d'autres utilitaires en ligne de commande qui peuvent être utilisés. Par exemple :

- **cpio** : pour copier des fichiers depuis et vers des archives : http://www.gnu.org/software/cpio/ .
- **dd** : fait partie du paquet **coreutils**. Un utilitaire de bas niveau qui peut copier les données d'un format à un autre : http://www.gnu.org/software/coreutils/ .
- **rsnapshot**: un utilitaire de capture instantanée du système de fichiers utilisé pour créer des copies d'un système de fichiers : http://www.rsnapshot.org/ .
- **rsync**: un utilitaire flexible utilisé pour créer des copies incrémentielles des fichiers : http://www.samba.org/ftp/rsync/rsync.html .

19.2. Rotation des archives

Le script shell dans le *Chapitre 19, paragraphe 1. Scripts shell* permet seulement sept archives différentes. Pour un serveur dont les données ne changent pas souvent, cela peut suffire. Si le serveur dispose d'une grande quantité de données, un système de rotation plus complexe doit être utilisé.

19.2.1. Rotation des archives NFS

Dans cette section, le script shell sera légèrement modifié pour mettre en œuvre un système de rotation grand-parent - parent - enfant (mensuel, hebdomadaire, quotidien) :

- La rotation va effectuer une sauvegarde **journalière** du dimanche au vendredi.
- Le samedi une sauvegarde **hebdomadaire** est effectuée donnant 4 sauvegardes hebdomadaires par mois.
- La sauvegarde **mensuelle** est effectuée le premier du mois avec une rotation bimensuelle en fonction de la parité du mois.

Voici le nouveau script :

```
#!/bin/bash
###################################
#
# Sauvegarde vers un point de montage NFS en utilisant
# une rotation grand-parent - parent - enfant
#
###################################

# Ce qu'il faut sauvegarder
backup_files="/home /var/spool/mail /etc /root /boot /opt"

# Où le sauvegarder
dest="/mnt/backup"

# Initialisation des variables utilisées dans le nom de l'archive
day=$(date +%A)
hostname=$(hostname -s)

# Déterminer le numéro de semaine (1-4) du mois en cours
day_num=$(date +%d)
if (( $day_num <= 7 )); then
        week_file="$hostname-week1.tgz"
elif (( $day_num > 7 &amp;&amp; $day_num <= 14 )); then
        week_file="$hostname-week2.tgz"
elif (( $day_num > 14 &amp;&amp; $day_num <= 21 )); then
        week_file="$hostname-week3.tgz"
elif (( $day_num > 21 &amp;&amp; $day_num < 32 )); then
        week_file="$hostname-week4.tgz"
```

```
fi

# Déterminer si le mois est pair ou impair
month_num=$(date +%m)
month=$(expr $month_num % 2)
if [ $month -eq 0 ]; then
        month_file="$hostname-month2.tgz"
else
        month_file="$hostname-month1.tgz"
fi

# Création du nom de l'archive
if [ $day_num == 1 ]; then
archive_file=$month_file
elif [ $day != "Saturday" ]; then
        archive_file="$hostname-$day.tgz"
else
archive_file=$week_file
fi

# Affichage du commencement des opérations
echo "Sauvegarde de $backup_files vers $dest/$archive_file"
date
echo

# Sauvegarde des fichiers à l'aide de tar.
tar czf $dest/$archive_file $backup_files

# Affichage de la fin des opérations
echo
echo "Sauvegarde terminée"
date

# Listing détaillé des fichiers de $dest pour vérifier leur poids
ls -lh $dest/
```

Le script peut être exécuté en utilisant les mêmes méthodes que dans le *Chapitre 19, paragraphe 1. Scripts shell.2. Exécution du script*.

Il est conseillé de prendre des supports de sauvegarde hors site en cas de catastrophe. Dans l'exemple de ce script shell le support de sauvegarde est un autre serveur fournissant un partage NFS. Selon toute vraisemblance, prendre le serveur NFS vers un autre emplacement ne serait pas pratique. Selon les vitesses de connexion, une option possible est de copier le fichier d'archive via une liaison WAN à un serveur à un autre endroit.

Une autre option est de copier le fichier d'archive vers un disque dur externe qui peut ensuite être retiré du site. Comme le prix des disques durs externes continue de diminuer, il peut être rentable d'utiliser deux lecteurs pour chaque niveau d'archive. Cela vous permettra d'avoir un disque dur externe connecté au serveur de sauvegarde et un dans un autre emplacement.

19.2.2. Lecteurs de bande

Un lecteur de bande connecté au serveur peut être utilisé au lieu d'un partage NFS. L'utilisation d'un lecteur

de bande simplifie la rotation des archives, et permet également de prendre les médias hors du site plus facilement.

Lors de l'utilisation d'un lecteur de bandes, les parties de nom de fichier du script ne sont pas nécessaires parce que les données sont envoyées directement au périphérique à bande. Certaines commandes de manipulation de la bande sont nécessaires. Ceci est accompli en utilisant **mt**, un utilitaire de contrôle de bandes magnétiques faisant parti du paquet **cpio**.

Voici le script shell modifié pour l'utilisation d'un lecteur de bande :

```
#!/bin/bash
###################################
#
# Sauvegarde vers une cassette
#
###################################

# Ce qu'il faut sauvegarder
backup_files="/home /var/spool/mail /etc /root /boot /opt"

# Où le sauvegarder
dest="/dev/st0"

# Affichage du commencement des opérations
echo "Backing up $backup_files to $dest"
date
echo

# S'assurer que la cassette est rembobinée
mt -f $dest rewind

# Sauvegarde à l'aide de tar.
tar czf $dest $backup_files

# Rembobinage et ejection de la cassette
mt -f $dest rewoffl

# Affichage de la fin des opérations
echo
echo "Sauvegarde terminée"
Date
```

> Le nom de périphérique par défaut pour un lecteur de bandes SCSI est /dev/st0. Employez le chemin correspondant à votre système.

La restauration à partir d'un lecteur de bandes est essentiellement équivalente à la restauration à partir d'un fichier. Il suffit de rembobiner la bande et remplacer le chemin du fichier par celui du périphérique. Par exemple, pour restaurer le fichier /etc/hosts vers /tmp/etc/hosts :

```
mt -f /dev/st0 rewind
tar -xzf /dev/st0 -C /tmp etc/hosts
```

19.3. Bacula

Bacula est un programme de sauvegarde qui vous permet de sauvegarder, restaurer et vérifier les données de votre réseau. Il existe des clients Bacula pour Linux, Windows et Mac OS X - ce qui en fait une solution multi-plate-forme à l'échelle de votre réseau.

19.3.1. Vue d'ensemble

Bacula est constitué de plusieurs composants et services utilisés pour gérer les fichiers à sauvegarder et les emplacements de sauvegarde :

- **Bacula Director :** service contrôlant les opérations de sauvegarde, de restauration, de vérification et d'archivage.
- **Bacula Console :** application permettant de communiquer avec Bacula Director. Il existe trois versions de la Console :
  - Version en mode texte via ligne de commande.
  - Version graphique GTK+ (Gnome).
  - Version graphique wxWidgets.
- **Bacula File :** connu aussi sous le nom **Bacula Client**. Cette application est installée sur les machines à sauvegarder et se charge d'envoyer les données demandées par Bacula Director.
- **Bacula Storage :** programmes effectuant le stockage et la récupération des données sur le support physique.
- **Bacula Catalog :** responsable de la mise à jour des index de fichiers et des bases de données de volumes pour tous les fichiers sauvegardés, permettant ainsi la localisation et la restauration rapide des fichiers archivés. Bacula Catalog prend en charge trois types de bases de données : MySQL, PostgreSQL et SQLite.
- **Bacula Monitor :** permet le contrôle de Director et des démons File et Storage. Actuellement, Monitor est uniquement disponible avec une interface GTK+.

Ces services et applications peuvent être lancées sur de multiples serveurs et clients, ou ils peuvent être installés sur une machine, dans le cas de la sauvegarde d'un seul disque ou volume.

19.3.2. Installation

> Si vous utilisez MySQL ou PostgreSQL comme base de données, vous devriez déjà avoir les services disponibles. **Bacula** ne les installera pas pour vous.

Il existe plusieurs paquets contenant les différents composants de **Bacula**. Pour installer Bacula, saisissez dans un terminal :

```
sudo apt install bacula
```

L'installation par défaut du paquet **bacula** va utiliser une base de données **MySQL** pour le catalogue. Si

vous voulez utiliser SQLite ou PostgreSQL pour le catalogue, installez respectivement **bacula-director-sqlite3** ou **bacula-director-pgsql**.

Pendant le processus d'installation, il vous sera demandé de fournir des informations d'authentification pour **l'administrateur** de la base de données et le **propriétaire** de la base de données **bacula**. L'administrateur de la base de données devra avoir les droits adéquats pour créer une base de données, consultez le *Chapitre 12, paragraphe 1. MySQL* pour plus d'informations.

19.3.3. Configuration

Les fichiers de configuration de **Bacula** sont constitués de **ressources** comprenant des **directives** entre accolades "{}". Chaque composant Bacula possède un fichier individuel dans le répertoire /etc/bacula.

Les divers composant de **Bacula** doivent s'autoriser mutuellement. Ceci est effectué par la directive **password**. Par exemple, le mot de passe de la ressource **Storage** dans le fichier /etc/bacula/bacula-dir.conf doit correspondre à celui de la ressource **Director** dans le fichier /etc/bacula/bacula-sd.conf.

Par défaut, la tâche de sauvegarde appelée **Client1** est configurée pour archiver le catalogue **Bacula**. Si vous envisagez d'utiliser le serveur pour sauvegarder plus d'un client, vous devriez changer le nom de cette tâche pour quelque chose de plus descriptif. Pour changer ce nom, modifiez le fichier /etc/bacula/bacula-dir.conf :

```
#
# Definition des principales tâches nocturnes de sauvegardes
# Par défaut, cette tâche sauvegardera sur le disque dans
Job {
  Name = "BackupServer"
  JobDefs = "DefaultJob"
  Write Bootstrap = "/var/lib/bacula/Client1.bsr"
}
```

L'exemple ci-dessus remplace le nom de la tâche par **BackupServer**, correspondant au nom d'hôte de la machine. Remplacez "BackupServer" avec votre nom d'hôte adéquat, ou un autre nom descriptif.

La **Console** peut être utilisée pour interroger le **Director** sur des tâches, mais pour utiliser la Console avec un utilisateur **non root**, celui-ci doit être dans le groupe **bacula**. Pour ajouter un utilisateur au groupe bacula, saisissez la commande suivante dans un terminal :

```
sudo adduser $username bacula
```

Remplacez **$username** par le véritable nom d'utilisateur. De plus, si vous ajoutez l'utilisateur courant au groupe, vous devrez vous déconnecter puis vous reconnecter pour que les nouvelles autorisations prennent effet.

19.3.4. Sauvegarde de l'hôte local

Cette section décrit la façon de sauvegarder les répertoires spécifiés pour un unique hôte sur un lecteur de bande local.

- Tout d'abord, le périphérique de **stockage** doit être configuré. Ajoutez, dans le fichier /etc/bacula/bacula-sd.conf :

```
Device {
  Name = "Tape Drive"
  Device Type = tape
  Media Type = DDS-4
  Archive Device = /dev/st0
  Hardware end of medium = No;
  AutomaticMount = yes; # when device opened, read it
  AlwaysOpen = Yes;
  RemovableMedia = yes;
  RandomAccess = no;
  Alert Command = "sh -c 'tapeinfo -f %c | grep TapeAlert'"
}
```

Cet exemple est pour un lecteur de bande **DDS-4**. Réglez le "Type de Média" et " Périphérique d'archivage" pour correspondre à votre matériel.

Vous pouvez également dé-commenter l'un des autres exemples du fichier.

- Après avoir modifié /etc/bacula/bacula-sd.conf, le démon **Storage** devra être redémarré :

```
sudo systemctl restart bacula-sd.service
```

- Ajoutez maintenant une ressource **Storage** dans /etc/bacula/bacula-dir.conf pour utiliser le nouveau périphérique :

```
# Définition de"Tape Drive" périphérique de stockage
Storage {
om de n = TapeDrive
# Ne pas utiliser"localhost" ici
= Adresse backupserver             # NB Utilisez un nom qualifié complet ici
SDPort = 9103
Mot de passe ="Cv70F6pf1t6pBopT4vQOnigDrR0v3LT3Cgkiyjc"
Device n ="Tape Drive"
Type de support = tape
}
```

La directive **Address** doit être le nom de domaine entièrement qualifié (FQDN) du serveur. Remplacez **backupserver** par le véritable nom d'hôte.

Assurez-vous également que la directive **Password** corresponde à celle dans /etc/bacula/bacula-sd.conf.

- Créez une nouvelle ressource **FileSet** (jeu de fichiers) qui définira les répertoires à sauvegarder, en ajoutant :

```
# LocalhostBacup FileSet.
FileSet {
  Name = "LocalhostFiles"
  Include {
    Options {
      signature = MD5
      compression=GZIP
    }
    File = /etc
    File = /home
```

```
  }
}
```

Ce **FileSet** permet de sauvegarder les répertoires /etc et /home. Les directives de ressource **options** configurent le FileSet pour créer une signature MD5 pour chaque fichier sauvegardé, et pour compresser les fichiers en utilisant GZIP.

- Ensuite, créez une nouvelle ressource **Schedule** (planification) pour la tâche de sauvegarde :

```
# Planification de la sauvegarde de l'hôte local -- quotidienne.
Schedule {
  Name = "LocalhostDaily"
  Run = Full daily at 00:01
}
```

La tâche sera lancée chaque jour à 00 h 01. Il y a bien d'autres possibilités de planification.

- Pour terminer, créez la **tâche** :

```
# sauvegarde de l'hôte local.
Job {
  Name = "LocalhostBackup"
  JobDefs = "DefaultJob"
  Enabled = yes
  Level = Full
  FileSet = "LocalhostFiles"
  Schedule = "LocalhostDaily"
  Storage = TapeDrive
  Write Bootstrap = "/var/lib/bacula/LocalhostBackup.bsr"
}
```

La tâche effectuera une sauvegarde **complète** (« Full ») et quotidienne sur bande.

- Chaque bande utilisée devra posséder un **label**. Si la bande courante n'en possède pas, **Bacula** vous enverra un courriel vous en informant. Pour donner un label à une bande en utilisant la **Console**, saisissez la commande suivante dans un terminal :

```
bconsole
```

- À l'invite de commande de la console de Bacula saisissez :

```
label
```

- Il vous sera alors demandé de choisir la ressource de **stockage** (« storage ») :

```
Automatically selected Catalog: MyCatalog
Using Catalog "MyCatalog"
The defined Storage resources are:
     1: File
     2: TapeDrive
Select Storage resource (1-2):
```

- Saisissez le nouveau nom du **volume** :

```
Enter new Volume name: dimanche
```

```
Defined Pools:
     1: Default
     2: Scratch
```

Remplacez **dimanche** par l'étiquette désirée.

- Sélectionnez maintenant le **pool**:

```
Select the Pool (1-2):
Connecting to Storage daemon TapeDrive at backupserver:9103 ...
Sending label command for Volume "Sunday" Slot 0 …
```

Félicitations, vous venez de configurer **Bacula** pour sauvegarder l'hôte local vers un lecteur de bande connecté.

19.3.5. Ressources

Pour plus d'options de configuration de **Bacula**, consultez **la documentation de Bacula** : http://blog.bacula.org/documentation/documentation/ .

La **page d'accueil de Bacula** contient les dernières informations et versions de développement : http://www.bacula.org/ .

Référez-vous également à la page **du wiki anglophone d'Ubuntu sur Bacula :** https://help.ubuntu.com/community/Bacula .

Chapitre 20. Virtualisation

La virtualisation est adoptée dans plusieurs environnements et situations différents. Si vous êtes développeur, la virtualisation peut vous procurer un environnement confiné (dans une machine virtuelle) où vous pouvez effectuer à peu près n'importe quel type de développement sans abandonner votre environnement de travail principal. Si vous êtes administrateur système, vous pouvez utiliser la virtualisation pour isoler plus facilement vos services les uns des autres et les déplacer en fonction de la demande.

La technologie de virtualisation prise en charge par défaut dans Ubuntu est KVM. KVM nécessite des extensions de virtualisation intégrées aux processeurs Intel et AMD. Xen est aussi pris en charge par Ubuntu. Xen peut tirer profit des extensions de virtualisation, quand elles sont disponibles, mais peut aussi être utilisé sur des matériels sans extensions de virtualisation. Qemu est une autre solution populaire tournant sur des matériels sans extensions de virtualisation.

20.1. libvirt

La bibliothèque libvirt est utilisée pour s'interfacer avec différentes technologies de virtualisation. Avant de commencer avec libvirt, il est judicieux de s'assurer que votre matériel **prend en charge** les extensions de virtualisation pour KVM. Saisissez la commande suivante dans un terminal :

```
kvm-ok
```

Un message vous informera si votre processeur **prend en charge** ou **non** la virtualisation matérielle.

Sur beaucoup d'ordinateurs équipés de microprocesseurs prenant en charge la virtualisation matérielle assistée, il est nécessaire d'activer une option dans le BIOS afin de pouvoir l'utiliser.

20.1.1. Virtualisation du réseau

Il existe quelques façons différentes pour permettre un accès à la machine virtuelle sur le réseau externe. La configuration de réseau virtuel par défaut inclut **combler** et **iptables** les modalités d'application **usermode** en réseau, qui utilise le protocole SLIRP. Le trafic est NATed via l'interface hôte pour le réseau extérieur.

Pour permettre aux hôtes externes d'accéder directement aux services sur les machines virtuelles, un **pont** différent de celui par défaut doit être configuré. Ceci permet aux interfaces virtuelles de se connecter au réseau externe par l'intermédiaire de l'interface physique, leur permettant de paraître comme des hôtes traditionnels aux yeux du reste du réseau.

20.1.2. Installation

Pour installer les paquets nécessaires, saisissez dans un terminal :

```
sudo apt install qemu-kvm libvirt-bin
```

Après l'installation de libvirt-bin, l'utilisateur qui doit gérer les machines virtuelles devra être ajouté au groupe **libvirtd**. Ceci lui donnera les droits d'accès aux options avancés de configuration réseau.

Dans un terminal saisissez :

```
sudo adduser $USER libvirtd
```

Si vous avez choisi l'utilisateur courant, vous devrez vous déconnecter, puis vous reconnecter pour que l'appartenance au nouveau groupe soit prise en compte.

Dans les versions plus récentes (>= Yakkety), le groupe a été renommé **libvirt**. Les systèmes mis à jour obtiennent un nouveau groupe **libvirt** avec le même gid que le groupe **libvirtd** pour que cela corresponde.

Vous êtes maintenant prêt à installer un système d'exploitation **Invité**. L'installation d'une machine virtuelle suit le même processus que l'installation d'un système d'exploitation directement sur le matériel. Vous avez

besoin d'un moyen pour automatiser l'installation ou bien un clavier ainsi qu'un moniteur devront être rattachés à la machine physique.

Dans le cas des machines virtuelles une interface graphique (GUI) est analogue à l'utilisation d'un clavier physique et de la souris. Au lieu d'installer une interface graphique, virt-viewer peut être utilisé pour se connecter à la console d'une machine virtuelle grâce à VNC. Consultez le *Chapitre 20, paragraphe 1. libvirt .6. Afficheur de machine virtuelle* pour plus d'informations.

Il existe plusieurs façons d'automatiser le processus d'installation Ubuntu, par exemple en utilisant preseeds, kickstart, etc. Reportez-vous au Guide d'Installation Ubuntu pour plus de détails : https://help.ubuntu.com/16.04/installation-guide/

Encore un autre moyen d'installer une machine virtuelle Ubuntu est d'utiliser uvtool. Cette application, disponible depuis 14.04, vous permet de paramétrer des options spécifiques à VM, exécuter des scripts personnalisés post-installation, etc. Référez-vous au *Chapitre 20, paragraphe 3. Images cloud et uvtool* pour plus de détails.

Libvirt peut également être configuré avec Xen. Pour plus de détails, voir la page de la communauté Xen Ubuntu référencée ci-dessous.

20.1.3. virt-install

virt-install fait partie du paquet virtinst. Pour l'installer, saisissez dans un terminal :

```
sudo apt install virtinst
```

Il y a plusieurs options disponibles pour utiliser virt-install. Par exemple :

```
sudo virt-install -n web_devel -r 256 \
--disk path=/var/lib/libvirt/images/web_devel.img,bus=virtio,size=4 -c \
 ubuntu-16.04-server-i386.iso --network network=default,model=virtio \
--graphics vnc,Listen=0.0.0.0 --noautoconsole -v
```

- **-n Web_devel :** le nom de la machine virtuelle sera Web_devel dans cet exemple.
- **-r 256 :** spécifie la quantité de mémoire qu'utilisera la machine virtuelle en mégaoctets.
- **--chemin du disque=/var/lib/libvirt/images/web_devel.img,size=4 :** montre le chemin d'accès au disque virtuel qui peut être un fichier, une partition ou un volume logique. Dans cet exemple, un fichier nommé web_devel.img dans le répertoire /var/lib/libvirt/images/, avec une taille de 4 gigaoctets, et utilisant **virtio** pour le bus disque.
- **-c ubuntu-16.04-server-i386.iso :** fichier à utiliser en tant que CDROM virtuel. Le fichier peut soit être un fichier ISO ou le chemin vers le dispositif CDROM de l'hôte.
- **--network :** fournit des détails liés à l'interface réseau de la machine virtuelle. Ici le réseau par **défaut** est utilisé, et le modèle d'interface est configuré pour **virtio**.
- **--graphics vnc,Listen=0.0.0.0 :** exporte la console virtuelle du client en utilisant VNC et sur toutes les interfaces hôte. Habituellement, les serveurs n'ont pas d'interface graphique, alors, un autre ordinateur muni d'une IG sur le réseau local (LAN) peut se connecter avec VNC pour terminer l'installation.
- **--noautoconsole :** ne se connectera pas automatiquement à la console de la machine virtuelle.
- **-v :** crée un invité totalement virtualisé.

Après avoir lancé virt-install vous pouvez vous connecter à la console de la machine virtuelle soit en utilisant une interface graphique (si votre serveur en possède une), ou par un client VNC distant à partir d'un ordinateur possédant une interface graphique.

20.1.4. virt-clone

L'application virt-clone peut être utilisée pour copier une machine virtuelle vers une autre. Par exemple :

```
sudo virt-clone -o web_devel -n database_devel -f \
/path/to/database_devel.img
```

- **-o** : original virtual machine.
- **-n** : nom de la nouvelle machine virtuelle.
- **-f** : chemin du fichier, volume logique ou partition utilisé par la nouvelle machine virtuelle.

Vous pouvez également utiliser l'option **-d** ou **--debug** pour vous aider à résoudre les problèmes avec virt-clone.

R emplacez **Web_devel** et **database_devel** par les noms appropriés des machines virtuelles.

20.1.5. Gestion des machines virtuelles

20.1.5.1. virsh

Il existe plusieurs utilitaires disponibles pour gérer les machines virtuelles et libvirt. L'application virsh s'utilise en ligne de commande. Quelques exemples :

- Pour lister les machines virtuelles en cours d'exécution :

```
virsh list
```

- Pour démarrer une machine virtuelle :

```
virsh start web_devel
```

- De la même façon, pour lancer une machine virtuelle au démarrage :

```
virsh autostart web_devel
```

- Redémarrez une machine virtuelle avec :

```
virsh reboot web_devel
```

- L'**état** des machine virtuelles peut être enregistré dans un fichier pour pouvoir être restauré plus tard. Ce qui suit enregistrera l'état d'une machine virtuelle dans un fichier nommé d'après la date :

```
virsh save web_devel web_devel-022708.state
```

Une fois son état enregistré, une machine virtuelle ne sera plus en cours d'exécution.

- Une machine virtuelle dont l'état est enregistré peut être restaurée en utilisant :

```
virsh restore web_devel-022708.state
```

- Pour arrêter une machine virtuelle :

```
virsh shutdown web_devel
```

- Un CDROM peut être monté dans une machine virtuelle en saisissant :

```
virsh attach-disk web_devel /dev/cdrom /media/cdrom
```

Dans les exemples ci-dessus, remplacez **Web_devel** par le nom approprié pour la machine virtuelle, et Web_devel-022708.state par un nom de fichier explicite.

Si virsh (ou un autres outil vir*) doit se connecter à quelque chose d'autre que l'hyperviseur par défaut qemu-kvm/system, des alternatives à l'option **connect** sont disponibles dans **man virsh** ou dans la documentation de libvirt : http://libvirt.org/uri.html

20.1.5.2. Migration

Il y a plusieurs types de migration disponibles selon la version de libvirt et l'hyperviseur utilisés. En général, ces types sont :

- migration hors ligne : https://libvirt.org/migration.html#offline
- migration pendant l'exécution : https://libvirt.org/migration.html
- migration dès que possible (postcopy) : http://wiki.qemu.org/Features/PostCopyLiveMigration

Plusieurs options sont disponibles pour chacune de ces méthodes mais leur point d'entrée commun est **virsh migrate**. Consultez l'aide intégrée pour plus de détails.

```
virsh migrate --help
```

Vous trouverez des informations utiles sur les contraintes et éléments à considérer à propos la migration pendant l'exécution dans le wiki d'Ubuntu : https://wiki.ubuntu.com/QemuKVMMigration

20.1.5.3. Gestionnaire de machine virtuelle

Le paquet virt-manager contient un outil en mode graphique pour gérer les machines virtuelles locales et distantes. Pour installer virt-manager saisissez :

```
sudo apt install virt-manager
```

Étant donné que virt-manager exige un environnement contenant une interface graphique (GUI), il est

recommandé de l'installer sur un poste de travail ou une machine de test mais pas sur un serveur de production. Pour vous connecter au service locallibvirt tapez :

```
virt-manager -c qemu:///system
```

Vous pouvez vous connecter au service libvirt s'exécutant sur un autre hôte en saisissant ce qui suit dans un terminal :

```
virt-manager -c qemu+ssh://virtnode1.mydomain.com/system
```

L'exemple ci-dessus suppose que la connectivité SSH entre le système de gestion et virtnode1.mydomain.com a déjà été configurée, et utilise les clés SSH pour l'authentification. **Les clés** SSH sont nécessaires car libvirt envoie le mot de passe à un autre processus. Pour plus de renseignements sur la configuration de SSH, consultez le *Chapitre 6, paragraphe 1. Serveur OpenSSH*.

20.1.6. Afficheur de machine virtuelle

L'application virt-viewer vous permet de vous connecter à une console de la machine virtuelle. virt-viewer nécessite une interface graphique utilisateur (GUI) pour interagir avec la machine virtuelle.

Pour installer virt-viewer, depuis un terminal saisissez :

```
sudo apt install virt-viewer
```

Une fois qu'une machine virtuelle est installée et est en exécution vous pouvez vous connectez à la console de la machine virtuelle en utilisant :

```
virt-viewer web_devel
```

De même que virt-manager, virt-viewer peut se connecter à un hôte distant en utilisant **SSH** avec authentification par clé, comme ceci :

```
virt-viewer -c qemu+ssh://virtnode1.mydomain.com/system web_devel
```

Assurez-vous de remplacer **web_devel** par le nom de la machine virtuelle approprié.

Si configuré pour utiliser une interface réseau **pontée**, vous pouvez également configurer l'accès par SSH à la machine virtuelle.

20.1.7. Ressources

- Voir la **page d'accueil de KVM** pour plus de détails : http://www.linux-kvm.org/ .
- Pour plus d'informations sur libvirt voir l**a page d'accueil libvirt** : http://libvirt.org/ .
- Le site **Virtual Machine Manager** a plus d'informations sur le développement de virt-manager : http://virt-manager.org/ .
- Également, allez vous poser sur le canal IRC **#ubuntu-virt** sur **freenode** pour discuter de la technologie de virtualisation dans Ubuntu : http://freenode.net/

- Une autre source d'information est **la page du Wiki Ubuntu** consacrée à **KVM** : https://help.ubuntu.com/community/KVM .
- Pour plus d'informations sur Xen, y compris l'utilisation Xen avec libvirt, veuillez voir **la page du Wiki Ubuntu sur Xen** : https://help.ubuntu.com/community/Xen .

20.2. Qemu

Qemu est un émulateur de machine qui exécute des systèmes d'exploitation et des programmes pour une machine sur une autre machine. La plupart du temps il n'est pas utilisé comme un émulateur mais comme un virtualisateur, en collaboration avec les composants du noyau KVM ou XEN. Dans ce cas, il utilise la technologie de virtualisation du matériel pour virtualiser les hôtes. Voir : http://wiki.qemu.org/ .

Qemu dispose d'une interface en lignes de commandes : http://wiki.qemu.org/download/qemu-doc.html#sec_005finvocation et d'un moniteur http://wiki.qemu.org/download/qemu-doc.html#pcsys_005fmonitor pour interagir avec les hôtes en cours d'exécution, mais ceux-ci sont rarement utilisés ainsi, si ce n'est à des fins de développement. Libvirt permet de s'abstraire des versions et des hyperviseurs spécifiques, et comporte des solutions et des bonnes pratiques.

20.2.1. Mise à jour du type de machine

Cet aspect est également documenté, avec des contraintes et des éléments à considérer, dans le wiki d'Ubuntu : https://wiki.ubuntu.com/QemuKVMMigration#Upgrade_machine_type

Vous voudrez peut-être mettre à jour le type de votre machine d'un hôte défini et existant pour :

- récupérer les dernières corrections et fonctionnalités de sécurité
- continuer d'utiliser un hôte créé avec une version à présent non supportée

Il est généralement recommandé de mettre à jour les types de machines lors d'une mise à jour majeure de qemu/kvm. Mais cette tâche ne peut vraisemblablement jamais être automatisée car elle est visible par les hôtes. Les périphériques hôtes pourraient changer d'apparence, les nouveaux éléments seront annoncés à l'hôte, et ainsi de suite. Linux tolère généralement bien de tels changements mais cela dépend tellement de la configuration et de la charge de travail de l'hôte que cela doit être évalué par le propriétaire ou l'administrateur du système. D'autres systèmes d'exploitation sont connus pour être souvent sévèrement affectés par un changement de matériel. Considérez qu'un changement de type de machine est similaire à remplacer tous les périphériques et microprogrammes d'une machine physique par leur plus récente version : toutes les considérations qui s'appliquent à ce cas de figure s'appliquent également lorsqu'on envisage une mise à jour le type de machine.

Comme il est d'usage pour tout changement majeur de configuration, il est sage de sauvegarder votre définition de l'hôte et l'état du disque, afin d'être en mesure de revenir en arrière, si besoin. Il n'y a pas de commande intégrée pour mettre à jour le type de machine, ni via virsh, ni via d'autre outils similaires. C'est un élément normal de votre définition de machine. Pour cette raison, il se met à jour de la même manière que la plupart des autres éléments de définition de machine.

Tout d'abord, éteignez votre machine et attendez qu'elle soit effectivement éteinte.

```
virsh shutdown <votremachine>
# attendez
virsh list --inactive
# votre machine devrait maintenant être indiquée comme "shut off"
```

Éditez ensuite la définition de la machine et trouvez, dans l'indicateur de type, le type de machine qui correspond à l'attribut de la machine.

```
virsh edit <votremachine>
```

```
<type arch='x86_64' machine='pc-i440fx-xenial'>hvm</type>
```

Changez ceci pour le type que vous voulez. Si vous avez besoin de chercher quels types sont disponibles via « -M ? », notez que bien que les types génériques sont proposés par commodité, seul les types Ubuntu sont supportés. Ici, vous pouvez voir également quelle devrait être la valeur par défaut courante. En général, il est fortement recommandé que vous changiez les types les plus récents s'il est possible d'exploiter les fonctionnalités les plus récentes, mais aussi pour bénéficier des corrections de bogues qui ne s'appliquent qu'aux virtualisations des périphériques les plus récents.

```
kvm -M ?
# liste les types de machine, par exemple
pc-i440fx-xenial       Ubuntu 16.04 PC (i440FX + PIIX, 1996) (default)
…
```

Après cela, vous pouvez redémarrer votre hôte. Vous pouvez vérifier le type de machine en cours d'exécution depuis l'invité ou depuis l'hôte selon vos besoin.

```
virsh start <votremachine>
# vérifier depuis l'hôte, en déchargeant la définition xml active
virsh dumpxml <votremachine> | xmllint --xpath "string(//domaine/os/type/@machine)" -
# ou depuis l'invité, via dmidecode
sudo dmidecode | grep Produit -A 1
       Product Name: Standard PC (i440FX + PIIX, 1996)
       Version: pc-i440fx-xenial
```

Si vous gardez certaines définitions inactives comme les définitions xml, n'oubliez pas de les mettre à jour également.

20.3. Images cloud et uvtool

20.3.1. Introduction

Ubuntu étant un des systèmes d'exploitation les plus utilisés sur de nombreuses plate-formes de cloud, la disponibilité d'images cloud stables et sûres est devenue très importante. Depuis 12.04, l'utilisation d'images cloud en dehors d'une infrastructure cloud a été améliorée. Il est désormais possible d'utiliser ces images pour créer une machine virtuelle ne nécessitant pas une installation complète.

20.3.2. Création de machines virtuelles utilisant uvtool

A partir de la version 14.04 LTS d'Ubuntu, un outil nommé **uvtool** facilite grandement la génération de machines virtuelles (VM) en utilisant les images cloud. **Uvtool** propose un mécanisme simple pour synchroniser des images cloud localement et pour les utiliser pour créer de nouvelles VM en quelques minutes.

20.3.2.1. Paquets Uvtool

Les paquets suivants et leurs dépendances sont nécessaires à l'utilisation d'uvtool :

- uvtool
- uvtool-libvirt

Pour installer **uvtool**, exécutez :

```
$ apt -y install uvtool
```

Ceci installera les commandes principales de uvtool :

- uvt-simplestreams-libvirt
- uvt-kvm

20.3.2.2. Obtenez l'image cloud Ubuntu avec UVT-simplestreams-libvirt

Ceci est l'une des principales simplifications que **uvtool** apporte. Il sait où trouver les images cloud et de ce fait, une seule commande est nécessaire pour en obtenir une nouvelle. Par exemple, si vous vouliez synchroniser toutes les images cloud pour l'architecture amd64, la commande uvtool serait :

```
$ uvt-simplestreams-libvirt sync arch=amd64
```

Après un moment nécessaire au téléchargement de toutes les images depuis internet, vous obtiendrez un jeu complet d'images cloud stockées localement. Pour visualiser ce qui a été téléchargé, utilisez la commande suivante :

```
$ uvt-simplestreams-libvirt query
release=oneiric arch=amd64 label=release (20130509)
release=precise arch=amd64 label=release (20160315)
```

```
release=quantal arch=amd64 label=release (20140409)
release=raring arch=amd64 label=release (20140111)
release=saucy arch=amd64 label=release (20140709)
release=trusty arch=amd64 label=release (20160314)
release=utopic arch=amd64 label=release (20150723)
release=vivid arch=amd64 label=release (20160203)
release=wily arch=amd64 label=release (20160315)
release=xenial arch=amd64 label=beta1 (20160223.1)
```

Dans le cas où vous voulez synchroniser une image cloud spécifique, vous devez utiliser les filtres release= et arch= pour identifier quelle image doit être synchronisée.

```
$ uvt-simplestreams-libvirt sync release=xenial arch=amd64
```

20.3.2.3. Créez la machine virtuelle à l'aide de uvt-kvm

De manière à vous connecter à la machine virtuelle une fois qu'elle a été créée, vous devez posséder une clé SSH valide disponible pour l'utilisateur d'Ubuntu. Si votre environnement ne dispose pas d'une clé SSH, vous pouvez aisément en créer une en utilisant la commande suivante :

```
$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/ubuntu/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/ubuntu/.ssh/id_rsa.
Your public key has been saved in /home/ubuntu/.ssh/id_rsa.pub.
The key fingerprint is:
4d:ba:5d:57:c9:49:ef:b5:ab:71:14:56:6e:2b:ad:9b ubuntu@xenialS
The key's randomart image is:
+--[ RSA 2048]----+
|               ..|
|              o.=|
|          .    **|
|         +    o+=|
|        S . ...=.|
|         o . .+ .|
|        . .  o o |
|              *  |
|             E   |
+-----------------+
```

Pour créer une nouvelle machine virtuelle en utilisant uvtool, lancez ce qui suit dans un terminal :

```
$ uvt-kvm create firsttest
```

Cela créera une machine virtuelle nommée **firsttest** utilisant l'image cloud LTS actuelle disponible localement. Si vous souhaitez spécifier une version à utiliser pour créer la machine virtuelle, vous aurez besoin d'utiliser le filtre **release=** :

```
$ uvt-kvm create secondtest release=xenial
```

uvt-kvm wait peut être utiliser pour patienter jusqu'à la création complète de la machine virtuelle :

```
$ uvt-kvm wait secondttest –insecure
Warning: secure wait for boot-finished not yet implemented; use --insecure.
```

20.3.2.4. Connectez-vous à la machine virtuelle en cours d'exécution

Une fois la création de la machine virtuelle terminée, vous pouvez vous y connecter en utilisant SSH :

```
$ uvt-kvm ssh secondtest --insecure
```

Jusqu'à présent, **--insecure** est obligatoire, utilisez donc ce mécanisme pour vous connecter à votre machine virtuelle uniquement si vous avez une confiance totale dans l'infrastructure de votre réseau.

Vous pouvez aussi vous connecter à votre machine virtuelle en utilisant une session SSH normale utilisant l'adresse IP de la machine virtuelle. L'adresse peut être recherchée en appliquant la commande suivante :

```
$ uvt-kvm ip secondtest
192.168.122.199
$ ssh -i ~/.ssh/id_rsa ubuntu@192.168.122.199
The authenticity of host '192.168.122.199 (192.168.122.199)' can't be established.
ECDSA key fingerprint is SHA256:8oxaztRWzTMtv8SC9LYyjuqBu79Z9JP8bUGh6G8R8cw.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.122.199' (ECDSA) to the list of known hosts.
Welcome to Ubuntu Xenial Xerus (development branch) (GNU/Linux 4.4.0-X-generic ARCH)

* Documentation: https://help.ubuntu.com/

Get cloud support with Ubuntu Advantage Cloud Guest:
http://www.ubuntu.com/business/services/cloud

0 packages can be updated.
0 updates are security updates.



The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo ".
See "man sudo_root" for details.

ubuntu@secondtest:~$
```

20.3.2.5. Obtenez la liste des machines virtuelles en cours d'exécution

Vous pouvez obtenir la liste des machines virtuelles tournant sur votre système avec cette commande :

```
$ uvt-kvm list
secondtest
```

20.3.2.6. Détruisez votre machine virtuelle

Une fois que vous avez terminé avec votre machine virtuelle, vous pouvez la détruire avec :

```
$ uvt-kvm destroy secondtest
```

20.3.2.7. Plus d'options uvt-kvm

Les options suivantes peuvent être utilisées pour modifier certaines des caractéristiques de la machine virtuelle que vous êtes en train de créer :

- --memory : Total de RAM en megaoctets. Par défaut : 512.
- --disk : Taille du disque du système d'exploitation en gigaoctets. Par défaut : 8.
- --cpu : Nombre de cœurs du processeur. Par défaut : 1.

Quelques autres paramètres auront un impact que la configuration initiale du cloud :

- --password password : permet de s'identifier auprès de la machine virtuelle en utilisant le compte Ubuntu et son mot de passe fourni.
- --run-script-once fichier_script : Exécute le fichier_script en tant que root sur la machine virtuelle seulement la première fois qu'elle est démarrée.
- --packages package_list : Installe les paquets séparés par des virgules, spécifiés dans package_list au premier démarrage.

Une description complète de tous les paramètres disponibles est disponible dans la page man de uvt-kvm.

20.3.3. Ressources

Si vous voulez en apprendre davantage, si vous avez des questions ou des suggestions, veuillez contacter l'équipe Ubuntu Server à cette adresse :

- IRC: **#ubuntu-server** sur freenode
- Liste de diffusion : **ubuntu-server at lists.ubuntu.com** : https://lists.ubuntu.com/mailman/listinfo/ubuntu-server

20.4. Cloud Ubuntu

Cloud computing est un modèle informatique qui permet à de nombreuses ressources d'être allouées à la demande. Ces ressources telles que le stockage, la puissance de calcul, le réseau et les logiciels sont dématérialisés et livrés comme des services sur Internet, n'importe où, n'importe quand. Ces services sont facturés au temps tels les services publics comme l'électricité, l'eau et la téléphonie. **Ubuntu Cloud Infrastructure** utilise le logiciel open source OpenStack pour aider à construire un modèle de cloud computing fortement évolutif pour les clouds publics et privés.

20.4.1. Installation et configuration

En raison du fort développement actuel de cette technologie complexe, nous renvoyons le lecteur à la documentation générique pour toutes les questions concernant l'installation et la configuration : http://doc.ubuntu-fr.org/openstack .

20.4.2. Assistance et dépannage

Support communautaire :

Liste de discussion OpenStack : http://docs.openstack.org/havana/install-guide/install/apt/content/

La recherche Wiki pour OpenStack : https://launchpad.net/~openstack

Zone de bogues Launchpad : https://bugs.launchpad.net/nova

Rejoignez le canal IRC **#OpenStack** sur freenode.

20.4.3. Ressources

Cloud Computing - Modèles de services : http://en.wikipedia.org/wiki/Cloud_computing#Service_Models

OpenStack Compute : http://www.openstack.org/software/openstack-compute/

Service d'image OpenStack :

http://docs.openstack.org/diablo/openstack-compute/starter/content/GlanceMS-d2s21.html

Guide d'administration OpenStack Object Storage :

http://docs.openstack.org/trunk/openstack-object-storage/admin/content/index.html

Installation de OpenStack Object Storage sur Ubuntu :

http://docs.openstack.org/trunk/openstack-object-storage/admin/content/installing-openstack-object-storage-on-ubuntu.html

http://cloudglossary.com/

20.5. LXD

LXD (prononcé lex-di) est le léger-viseur, ou hyperviseur de conteneur léger. Bien que cette revendication fût controversée, cela restait assez justifié d'après l'article universitaire original : http://blog.dustinkirkland.com/2015/09/container-summit-presentation-and-live.html

Il distingue aussi très bien LXD de LXC : https://help.ubuntu.com/lts/serverguide/lxc.html

LXC (lex-ci) est un programme qui crée et administre des « conteneurs » sur un système local. Il fournit aussi une API pour permettre aux gestionnaires de plus haut niveau, tels que LXD, d'administrer des conteneurs. Dans une certaine mesure, on peut comparer LXC à QEMU, tout en comparant LXD à libvirt.

L'API LXC gère un « conteneur ». L'API LXD gère avec des « distants », qui servent des images et des conteneurs. Cela étend la fonctionnalité de LXC aux réseaux, et permet la gestion précise de tâches telles que la migration de conteneurs et l'édition d'image de conteneur.

LXD utilise LXC sous le manteau pour certaines tâches de gestion de conteneur. Quoi qu'il en soit, il conserve ses propres information de configuration de conteneur et possède ses propres conventions. Par conséquent, il vaut mieux ne pas utiliser des commandes LXC classiques manuellement avec des conteneurs LXD. Ce document se focalisera sur la manière de configurer et administrer LXD sur des systèmes Ubuntu.

20.5.1. Ressources en ligne

Il existe une excellente documentation pour démarrer avec LXD dans le README LXD en ligne : http://github.com/lxc/lxd

Il y a aussi un serveur en ligne vous permettant d'essayer LXD à distance : http://linuxcontainers.org/lxd/try-it

Stephane Graber possède également une série d'excellents blogs sur LXD 2.0 : https://www.stgraber.org/2016/03/11/lxd-2-0-blog-post-series-012/

Enfin, il y a une bonne documentation sur la manière de piloter lxd en utilisant juju : https://jujucharms.com/docs/devel/config-LXD

Ce document offre un aperçu de LXD spécifique à Ubuntu Server, se focalisant sur l'administration.

20.5.2 Installation

LXD est pré-installé sur les images cloud d'Ubuntu Server. Sur d'autres systèmes, le paquet lxd peut être installé avec :

```
sudo apt install lxd
```

Ceci installera LXD ainsi que les dépendances recommandées, y compris la bibliothèque LXC et lxcfs.

20.5.3. Préparation du noyau

En général, Ubuntu 16.04 devrait posséder toutes les fonctionnalités désirées activées par défaut.

L'exception est qu'afin de permettre le changement de compte, l'argument de démarrage **swapaccount=1** doit être paramétré. Ceci peut être réalisé en l'ajoutant à la variable **GRUB_CMDLINE_LINUX_DEFAULT=** dans /etc/default/grub, puis exécuter « update-grub » en tant que root et redémarrer.

20.5.4. Configuration

Par défaut, LXD est installé à l'écoute d'un socket UNIX local, auquel les membres du groupe LXD peuvent s'adresser. Il n'a pas de configuration de mot de passe de confiance. Et il utilise le système de fichiers dans /var/lib/lxd pour stocker des conteneurs. Pour configurer LXD avec des paramètres différents, utilisez **lxd init**. Cela vous permettra de choisir :

- Le dossier ou conteneur ZFS de sortie. Si vous choisissez ZFS, vous pouvez choisir quels dispositifs blocs utiliser, ou la taille d'un fichier à utiliser comme espace de sauvegarde. Voir : http://open-zfs.org
- La disponibilité sur le réseau
- Un « mot de passe de confiance » utilisé par les clients distants pour garantir leur certificat client.

Vous devez exécuter « **lxd init** » en tant que root. Les commandes « lxc » peuvent être lancées par tout utilisateur faisant partie du groupe lxd. Si l'utilisateur joe n'est pas un membre du groupe « lxd », vous devrez exécuter :

```
adduser joe lxd
```

en tant que root pour modifier cela. La nouvelle adhésion prendra effet à la prochaine identification, ou après le lancement de « newgrp lxd » à partir d'une identité existante.

Pour de plus amples informations sur les configurations serveur, conteneur, profil, et dispositif, veuillez vous reporter à la configuration définitive fournie avec le code source, pouvant être retrouvée en ligne : https://github.com/lxc/lxd/blob/master/doc/configuration.md

20.5.5. Création de votre premier conteneur

Cette section décrit la plus simple des tâches de conteneur.

20.5.5.1. Création d'un conteneur

Chaque nouveau conteneur est basé soit sur une image, un conteneur existant, ou un instantané d'un conteneur. Au moment de l'installation, LXD est configuré avec les serveurs d'image suivants :

- ubuntu : il sert les versions officielles d'images cloud d'Ubuntu server.
- ubuntu-daily : il sert les versions officielles du développement quotidien d'images cloud d'Ubuntu server.
- images : il s'agit d'un alias installé par défaut pour images.linuxcontainers.org. Il sert les images lxc classiques construites en utilisant les mêmes images que celles employées par le modèle « download » de LXC. Cela comprend diverses distribution et des images Ubuntu minimales sur mesure. Il ne s'agit pas du serveur recommandé pour les images Ubuntu.

La commande pour créer et démarrer un conteneur est :

```
lxc launch remote:image containername
```

Les images sont identifiées par leur hachage, mais également par leur alias. Le serveur « ubuntu » connaît plusieurs alias tels que « 16.04 » ou « xenial ». Une liste des images disponibles sur le Ubuntu Server se visualise avec :

```
lxc image list ubuntu:
```

Pour visualiser encore plus d'informations à propos d'une image particulière, y compris tous ses alias, vous pouvez utiliser :

```
lxc image info ubuntu:xenial
```

En général, vous pouvez vous référer à une image Ubuntu en utilisant le nom de version (« xenial ») ou son numéro (16.04). En complément, « lts » est un alias pour la dernière version LTS prise en charge. Pour choisir une architecture différente, vous pouvez spécifier l'architecture voulue :

```
lxc image info ubuntu:lts/arm64
```

Maintenant, démarrons notre premier conteneur :

```
lxc launch ubuntu:xenial x1
```

Ceci télécharge l'image cloud officielle actuelle Xenial pour votre architecture actuelle, puis crée un conteneur utilisant cette image, et enfin, le démarre. Après le retour de la commande, vous pouvez le voir en utilisant :

```
lxc list
lxc info x1
```

et ouvrir un shell à l'intérieur en utilisant :

```
lxc exec x1 bash
```

La page Essayez-le donne un résumé complet des commandes utilisables pour administrer les conteneurs.

Maintenant que l'image « xenial » a été téléchargée, elle sera conservée synchronisée pendant 10 jours (par défaut) tant qu'aucun nouveau conteneur ne soit créé à partir d'elle. Après quoi, elle sera effacée.

20.5.6. Configuration du Serveur LXD

Par défaut, LXD est activé et configuré pour écouter uniquement un socket UNIX local. Alors que LXD pourrait ne pas s'exécuter lorsque vous jetez un premier coup d'œil à la liste des processus, n'importe quelle commande LXC le démarrera. Par exemple :

```
lxc list
```

Cela créera votre certificat client et contactera le serveur LXD pour une liste de conteneurs. Pour rendre le serveur accessible par le réseau, vous pouvez définir le port http en utilisant :

```
lxc config set core.https_address :8443
```

Cela demandera à LXD d'écouter le port 8843 sur toutes les adresses.

20.5.6.1. Authentification

Par défaut, LXD permettra à tous les membres du groupe « lxd » (qui comprend par défaut tous les membres du groupe admin) de lui parler par le socket UNIX. La communication par le réseau est autorisée en utilisant des certificats serveur et client.

Avant que le client c1 souhaite utiliser le distant r1, celui-ci doit être enregistré en utilisant :

```
lxc remote add r1 r1.example.com:8443
```

L'empreinte du certificat de r1 sera affichée, pour permettre à l'utilisateur en c1 de rejeter un certificat erroné. Le serveur vérifie à son tour qu'il peut porter confiance à c1 d'une des deux manières. La première est de l'enregistrer à l'avance à partir de n'importe quel client déjà enregistré, en utilisant :

```
lxc config trust add r1 certfile.crt
```

Désormais, lorsque le client ajoute r1 comme distant connu, il n'aura pas à fournir un mot de passe puisque le serveur lui fait déjà confiance.

La seconde est de configurer un « mot de passe de confiance » avec r1, soit dès la configuration initiale par le biais de « **lxd init** », ou après coup en utilisant :

```
lxc config set core.trust_password PASSWORD
```

Le mot de passe peut alors être fourni lorsque le client enregistre r1 comme distant connu.

20.5.6.2. Stockage de sauvegarde

LXD prend en charge plusieurs mémoires de sauvegarde. Celle recommandée est ZFS, bien qu'elle ne soit pas disponible sur toutes les plate-formes. Les mémoires de sauvegarde prises en charge comprennent :

- ext4 : Celle par défaut, et la plus simple à utiliser. Avec une mémoire de sauvegarde ext4, les conteneurs et images sont simplement stockés en tant que dossiers sur le système de fichiers hôte. Le lancement de nouveaux conteneurs nécessite une copie complète du système de fichiers, et 10 conteneurs prendront jusqu'à 10 fois plus de place qu'un conteneur.
- ZFS : si ZFS est pris en charge pour votre architecture (amd64, arm64, ou ppc64le), vous pouvez paramétrer LXD pour l'utiliser avec « **lxd init** ». Si vous possédez déjà une partition ZFS configurée, vous pouvez indiquer à LXD de l'utiliser en paramétrant la clé de configuration zfs_pool_name :

  ```
  lxc config set storage.zfs_pool_name lxd
  ```

  Avec ZFS, le lancement d'un nouveau conteneur est rapide car le système de fichier démarre en tant que clone « copie sur écriture » du système de fichier des images. Notez qu'à moins que le conteneur possède des privilèges (voir ci-dessous) LXD devra modifier la propriété de tous les fichiers avant que le conteneur puisse démarrer. Toutefois, ceci est rapide et modifie très peu de données du véritable système de fichier.
- Btrfs : btrfs peut être utilisé avec plusieurs des mêmes avantages que ZFS. Pour utiliser BTRFS en

tant que mémoire de stockage LXD, montez simplement un système de fichiers Btrfs dans /var/lib/lxd. LXD le détectera et exploitera la fonctionnalité de sous-volume Btrfs à chaque lancement de nouveau conteneur ou à l'occasion d'un instantané d'un conteneur.

- LVM : Pour utiliser un groupe de volume LVM nommé « lxd », vous pouvez indiquer à LXD d'utiliser cela pour les conteneurs et images en utilisant la commande :

```
lxc config set storage.lvm_vg_name lxd
```

Lors du lancement d'un nouveau conteneur, son système de fichier root démarrera en tant que clone lv. Il est immédiatement monté de telle sorte que les identifiants utilisateur fichier peuvent être déplacés, puis démonté. Les instantanés de conteneur sont aussi créés en tant qu'instantanés lv.

20.5.7. Configuration de conteneur

Les conteneurs sont configurés selon un ensemble de profils, décrits dans la section suivante, et selon un ensemble de configuration spécifique au conteneur. Les profils sont appliqués en premier, de telle sorte que la configuration spécifique du conteneur puisse prendre le pas sur la configuration par profil.

La configuration de conteneur comprend des propriétés telles que l'architecture, les limites de ressources comme le processeur et la mémoire, des détails de sécurité y compris les priorités d'**apparmor** sur les restrictions, et les périphériques où appliquer le conteneur.

Les périphériques peuvent être de plusieurs types, y compris caractère UNIX, bloc UNIX, interface réseau ou « disque ». De manière à insérer un montage d'hôte dans un conteneur, un périphérique « disque » devrait être utilisé. Par exemple, pour monter /opt dans le conteneur c1 à /opt, vous pouvez utiliser :

```
lxc config device add c1 opt disk source=/opt path=opt
```

Voir :

```
lxc help config
```

pour plus d'information au sujet de l'édition des configurations de conteneur. Vous pouvez aussi utiliser :

```
lxc config edit c1
```

pour éditer la configuration complète de c1 dans votre $EDITOR spécifié. Des commentaires en tête de la configuration montreront des exemples de syntaxes correctes pour aider les administrateurs à faire tourner la base. Si la configuration éditée est invalide lorsque $EDITOR est quitté, alors il sera relancé.

20.5.8. Profils

Les profils sont des collections nommées de configurations pouvant être appliquées à plus d'un conteneur. Par exemple, tous les conteneurs créés avec « lxc launch », par défaut, incluront le profil « default » qui fournit une interface réseau « eth0 ».
Pour masquer un périphérique qui serait hérité d'un profil mais qui ne devrait pas être dans le conteneur final, définissez un périphérique du même nom, mais de type « none » :

```
lxc config device add c1 eth1 none
```

20.5.9. Imbrication

Les conteneurs partagent tous le même noyau hôte. Cela signifie qu'il existe toujours un compromis inhérent entre les fonctionnalités exposées au conteneur et la sécurité de l'hôte de la part de conteneurs malveillants. Par conséquent, les conteneurs ne disposent pas, par défaut, de fonctionnalités nécessaires pour engendrer d'autres conteneurs. Afin de lancer des conteneurs lxc ou lxd à partir d'un conteneur lxd, la fonctionnalité « security.nesting » doit être paramétrée sur « true » :

```
lxc config set container1 security.nesting true
```

Une fois fait, container1 sera en mesure de démarrer des sous-conteneurs.

Afin de lancer des conteneurs sans privilèges (par défaut dans LXD) imbriqués dans un conteneur sans privilège, vous devrez vous assurer d'un mappage d'identifiants utilisateur suffisant. Veuillez lire la section « Mappage UID » ci-dessous.

20.5.9.1. Docker

Afin de faciliter des conteneurs dockers à l'intérieur d'un conteneur LXD, un profil « docker » est fourni. Pour lancer un nouveau conteneur avec le profil docker, vous pouvez exécuter :

```
lxc launch xenial container1 -p default -p docker
```

Notez qu'actuellement le paquet docker est préparé dans Ubuntu 16.04 pour faciliter l'exécution dans un conteneur. Cette prise en charge est en passe d'être généralisée prochainement.

Notez que la prise en charge de « cgroup namespace » est également requise. Cela est disponible dans le noyau 16.04 ainsi que dans la source générique 4.6.

20.5.10. Limites

LXD prend en charge des contraintes flexibles sur les ressources que consomment les conteneurs. Les limites surviennent dans les catégories suivantes :

- CPU : limite le processeur disponible pour le conteneur de plusieurs façons.
- Disque : configure la priorité des requêtes d'E/S en charge
- RAM : configure la disponibilité mémoire et tampon
- Réseau : configure la priorité réseau en charge
- Processus : limite le nombre de processus concomitants dans le conteneur.

Pour une liste exhaustive de limites reconnues par LXD, voir la documentation de configuration : https://github.com/lxc/lxd/blob/master/doc/configuration.md

20.5.11. Mappages d'identifiant utilisateur et Conteneurs à privilèges

Par défaut, LXD crée des conteneurs sans privilèges. Cela signifie que root dans le conteneur est un identifiant utilisateur distinct de root sur l'hôte. Il a des privilèges envers les ressources possédées par le conteneur, mais reste sans privilèges en respect de l'hôte, faisant à peu près de root dans un conteneur l'équivalent d'un utilisateur sans privilèges sur l'hôte. (La principale exception est la surface d'attaque accrue exposée par l'interface d'appel du système).

En bref, dans un conteneur sans privilèges, 65536 identifiants utilisateur sont « déplacés » dans le conteneur. Par exemple, l'identifiant utilisateur 0 dans le conteneur peut être 100000 sur l'hôte, l'identifiant utilisateur 1 dans le conteneur est 100001, etc, jusqu'à 165535. La valeur de départ pour les identifiants utilisateur ou de groupe, est déterminée par l'entrée « root » respectivement, dans les fichiers /etc/subuid et /etc/subgid. Consultez la page de manuel subuid(5) : http://manpages.ubuntu.com/manpages/xenial/en/man5/subuid.5.html .

Il est possible de demander l'exécution d'un conteneur sans un mappage d'identifiant utilisateur en paramétrant l'indicateur security.privileged à true :

```
lxc config set c1 security.privileged true
```

Notez toutefois que dans ce cas, l'utilisateur root dans le conteneur est l'utilisateur root sur l'hôte.

20.5.12. Apparmor

LXD confine les conteneurs par défaut avec un profil apparmor qui protège les conteneurs les uns des autres et protège l'hôte des conteneurs. Par exemple, cela empêche root dans un conteneur de signaler root dans un autre conteneur, même si ils possèdent le même mappage d'identifiant utilisateur. Cela empêche aussi d'écrire vers des fichiers dangereux nommés sans espace, tels de nombreux sysctls et /proc/sysrq-trigger.

Si la politique apparmor pour un conteneur doit être modifiée pour un conteneur c1, des lignes spécifiques de politique apparmor peuvent être ajoutées dans la clé de configuration « raw.apparmor ».

20.5.13. Seccomp

Tous les conteneurs sont confinés par une politique seccomp par défaut. Cette politique empêche certaines actions dangereuses telles que des démontages forcés, des chargements et déchargements de modules du noyau, kexec, et l'appel système open_by_handle_at. La configuration seccomp ne peut pas être modifiée, toutefois, une politique seccomp complètement différente - ou aucune - peut être demandée en utilisant raw.lxc (voir ci-dessous).

20.5.14. Configuration LXC brute

LXD configure les conteneurs pour le meilleur équilibre entre la sécurité de l'hôte et la facilité d'utilisation du conteneur. Autant que possible, il est fortement recommandé d'utiliser les paramètres par défaut, et d'utiliser les clés de configuration LXD pour demander à LXD de modifier si besoin. Pourtant, il est parfois nécessaire de parler au pilote lxc sous-jacent lui-même. Cela peut être réalisé en spécifiant les éléments de configuration LXC dans la clé de configuration LXD « raw.lxc ». Ces éléments doivent être valides au sens de la page de manuel lxc.container.conf(5) : http://manpages.ubuntu.com/manpages/xenial/en/man5/lxc.container.conf.5.html

20.5.15. Images et conteneurs

LXD est à base d'image. Lorsque vous créez votre premier conteneur, vous utiliserez en général une image existante. LXD est livré pré-configuré avec trois images distantes par défaut :

- ubuntu : il s'agit d'une image distante basé sur simplestreams servant des images de cloud ubuntu versionnées : https://launchpad.net/simplestreams
- ubuntu-daily : Il s'agit d'une autre image distante basée sur simplestreams servant des images « quotidiennes » de cloud ubuntu. Elles produisent des images plus rapides mais potentiellement moins stables.
- images : Il s'agit d'images distantes publiant des images conteneur au mieux pour plusieurs distributions, créées en utilisant des scripts construits fournis par la communauté.

Pour visualiser les images disponibles sur un de ces serveurs, vous pouvez utiliser :

La plupart des images sont reconnues par plusieurs alias pour un référencement plus aisé. Pour consulter la liste complète des alias, vous pouvez utiliser :

```
lxc image alias list images:
```

Tout alias ou empreinte d'image peut être utilisé pour spécifier comment créer le nouveau conteneur. Par exemple, pour créer un conteneur amd64 Ubuntu 14.04, quelques options sont :

```
lxc launch ubuntu:14.04 trusty1
lxc launch ubuntu:trusty trusty1
lxc launch ubuntu:trusty/amd64 trusty1
lxc launch ubuntu:lts trusty1
```

L'alias « lts » se réfère toujours à l'image de la dernière version LTS.

20.5.15.1. Instantanés

Les conteneurs peuvent être renommés et transférés en direct en utilisant la commande « lxc move »:

```
lxc move c1 final-beta
```

Ils peuvent aussi être pris en instantané :

```
lxc snapshot c1 YYYY-MM-DD
```

Les modifications ultérieures à c1 peuvent alors être annulées en restaurant l'instantané :

```
lxc restore u1 YYYY-MM-DD
```

De nouveaux conteneurs peuvent aussi être créés en copiant un conteneur ou un instantané :

```
lxc copy u1/YYYY-MM-DD testcontainer
```

20.5.15.2. Publication d'images

Lorsqu'un conteneur ou un instantané de conteneur est prêt à être consommé par d'autres, il peut être publié en tant que nouvelle image en utilisant :

```
lxc publish u1/YYYY-MM-DD --alias foo-2.0
```

L'image publiée sera privée par défaut, signifiant que LXD n'autorisera pas des clients sans certificat de confiance à les visualiser. Si l'image est sûre pour une visualisation publique (c'est à dire ne contient aucune information privée), alors l'indicateur « public » peut être paramétré, soit au moment de la publication en utilisant :

```
lxc publish u1/YYYY-MM-DD --alias foo-2.0 public=true
```

ou après coup en utilisant :

```
lxc image edit foo-2.0
```

et en modifiant la valeur du champ public.

20.5.15.3. Export et import d'image

Une image peut être exportée en tant que, ou importée à partir d'archives :

```
lxc image export foo-2.0 foo-2.0.tar.gz
lxc image import foo-2.0.tar.gz --alias foo-2.0 --public
```

20.5.16. Dépannage

Pour visionner les informations de débogage de LXD lui-même, sur un hôte basé sur systemd, utilisez :

```
journalctl -u LXD
```

Sur un système basé sur Upstart, vous pouvez trouver le journal dans /var/log/upstart/lxd.log. Pour que LXD fournisse encore plus d'informations à propos des demandes qu'il sert, ajoutez « --debug » aux arguments de LXD. Dans systemd, ajoutez « --debug » à la ligne « ExecStart= » dans /lib/systemd/system/lxd.service. Dans Upstart, ajoutez à la ligne **exec /usr/bin/lxd** dans /etc/init/lxd.conf.

Les fichiers journaux de conteneur pour le conteneur c1 peuvent être visualisés en utilisant :

```
lxc info c1 --show-log
```

Le fichier de configuration qui a été utilisé peut être trouvé dans /var/log/lxd/c1/lxc.conf alors que les profils apparmor peuvent être trouvés dans /var/lib/lxd/security/apparmor/profiles/c1 et les profils seccomp dans /var/lib/lxd/security/seccomp/c1.

20.6. LXC

Les conteneurs sont une technologie légère de virtualisation. Ils s'apparentent davantage à un chroot amélioré par rapport à la virtualisation totale de Qemu ou VMware, à la fois parce qu'ils n'émulent pas le matériel et parce que les conteneurs partagent le même système d'exploitation que l'hôte. Les conteneurs sont similaires aux zones Solaris ou aux « jails » BSD. Linux-vserver et OpenVZ sont deux implémentations pré-existantes, développés indépendamment de la fonctionnalité simili-conteneur pour Linux. En fait, les conteneurs sont venus à la suite des travaux pour généraliser les fonctionnalités vserver et OpenVZ.

Il existe deux implémentations des conteneurs en espace utilisateur, chacune exploitant les mêmes fonctionnalités du noyau. Libvirt permet l'utilisation de conteneurs par l'intermédiaire du pilote LXC en se connectant sur « lxc :/// ». Cela peut être très pratique car il prend en charge la même utilisation que ses autres pilotes. L'autre implémentation, appelée simplement « LXC », n'est pas compatible avec libvirt, mais est plus souple avec un plus grand nombre d'outils d'espace utilisateur. Il est possible de basculer entre les deux, mais il y a des particularités qui peuvent prêter à confusion.

Dans ce document, nous décrirons essentiellement le paquet lxc. L'utilisation de libvirt-lxc n'est généralement pas recommandée en raison d'un manque de protection d'Apparmor pour les conteneurs libvirt-lxc.

Dans ce document, un nom de conteneur sera affiché comme CN, C1 ou C2.

20.6.1. Installation

Le paquet **lxc** peut être installé à l'aide de :

```
sudo apt install lxc
```

Ceci piochera dans les dépendances nécessaires et recommandées, et mettra en place un pont réseau qu'utiliseront les conteneurs. Si vous souhaitez utiliser des conteneurs sans privilèges, vous devrez vous assurer que les utilisateurs ont suffisamment de sous-identifiants utilisateur et de sous-identifiants de groupe alloués, et vous souhaiterez probablement permettre aux utilisateurs de connecter des conteneurs à un pont (voir *6.2.3. Utilisation de base non privilégiée*).

20.6.2. Utilisation basique

LXC peut s'utiliser de deux manières distinctes - avec privilèges, en exécutant les commandes lxc en tant qu'utilisateur root ; ou sans privilèges, en exécutant les commandes lxc en tant qu'utilisateur non-root. (Le démarrage de conteneurs sans privilèges par l'utilisateur root est possible, mais non décrit ici). Les conteneurs sans privilèges sont plus limités, par exemple incapables de créer des nœuds périphériques ou de monter des systèmes de fichiers sauvegardés sur des périphériques blocs. Ils sont toutefois moins dangereux pour l'hôte, car l'identifiant utilisateur root dans le conteneur est mappé comme un identifiant utilisateur non-root sur l'hôte.

20.6.2.1. Utilisation privilégiée basique

Pour créer un conteneur avec privilèges, vous pouvez simplement lancer :

```
sudo lxc-create --template download --name u1
```

ou, en abrégé

```
sudo lxc-create -t download -n u1
```

Ceci demandera interactivement un type de système de fichiers racine de conteneur à télécharger - notamment la distribution, la version et l'architecture. Pour créer le conteneur de façon non-interactive, vous pouvez spécifier ces valeurs sur la ligne de commande :

```
sudo lxc-create -t download -n u1 -- --dist ubuntu --release xenial \
--arch amd64
```

ou

```
sudo lxc-create -t download -n u1 -- -d ubuntu -r xenial -a amd64
```

Vous pouvez maintenant utiliser la commande **lxc-ls** pour lister les conteneurs, **lxc-info** pour obtenir des informations détaillées de conteneurs, **lxc-start** pour démarrer un conteneur et **lxc-stop** pour l'arrêter. **lxc-attach** et **lxc-console** vous permettent d'entrer dans un conteneur, si ssh n'est pas disponible. **lxc-destroy** supprime le conteneur, y compris ses fichiers système racine. Veuillez voir les pages de manuel pour plus d'informations sur chaque commande. Un exemple de session pourrait ressembler à :

```
sudo lxc-ls --fancy
sudo lxc-start --name u1 --daemon
sudo lxc-info --name u1
sudo lxc-stop --name u1
sudo lxc-destroy --name u1
```

20.6.2.2. Espaces de noms utilisateur

Les conteneurs sans privilèges permettent aux utilisateurs de créer et d'administrer des conteneurs sans avoir aucun privilège root. La fonctionnalité soutenant ceci est appelée espaces de nom utilisateur. Ces derniers sont hiérarchiques, avec des tâches à privilèges dans un espace de nom parent capable de mapper ses identifiants dans des espaces de nom engendrés. Toute tâche sur l'hôte s'exécute par défaut dans le nom d'espace utilisateur, où l'intégralité des identifiants est mappée sur tout l'intervalle. Cela se voit dans /proc/self/uid_map et /proc/self/gid_map, chacun affichant « 0 0 4294967295 » lors de la lecture depuis l'espace de nom utilisateur initial. Depuis Ubuntu 14.04, lorsque de nouveaux utilisateurs sont créés, ils se voient offrir par défaut un intervalle d'identifiants utilisateur. La liste des identifiants assignés peut être vue dans les fichiers /etc/subuid et /etc/subgid. Consultez leurs pages de manuel respectives pour plus d'information. Les sous-identifiants utilisateur et les sous-identifiants de groupe démarrent par convention à 100000 pour éviter tout conflit avec les utilisateurs système.

Si un utilisateur a été créé sur une version antérieure, il peut lui être accordé une plage d'identifiants en utilisant la commande **usermod**, comme suit :

```
sudo usermod -v 100000-200000 -w 100000-200000 user1
```

Les programmes **newuidmap** et **newgidmap** sont des programmes root paramétrant les identifiants utilisateur dans le paquet uidmap, utilisé de manière interne par lxc pour mapper des sous-identifiants

utilisateur et des sous-identifiants de groupe à partir de l'hôte dans le conteneur sans privilèges. Ils s'assurent que l'utilisateur mappe uniquement des identifiants autorisés par la configuration de l'hôte.

20.6.2.3. Utilisation de base non privilégiée

Pour créer des conteneurs sans privilèges, quelques étapes préalables sont nécessaires. Vous avez besoin de créer un fichier de configuration de conteneur par défaut, en spécifiant vos souhaits de mappage d'identifiants et de configuration réseau, aussi bien que de configurer l'hôte pour permettre à l'utilisateur sans privilèges de se raccorder au réseau de l'hôte. L'exemple ci-dessous présume que votre intervalle mappé d'identifiants utilisateur et groupe est 100000-165536. Vérifiez vos intervalles réels d'identifiants utilisateur et groupe et modifiez l'exemple en conséquence :

```
grep $USER /etc/subuid
grep $USER /etc/subgid

mkdir -p ~/.config/lxc
echo "lxc.id_map = u 0 100000 65536" > ~/.config/lxc/default.conf
echo "lxc.id_map = g 0 100000 65536" >> ~/.config/lxc/default.conf
echo "lxc.network.type = veth" >> ~/.config/lxc/default.conf
echo "lxc.network.link = lxcbr0" >> ~/.config/lxc/default.conf
echo "$USER veth lxcbr0 2" | sudo tee -a /etc/lxc/lxc-usernet
```

Après cela, vous pouvez créer des conteneurs non privilégiés et privilégiés de la même manière, sans utiliser sudo.

```
lxc-create -t download -n u1 -- -d ubuntu -r xenial -a amd64
lxc-start -n u1 -d
lxc-attach -n u1
lxc-stop -n u1
lxc-destroy -n u1
```

20.6.2.4. Imbrication

Afin d'exécuter des conteneurs à l'intérieur de conteneurs - appelés conteneurs imbriqués - deux lignes doivent être présentes dans le fichier de configuration du conteneur parent :

```
lxc.mount.auto = cgroup
lxc.aa_profile = lxc-container-default-with-nesting
```

La première provoque la limitation au conteneur de la prise du gestionnaire cgroup, de sorte que lxc à l'intérieur du conteneur soit en mesure d'administrer des cgroups pour ses conteneurs imbriqués. La seconde provoque l'exécution du conteneur sous une politique Apparmor plus souple qui permet au conteneur de réaliser le montage nécessaire au démarrage de conteneurs. Notez que cette politique, lorsqu'elle est utilisée dans un conteneur avec privilèges, est bien moins sûre que la politique normale ou qu'un conteneur sans privilège. Voir le *Chapitre 20, paragraphe 6. LXC.9 Apparmor* pour plus d'informations.

20.6.3. Configuration globale

Les fichiers de configuration suivants sont consultés par LXC. Pour une utilisation privilégiée, ils se trouvent dans /etc/lxc, et pour une utilisation non privilégié, ils sont dans ~/.config/lxc.

- lxc.conf peut éventuellement spécifier d'autres valeurs pour plusieurs paramètres lxc, y compris lxcpath, la configuration par défaut, les cgroups à utiliser, un modèle de création de cgroup, et les paramètres de moteur de stockage pour lvm et zfs.
- default.conf spécifie la configuration que tout conteneur nouvellement créé devrait contenir. Celui-ci contient habituellement a minima une section réseau, et, pour les utilisateurs sans privilèges, une section de mappage d'identifiants
- lxc-usernet.conf spécifie comment les utilisateurs non privilégiés peuvent connecter leurs conteneurs au réseau appartenant à l'hôte.

lxc.conf et default.conf sont tous deux dans /etc/lxc et $HOME/.config/lxc, alors que lxc-usernet.conf est uniquement dans l'hôte.

Par défaut, les conteneurs sont dans /var/lib/lxc pour l'utilisateur root, et dans $HOME/.local/share/lxc pour les autres utilisateurs. L'emplacement peut être spécifié pour toutes les commandes lxc en utilisant l'argument « -P|--lxcpath ».

20.6.4. Mise en réseau

LXC crée par défaut un espace privé de noms de réseau pour chaque conteneur, qui comprend une pile de réseau de couche 2. Les conteneurs se connectent généralement au monde extérieur soit en ayant une carte d'interface réseau ou un point de terminaison du tunnel veth passé dans le conteneur. LXC crée un pont NAT, lxcbr0, au démarrage de l'hôte. Les conteneurs créés en utilisant la configuration par défaut auront une carte d'interface réseau veth ayant l'extrémité distante branchée sur le pont lxcbr0. Une carte d'interface réseau ne peut exister que dans un seul espace de noms à la fois, par conséquent une carte d'interface réseau physique passée dans le conteneur n'est pas utilisable sur l'hôte.

Il est possible de créer un conteneur sans un espace privé de noms de réseau. Dans ce cas, le conteneur aura accès au réseau de l'hôte comme n'importe quelle autre application. Notez que ceci est particulièrement dangereux si le conteneur exécute une distribution avec upstart, comme Ubuntu, puisque des programmes parlant à l'init, comme **shutdown**, parleront au-delà du domaine d'abstraction Unix directement à l'upstart de l'hôte, et arrêteront l'hôte.

Pour donner aux conteneurs sur lxcbr0 une adresse ip permanente basée sur le nom de domaine, vous pouvez écrire des entrées dans /etc/lxc/dnsmasq.conf comme :

```
dhcp-host=lxcmail,10.0.3.100
dhcp-host=TTRSS,10.0.3.101
```

Si vous souhaitez que le conteneur soit publiquement accessible, il y a quelques façons d'aller dans ce sens. L'une est d'utiliser la commande **iptables** pour rediriger les ports de l'hôte vers le conteneur, par exemple :

```
iptables -t nat -A PREROUTING -p tcp -i eth0 --dport 587 -j DNAT \
  --to-destination 10.0.3.100:587
```

Une autre façon est de ponter l'interface réseau de l'hôte (voir le *Chapitre 4, paragraphe 1. Configuration du réseau.4. Pont réseau*). Ensuite, précisez le pont de l'hôte dans le fichier de configuration du conteneur à la place de lxcbr0, par exemple :

```
lxc.network.type = veth
```

```
lxc.network.link = br0
```

Pour terminer, vous pouvez demander à LXC d'utiliser macvlan pour le NIC (carte d'interface réseau) du conteneur. Veuillez noter que ceci à ses limites et selon la configuration peut ne pas permettre au conteneur de parler à l'hôte lui-même. Par conséquent, les deux autres options sont préférées et plus communément utilisées.

Il ya plusieurs façons de déterminer l'adresse IP d'un conteneur. D'abord, vous pouvez utiliser **lxc-ls --fancy** qui affichera les adresses IP pour tous les conteneurs en cours d'exécution, ou **lxc-info -i -H -n C1** qui affichera l'adresse IP du conteneur C1. Si Dnsmasq est installé sur l'hôte, vous pouvez également aussi ajouter une entrée dans /etc/dnsmasq.conf comme suit :

```
server =/lxc/10.0.3.1
```

après quoi dnsmasq résoudra C1.lxc localement, de sorte que vous puissiez faire :

```
ping C1
ssh C1
```

Pour plus d'informations, consultez la page de manuel lxc.conf ainsi que les exemples de configurations réseau dans /usr/share/doc/lxc/examples/.

20.6.5. Démarrage de LXC

LXC n'a pas un démon de longue durée. Toutefois, il a trois taches upstart.

- /etc/init/lxc-net.conf: est une tâche optionnelle qui fonctionne uniquement si /etc/default/lxc-net spécifie USE_LXC_BRIDGE (true par défaut). Il met en place un pont NAT à utiliser par les conteneurs.
- /etc/init/lxc.conf charge les profils apparmor lxc et démarre éventuellement tout conteneur à démarrage automatique. Les conteneurs à démarrage automatique seront ignorés si LXC_AUTO (true par défaut) est paramétré à true dans /etc/default/lxc. Voir la page de manuel de **lxc-autostart** pour plus d'informations sur les conteneurs à démarrage automatique.
- /etc/init/lxc-instance.conf est utilisé par /etc/init/lxc.conf pour démarrer automatiquement un conteneur.

20.6.6. Magasins de sauvegarde

LXC prend en charge plusieurs magasins de sauvegarde pour les conteneurs de systèmes de fichiers root. Celui par défaut est un simple dossier de sauvegarde, car il ne nécessite aucune personnalisation préalable de l'hôte, aussi longtemps que le système de fichiers sous-jacent est assez grand. Il n'y a besoin d'aucun privilège root pour créer le magasin de sauvegarde, de sorte qu'il est transparent pour une utilisation sans privilèges. Le sytème de fichiers root pour un conteneur avec privilèges sauvegardé dans un dossier se trouve (par défaut) dans /var/lib/lxc/C1/rootfs, alors que le système de fichiers root pour un conteneur sans privilèges se trouve dans ~/.local/share/lxc/C1/rootfs. Si un chemin lxcpath est spécifié dans lxc.system.com, alors le conteneur du système de fichier root se trouvera dans $lxcpath/C1/rootfs.

Un clône instantané C2 d'un dossier de sauvegarde d'un conteneur C1 devient un conteneur sauvegardé overlayfs, avec un système de fichiers root appelé overlayfs:/var/lib/lxc/C1/rootfs:/var/lib/lxc/C2/delta0. Les autres types de magasin de stockage comprennent loop, btrfs, LVM et zfs.

Un conteneur sauvegardé btrfs ressemble la plupart du temps à un conteneur sauvegardé de répertoire, avec son système de fichier root au même endroit. Cependant, le système de fichier root comprend un sous-volume, de sorte qu'un clone instantané est créé en utilisant un instantané de sous-volume.

Le système de fichier root pour un conteneur sauvegardé LVM peut être tout volume logique séparé. Le nom de groupe de volume par défaut peut être spécifié dans lxc.conf. Le type et la taille du système de fichier sont configurables par conteneur en utilisant **lxc-create**.

Le système de fichier root pour un conteneur sauvegardé ZFS est un système de fichier zfs séparé, monté sous l'emplacement traditionnel /var/lib/lxc/C1/rootfs. Le zfsroot peut être spécifié avec **lxc-create**, et celui par défaut peut être spécifié dans lxc.system.conf.

Plus d'informations sur la création de conteneurs avec les différentes banques de sauvegarde peuvent être trouvées dans la page de manuel de **lxc-create**.

20.6.7. Modèles

La création d'un conteneur implique généralement de créer un système de fichier root pour le conteneur. **lxc-create** délègue ce travail aux **modèles**, généralement propres à la distribution. Les modèles lxc fournis avec lxc se trouvent dans /usr/share/lxc/templates, et comprennent des modèles pour créer des conteneurs Ubuntu, Debian, Fedora, Oracle, centos, et gentoo entre autres.

La création d'images de distribution nécessite dans la plupart des cas la capacité de créer des noeuds de périphériques, nécessite souvent des outils non disponibles dans d'autres distributions, et reste généralement chronophage. Par conséquent, lxc est livré avec un modèle spécial **télécharger**, qui télécharge des images de conteneurs pré-construites, sur un serveur central lxc. Le cas d'utilisation la plus importante est de permettre aux utilisateurs non-root de simplement créer des conteneurs sans privilèges, car ces utilisateurs ne pouvaient par exemple pas exécuter facilement la commande **debootstrap**.

Lors de l'exécution de **lxc-create**, toutes les options venant après **--** sont passées au modèle. Dans la commande suivante, **--name**, **--template** et **--bdev** sont passés à **lxc-create**, alors que **--release** est passé au modèle :

```
lxc-create --template ubuntu --name c1 --bdev loop -- --release xenial
```

Vous pouvez obtenir de l'aide pour les options prises en charge par un conteneur en particulier en passant **--help** et le nom du modèle à **lxc-create**. Par exemple, pour l'aide avec le modèle de téléchargement :

```
lxc-create télécharger --template --help
```

20.6.8. Démarrage automatique

LXC prend en charge le marquage de conteneurs à démarrer au démarrage système. Avant Ubuntu 14.04, ceci était réalisé en utilisant des liens symboliques dans le répertoire /etc/lxc/auto. A partir d'Ubuntu 14.04, ceci est réalisé par les fichiers de configuration de conteneur. Une entrée :

```
lxc.start.auto = 1
lxc.start.delay = 5
```

signifierait que le conteneur doit être lancé au démarrage, et que le système doit attendre 5 secondes avant le démarrage du conteneur suivant. LXC prend aussi en charge l'ordonnancement et le regroupement de conteneurs, ainsi que le redémarrage et l'arrêt par des groupes à démarrage automatique. Consultez les pages de manuel de lxc-autostart et lxc.container.conf pour plus d'informations.

20.6.9. Apparmor

LXC est livré avec un profil Apparmor censé protéger l'hôte d'une mauvaise manipulation de privilèges dans le conteneur. Par exemple, le conteneur ne pourra pas écrire dans /proc/sysrq-trigger ou dans la plupart des fichiers /sys.

Le profil usr.bin.lxc-start est entré en exécutant **lxc-start**. Ce profil empêche principalement **lxc-start** de monter de nouveaux systèmes de fichier en dehors de celui root du conteneur. Avant d'exécuter l'**init** du conteneur, **LXC** demande un commutateur au profil du conteneur. Par défaut, ce profil est la politique lxc-container-default définie dans /etc/apparmor.d/lxc/lxc-default. Ce profil empêche le conteneur d'accéder à de nombreux chemins critiques, et de monter trop de systèmes de fichier.

Des programmes dans un conteneur ne peuvent plus être confinés - par exemple, MySQL fonctionne sous le profil de conteneur (protection de l'hôte), mais ne sera pas en mesure d'entrer dans le profil MySQL (pour protéger le conteneur).

La commande **lxc-execute** n'entre pas un profile Apparmor, mais le conteneur qu'il engendre sera confiné.

20.6.9.1. Personnalisation des politiques de sécurité du conteneur

Si vous constatez que **lxc-start** échoue malgré un accès légitime, refusé par la politique d'AppArmor, vous pouvez désactiver le profil de **lxc-start** en faisant :

```
sudo apparmor_parser -R /etc/apparmor.d/usr.bin.lxc-start
sudo ln -s /etc/apparmor.d/usr.bin.lxc-start /etc/apparmor.d/disabled/
```

Cela rendra l'exécution de **lxc-start** en mode non confiné, tout en continuant le confinement du conteneur lui-même. Si vous souhaitez également désactiver le confinement du conteneur, alors en supplément de la désactivation du profil usr.bin.lxc-start, vous devez ajouter :

```
lxc.aa_profile = unconfined
```

dans le fichier de configuration du conteneur.

LXC est livré avec quelques politiques alternatives pour les conteneurs. Si vous souhaitez exécuter des conteneurs à l'intérieur de conteneurs (imbrication), alors vous pouvez utiliser le profil lxc-container-default-with-nesting en ajoutant la ligne suivante au fichier de configuration du conteneur :

```
lxc.aa_profile = lxc-container-default-with-nesting
```

Notez que la politique d'imbrication avec des conteneurs privilégiés est beaucoup moins sûre que la politique par défaut, car il permet aux conteneurs de remonter les fichiers /sys et /proc dans des endroits non standards, contournant les protections de AppArmor. Les conteneurs non privilégiés n'ont pas cet inconvénient puisque la racine du conteneur ne peut pas écrire dans les fichiers proc et sys appartenant à la racine.

Un autre profil livré avec lxc permet aux conteneurs de monter des systèmes de fichiers de type bloc comme ext4. Cela peut être utile dans certains cas comme l'approvisionnement maas, mais est réputé généralement dangereux puisque les gestionnaires de superbloc dans le noyau n'ont pas été vérifiés pour une manipulation sûre d'entrée non fiable.

Si vous devez exécuter un conteneur avec un profil personnalisé, vous pouvez créer un nouveau profil sous /etc/apparmor.d/lxc/. Son nom doit commencer par lxc- pour que **lxc-start** puisse être autorisé à passer à ce profil. Le profil lxc-default comprend le fichier des abstractions réutilisables /etc/apparmor.d/abstractions/lxc/container-base. Un moyen facile de démarrer un nouveau profil est donc de faire la même chose, puis d'ajouter des autorisations supplémentaires à la fin de votre politique.

Après la création de la stratégie, chargez-la à l'aide de :

```
sudo apparmor_parser -r /etc/apparmor.d/lxc-containers
```

Le profil sera automatiquement chargé après un redémarrage, parce qu'il est alimenté par le fichier /etc/apparmor.d/lxc-containers. Enfin, pour faire que le conteneur CN utilise le nouveau lxc-profile-CN, ajoutez la ligne suivante dans son fichier de configuration :

```
lxc.aa_profile = lxc-CN-profile
```

20.6.10. Groupes de contrôle

Les groupes de contrôle (cgroups) sont une fonctionnalité du noyau fournissant regroupement hiérarchique de tâches et comptabilité et limitations des ressources par-cgroup. Ils sont utilisés dans des conteneurs pour limiter l'accès au périphérique bloc et périphérique caractère et pour geler (suspendre) des conteneurs. Ils peuvent en outre être utilisés pour limiter l'utilisation de la mémoire et bloquer les entrées/sorties, garantir les partages minimaux de processeur, et pour verrouiller des conteneurs aux processeurs spécifiques.

Par défaut, un conteneur CN avec privilèges sera assigné à un cgroup nommé /lxc/CN. En cas de conflits de nom (ce qui peut arriver en utilisant des lxcpaths personnalisés) un suffixe « -n », où n est un entier supérieur ou égal à 0, sera ajouté au nom de cgroup.

Par défaut, un conteneur CN avec privilèges sera assigné à un cgroup nommé CN sous le cgroup de la tâche ayant démarré le conteneur, par exemple /usr/1000.user/1.session/CN. Le conteneur racine recevra la possession du groupe du répertoire (mais pas de tous les fichiers) de telle sorte qu'il soit autorisé à engendrer de nouveaux cgroups.

A partir d'Ubuntu 14.04, LXC utilise le gestionnaire de cgroup (cgmanager) pour administrer des cgroups. Le manager de cgroup reçoit des demandes D-Bus par le socket Unix /sys/fs/cgroup/cgmanager/sock. Pour faciliter la sécurité des conteneurs imbriqués, la ligne :

```
lxc.mount.auto = cgroup
```

peut être ajoutée à la configuration du conteneur provoquant le montage lié du répertoire /sys/fs/cgroup/cgmanager dans le conteneur. À son tour, le conteneur devrait démarrer le proxy de gestion de cgroup (actionné par défaut si le paquet cgmanager est installé dans le conteneur) qui déplacera le répertoire /sys/fs/cgroup/cgmanager vers /sys/fs/cgroup/cgmanager.lower, puis démarrera l'écoute des demandes au proxy sur son propre socket /sys/fs/cgroup/cgmanager/sock. L'hôte cgmanager assurera que les conteneurs imbriqués ne peuvent s'échapper de leurs cgroups assignés ou ne peuvent effectuer des requêtes auxquelles ils ne sont pas autorisés.

20.6.11. Clonage

Pour un remplissage rapide, vous pouvez personnaliser un conteneur canonical selon vos besoins puis en faire plusieurs copies. Cela peut être fait avec la commande **lxc-clone**.

Les clones sont soit des instantanés soit des copies d'un autre conteneur. Une copie est un nouveau conteneur copié à partir de l'original, et prend beaucoup plus de place sur l'hôte que l'original. Un instantané exploite la capacité d'instantané du dispositif de sauvegarde sous-jacent pour réaliser un conteneur en copie sur écriture faisant référence au premier. Les instantanés peuvent être créés depuis des conteneurs sauvegardés btrfs, LVM, zfs ou répertoire. Chaque dispositif de sauvegarde possède ses propres particularités - par exemple, les conteneurs LVM qui ne n'ont pas de partition en allocation fine ne peuvent prendre en charge des instantanés d'instantanés ; les conteneurs zfs avec instantanés ne peuvent être supprimés sans que tous les instantanés ne soient libérés ; Les conteneurs LVM doivent être planifiés plus soigneusement car le système de fichier sous-jacent pourrait ne pas prendre en charge l'accroissement ; btrfs ne souffre plus de ces défauts, mais subit une réduction de performance de fsync provoquant le ralentissement de dpkg et apt.

Les instantanés de conteneurs de répertoires empaquetés sont créés en utilisant le système de fichier superposé. Par exemple, un conteneur C1 avec privilèges sauvegardé en répertoire aura sont système de fichier root sous /var/lib/lxc/C1/rootfs. Un clone instantané de C1 nommé C2 sera démarré avec le système de fichier root de C1 monté en lecture seule sous /var/lib/lxc/C2/delta0. De manière significative, dans ce cas, C1 ne devrait pas être autorisé à exécuter ou être supprimé tant que C2 est exécuté. Il est conseillé, à la place, d'envisager C1 comme conteneur de base **canonical**, et d'utiliser uniquement ses instantanés.

Considérant un conteneur existant appelé C1, une copie peut en être créé en utilisant :

```
sudo lxc-clone -o C1 -n C2
```

Un instantané peut être créé en utilisant :

```
sudo lxc-clone -s -o C1 -n C2
```

Voir la page **lxc-clone** pour plus d'informations.

20.6.11.1. Instantanés

Afin de soutenir plus facilement l'utilisation de clones instantanés pour le développement de conteneurs répétitifs, LXC supporte les **instantanés**. En travaillant sur un conteneur C1, avant de faire un changement potentiellement dangereux ou difficilement réversible, vous pouvez en créer un instantané :

```
sudo lxc-snapshot -n C1
```

qui est un instantané clone appelé 'snap0' sous /var/lib/lxcsnaps ou $HOME/.local/share/lxcsnaps. Le prochain snapshot sera appelé 'snap1 », etc. instantanés existants peut être énumérée en utilisant **lxc-snapshot -L -n C1**, et un instantané peut être restauré - effacer le conteneur C1 actuelle - en utilisant la commande **lxc-snapshot snap1 -r -n C1**. Après la commande de restauration, l'instantané de snap1 continue d'exister, et de la C1 précédent est effacé et remplacé par l'instantané de snap1.

Les instantanés sont pris en charge pour les conteneurs btrfs, lvm, zfs et overlayfs. Si **lxc-snapshot** est lancé sur un conteneur de répertoire sauvegardé, une erreur sera générée et l'instantané sera créé en tant que clone copié. La raison en est que si l'utilisateur crée un instantané overlayfs d'un conteneur de répertoire sauvegardé, puis effectue des modifications dans le conteneur de répertoire sauvegardé, alors, les modifications du conteneur d'origine seront partiellement reproduites dans l'instantané. Si des instantanés d'un conteneur C1 de répertoire sauvegardé sont souhaités, alors un clone overlayfs de C1 doit être créé, C1 ne doit dès lors plus être modifié, et le clone overlayfs peut être modifié et servir de base d'instantanés à volonté, comme :

```
lxc-clone -s -o C1 -n C2
lxc-start -n C2 -d # réaliser quelques modifications
lxc-stop -n C2
lxc-snapshot -n C2
lxc-start -n C2 # etc.
```

20.6.11.2. Conteneurs éphémères

Alors que les instantanés sont utiles pour le développement incrémental d'images à plus long terme, les conteneurs éphémères utilisent des instantanés pour un usage rapide et unique. Considérons un conteneur

de base C1, vous pouvez démarrer un conteneur éphémère en utilisant la commande :

```
lxc-start-ephemeral -o C1
```

Le conteneur démarre comme un instantané de C1. Les instructions pour vous enregistrer dans le conteneur seront affichées dans la console. Après l'arrêt, le conteneur éphémère sera détruit. Veuillez voir la page de manuel lxc-start-ephemeral pour plus d'options.

20.6.12. Crochets de gestion du cycle de vie

Depuis Ubuntu 12.10, il est possible de définir des crochets à exécuter à des points spécifiques dans la vie d'un conteneur :

- Les crochets pré-démarrés sont lancés dans l'espace de nom de l'hôte avant la configuration des ttys, consoles ou montage du conteneur. Si plusieurs sont réalisés dans ce crochet, ils doivent être nettoyés dans la phase post-arrêt du crochet.
- Les crochets pré-montés sont lancés dans les espaces de nom du conteneur, mais avant le montage du système de fichier root. Les montages réalisés dans ce crochet seront nettoyés automatiquement lorsque le conteneur s'arrête.
- Les crochets de montage sont lancés après le montage des systèmes de fichier du conteneur, mais avant que le conteneur n'appelle **pivot_root** pour modifier son système de fichier root.
- Les crochets de démarrage sont lancés immédiatement avant l'exécution de l'initialisation du conteneur. Puisqu'ils sont exécutés après le pivotement dans le système de fichier du conteneur, la commande à exécuter doit être copiée dans le système de fichier du conteneur.
- Les crochets post-arrêt sont exécutés après l'arrêt du conteneur.

Si un crochet retourne une erreur, le lancement du conteneur sera annulé. Tout crochet **post-stop** sera néanmoins exécuté. Toute sortie générée par le script sera journalisée selon la priorité de débogage.

Veuillez consulter la page de manuel de lxc.container.conf pour le format de fichier de configuration avec lequel spécifier les crochets. Quelques modèles de crochets sont fournis avec le paquet lxc pour servir d'exemple d'écriture et d'utilisation de tels crochets.

20.6.13. Consoles

Les conteneurs ont un nombre configurable de consoles. Il en existe toujours une dans le /dev/console du conteneur. Elle est affichée sur le terminal à partir duquel vous avez exécuté **lxc-start**, à moins que l'option **-d** soit spécifiée. La sortie sur /dev/console peut être redirigée vers un fichier en utilisant l'option **-c console-file** pour **lxc-start**. Le nombre de consoles supplémentaires est spécifié par la variable **lxc.tty**, et généralement paramétré à 4. Ces consoles sont affichées sur /dev/ttyN (avec 1 <= N <= 4). Pour se connecter à la console 3 à partir de l'hôte, utilisez :

```
sudo lxc-console -n container -t 3
```

ou si l'option **-t N** n'est pas spécifiée, une console inutilisée sera automatiquement choisie. Pour quitter la console, utilisez la séquence d'échappement Ctrl-a q. Notez que cette séquence ne fonctionnera pas dans la console provenant de **lxc-start** sans l'option **-d**.

Chaque console de conteneur est en fait un pty Unix98 dans le montage pty de l'hôte (et non du client), monté avec lien sur les /dev/ttyN et /dev/console de l'invité. Par conséquent, si l'invité les démonte ou tente par ailleurs d'accéder au véritable périphérique **4:N** en mode caractère, il ne servira pas getty aux consoles

LXC. (Avec les paramètres par défaut, le conteneur ne sera pas en mesure d'accéder à ce périphérique en mode caractère et par conséquent, getty sera rejeté.) Cela peut facilement se produire lorsqu'un script de démarrage monte aveuglément un nouveau /dev.

20.6.14. Dépannage

20.6.14.1. Journal

Si quelque chose se passe mal lors du démarrage d'un conteneur, la première étape consisterait à obtenir la journalisation complète depuis LXC :

```
sudo lxc-start -n C1 -l trace -o debug.out
```

Ceci forcera lxc à se connecter au niveau le plus détaillé, **tracer**, et sortir les information du journal dans un fichier nommé « debug.out ». Si le fichier **debug.out** existe déjà, les nouvelles informations du journal y seront ajoutées.

20.6.14.2. Surveillance de l'état des conteneurs

Deux commandes sont disponibles pour surveiller les changements d'état de conteneurs. La commande **lxc-monitor** surveille un ou plusieurs conteneurs pour tout changement d'état. Il prend un nom de conteneur avec l'option **-n** comme toujours, mais dans ce cas, le nom du conteneur peut être une expression rationnelle POSIX pour permettre le suivi d'ensembles voulus de conteneurs. **lxc-monitor** continuera de fonctionner en affichant les changements des conteneurs. **lxc-wait** attend un changement d'état spécifique et quitte. Par exemple,

```
sudo lxc-monitor -n cont[0-5]*
```

afficherait tous les changements d'état de tout conteneurs correspondant à l'expression rationnelle listée, alors que

```
sudo lxc-wait -n cont1 -s 'STOPPED|FROZEN'
```

attendra jusqu'à ce que le conteneur cont1 passe à l'état ARRÊT ou à l'état GELÉ et ensuite se termine.

20.6.14.3. Joindre

Comme d'Ubuntu 14.04, il est possible d'attacher aux espaces de noms d'un conteneur. Le cas le plus simple est de simplement faire :

```
sudo lxc rattacher -n C1
```

qui débutera une coquille attachée aux espaces de noms de C1, ou, de manière efficace à l'intérieur du récipient. La fonctionnalité joindre est très flexible, ce qui permet la fixation à un sous-ensemble des espaces de noms du conteneur et le contexte de sécurité. Voir la page de manuel pour plus d'informations.

20.6.14.4. La verbosité des conteneurs

Si LXC complète le démarrage du conteneur, mais l'initialisation du conteneur ne parvient pas à remplir (par exemple, aucune invite de connexion est affiché), il peut être utile de demander verbosité supplémentaire du processus init. Pour un récipient parvenu, cela pourrait être :

sudo lxc-start -n C1 /sbin/init loglevel=debug

Vous pouvez également démarrer un tout programme différent à la place de init, par exemple :

```
sudo lxc-start -n C1 /bin/bash
sudo lxc-start -n C1 /bin/sleep 100
sudo lxc-start -n C1 /bin/cat /proc/1/status
```

20.6.15. API LXC

La plupart des fonctionnalités de LXC sont maintenant accessibles via une application de programmation d'interface (API) exportée par liblxc pour laquelle les liaisons sont disponibles en plusieurs langages, y compris Python, lua, rubis et go.

Voici un exemple utilisant les liaisons Python (qui sont disponibles dans le paquet **python3-lxc**) qui créent et démarrent un conteneur, puis attendent son arrêt :

```
# sudo python3
Python 3.2.3 (default, Aug 28 2012, 08:26:03)
[GCC 4.7.1 20120814 (prerelease)] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import lxc
__main__:1: Warning: The python-lxc API isn't yet stable and may change at any p
oint in the future.
>>> c=lxc.Container("C1")
>>> c.create("ubuntu")
True
>>> c.start()
True
>>> c.wait("STOPPED")
True
```

20.6.16. Sécurité

Un espace de nommage des identifiants des cartes de ressources. En ne fournissant pas un conteneur d'id avec laquelle faire référence à une ressource, la ressource peut être protégé. C'est la base de certains de la sécurité offerte aux utilisateurs de conteneurs. Par exemple, les espaces de noms CIB sont complètement isolés. Autres espaces de noms, cependant, ont diverses *fuites* qui allouent le privilège d'être exercée de façon inappropriée à partir d'un conteneur dans un autre conteneur ou depuis l'hôte.

Par défaut, les conteneurs sont LXC commencé sous une politique Apparmor de restreindre certaines actions. Les détails de l'intégration avec AppArmor lxc sont dans la section *20.6.9. Apparmor*. Les récipients non privilégiés vont plus loin en cartographie racine dans le conteneur à un ID utilisateur non privilégié hôte.

Cela empêche l'accès à /proc et /sys fichiers représentant des ressources d'accueil, ainsi que tous les autres fichiers appartenant à root sur l'hôte.

20.6.16.1. Appels système exploitables

C'est une caractéristique de base des conteneurs que de partager un noyau avec l'hôte. Par conséquent, si le noyau contient des appels système exploitables, le conteneur peut les exploiter aussi. Une fois que le conteneur contrôle le noyau, il peut contrôler entièrement toute ressource connue de l'hôte.

Depuis Ubuntu 12.10 (Quantal), un conteneur peut également être limitée par un filtre seccomp. Seccomp est une option pour nouveau noyau qui filtre les appels systèmes qui peuvent être utilisés par une tâche et ses enfants. Bien qu'une amélioration et la simplification de la gestion des politiques soient prévues dans un avenir proche, la politique actuelle consiste en une liste blanche simple de numéros d'appel système. Le fichier de stratégie commence par un numéro de version (qui doit être 1) sur la première ligne et un type de stratégie (qui doit être 'liste blanche') sur la deuxième ligne. Elle est suivie par une liste de numéros, un par ligne.

En général, pour exécuter un conteneur de distribution intégrale, un grand nombre d'appels système sera nécessaire. Toutefois, pour les conteneurs d'application, il peut être possible de réduire le nombre d'appels système disponible à seulement quelques-uns. Même pour les conteneurs de système en exécution, une augmentation de sécurité de distribution complète peut être obtenue, par exemple, en supprimant les appels système à compatibilité 32 bits, dans un conteneur 64 bits. Voir la page de manuel **lxc.container.conf** pour savoir comment configurer un conteneur pour utiliser seccomp. Par défaut, aucune politique de seccomp n'est chargée.

20.6.17. Ressources

L'article de DeveloperWorks sur LXC : **Linux container tools** était une introduction rapide à l'usage des conteneurs : https://www.ibm.com/developerworks/linux/library/l-lxc-containers/ .

Le **Livre de recettes des Conteneurs Sécurisés** (Secure Linux Containers Cookbook) a fait la démonstration de l'utilisation de modules de sécurité pour faire des conteneurs plus sûrs : http://www.ibm.com/developerworks/linux/library/l-lxc-security/index.html .

Les pages de manuel référencées ci-dessus peuvent être trouvées sur :

```
Capacités : http://manpages.ubuntu.com/manpages/en/man7/capabilities.7.html
lxc.conf : http://manpages.ubuntu.com/manpages/en/man5/lxc.conf.5.html .
```

Le projet LXC générique est hébergé à l'adresse : http://linuxcontainers.org .

Les question de sécurité de LXC sont répertoriées et discutées sur la page wiki de la sécurité de LXC : http://wiki.ubuntu.com/LxcSecurity .

Pour en savoir plus sur les espaces de noms dans Linux, voir: S. Bhattiprolu, EW Biederman, SE Hallyn, et D. Lezcano. Virtual Servers and Check- point/Restart in Mainstream Linux. SIGOPS Operating Systems Review, 42(5), 2008.

Chapitre 21. Les Groupes de contrôle (cgroups)

Les Groupes de contrôle (cgroups) forment un mécanisme de noyau pour le regroupement, le suivi et la limitation de l'utilisation de tâches de ressource. L'interface d'administration fournie par le noyau est présentée via un système de fichiers virtuel. Des outils d'administration de groupes de contrôle de haut niveau ont été développés, y compris libcgroup et lmctfy. En outre, il y a des conseils sur http//:www.freedesktop.org pour savoir comment les applications peuvent coopérer au mieux en utilisant l'interface de système de fichiers de groupes de contrôle (voir Ressources).

Comme pour Ubuntu 14.04, le gestionnaire de groupes de contrôle (cgmanager) est disponible comme une autre interface d'administration de groupes de contrôle. Son but est de répondre aux demandes **dbus** de tout utilisateur, lui permettant d'administrer uniquement les groupes de contrôle qui lui ont été délégués.

Le paragraphe *1. Vue d'ensemble* décrira plus en détail les groupes de contrôle. Le paragraphe *2. Système de fichiers* décrira l'interface de longue date de système de fichiers de groupes de contrôle. Le paragraphe *4. Gestionnaire (cmanager)* décrira le gestionnaire de groupes de contrôle cmanager.

21.1. Vue d'ensemble

Les groupes de contrôle représentent la caractéristique généralisée pour le regroupement des tâches. Le suivi et les limites des ressources réelles sont mises en œuvre par les sous-systèmes. Une **hiérarchie** est un ensemble de sous-systèmes montés ensemble. Par exemple, si la mémoire et des sous-systèmes de périphériques sont montés ensemble sous /sys/fs/cgroups/set1, alors n'importe quelle tâche qui est en /child1 (/set1 ? NDLT) sera soumise aux limites correspondantes des deux sous-systèmes.

Chaque ensemble de sous-systèmes montés constitue une **hiérarchie**. À quelques exceptions près, les groupes de contrôle qui sont les enfants de /child1 seront soumises à toutes les limites placées sur /child1, et leur utilisation de ressource sera comptabilisée à /child1.

Les sous-systèmes existants comprennent :

- **cpusets** : facilite l'attribution d'un ensemble de CPUs et de nœuds de mémoire à un groupe de contrôle. Les tâches dans un groupe de contrôle **cpuset** ne peuvent être programmées que sur les processeurs affectés à ce **cpuset**.
- **blkio** : limite les E/S par bloc de groupes de contrôle.
- **cpuacct**: fournit la comptabilité de l'utilisation du processeur par groupe de contrôle.
- **devices** : contrôle la capacité des tâches pour créer ou disposer des nœuds en utilisant soit une liste noire ou une liste blanche.
- **freezer** : fournit un moyen de **geler** et **dégeler** des groupes de contrôle entiers. Les tâches dans le groupe de contrôle ne seront pas programmées tant qu'elles seront gelées : **frozen**.
- **hugetlb** : facilite l'utilisation de la limitation de hugetlb par groupe de contrôle.
- **memory** : alloue de la mémoire, de la mémoire du noyau, et de l'utilisation du swap afin d'être suivie et limitée.
- **net_cls** : fournit une interface pour le marquage des paquets basée sur le groupe de contrôle de l'expéditeur. Ces balises peuvent ensuite être utilisés par **tc** (contrôleur de circulation) pour attribuer des priorités.
- **net_prio** : permet le réglage de la priorité du trafic réseau par groupes de contrôle.
- **cpu** : active le réglage des préférences de planification par groupes de contrôle.
- **perf_event** : active le mode par CPU pour surveiller seulement les discussions dans certains groupes de contrôle.

En outre, des groupes de contrôle nommés peuvent être créés sans aucun sous-système lié pour améliorer le suivi de processus. A titre d'exemple, systemd le fait pour suivre des services et des sessions utilisateur.

21.2. Système de fichiers

Une hiérarchie est créée par le montage d'une instance du système de fichier de groupes de contrôle avec chacun des sous-systèmes souhaités énumérés comme une option de montage. Par exemple :

```
mount -t cgroup -o devices,memory,freezer cgroup /cgroup1
```

instancierait une hiérarchie avec les périphériques et la mémoire, du groupe de contrôle, montés ensemble. Un groupe de contrôle enfant /child1 peut être créé en utilisant **mkdir** :

```
mkdir /cgroup1/child1
```

et des tâches peuvent être déplacées dans le nouveau groupe de contrôle enfant en écrivant leurs identifiants de processus dans le fichier **tasks** ou **cgroup.procs** :

```
sleep 100 &
echo $! > /cgroup1/child1/cgroup.procs
```

L'autre administration est réalisée par des fichiers dans les répertoires du groupe de contrôle. Par exemple, pour geler toutes les tâches dans child1 :

```
echo FROZEN > /cgroup1/child1/freezer.state
```

Une grande quantité d'informations sur les groupes de contrôle et ses sous-systèmes peut être trouvée dans le répertoire de documentation des groupes de contrôle dans l'arborescence source du noyau (voir Ressources).

21.3. Délégation

Les fichiers et répertoires des groupes de contrôle peuvent être détenus par des utilisateurs qui ne sont pas administrateurs, permettant la délégation de l'administration des groupes de contrôle. En général, le noyau impose des contraintes hiérarchiques aux limitations, de sorte que, par exemple, si des périphériques des groupes de contrôle /child1 ne peuvent accéder à un lecteur de disque, alors /child1/child2 ne peut pas se donner ces droits.

A partir d'Ubuntu 14.04, les utilisateurs sont automatiquement placés dans un ensemble de groupes de contrôles dont ils sont propriétaires, leur permettant en toute sécurité de maîtriser leurs propres tâches en utilisant des groupes de contrôles enfants. On compte sur cette fonctionnalité, par exemple, pour la création de conteneur sans privilège dans lxc.

21.4. Gestionnaire (cmanager)

Le gestionnaire des groupes de contrôle (cgmanager) fournit un service D-Bus permettant aux programmes et aux utilisateurs d'administrer des groupes de contrôles sans avoir une connaissance directe ou l'accès au système de fichiers du groupe de contrôle. Pour les demandes depuis des tâches, dans les mêmes espaces de noms que le gestionnaire, celui-ci peut directement effectuer les contrôles de sécurité nécessaires pour assurer que les demandes sont légitimes. Pour les autres demandes - telles que celles d'une tâche dans un conteneur - des demandes D-Bus améliorées doivent être faites, où les identifiants de processus, d'utilisateur et de groupe sont passés comme SCM_CREDENTIALS, de sorte que le noyau cartographie les identifiants à leurs valeurs globales dans l'hôte.

Pour faciliter l'utilisation d'appels D-Bus simples par tous les utilisateurs, un **proxy de gestionnaire de groupes de contrôle** (**cgproxy**) est automatiquement démarré lorsqu'il est dans un conteneur. Le proxy accepte des demandes D-Bus standard générées par des tâches dans les mêmes espaces de noms où il se situe, et les convertit en demandes D-Bus SCM-améliorées qu'il transmet au cgmanager.

Un exemple simple de création d'un nouveau groupe de contrôle dans lequel exécuter une compilation utilisant intensivement le processeur ressemblerait à :

```
cgm create cpuset build1
cgm movepid cpuset build1 $$
cgm setvalue cpuset build1 cpuset.cpus 1
make
```

21.5. Ressources

Les pages de manuel référencées ci-dessous, peuvent être trouvées à l'adresse suivante :

cgm : http://manpages.ubuntu.com/manpages/en/man8/cgm.1.html

cgconfig.conf : http://manpages.ubuntu.com/manpages/en/man5/cgconfig.conf.5.html

cgmanager : http://manpages.ubuntu.com/manpages/en/man8/cgmanager.8.html

cgproxy : http://manpages.ubuntu.com/manpages/en/man8/cgproxy.8.html .

Le projet générique de cgmanager est hébergé sur **linuxcontainers.org** :
http://cgmanager.linuxcontainers.org .

La page de documentation générique du noyau sur les groupes de contrôles peut être visualisée à l'adresse : https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/tree/Documentation/cgroups .

Les lignes directrices de l'utilisation du groupes de contrôle de freedesktop.org peuvent être visionnées à l'adresse : http://www.freedesktop.org/wiki/Software/systemd/PaxControlGroups/ .

Chapitre 22. Mise en grappe (Clustering)

22.1. DRBD

Un périphérique en mode bloc répliqué et distribué (**Distributed Replicated Block Device** ou DRBD) met en miroir des périphériques en mode bloc entre plusieurs hôtes. La réplication est transparente pour les autres applications sur les systèmes hôtes. N'importe quel périphérique en mode bloc (disque dur, partitions, périphériques RAID, volumes logiques, etc.) peut être mis en miroir.

Pour commencer à utiliser **drbd**, installez d'abord les paquets nécessaires. Dans un terminal, écrivez :

```
sudo apt install drbd8-utils
```

Si vous utilisez le **noyau virtuel** comme une partie d'une machine virtuelle, vous devrez compiler manuellement le module **drbd**. Il serait plus simple d'installer le paquet **linux-server** dans la machine virtuelle.

Cette section décrit le paramétrage de **drbd** pour répliquer une partition /srv distincte, avec un système de fichiers **ext3**, entre deux hôtes. La taille de partition n'est pas importante, mais les deux partitions doivent être de la même taille.

22.1.1. Configuration

Les deux hôtes dans cet exemple s'appellent **drbd01** et **drbd02**. Ils auront besoin d'avoir la résolution d'adresse configurée soit par DNS, soit à l'aide du fichier /etc/hosts. Consultez le *Chapitre 8. Service de nom de domaine (DNS)* pour de plus amples informations.

- Pour configurer **drbd**, modifiez sur le premier hôte le fichier /etc/drbd.conf :

```
global { usage-count no; }
common { syncer { rate 100M; } }
resource r0 {
        protocol C;
        startup {
                wfc-timeout 15;
                degr-wfc-timeout 60;
        }
        net {
                cram-hmac-alg sha1;
                shared-secret "secret";
        }
        on drbd01 {
                device /dev/drbd0;
                disk /dev/sdb1;
                address 192.168.0.1:7788;
                meta-disk internal;
        }
        on drbd02 {
                device /dev/drbd0;
                disk /dev/sdb1;
```

```
                address 192.168.0.2:7788;
                meta-disk internal;
        }
}
```

Beaucoup d'autres options sont disponibles dans le fichier /etc/drbd.conf mais leur valeur par défaut seront suffisantes pour cet exemple.

- Copiez maintenant /etc/drbd.conf vers le deuxième hôte :

```
scp /etc/drbd.conf drbd02:~
```

- Déplacez ensuite le fichier dans /etc sur **drbd02** :

```
sudo mv drbd.conf /etc/
```

- Initialisez maintenant les méta données de stockage en utilisant **drbdadm**. Exécutez la commande suivante sur les deux serveurs :

```
sudo drbdadm create-md r0
```

- Lancez ensuite le démon **drbd** sur les deux hôtes :

```
sudo systemctl start drbd.service
```

- Sur l'hôte **drbd01**, ou celui que vous souhaitez définir comme hôte primaire, saisissez :

```
sudo drbdadm -- --overwrite-data-of-peer primary all
```

- Après l'exécution de la commande ci-dessus, les données commenceront à se synchroniser avec l'hôte secondaire. Pour suivre la progression, saisissez la commande suivante dans **drbd02** :

```
watch -n1 cat /proc/drbd
```

  Appuyez sur **Ctrl+c** pour arrêter la commande « watch ».

- Pour finir, ajoutez un système de fichier à /dev/drbd0 et montez-le :

```
sudo mkfs.ext3 /dev/drbd0
sudo mount /dev/drbd0 /srv
```

22.1.2. Vérification

Pour vérifier que les données se synchronisent réellement entre les deux hôtes, copiez quelques fichiers de **drbd01**, l'hôte primaire, sur /srv :

```
sudo cp -r /etc/default /srv
```

Démontez ensuite /srv :

```
sudo umount /srv
```

Rétrogradez le serveur **primaire** au rôle **secondaire** :

```
sudo drbdadm secondary r0
```

Maintenant, sur le serveur **secondaire**, le **promouvoir** au rôle **principal** :

```
sudo drbdadm primary r0
```

Enfin, montez la partition :

```
sudo mount /dev/drbd0 /srv
```

Avec **ls**, vous devriez voir le fichier /srv/default copié depuis l'ancien hôte **primaire drbd01**.

22.1.3. Références

Pour plus d'informations sur **DRBD**, consultez le **site Web DRBD** : http://www.drbd.org/ .

La **page de man de drbd.conf** contient des détails sur les options qui ne sont couvertes par ce guide : http://manpages.ubuntu.com/manpages/xenial/en/man5/drbd.conf.5.html

Également, voyez **la page de man de drbdadm** : http://manpages.ubuntu.com/manpages/xenial/en/man8/drbdadm.8.html .

La page **du wiki anglophone d'Ubuntu sur DRBD** contient également des informations complémentaires : https://help.ubuntu.com/community/DRBD .

Chapitre 23. Réseau privé virtuel (VPN)

OpenVPN est une solution de réseau privé virtuel (VPN - Virtual Private Networking) disponible dans les dépôts Ubuntu. Il est flexible, fiable et sécurisé. Il appartient à la famille des piles VPN SSL/TLS (différentes des VNP IPSec). Ce chapitre traite de l’installation et de la configuration de OpenVPN pour créer un VPN.

23.1. OpenVPN

Si vous voulez plus que de simples clés pré-partagées OpenVPN rend la configuration facile et emploie une Infrastructure à Clé Publique (Public Key Infrastructure : PKI) pour utiliser des certificats SSL/TLS à des fins d'authentification et un échange de clés entre le serveur VPN et les clients. OpenVPN peut être utilisé en mode VPN route ou passerelle et il peut être configuré pour utiliser UDP ou TCP. Le numéro de port peut être également configuré, mais le port 1194 est l'officiel. Et il utilise seulement ce port pour toutes les communications. Les implémentations du client VPN sont disponibles pour presque toutes les distributions Linux, OS X, Windows et les routeurs WLAN basés sur OpenWRT.

23.1.1. Installation du serveur

Pour installer openvpn, exécutez la commande suivante dans un terminal :

```
sudo apt install openvpn easy-rsa
```

23.1.2. Configuration d'une infrastructure à clés publiques

La première étape dans la construction d'une configuration OpenVPN est d'établir une Infrastructure à Clé Publique PKI. La PKI est composée de :

- un certificat distinct (également connu sous le nom de clé publique) et la clé privée pour le serveur et chaque client et
- le certificat de l'Autorité de Certification maître (Certificate Authority : CA) et la clé qui est utilisée pour identifier les certificats serveurs et clients.

OpenVPN supporte l'authentification bidirectionnelle basée sur les certificats, ce qui signifie que le client doit authentifier le certificat du serveur et le serveur doit authentifier le certificat client avant que la confiance mutuelle soit établie.

Tant le serveur que le client authentifieront l'autre en commençant par vérifier que le certificat présenté a été signé par l'Autorité de Certification maître (CA), et ensuite en testant les informations dans l'en-tête du certificat maintenant authentifié, comme le nom commun du certificat ou le type de certificat (client ou serveur).

23.1.2.1. Configuration de l'Autorité de Certification (CA)

Pour configurer votre propre Autorité de Certification (CA) et générer des certificats et des clés pour un serveur OpenVPN et clients multiples, copiez d'abord le répertoire easy-rsa dans /etc/openvpn. Cela vous permettra de vous assurer que toutes les modifications apportées aux scripts ne seront pas perdues lorsque le paquet sera mis à jour. Depuis une console mettez vous en super-utilisateur et :

```
mkdir /etc/openvpn/easy-rsa/
cp -r /usr/share/easy-rsa/* /etc/openvpn/easy-rsa/
```

Ensuite, modifiez /etc/openvpn/easy-rsa/vars en ajustant les valeurs pour votre environnement :

```
export KEY_COUNTRY="US"
export KEY_PROVINCE="NC"
export KEY_CITY="Winston-Salem"
export KEY_ORG="Example Company"
export KEY_EMAIL="steve@example.com"
export KEY_CN=MyVPN
export KEY_NAME=MyVPN
export KEY_OU=MyVPN
```

Saisissez ce qui suit pour générer le certificat maître Certificate Authority (CA) et une clé :

```
cd /etc/openvpn/easy-rsa/
source vars
./clean-all
./build-ca
```

23.1.2.2. Certificats du serveur

Ensuite, nous allons générer un certificat et une clé privée pour le serveur :

```
./build-key-server myservername
```

Comme dans l'étape précédente, la majorité des paramètres peuvent être définis par défaut.

Deux autres requêtes nécessitent des réponses positives :

- "Sign the certificate? [y/n]" : « Signez-vous le certificat ? [o/n] »
- "1 out of 1 certificate requests certified, commit? [y/n]" : « 1 de 1 certifié des demandes de certificat, validez-vous ? [o/n] »

Des paramètres Diffie Hellman doivent être générés pour le serveur OpenVPN :

```
./build-dh
```

Tous les certificats et les clés ont été générés dans le sous-répertoire keys/. La pratique courante est de les copier dans /etc/openvpn/ :

```
cd keys/
cp myservername.crt myservername.key ca.crt dh2048.pem /etc/openvpn/
```

23.1.2.3. Certificats du client

Le client VPN a également besoin d'un certificat pour s'authentifier auprès du serveur. Habituellement, vous créez un certificat différent pour chaque client. Pour créer le certificat, tapez ce qui suit dans un terminal avec les droits super-utilisateur :

```
cd /etc/openvpn/easy-rsa/
source vars
./build-key client1
```

Copiez les fichiers suivants sur le client à l'aide d'une méthode sécurisée :

```
/etc/openvpn/ca.crt
/etc/openvpn/easy-rsa/keys/client1.crt
/etc/openvpn/easy-rsa/keys/client1.key
```

Comme les certificats clients et les clés ne sont nécessaires que sur la machine client, vous devez les supprimer du serveur.

23.1.3. Configuration d'un serveur simple

Avec votre installation de OpenVPN, vous avez obtenu ces exemples de fichiers de configuration (et beaucoup plus si vous vérifiez) :

```
root@server:/# ls -l /usr/share/doc/openvpn/examples/sample-config-files/
total 68
-rw-r--r-- 1 root root 3427 2011-07-04 15:09 client.conf
-rw-r--r-- 1 root root 4141 2011-07-04 15:09 server.conf.gz
```

Commencez par copier et décompresser server.conf.gz vers /etc/openvpn/server.conf.

```
sudo cp /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz \
/etc/openvpn/
sudo gzip -d /etc/openvpn/server.conf.gz
```

Modifiez le fichier /etc/openvpn/server.conf pour vous assurer que les lignes suivantes pointent vers les certificats et les clés que vous avez créés dans la section ci-dessus.

```
ca ca.crt
cert myservername.crt
key myservername.key
dh dh2048.pem
```

Éditez /etc/sysctl.conf et supprimez la ligne suivante pour activer le routage IP :

```
#net.ipv4.ip_forward=1
```

Rechargez ensuite sysctl :

```
sudo sysctl -p /etc/sysctl.conf
```

Il s'agit du minimum à configurer pour obtenir un serveur OpenVPN fonctionnel. Vous pouvez utiliser tous les paramètres par défaut dans le fichier d'exemple server.conf . Démarrez maintenant le serveur. Vous trouverez des messages d'erreur et de journalisation dans votre journal via. En fonction de ce que vous recherchez :

sudo journalctl -xe

Si vous avez démarré un service modélisé openvpn@server, vous pouvez filtrer cette source de message en particulier avec :

sudo journalctl --identifier ovpn-server

Soyez attentifs à ce que "service openvpn start" ne démarre pas le openvpn que vous venez juste de définir. Openvpn utilise des tâches systemd normalisées, openvpn@CONFIGFILENAME. Ainsi, par exemple, si votre fichier de configuration est "server.conf", votre service est nommé openvpn@server. Vous pouvez lancer toute sorte de service et de commandes systemctl telles que start/stop/enable/disable/preset vers un service normalisé comme openvpn@server.

```
ubuntu@testopenvpn-server:~$ sudo service openvpn@server start

ubuntu@testopenvpn-server:~$ sudo service openvpn@server status
. openvpn@server.service - OpenVPN connection to server
Loaded: loaded (/lib/systemd/system/openvpn@.service; enabled; vendor preset: enabled)
      Active: active (running) since Tue 2016-04-12 08:51:14 UTC; 1s ago
        Docs: man:openvpn(8)
              https://community.openvpn.net/openvpn/wiki/Openvpn23ManPage
              https://community.openvpn.net/openvpn/wiki/HOWTO
     Process: 1573 ExecStart=/usr/sbin/openvpn --daemon ovpn-%i --status
/run/openvpn/%i.status 10 --cd /etc/openvpn --script-security 2 --config
/etc/openvpn/%i.conf --writep
    Main PID: 1575 (openvpn)
       Tasks: 1 (limit: 512)
      CGroup: /system.slice/system-openvpn.slice/openvpn@server.service
              |-1575 /usr/sbin/openvpn --daemon ovpn-server --status
/run/openvpn/server.status 10 --cd /etc/openvpn --script-security 2 --config
/etc/openvpn/server.conf --wr

Apr 12 08:51:14 testopenvpn-server ovpn-server[1575]: /sbin/ip route add 10.8.0.0/24
via 10.8.0.2
Apr 12 08:51:14 testopenvpn-server ovpn-server[1575]: UDPv4 link local (bound): [undef]
Apr 12 08:51:14 testopenvpn-server ovpn-server[1575]: UDPv4 link remote: [undef]
Apr 12 08:51:14 testopenvpn-server ovpn-server[1575]: MULTI: multi_init called, r=256
v=256
Apr 12 08:51:14 testopenvpn-server ovpn-server[1575]: IFCONFIG POOL: base=10.8.0.4
size=62, ipv6=0
Apr 12 08:51:14 testopenvpn-server ovpn-server[1575]: ifconfig_pool_read(),
in='client1,10.8.0.4', TODO: IPv6
Apr 12 08:51:14 testopenvpn-server ovpn-server[1575]: succeeded -> ifconfig_pool_set()
Apr 12 08:51:14 testopenvpn-server ovpn-server[1575]: IFCONFIG POOL LIST
Apr 12 08:51:14 testopenvpn-server ovpn-server[1575]: client1,10.8.0.4
Apr 12 08:51:14 testopenvpn-server ovpn-server[1575]: Initialization Sequence Completed
```

Vous pouvez activer/désactiver divers services openvpn sur un système, mais vous pouvez aussi laisser Ubuntu réaliser cette louche târde. Il existe une configuration pour AUTOSTART dans /etc/default/openvpn. Les valeurs autorisées sont "all", "none" ou une liste de noms des VPNs séparés par des espaces. Si elle est vide, "all" est présumée. Le nom VPN se réfère au nom de fichier de configuration. C'est à dire que "home" serait /etc/openvpn/home.conf. Si vous exécutiez systemd, le changement de cette variable va nécessiter l'exécution de "systemctl daemon-reload" suivie d'un redémarrage du service openvpn (si vous

avez supprimé des entrées, vous aurez à les stopper manuellement). Après "systemctl daemon-reload" un redémarrage du openvon "générique" redémarrera tous les services dépendants que le générateur avait créé dans /lib/systemd/system-generators/openvpn-generator pour vos fichiers de configuration lorsque vous aviez appelé daemon-reload.

Il s'agit du minimum à configurer pour obtenir un serveur OpenVPN fonctionnel. Vous pouvez utiliser tous les paramètres par défaut dans le fichier d'exemples server.conf . Démarrez maintenant le serveur. Vous trouverez des messages d'erreur et de journalisation dans votre journal.

Maintenant, vérifiez si OpenVPN a créé une interface tun0 :

```
root@server:/etc/openvpn# ifconfig tun0
tun0      Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:10.8.0.1 P-t-P:10.8.0.2 Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1500 Metric:1
[…]
```

23.1.4. Configuration du client simple

Il existe différentes variantes de clients OpenVPNavec ou sans interface graphique. Vous trouverez plus de détails dans une prochaine section. Pour le moment, nous utilisons le client OpenVPN pour Ubuntu, qui est le même exécutable que le serveur. Vous devez donc également installer le paquet openvpn sur la machine client :

```
sudo apt install openvpn
```

Cette fois, copiez le fichier de configuration d'exemple client.conf dans /etc/openvpn/ :

```
sudo cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf \
/etc/openvpn/
```

Copiez les clés du client et le certificat du CA que vous avez créés dans la section ci-dessus dans, par exemple, /etc/openvpn/ et modifiez /etc/openvpn/client.conf pour vous assurer que les lignes suivantes pointent bien vers ces fichiers. Si vos fichiers se trouvent dans /etc/openvpn/ vous pouvez omettre le chemin.

```
ca ca.crt
cert client1.crt
key client1.key
```

Et vous devez au moins préciser le nom ou l'adresse du serveur OpenVPN. Assurez-vous que le mot-clé client est dans la configuration. C'est ce qui permet le mode client.

```
client
remote vpnserver.example.com 1194
```

De plus, assurez-vous de bien spécifier les noms des fichiers des clés copiés depuis le serveur.

```
ca ca.crt
cert client1.crt
key client1.key
```

Maintenant, lancez le client OpenVPN:

```
ubuntu@testopenvpn-client:~$ sudo service openvpn@client start
ubuntu@testopenvpn-client:~$ sudo service openvpn@client status
. openvpn@client.service - OpenVPN connection to client
   Loaded: loaded (/lib/systemd/system/openvpn@.service; disabled; vendor preset:
enabled)
   Active: active (running) since Tue 2016-04-12 08:50:50 UTC; 3s ago
     Docs: man:openvpn(8)
           https://community.openvpn.net/openvpn/wiki/Openvpn23ManPage
           https://community.openvpn.net/openvpn/wiki/HOWTO
 Process: 1677 ExecStart=/usr/sbin/openvpn --daemon ovpn-%i --status
/run/openvpn/%i.status 10 --cd /etc/openvpn --script-security 2 --config
/etc/openvpn/%i.conf --writep
Main PID: 1679 (openvpn)
   Tasks: 1 (limit: 512)
  CGroup: /system.slice/system-openvpn.slice/openvpn@client.service
          |-1679 /usr/sbin/openvpn --daemon ovpn-client --status
/run/openvpn/client.status 10 --cd /etc/openvpn --script-security 2 --config
/etc/openvpn/client.conf --wr

Apr 12 08:50:52 testopenvpn-client ovpn-client[1679]: OPTIONS IMPORT: --ifconfig/up
options modified
Apr 12 08:50:52 testopenvpn-client ovpn-client[1679]: OPTIONS IMPORT: route options
modified
Apr 12 08:50:52 testopenvpn-client ovpn-client[1679]: ROUTE_GATEWAY
192.168.122.1/255.255.255.0 IFACE=eth0 HWADDR=52:54:00:89:ca:89
Apr 12 08:50:52 testopenvpn-client ovpn-client[1679]: TUN/TAP device tun0 opened
Apr 12 08:50:52 testopenvpn-client ovpn-client[1679]: TUN/TAP TX queue length set to
100
Apr 12 08:50:52 testopenvpn-client ovpn-client[1679]: do_ifconfig, tt->ipv6=0, tt-
>did_ifconfig_ipv6_setup=0
Apr 12 08:50:52 testopenvpn-client ovpn-client[1679]: /sbin/ip link set dev tun0 up mtu
1500
Apr 12 08:50:52 testopenvpn-client ovpn-client[1679]: /sbin/ip addr add dev tun0 local
10.8.0.6 peer 10.8.0.5
Apr 12 08:50:52 testopenvpn-client ovpn-client[1679]: /sbin/ip route add 10.8.0.1/32
via 10.8.0.5
Apr 12 08:50:52 testopenvpn-client ovpn-client[1679]: Initialization Sequence Completed
```

Vérifiez si cela a créé une interface tun0 :

```
root@client:/etc/openvpn# ifconfig tun0
tun0      Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:10.8.0.6 P-t-P:10.8.0.5 Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1500 Metric:1
```

Vérifiez si vous pouvez faire un ping sur le serveur OpenVPN :

```
root@client:/etc/openvpn# ping 10.8.0.1
PING 10.8.0.1 (10.8.0.1) 56(84) bytes of data.
64 bytes from 10.8.0.1: icmp_req=1 ttl=64 time=0.920 ms
```

> Le serveur OpenVPN utilise toujours la première adresse IP utilisable dans le réseau du client et seulement cette adresse peut être atteinte par les requêtes de la commande ping. Par exemple, si vous avez configuré le masque réseau du client en /24, l'adresse **.1** sera utilisée. L'adresse P-t-P (Peer to Peer, Pair à Pair) que vous voyez dans la sortie ifconfig ci-dessous ne répond généralement pas aux requêtes de ping.

Vérifiez vos itinéraires :

```
root@client:/etc/openvpn# netstat -rn
Kernel IP routing table
Destination      Gateway          Genmask          Flags MSS   Window irtt Iface
10.8.0.5         0.0.0.0          255.255.255.255  UH    0     0      0    tun0
10.8.0.1         10.8.0.5         255.255.255.255  UGH   0     0      0    tun0
192.168.42.0     0.0.0.0          255.255.255.0    U     0     0      0    eth0
0.0.0.0          192.168.42.1     0.0.0.0          UG    0     0      0    eth0
```

23.1.5. Premier dépannage

Si ce qui précède ne fonctionne pas pour vous, vérifiez ceci :

- Vérifiez votre journal, par exemple journalctl --identifier ovpn-server (pour server.conf)
- Vérifiez si vous avez correctement spécifié les noms des fichiers des clés dans client.conf et server.conf.
- Est-ce que le client peut se connecter au serveur ? Peut-être qu'un firewall bloque l'accès ? Vérifiez le journal sur le serveur.
- Client et serveur doivent utiliser le même protocole et port, par exemple, le port UDP 1194, voir l'option de configuration port et proto.
- Client et serveur doivent utiliser la même configuration en ce qui concerne la compression, voir l'option comp-lzo config.
- Le client et le serveur doivent utiliser la même configuration pour ce qui est du mode pontage ou routage, voir les options de configuration serveur ou pont de serveur.

23.1.6. Configuration avancée

23.1.6.1 Configuration de routage VPN avancée sur le serveur

Ce qui précède est un réseau privé virtuel (VPN) fonctionnel très simple. Le client peut accéder à des services sur le serveur VPN via un tunnel crypté. Si vous voulez atteindre plus de serveurs ou quoi que ce soit dans d'autres réseaux, créez certains routages aux clients. Par exemple, si votre réseau d'entreprise peut se résumer au réseau 192.168.0.0/16, vous pouvez appuyer sur cette voie pour les clients. Mais vous devrez également modifier le routage pour le retour - vos serveurs ont besoin de savoir la routage vers le client VPN-réseau.

Ou bien vous pouvez donner une passerelle par défaut à tous les clients pour envoyer d'abord tout leur trafic Internet vers la passerelle VPN, et de là, via le pare-feu d'entreprise vers Internet. Cette section vous montre quelques options possibles.

Forcer les routes du client pour l'autoriser à accéder aux autres sous-réseaux privés derrière le serveur. Souvenez vous que ces sous-réseaux auront également besoin de router le pool d'adresses du client OpenVPN (10.8.0.0/24) jusqu'au serveur OpenVPN.

```
push "route 10.0.0.0 255.0.0.0"
```

Si activée, cette directive permettra de configurer tous les clients pour que leur passerelle par défaut emprunte le VPN, entraînant tout le trafic IP comme la navigation web ou la résolution DNS à passer par le

VPN (le serveur OpenVPN ou votre pare-feu central peut avoir besoin d'ajouter une règle NAT pour l'interface TUN/TAP afin que cela fonctionne correctement).

```
push "redirect-gateway def1 bypass-dhcp"
```

Configure le mode serveur et fournis un sous-réseau VPN pour que OpenVPN puisse récupérer les adresses des clients VPN. Le serveur aura comme adresse 10.8.0.1, les adresses restantes seront mises à disposition pour les clients. Chaque client pourra contacter le serveur à l'adresse 10.8.0.1.

```
Server 10.8.0.0 255.255.255.0
```

Maintenez un enregistrement d'association des clients aux d'adresses IP virtuelles dans ce fichier. Si OpenVPN tombe en panne ou est redémarré, la reconnexion des clients pourra se faire à la même adresse IP virtuelle du pool d'adresses qui a été précédemment attribué.

```
ifconfig-pool-persist ipp.txt
```

Poussez les serveurs DNS au client.

```
push "dhcp-option DNS 10.0.0.2"
push "dhcp-option DNS 10.1.0.2"
```

Permettez la communication client à client.

```
Client-to-client
```

Activez la compression sur le lien VPN.

```
Comp-lzo
```

La directive **keepalive** réalise l'envoi de messages similaires à un ping de part et d'autre du lien de telle sorte que chaque extrémité sache lorsque l'autre est tombée. Avec un ping chaque seconde, il est présumé que le pair distant est tombé si aucun ping n'est reçu dans un intervalle de 3 secondes.

```
keepalive 1 3
```

C'est une bonne idée de réduire les privilèges du démon OpenVPN après l'initialisation.

```
user nobody
group nogroup
```

OpenVPN 2.0 inclut une fonctionnalité qui permet au serveur OpenVPN d'obtenir de manière sécurisée un nom d'utilisateur et un mot de passe d'un client qui tente de se connecter,et d'utiliser ces informations comme base pour l'authentification du client. Pour utiliser cette méthode d'authentification, vous devez d'abord ajouter la directive **auth-user-pass** à la configuration du client. Cela donnera l'instruction au client OpenVPN de demander à l'utilisateur son identifiant et son mot de passe, pour les transmettre au serveur via le canal TLS sécurisé.

```
# client config!
auth-user-pass
```

Ceci indique au serveur OpenVPN de valider le nom d'utilisateur/mot de passe saisi par les clients qui utilisent le module de connexion PAM. Utile si vous avez une authentification centralisée avec, par exemple, Kerberos.

```
plugin /usr/lib/openvpn/openvpn-plugin-auth-pam.so login
```

Veuillez lire le guide de durcissement de la sécurité OpenVPN pour obtenir des conseils de sécurité supplémentaires : http://openvpn.net/index.php/open-source/documentation/howto.html#security.

23.1.6.2. Configuration avancée de VPN ponté sur le serveur

OpenVPN peut être configurée soit en mode VPN routé ou ponté. Parfois, cela s'appelle un VPN OSI layer-2 ou layer-3. Dans un VPN ponté, toutes les trames layer-2 - c'est à dire toutes les trames ethernet - sont envoyées aux partenaires VPN et dans un VPN routé, seuls les paquets layer-3 sont envoyés aux partenaires VPN. En mode ponté, tout le trafic y compris celui traditionnel du LAN-local, comme les émissions de réseau local, requêtes DHCP, requêtes ARP, etc est envoyé aux partenaires VPN alors qu'en mode routé, cela sera filtré.

23.1.6.2.1 Préparez la configuration de l'interface pour le pontage sur le serveur

Assurez-vous que vous avez installé le paquet bridge-utils :

```
sudo apt install bridge-utils
```

Avant de configurer OpenVPN en mode ponté, il faut changer la configuration de votre interface. Supposons que votre serveur dispose d'une interface eth0 connectée à internet et une interface eth1 connectée au réseau local que vous voulez ponter. Votre /etc/network/interfaces devrait ressembler à ceci :

```
auto eth0
iface eth0 inet static
  address 1.2.3.4
  netmask 255.255.255.248
  default 1.2.3.1

auto eth1
iface eth1 inet static
  address 10.0.0.4
  Netmask 255.255.255.0
```

Cette interface simple besoin de config pour être transformé en un mode ponté comme l'endroit où la configuration de l'interface eth1 se déplace vers la nouvelle interface de br0. De plus, nous configurer br0 que doit combler l'interface eth1. Nous devons également veiller à ce que l'interface eth1 est toujours en mode promiscuous - ceci indique l'interface de transmettre toutes les trames Ethernet pour la pile IP.

```
auto eth0
iface eth0 inet static
  address 1.2.3.4
  netmask 255.255.255.248
  default 1.2.3.1

auto eth1
iface eth1 inet manual
  up ip link set $IFACE up promisc on

auto br0
iface br0 inet static
  address 10.0.0.4
  netmask 255.255.255.0
  bridge_ports eth1
```

À ce stade, vous devez mettre en place la passerelle. Il se peut que cela ne fonctionne pas du premier coup et que vous perdiez la connexion distante. Assurez-vous que vous pouvez régler les problèmes en ayant un accès local.

```
sudo ifdown eth1 &amp;amp;&amp;amp; sudo ifup -a
```

23.1.6.2.2. Préparer la configuration du serveur pour le pontage

Editez /etc/openvpn/server.conf avec les options suivantes :

```
;dev tun
dev tap
up "/etc/openvpn/up.sh br0 eth1"
;server 10.8.0.0 255.255.255.0
Server-bridge 10.0.0.4 255.255.255.0 10.0.0.128 10.0.0.254
```

Ensuite, créez un script d'aide pour ajouter l'interface **tap** à la passerelle et assurez vous que eth1 est en mode espion. Créez /etc/openvpn/up.sh :

```
#!/bin/sh

BR=$1
ETHDEV=$2
TAPDEV=$3

/sbin/ip link set "$TAPDEV" up
/sbin/ip link set "$ETHDEV" promisc on
/sbin/brctl addif $BR $TAPDEV
```

Puis rendez-le exécutable :

```
sudo chmod 755 /etc/openvpn/up.sh
```

Après avoir configuré le serveur, redémarrez openvpn en tapant :

```
sudo service openvpn@server restart
```

23.1.6.2.3. Configuration du client

Installez d'abord **openvpn** sur le client :

```
sudo apt install openvpn
```

Puis, une fois le serveur configuré et les certificats du client copiés dans le répertoire /etc/openvpn/, créez un fichier de configuration client en copiant l'exemple. Dans un terminal sur la machine client, saisissez :

```
sudo cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf \
/etc/openvpn
```

Maintenant, éditez /etc/openvpn/client.conf en modifiant les options suivantes :

```
dev tap
;dev tun
ca ca.crt
cert client1.crt
key client1.key
```

Enfin, redémarrez openvpn :

```
sudo service openvpn@client restart
```

Vous devriez maintenant être en mesure de vous connecter au réseau LAN distant via le VPN.

23.1.7. Implémentations logicielles des clients

23.1.7.1. Interface graphique Linux Network-Manager pour OpenVPN

De nombreuses distributions Linux notamment les variantes de bureau Ubuntu sont livrées avec Network Manager, une interface graphique agréable pour configurer vos paramètres réseau. Il peut également gérer vos connexions VPN. Assurez-vous que le paquet network-manager-openvpn est bien installé. Ici vous pouvez voir que le programme d'installation installe aussi tous les autres paquets nécessaires :

```
root@client:~# apt install network-manager-openvpn
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
liblzo2-2 libpkcs11-helper1 network-manager-openvpn-gnome openvpn
Suggested packages:
resolvconf
The following NEW packages will be installed:
liblzo2-2 libpkcs11-helper1 network-manager-openvpn
network-manager-openvpn-gnome openvpn
0 upgraded, 5 newly installed, 0 to remove and 631 not upgraded.
Need to get 700 kB of archives.
After this operation, 3,031 kB of additional disk space will be used.
Do you want to continue [Y/n]?
```

Pour informer network-manager sur les nouveaux paquets installés, vous devrez le redémarrer :

```
root@client:~# restart network-manager
network-manager start/running, process 3078
```

Ouvrez le Gestionnaire GUI réseau, sélectionnez l'onglet VPN et puis sur le bouton "Ajouter". Sélectionnez OpenVPN que le type VPN dans le demandeur d'ouverture et appuyez sur «Créer». Dans la fenêtre suivante ajouter le nom du serveur de l'OpenVPN comme «Gateway», réglez Type sur «Certificats (TLS)», le point «Certificat utilisateur 'à votre certificat d'utilisateur,"certificat de CA" à votre certificat de CA et «clé privée» à votre fichier de clé privée. Utilisez le bouton Avancé pour activer la compression (par exemple comp-lzo), dev robinet, ou d'autres paramètres spéciaux que vous définissez sur le serveur. Maintenant, essayez d'établir votre VPN.

23.1.7.2. OpenVPN avec interface graphique pour Mac OS X : Tunnelblick

Tunnelblick est une excellente implémentation, libre et open source d'une interface graphique pour OpenVPN sur OS X. La page d'accueil du projet est sur http://code.google.com/p/tunnelblick/ . Téléchargez ici la dernière version pour OS X et installez-la. Ensuite, mettez votre fichier de configuration avec les certificats et clés de client.ovpn dans

/Users/nom_d'utilisateur/Library/Application Support/Tunnelblick/Configurations/ et lancez Tunnelblick depuis votre dossier Applications.

```
# sample client.ovpn for Tunnelblick
client
remote blue.example.com
port 1194
proto udp
dev tun
dev-type tun
ns-cert-type server
reneg-sec 86400
auth-user-pass
auth-nocache
auth-retry interact
comp-lzo yes
verb 3
ca ca.crt
cert client.crt
key client.key
```

23.1.7.3 OpenVPN avec interface graphique pour Win 7

Pour commencer, téléchargez et installez l'installateur Windows OpenVPN le plus récent : http://www.openvpn.net/index.php/open-source/downloads.html. OpenVPN 2.3.2 était le plus récent quand ceci a été écrit. À ce jour, l'interface de gestion est incluse avec l'installateur binaire Windows.

Vous devez démarrer le service OpenVPN. Allez à Démarrer > Ordinateur > Gestion > Services et Applications > Services. Cherchez le service OpenVPN et démarrez-le. Mettez son type de démarrage sur automatique. Pour la première exécution de l'interface graphique OpenVPN MI, vous devrez la lancer avec les droits administrateur. Faites un clic droit dessus et vous verrez cette option.

Vous devrez écrire votre configuration OpenVPN dans un fichier texte et le placer dans C:\Program Files\OpenVPN\config\client.ovpn avec le certificat d'AC. Vous pourriez placer le certificat de l'utilisateur dans le répertoire home de l'utilisateur comme dans l'exemple suivant.

```
# C:\Program Files\OpenVPN\config\client.ovpn
client
remote server.example.com
port 1194
proto udp
dev tun
dev-type tun
ns-cert-type server
reneg-sec 86400
auth-user-pass
auth-retry interact
```

```
comp-lzo yes
verb 3
ca ca.crt
cert "C:\\Users\\username\\My Documents\\openvpn\\client.crt"
key "C:\\Users\\username\\My Documents\\openvpn\\client.key"
management 127.0.0.1 1194
management-hold
management-query-passwords
auth-retry interact
; Set the name of the Windows TAP network interface device here
dev-node MyTAP
```

Note : si vous n'utilisez pas l'authentification utilisateur et/ou si vous voulez exécuter le service sans interaction de l'utilisateur, basculez les options suivantes en commentaire :

```
auth-user-pass
auth-retry interact
management 127.0.0.1 1194
management-hold
Management-query-passwords
```

Vous voudrez peut être régler le service Windows sur « automatique ».

23.1.7.4. OpenVPN pour OpenWRT

OpenWRT est décrit comme une distribution Linux pour les systèmes embarqués comme les routeurs sans fil. Il y a certains types de routeurs WLAN qui peuvent être flashés pour exécuter OpenWRT. En fonction de la mémoire disponible sur votre routeur OpenWRT, vous pouvez exécuter un logiciel tel que OpenVPN et vous pouvez par exemple construire un petit routeur de succursale bon marché avec une connectivité VPN au bureau central. Plus d'informations pour OpenVPN sur OpenWRT se trouvent ici : http://wiki.openwrt.org/doc/howto/vpn.overview. Et voici la page d'accueil du projet OpenWRT : http://openwrt.org

Connectez-vous à votre routeur OpenWRT et installez OpenVPN :

```
opkg update
opkg install openvpn
```

Consultez /etc/config/openvpn et mettez-y votre configuration client. Copiez les certificats et les clés dans /etc/openvpn/ :

```
config openvpn client1
        option enable 1
        option client 1
#    option dev tap
        option dev tun
        option proto udp
        option ca /etc/openvpn/ca.crt
        option cert /etc/openvpn/client.crt
        option key /etc/openvpn/client.key
        option comp_lzo 1
```

Redémarrez OpenVPN sur routeur OpenWRT pour reprendre la configuration.

Vous devrez voir si vous avez besoin d’ajuster les règles de routage et de filtrage de votre routeur.

23.1.8. Références

- Consultez le site web OpenVPN pour plus d’informations : http://openvpn.net/
- Guide de durcissement de la sécurité OpenVPN :

  http://openvpn.net/index.php/open-source/documentation/howto.html#security
- En outre, OpenVPN par Pakt : Building and Integrating Virtual Private Networks (en anglais) est une lecture conseillée : http://www.packtpub.com/openvpn/book

Chapitre 24. Autres programmes utiles

Il existe de nombreuses applications utiles développées par l’équipe serveur d’Ubuntu, bien intégrées dans l’édition serveur d’Ubuntu, qui peuvent être méconnues. Ce chapitre va décrire certaines de ces applications pouvant largement faciliter l’administration d’un ou plusieurs serveurs Ubuntu.

24.1. pam_motd

Lorsque vous ouvrez une session sur un serveur Ubuntu, vous avez sans doute remarqué le message du jour (MOTD : Message Of The Day). Cette information est obtenue et affichée grâce à un couple de paquets :

- **landscape-common :** fournit les bibliothèques de base pour **landscape-client**, nécessaires à la gestion des systèmes avec **Landscape** (propriétaire) : http://landscape.canonical.com/ . Cependant, le paquet inclut aussi l'utilitaire **landscape-sysinfo** qui est chargé de l'affichage des données de base du système comprenant cpu, mémoire, espace disque, etc. Par exemple :

```
Charge système : 0.0                     Processus : 76
Utilisation de / : 30.2% sur 3.11Go      Utilisateurs connectés : 1
Utilisation mémoire : 20%                Adresse IP pour eth0 : 10.153.107.115
Utilisation du fichier d'échange : 0%

Mettez ces données sous forme de graphique et gérez ce système sur
https://landscape.canonical.com/
```

  V ous pouvez executer landscape-sysinfo manuellement à n'importe quel moment.

- **update-notifier-common** : fournit des informations sur des mises à jour de paquets disponibles, vérification du système de fichiers imminente (fsck), et redémarrages nécessaires (par exemple : après une mise à niveau du noyau).

pam_motd exécute les scripts du fichier /etc/update-motd.d dans l'ordre de nommage des scripts. La sortie de ces scripts est écrite dans le fichier /var/run/motd, tout en gardant l'ordre numérique, puis concaténé avec le fichier /etc/motd.tail.

Vous pouvez ajouter des informations dynamiques au message du jour (MOTD). Par exemple, pour ajouter la météo locale :

- Installez d'abord le paquet **weather-util** :

```
sudo apt install weather-util
```

- Le programme **weather** utilise les données METAR de la National Oceanic and Atmospheric Administration et les prévisions du National Weather Service. Pur avoir les informations locales, vous aurez besoin de l'indicateur à 4 caractères du lieu désiré. Vous pouvez le trouver en cherchant sur le site du **National Weather Service** : http://www.weather.gov/tg/siteloc.shtml .

  Bien que le National Weather Service soit une agence gouvernementale américaine, il y a des stations météo disponibles pour le monde entier. Cependant, toutes les informations météorologiques en dehors des États-Unis ne sont pas forcement disponibles.

- Créez /usr/local/bin/local-weather, simple script shell pour utiliser **weather** avec votre indicateur :

```
#!/bin/sh
#
#
# Affiche les informations météorologiques locales pour le MOTD.
#
#
```

```
# Remplacez KINT par votre station météo locale.
# Des stations locales sont disponibles ici :
http://www.weather.gov/tg/siteloc.shtml

echo
weather -i KINT
echo
```

- Rendez le script exécutable :

```
sudo chmod 755 /usr/local/bin/local-weather
```

- Ensuite, créez un lien symbolique vers /etc/update-motd.d/98-local-weather :

```
sudo ln -s /usr/local/bin/local-weather /etc/update-motd.d/98-local-weather
```

- Pour terminer, déconnectez-vous du serveur et reconnectez-vous pour voir le nouveau MOTD.

Vous devriez maintenant être accueillis avec des informations utiles, et des informations sur la météo locale peut-être pas très utiles. Espérons que l'exemple de l'application **local-weather** démontre la flexibilité de **pam_motd**.

24.1.1. Ressources

Voyez la **page de man de update-motd** pour plus d'options disponibles de **update-motd** : http://manpages.ubuntu.com/manpages/xenial/en/man5/update-motd.5.html .

Le paquet Debian du jour (Debian Package of the Day) **weather** (en anglais) : http://debaday.debian.net/2007/10/04/weather-check-weather-conditions-and-forecasts-on-the-command-line/ contient plus de renseignements sur l'utilisation de **weather**.

24.2. etckeeper

etckeeper permet le contenu de répertoire /etc pour être stockés dans un système de contrôle de version (Version Control System : VCS) référentiel. Il se intègre avec **APT** et automatiquement engage les modifications dans /etc quand les paquets sont installés ou mis à niveau. Placer /etc sous contrôle de version est considérée comme une meilleure pratique de l'industrie, et l'objectif de **etckeeper** est de rendre ce processus aussi indolore que possible.

Installez **etckeeper** en tapant dans un terminal :

```
sudo apt install etckeeper
```

Le fichier de configuration principal, /etc/etckeeper/etckeeper.conf, est assez simple. L'option principale est de choisir quel système de contrôle de version utiliser, et par défaut, **etckeeper** est configuré pour utiliser **Bazaar**. Le dépôt est automatiquement initialisé (et envoyé pour la première fois) pendant l'installation du paquet. Il est possible d'annuler ceci en entrant la commande suivante :

```
sudo etckeeper uninit
```

Par défaut, etckeeper exportera les modifications de /etc non exportés, quotidiennement.. Ceci peut être désactivé avec l'option de configuration AVOID_DAILY_AUTOCOMMITS. Il exportera également les modifications avant et après une installation de paquet. Pour un suivi plus précis des changements, il est recommandé de les exporter manuellement avec un message d'exportation. Pour cela utilisez :

```
sudo etckeeper commit "..Motifdu changement de configuration.."
```

En utilisant le système de contrôle de version (VCS) de Bazaar, vous pouvez voir les informations du journal :

```
sudo bzr log /etc/passwd
```

Pour démontrer l'intégration avec le système de gestion des paquets (APT), installez **postfix** :

```
sudo apt install postfix
```

Lorsque l'installation est terminée, tous les fichiers de configuration de **postfix** devraient se trouver dans le dépôt CVS :

```
Committing to: /etc/
added aliases.db
modified group
modified group-
modified gshadow
modified gshadow-
modified passwd
modified passwd-
added postfix
added resolvconf
```

```
403Other Useful Applications
added rsyslog.d
modified shadow
modified shadow-
added init.d/postfix
added network/if-down.d/postfix
added network/if-up.d/postfix
added postfix/dynamicmaps.cf
added postfix/main.cf
added postfix/master.cf
added postfix/post-install
added
added
added
added postfix/postfix-files
postfix/postfix-script
postfix/sasl
ppp/ip-down.d
added
added
added
added
added
added ppp/ip-down.d/postfix
ppp/ip-up.d/postfix
rc0.d/K20postfix
rc1.d/K20postfix
rc2.d/S20postfix
rc3.d/S20postfix
added rc4.d/S20postfix
added rc5.d/S20postfix
added rc6.d/K20postfix
added resolvconf/update-libc.d
added resolvconf/update-libc.d/postfix
added rsyslog.d/postfix.conf
added ufw/applications.d/postfix
Committed revision 2.
```

Pour voir comment **etckeeper** garde un trace des changements manuels, ajoutez un nouvel hôte à /etc/hosts. En utilisant **bzr**, vous verrez quels fichiers ont été modifiés :

```
sudo bzr status /etc/
```

```
modified:
    hosts
```

Appliquez maintenant les changements :

```
sudo etckeeper commit "nouvel hôte ajouté"
```

Pour de plaus amples informations à propos de **bzr**, consultez le *Chapitre 17, paragraphe 1. Bazaar*.

24.2.1. Ressources

Voyez le site **etckeeper** pour plus de détail sur l'utilisation de **etckeeper :** http://etckeeper.branchable.com/

Pour plus d'informations à propos de **bzr**, consultez le site Web de **bzr** (en anglais) : http://bazaar-vcs.org/ .

24.3. Byobu

Une des applications les plus utiles pour tout administrateur système est un multiplexeur de xterm comme **écran** ou **tmux**. Il permet l'exécution de plusieurs coquilles dans une borne. Pour faire partie de l'multiplexeur fonctions avancées plus convivial et de fournir des informations utiles sur le système, le **byobu** package a été créé. Il agit comme une enveloppe pour ces programmes. Par défaut Byobu utilise tmux (si installé), mais cela peut être changé par l'utilisateur.

Invoquez le simplement avec :

```
byobu
```

Maintenant faites apparaître le menu de configuration. Par défaut, ceci est fait en appuyant sur la touche **F9**. Cela vous permettra de :

- Afficher le menu d'aide
- Modifier la couleur d'arrière-plan de Byobu
- Modifier la couleur de premier-plan de Byobu
- Changer les notification d'état
- Modifier les raccourcis claviers
- Changer la séquence d'échappement
- Créer de nouvelles fenêtres
- Gérer les fenêtres par défaut
- Byobu ne s'exécute actuellement pas à la connexion (activer)

Les **raccourcis clavier** déterminent certaines choses comme la séquence d'échappement, les nouvelles fenêtres, les changements de fenêtre, etc. il y a deux sets de raccourcis clavier à choisir des **touches-f** et des **touches-d'échappement-d'écran**. Si vous souhaitez utiliser les raccourcis clavier par défaut, choisissez le set **aucun**.

byobu est dotée d'un menu affichant la version d'Ubuntu, les renseignements sur le processeur et la mémoire, ainsi que l'heure et la date. Il ressemble au menu d'une station de travail.

L'option **« Byobu ne s'exécute actuellement pas à la connexion (activer) »** fait en sorte que **byobu** s'exécute à chaque fois qu'un terminal est ouvert. Les changements qu'un utilisateur apporte à **byobu** ne s'appliquent pas aux autres utilisateurs.

Une différence lors de l'utilisation de byobu est le mode **historique**. Pressez la touche **F7** afin d'entrer en mode historique. Le mode historique vous permet de naviguer dans les anciennes sorties en utilisant des commandes similaires à celle de**vi**. Voici une liste brève des commandes de mouvement :

- **h** - reculer le curseur d'un caractère
- **j** - descendre le curseur d'un ligne
- **k** - monter le curseur d'une ligne
- **l** - avancer le curseur d'un caractère
- **0** - aller au début de la ligne

- **$** - aller à la fin de la ligne
- **G** - aller à la ligne indiquée (par défaut va en fin de tampon)
- **/** - recherche en avant
- **?** - recherche en arrière
- **n** - Passe à la prochaine correspondance, en avant ou en arrière

24.3.1. Ressources

Pour plus d'informations à propos de **screen**, consultez le site Web de **screen** (en anglais) : http://www.gnu.org/software/screen/ .

Ainsi que la page du **Wiki Ubuntu consacrée à screen** : https://help.ubuntu.com/community/Screen **.**

Consultez également le **site Web de Byobu** pour plus d'informations : https://launchpad.net/byobu .

TABLE DES MATIÈRES

Annexe A

A.1. Soumettre un rapport d'anomalie dans Ubuntu Server Edition

Le projet Ubuntu, et donc Ubuntu Server, utilisent **Launchpad** : https://launchpad.net/ comme traceur de bogue. Pour déposer un bogue, vous aurez besoin d'un compte Launchpad. **En créer un ici** si besoin : https://help.launchpad.net/YourAccount/NewAccount .

A.1.1. Signaler des bogues avec apport-cli

La meilleure façon de signaler un bogue se fait avec la commande **apport-cli** commande. Il doit être exécuté sur la machine affectée parce qu'il recueille des informations du système sur lequel il est exécuté et les publient dans un rapport de bogue sur Launchpad. Envoyer ces informations à Launchpad peut donc être un défi si le système n'exécute pas un environnement graphique (comme les serveurs) ou si il n'y a pas d'accès à Internet. Les mesures à prendre dans ces situations sont décrites ci-dessous.

> Les commandes **apport-cli** et **ubuntu-bug** doivent donner le meme resultat sur un serveur CLI. Ce dernier est en fait un lien symbolique vers **apport-bug** qui est assez intelligent pour savoir si un environnement de bureau est en cours d'utilisation et choisira **apport-cli** dans le cas contraire. Comme les systèmes de serveurs ont tendance à être fournis uniquement avec CLI, apport-cli a été choisi dès le départ dans ce guide.

Les rapports de bogues dans Ubuntu doivent être déposés avec un logiciel spécifique, de sorte que le nom du paquet (paquet source ou nom/chemin du programme) affecté par le bogue doit être fourni à apport-cli :

```
apport-cli NOM_DU_PAQUET
```

> Consultez le *Chapitre 3. Gestionnaire de paquets* pour plus d'informations sur la gestion des paquets dans Ubuntu.

Une fois qu'apport-cli a terminé la collecte d'informations, vous devez dire ce que vous voulez en faire. Par exemple, pour signaler un bogue dans vim :

```
apport-cli vim
```

```
*** La collecte d'informations de problème

Le recueilli des informations peut être envoyé aux développeurs d'améliorer la
application. Cela peut prendre quelques minutes.
...

*** Envoyer rapport de problème aux développeurs?

Après le rapport de problème a été envoyé, se il vous plaît remplir le formulaire dans
le dossier
automatically ouvert navigateur Web.

Nouveautés souhaitez-vous faire? Vos options sont:
S: Envoyer un rapport (2,8 KB)
V: Voir rapport
```

```
K: Gardez fichier de rapport pour envoyer plus tard ou la copie à un autre endroit
I: Annuler et ignorons les accidents futurs de ce programme la version
C: Annuler
Veuillez choisir (S/V/K/I/C):
```

Les trois premières options sont décrites ci-dessous :

- **Send:** soumet les informations collectées à Launchpad dans le cadre du processus de dépôt d'un nouveau rapport de bogue. Vous aurez la possibilité de décrire le bogue avec vos propres mots.

  ```
  *** informations de problème de Téléchargement

  Le a recueilli des informations est envoyée au système de suivi des bogues.
  Ce peut durer quelques minutes.
  94%

  *** Pour continuer, vous devez visiter le URL suivante:

  https://bugs.launchpad.net/ubuntu/+source/vim/+filebug/09b2495a-e2ab-11e3-879b-
  68b5996a96c8?

  You peut lancer un navigateur maintenant, ou copier ce . URL dans un navigateur
  sur un autre ordinateur


  Choices:
  1: Lancez un navigateur maintenant
  C: Annuler
  Veuillez choisir (1/C): 1
  ```

  Le navigateur qui sera utilisé lors du choix d'une '' sera celui connu sur le système comme **www-navigateur** via le **Debian système d'alternatives :** http://manpages.ubuntu.com/manpages/fr/man8/update-alternatives.8.html . Des exemples de navigateurs en mode texte pour installer comprennent **liens**, **elinks**, **lynx**, et **w3m**. Vous pouvez aussi pointer manuellement un navigateur existant à l'URL donnée.

- **View:** affiche les informations recueillies sur l'écran pour examen. Cela peut être un grand nombre d'informations. Appuyez sur « Entrée » pour faire défiler écran par écran. Appuyez sur « q » pour quitter et revenir au menu.
- **Keep:** inscrit les informations collectées sur le disque. Le fichier en résultant peut être utilisé plus tard pour déposer le rapport de bogue, généralement après le transfert vers un autre système Ubuntu.

  ```
  Nouveautés souhaitez-vous faire? Vos options sont:
  S: Envoyer un rapport (2,8 KB)
  V: Voir rapport
  K: Gardez fichier de rapport pour envoyer plus tard ou la copie à un autre
  endroit
  I: Annuler et ignorons les accidents futurs de ce programme la version
  C: Annuler
  Veuillez choisir (S/V/K/I/C): k
  ```

```
Problem fichier de rapport: /tmp/apport.vim.1pg92p02.apport
```

Pour signaler le bug, obtenir le fichier sur un système Ubuntu compatible Internet et appliquer apport-cli à elle. Cela entraînera le menu apparaisse immédiatement (l'information est déjà recueillis). Vous devez puis appuyez sur "s" pour envoyer :

```
apport-cli apport.vim.1pg92p02.apport
```

Pour enregistrer directement un rapport sur le disque (sans les menus), vous pouvez faire :

```
apport-cli vim --save apport.vim.test.apport
```

Les noms de rapports doivent se terminer par .apport.

> Si ce système est connecté à Internet non-Ubuntu/Debian, apport-cli ne est pas disponible si le bogue devra être créé manuellement. Un rapport d'apport est également de ne pas être inclus dans une pièce jointe à un bogue soit il est donc complètement inutile dans ce scénario.

A.1.2. Faire un rapport de plantage d'une application

Le paquet de logiciels qui fournit l'utilitaire apport-cli, **apport**, peut être configuré pour capturer automatiquement l'état d'une application plantée. Ceci est activé par défaut (dans /etc/default/apport).

Après qu'une application plante et si il est activé, apport stockera un rapport de plantage dans le fichier /var/crash :

```
-rw-r----- 1 peter whoopsie 150K Jul 24 16:17 _usr_lib_x86_64-linux-gnu_libmenu-
cache2_libexec_menu-cached.1000.crash
```

Utilisez la commande **apport-cli** sans arguments pour traiter des rapports d'erreur en attente. Il proposera de les signaler un par un.

```
apport-cli
```

```
*** Signaler le problème aux développeurs ?

Après l'envoi du rapport de problème, veuillez remplir le formulaire dans le
navigateur web ouvert automatiquement.

Que souhaitez vous faire ? Les options sont :
  S : soumettre le rapport (153.0 KO)
  V : voir le rapport
  K : conserver le fichier de rapport pour l'envoyer plus tard ou le copier ailleurs
  I : annuler et ignorer les futurs plantages de cette version du programme
  C : annuler
Veuillez choisir (S/V/K/I/C) : s
```

Si vous envoyez le rapport, comme vous l'avez fait ci-dessus, l'invite sera retournée immédiatement et le fichier /var/crash contiendra alors deux fichiers supplémentaires :

```
-rw-r----- 1 peter whoopsie 150K Jul 24 16:17 _usr_lib_x86_64-linux-gnu_libmenu-
```

```
cache2_libexec_menu-cached.1000.crash
-rw-rw-r-- 1 peter whoopsie 0 Jul 24 16:37 _usr_lib_x86_64-linux-gnu_libmenu-
cache2_libexec_menu-cached.1000.upload
-rw------- 1 whoopsie whoopsie 0 Jul 24 16:37 _usr_lib_x86_64-linux-gnu_libmenu-
cache2_libexec_menu-cached.1000.uploaded
```

L'envoi dans un rapport de plantage comme celui-ci n'entraînera pas immédiatement la création d'un nouveau bogue public. Le rapport sera rendu privé sur Launchpad, ce qui signifie qu'il ne sera visible que par un ensemble limité de trieurs de bogues. Ces trieurs scruterons ensuite le rapport pour éliminer d'éventuelles données privées avant de créer un bogue public.

A.1.3. Ressources

Consultez la page du **Wiki Ubuntu consacrée au rapport de bugs** : https://help.ubuntu.com/community/ReportingBugs .

La page consacrée à **Apport** comporte également des informations utiles bien que certaines d'entre elles concernent l'utilisation d'une interface graphique: https://wiki.ubuntu.com/Apport .

Annexe B

Sigles et Définitions

A_record	A type of DNS record containing a host name and its associated IP address. An A record is used by messaging servers on the Internet to route email.	le type a de serveur de nom de domaine contient un nom d'hôte ainsi que son adresse ip. un serveur a_record est utilisé par des serveurs de messagerie sur internet pour acheminer des courriels.
ACL	Access Control Lists	listes de contrôle d'accès
AD	Active Directory	service d'annuaire LDAP(microsoft)
AJP	Apache Jserv Protocol	protocole apache jserv
API	Application Programming Interface	interface de programmation d'applications
APT	Advanced Packaging Tool	outil avancé de gestion des paquets
ARP	Address Resolution Protocol	protocole de résolution d'adresse
BDC	Backup Domain Controller	contrôleur de domaine de sauvegarde
BIND	Berkley Internet Name Daemon	démon de nom internet de l'université de berkley
CA	Certification Authority	autorité de certification
CARP	Cache Array Routing Protocol	protocole de routage des ensembles de cache
CIA	Certificate Issuing Authority	autorité de délivrance des certificats
CIFS	Common Internet Filesystem	système de fichier internet commun
CNAME	Canonical Name	nom canonique
CPU	Central Processing Unit	unité central de traitement
CSR	Certificate Signing Request	demande de signature de certificat
CUPS	Common UNIX Printing System	système d'impression unix commun
D-BUS	Desktop Bus	https://en.wikipedia.org/wiki/d-bus
DARPA	Defense Advanced Research Projects Agency	agence des projets de recherche avancée de défense
DbIndex	Data base Index	indice de base de données
DBMS	Data Base Management System	système de gestion de base de données
DHCP	Dynamic Host Configuration Protocol	protocole de configuration dynamique de l'hôte

DIT	Directory Information Tree	arbre d'information de répertoire
DKIM	DomainKeys Identified Mail	norme d'authentification fiable du nom de domaine de l'expéditeur d'un courriel
DMS	Domain Member Server	serveur membre du domaine
DMM	Device Mapper Multipathing	périphérique cartographe de périphériques à multiples chemins d'accès
DN	Distinguished Name	nom absolu. Le **DN** (*Distinguished Name*) d'un objet est un moyen d'identifier de façon unique un objet dans la hiérarchie. Un DN se construit en prenant le nom relatif de l'élément (RDN - *Relative Distinguished Name*), et en lui ajoutant l'ensemble des noms relatifs des entrées parentes. Le DN d'un élément est donc la concaténation de l'ensemble des RDN de ses ascendants hiérarchiques.
DNS	Domain Name System	système de résolution de noms de domaine
DPKP	Data Plane Development Kit	kit de développement de plan d'information
DRBD	Distributed Replicated Block Device	périphérique en mode bloc répliqué et distribué
EAL	Environment Abstraction Layer	couche d'abstraction de l'environnement
EXT	EXTended file system	système de fichiers étendu
FHS	Filesystem Hierarchy Standard	norme de hiérarchie de système de fichier
FTP	File Transfer Protocol	protocole de transfert de fichiers
FQDN	Fully Qualified Domain Names	nom de domaine entièrement qualifié
GID	Group IDentifier	identifiant de groupe
GPL	General Public License	licence publique générale
GUI	Graphical User Interface	interface graphique d'utilisateur
HBA	Host Bus Adaptor	adaptateur de bus hôte
HDB	Hard DataBase ?	
HTCP	Hyper Text Caching Protocol	protocole de cache hypertexte
HTTP	Hyper Text Transfer Protocol	protocole de transfert hypertexte
HTTPS	Hyper Text Transfer Protocol over Secure Sockets Layer	protocole hypertexte de transfert par couche de sorties sécurisées
HTTPD	Hyper Text Transport Protocol Daemon	démon de protocole de transport hypertexte
ICMP	Internet Control Messaging Protocol	protocole de contrôle de messagerie internet
ICP	Internet Cache Protocol	protocole de cache internet
ICS	Internet Connection Sharing	partage de connexion internet

ID	IDentifier	identifiant
IMAP	Internet Message Access Protocol	protocole d'accès de message internet
IMAPS	Internet Message Access Protocol SSL	protocole d'accès ssl de message internet
IMAPD	Internet Message Access Protocol Daemon	démon de protocole d'accès de message internet
IP	Internet Protocol	protocole internet
IPC	Inter-Process Communication	communication inter processus
IPP	Internet Printing Protocol	protocole internet d'impression
IRC	Internet Relay Chat	système de messagerie instantanée multi-utilisateurs
iSCSI	Internet Small Computer System Interface	interface internet de système de petits ordinateurs
JSP	Java Server Pages	pages de serveur java
JVM	Java Virtual Machine	machine virtuelle java
KDC	Key Distribution Center	centre de distribution de clef
KVM	Keyboard, Video, Mouse	clavier, écran, souris
LAMP	Linux Apache MySQL et Perl/Python/PHP	← sigle des composants
LAN	Local Area Network	réseau d'une zone local
LAPD	Link Access Procedures, Delta channel https://en.wikipedia.org/wiki/Link_Access_Procedures,_D_channel	Voir le lien pour explication
LDAP	Lightweight Directory Access Protocol	protocole d'accès de répertoire léger
LDIF	LDAP Data Interchange Format	format d'échange de données
LSM	Linux Security Module	module de sécurité linux
LTS	Long Term Support	support long terme
LTSP	Linux Terminal Server Project	projet de terminal de serveur linux
LUN	Logical Unity Number	numéro d'unité logique
LV	Logical Volume	volume logique
LVM	Logical Volume Manager	gestionnaire de volume logique
MAC	Media Access Control	contrôle d'accès au support ; adresse physique (matérielle) de 48 bits d'un périphérique réseau
MCE	Machine Check Exceptions	erreur détectée par le processeur
MDA	Mail Delivery Agent	agent serveur de réception

MIME	Multipurpose Internet Mail Extensions	extensions multifonctions du courrier Internet
MIT kerberos	Massachusetts Institute of Technology kerberos	logiciel kerberos de l'institut de technologie du massachusetts
MOTD	Message Of The Day	message du jour
MTA	Mail Transport Agent	agent de transport de courriel
MUA	Mail User Agent	agent client courriel
MX	Mail eXchange	échange de courriel
NAT	Network Address Translation	traduction d'adresse de réseau
NFS	Network File System	système de fichier réseau
NMI	Non-Masquable Interrupt	interruptions non masquables
NS	Netscape	entreprise netscape
NSS	Name Service Switch	commutateur de service de nom
NTP	Network Time Protocol	protocole du temps du réseau
PAM	Pluggable Authentication Modules	système d'authentification centralisé de linux http://artisan.karma-lab.net/petite-introduction-a-pam
PBX	Private Branch eXchange	échange de branche privée (commutation)
PDC	Primary Domain Controller	contrôleur de domaine principal
PE	Physical Extension	extension physique
PHP	Hypertext Preprocessor	préprocesseur hypertexte
PID	Process ID	identifiant processus
PKI	Public Key Infrastructure	infrastructure de clé publique
PPD	PostScript Printer Description	description d'imprimante postscript
PPP	Point-to-Point Protocol	protocole pair à pair
PPPoE	PPP over Ethernet	ppp par ethernet
PPTP	Point-to-Point Tunneling Protocol	protocole de mise en tunnel ppp
P-t-P	Peer to Peer	pair à pair
PTR	PoinTeR	pointeur, utilisé pour les enregistrements dns ; une adresse pointe vers un nom
PV	Physical Volume	volume physique
RAID	Redundant Array of Independent Disks	regroupement redondant de disques indépendants
RAM	Random Access Memory	mémoire vive

RARP	Reverse Address Resolution Protocol	protocole de résolution inversée d'adresse
RDN	Relative Distinguished Name	nom absolu relatif
RFC	Request For Comments	demande pour commentaires
RID	Replica ID	réplique d'identifiant unique à 3 chiffres qui définie la réplique
RIP	Router Information Protocol	protocole d'information de routeur
rootDN	root Distinguised Name. The root distinguished name, or root DN, is the first, or top-most, entry in an LDAP directory tree. In Netscape Directory Server, the root DN is commonly referred to as the directory manager. By default, the root DN uses no suffix; it is simply a common name attribute-data pair: CN=Directory Manager. For example, the root entry's DN could look like this: CN=Directory Manager, O=Siroe Corporation, C=US.	Nom absolu de la racine de l'arborescence
RSA	Rivest Shamir Adleman	le chiffrement rsa (nommé par les initiales de ses trois inventeurs) est un algorithme de cryptographie asymétrique.
RTC	Real Time Configuration	configuration temps réel
SAN	Storage Area Network	réseau d'une zone de stockage
SASL	Simple Authentication and Security Layer	mécanisme d'authentification d'un client et de couche de sécurité
SLAPD	Standalone LDAP Daemon https://en.wikipedia.org/wiki/Slapd	Voir le lien
SMB	Server Message Block	bloc de messages de serveur
SNMP	Simple Network Manager Protocol	protocole de gestionnaire de réseau simple
SOA	Start of Authority	point de départ d'autorité
SPF	Sender Policy Framework	cadre de politique de l'expéditeur
SRS	SCSI Request Sense	sentiment de demande scsi
SRV	Service Record	service d'enregistrement
SSC	Self-Signed Certificate	certificat auto-signé
SSSD	System Security Services Daemon	démon de service de sécurité du système
SSH	Secure SHell	protocole de connexion et de transfert de fichier sécurisé
SSHD	Secure SHell Daemon	démon ssh
SSID	Service Set Identifier	identifiant de groupe de service

SSL	Secure Sockets Layer	couche de sorties sécurisées
SSO	Single Sign On	système à authentification unique
TC	Traffic Controller	contrôleur de trafic
TCP	Transmission Control Protocol	protocole de contrôle de transmission
TGT	Ticket Granting Ticket	ticket d'octroi de ticket
TGS	Ticket Granting Server	serveur d'octroi de ticket
TLS	Transport Layer Security	sécurité de couche de transport
TUR	Test Unit Ready	test du statut de communication d'un périphérique
UBE	Unsolicited Bulk Email	courriers électroniques non sollicités
UDP	User Datagram Protocol	protocole de datagramme utilisateur. Défini par la RFC 768 de l'IETF, l'**UDP** permet la transmission de données entre deux entités avec une grande facilité, chacune d'entre elles possédant une adresse IP propre et un numéro de port.
UID	User Identifier	identifiant utilisateur
URL	Uniform Resource Locator	localisateur de ressource uniforme
VCS	Version Control System	système de contrôle de version
VG	Volume groupe	groupe de volumes
VLAN	Virtual Local Area Network	réseau virtuel d'une zone locale
VPN	Virtual Private Networking	mise en réseau virtuelle privée
WCCP	Web Cache Coordination Protocol	protocole de coordination de cache web
WWID	World Wide Identifier	identifiant monde entier
XMPP	eXtensible Messaging and Presence Protocol	protocole extensible de présence et de messagerie

Annexe C

Ont participé à la version française de ce guide au 31/05/2017 :

Legal warning Used in serverguide in Automated Suggestions for Ubuntu Server Guide trunk : proposition de traduction automatique par

Used in serverguide in Ubuntu Hardy package "ubuntu-docs" by : traduction rapatriée de la traduction d'un autre paquet par

Reviewed by : traduction revue par

Suggested in serverguide in Ubuntu Hardy package "ubuntu-docs" by : proposition de traduction par

Translated by ou Translated and reviewed by : traduction validée ou traduction validée et revue par

Toute omission ou erreur de ce tableau peut être relevée et signalée pour modification.

	Total	Legal warning	Used in	Reviewed by	Suggested by	Translated by
Totaux	9041	1706	347	**968**	2243	3777
(AJM)	1				1	
65GYgzf	42		42			
ABBAYES	1				1	
Accad	28	1	13		14	
Admin	1	1				
Administrators	2	2				
alexandre958	1				1	
ALT	1	1				
Amarokk	1					1
Anne017	5		5			
Aymeric	3				3	
Baerts	1				1	
Bailliot	1				1	
baj	144				144	
Banal	2				2	
baptiste	2				2	

Barrot	1				1	
Bastin	1		1			
Baudry	56				54	2
belsack	1				1	
Benichou	3				3	
Benschop	2	2				
Bertho	31		17		14	
Biardeaud	1	1				
blob	1		1			
Bob	1				1	
BobMauchin	2	2				
Bonifas	1	1				
Boos	3	3				
Bouchet-Valat	1				1	
BOUZIANE	4				4	
Bozhko	2	2				
bruno	3	1			2	
budgester	1	1				
Busquets	1	1				
Calinou	1	1				
Camilla	1		1			
CaptainCrook	4				4	
CarZ	18				18	
Casiope	1		1			
Cassirame	9				9	
Cassuto	1	1				
Cecconi	1	1				
Chambreuil	3	2	1			
Champémont	3				3	
chaussade	1				1	
CHAUVEAU	7				7	
CHAUVET	2	2				

CHEBBI	14				14	
Chelli	1	1				
Chevalley	1	1				
Choveaux	1				1	
Christophe	1		1			
Cinquin	4				4	
CK	24				24	
Claessens	1	1				
Clarke	15		3		12	
Clementi	1		1			
CLERGEOT	4				4	
Colin	1	1				
Cornavin	3	3				
Corpet	8				8	
Croteau	2				2	
da_norf	1		1			
Damiens	5				5	
Daniel	2	1			1	
Darby	1				1	
David	4				4	
de iz	1				1	
Delache	1		1			
Delvaux	14			**7**		7
DEMAY	27		2		25	
Derguech	1				1	
DERIVE	11		4		7	
Deroussen	14				14	
DI RUSCIO	4				4	
Dinendal	1				1	
Divaret	1				1	
Doctrinal	1				1	
Donk	81		51		30	

Dupin	434				434	
elaliberte	1				1	
Elmes	1	1				
Elmoussaoui	1		1			
Emmanuel	1		1			
Éric	2	2				
Esposito	2		1		1	
Eudes	1	1				
Fab	4				4	
FabriceColin	1	1				
fabrom	1				1	
fatalerrors	1	1				
Febwin	2		1		1	
Fernand	11				11	
Févry	1				1	
Fr-coord	2		1		1	
Francois	1				1	
Franke	3	2			1	
FredBezies	1				1	
French	1				1	
Friedmann	1	1				
Gallet	386	2	3	**286**		95
Gasparini	1	1				
geh	1		1			
George	1	1				
Gillier	1				1	
Gisbert	1		1			
GNIEWEK	1	1				
Goeminne	4				4	
Goetje	5	5				
goofy	1				1	
Goyvaerts	2	2				

Graber	1	1				
Greg	1		1			
Greizgh	1	1				
Grimpard	1		1			
GroNox	1				1	
Guillaume-Edouard	5				5	
Gwi	1				1	
Haïkal	22		1		21	
hardball	10				10	
Havet	19		3		16	
hickop	1	1				
Higby	1				1	
Hunting	23		2		21	
Immunoman	12				12	
istu5	1				1	
ivan	1				1	
JAN	3		3			
jb07	2	2				
Jean-Christophe	1		1			
Jean-Marc	690		7	**365**	1	317
Jean-Philippe	4		1		3	
Jean-Sébastien	1				1	
Johan	1				1	
Jonathan	1				1	
Jordan	1				1	
Julie	1		1			
karim	1				1	
Kcchouette	1				1	
kos!	31		30		1	
L’Africain	1		1			
L’homme	1	1				

Iann	7				7	
LAROCHE	1		1			
Lasnier	17				17	
Lassauge	1	1				
Lasserre	1	1				
Latouche	1				1	
Latry	2				2	
Laurent	1					1
Le Thanh Duong	1	1				
Le-Libriste	1		1			
Lebret	1				1	
LECHÊNE	6				6	
Lemaignan	3		3			
Lemery	1				1	
Leonarf	65				65	
Lionel	1				1	
Lojewski	2	2				
londumas	1				1	
Lopez Artica	1	1				
Luciani	17				17	
madden	1				1	
Malaise	1	1				
Malandain	7		1		6	
mallow	1				1	
ManuPeng	20				20	
Marchal	1	1				
marcon	7					7
Martignoni	1		1			
MARTIN	1				1	
Masaki	1	1				
MATHIEU	3		1		2	
Maugendre	269				264	5

Mazeland	1	1				
Mehdi	1	1				
mekolat	1		1			
Merlet	3	3				
Meschieri	1	1				
Michel	27		3		24	
Mika	4				4	
MikeB	1				1	
Millan	743	4			107	632
Miller	2	2				
Moiny	14		1		13	
molinard	1				1	
Monnerat	1	1				
Montrieux	2				2	
Morgan	1				1	
Nazo	1	1				
Nebaff	11				11	
Nemry	1	1				
netbyte	1				1	
nicolas	1		1			
Niset	3				3	
Noël	1				1	
Nottin	9		1		8	
Novak	3					3
NSV	19		3		16	
Olivier	39		17		22	
OpenEduCat	2	2				
Ortalo	1				1	
ozlr	1	1				
Pagès	1				1	
Painchaud	53	1			52	
Papouin	2	2				

Paroz	23	1	3		19	
Pascal	3				3	
Patri	155	1	41		113	
perreault	126			**83**		43
Perrier	4	4				
perrin	3				3	
Phnx	2				2	
Pietrowski	1	1				
Pineau	11				11	
Piquer	2				2	
Plano-Lesay	1				1	
pokekrom	1	1				
Porcheron	10		4		6	
Potrowl	1	1				
Psykocrash	1				1	
RAFFIN	1				1	
Raimbault	1	1				
Réau	15				15	
Ricard	1		1			
Riddell	1	1				
ridem	1		1			
Riusma	1				1	
Robin	3	3				
Roche	17		5		12	
Rocher	7				7	
rodriguez	3				3	
romjerome	1	1				
Rosina	5			**3**	1	1
royto	1		1			
Sala Soler	1	1				
SALAH	1				1	
sam101	1				1	

Sangy	1				1	
Sassoulas	1				1	
seb35690	24				24	
SEDKI	2				2	
SeeLook	1	1				
Sibelle	1	1				
Simons	1	1				
Slamich	2461	1573	24	**217**	31	616
sleid	3		3			
sm126	10		1		9	
Smythies	6			**2**		4
SOSAndroid	1		1			
Soyez	8				8	
Spok	1	1				
Sprauer	1	1				
Sunyer	2037	3			4	2030
SuperBOB	8		2		6	
Sylvain	1	1				
T0m-S	2				2	
taffit	2	1	1			
Taramarcaz	3		1		2	
Tarsus	13				13	
Tassin	1	1				
Ternisien	5	5				
Terry	1	1				
thebachman	1				1	
Thirioux	1				1	
THOBY	4				1	3
Thor	1	1				
Tissandier	1	1				
Tokyrn	1				1	
tomestla	1				1	

torglut	11				11	
Touch'	1		1			
Treyvaud	1				1	
Tsaeb	21		1		20	
V	69				69	
Van Wambeke	1				1	
Verne	1		1			
Vervelle	1		1			
Viaud	1	1				
Villoué	30		3		27	
Vilsafur	1				1	
Vincent	1	1				
vouzico	12		1		11	
WEBER	30		6		24	
Wukong	12				12	
X	47		1		46	
XIA	1	1				
Yionel	1				1	
YoBoY	15			**5**		10
Zarzuelo	1	1				
Zeller	1	1				
zoff99	1	1				
zoon01	1	1				
ســند	1				1	