

Ubuntu Server Guide

Ubuntu Server Guide

Copyright © 2008 Canonical Ltd. and members of the *Ubuntu Documentation Project*³

Abstract

Welcome to the *Ubuntu Server Guide*! It contains information on how to install and configure various server applications on your Ubuntu system to fit your needs. It is a step-by-step, task-oriented guide for configuring and customizing your system.

Credits and License

This document is maintained by the Ubuntu documentation team (<https://wiki.ubuntu.com/DocumentationTeam>). For a list of contributors, see the *contributors page*¹

This document is made available under the Creative Commons ShareAlike 2.5 License (CC-BY-SA).

You are free to modify, extend, and improve the Ubuntu documentation source code under the terms of this license. All derivative works must be released under this license.

This documentation is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE AS DESCRIBED IN THE DISCLAIMER.

A copy of the license is available here: *Creative Commons ShareAlike License*².

³ <https://launchpad.net/~ubuntu-core-doc>

¹ [../libs/C/contributors.xml](https://github.com/ubuntu/docs/blob/master/..../libs/C/contributors.xml)

² [/usr/share/ubuntu-docs/libs/C/ccbysa.xml](https://github.com/ubuntu/docs/blob/master/..../usr/share/ubuntu-docs/libs/C/ccbysa.xml)

Table of Contents

1. Introduction	1
1. Support	2
2. Installation	3
1. Preparing to Install	4
2. Installing from CD	6
3. Upgrading	9
4. Advanced Installation	10
3. Package Management	14
1. Introduction	15
2. dpkg	16
3. Apt-Get	17
4. Aptitude	19
5. Automatic Updates	21
6. Configuration	23
4. Networking	25
1. Network Configuration	26
2. TCP/IP	30
3. Dynamic Host Configuration Protocol (DHCP)	34
4. Time Synchronisation with NTP	37
5. Remote Administration	39
1. OpenSSH Server	40
2. eBox	43
6. Network Authentication	46
1. OpenLDAP Server	47
2. Samba and LDAP	61
3. Kerberos	66
7. Domain Name Service (DNS)	73
1. Installation	74
2. Configuration	75
3. Troubleshooting	80
4. References	84
8. Security	85
1. User Management	86
2. Console Security	92
3. Firewall	94
4. AppArmor	101
5. Certificates	105
9. Web Servers	110
1. HTTPD - Apache2 Web Server	111
2. PHP5 - Scripting Language	117

3. Squid - Proxy Server	119
4. Ruby on Rails	121
5. Apache Tomcat	123
10. Databases	127
1. MySQL	128
2. PostgreSQL	130
11. Wiki Applications	132
1. Moin Moin	133
2. MediaWiki	135
12. File Servers	136
1. FTP Server	137
2. Network File System (NFS)	139
3. CUPS - Print Server	141
13. Email Services	144
1. Postfix	145
2. Exim4	151
3. Dovecot Server	154
4. Mailman	156
5. Mail Filtering	162
14. Version Control System	168
1. Bazaar	169
2. Subversion	170
3. CVS Server	175
4. References	177
15. Windows Networking	178
1. Introduction	179
2. Samba File Server	180
3. Samba Print Server	182
4. Securing a Samba File and Print Server	183
5. Samba as a Domain Controller	187
6. Samba Active Directory Integration	191
7. Likewise Open	193
16. Backups	197
1. Shell Scripts	198
2. Archive Rotation	202
3. Bacula	205
17. Virtualization	210
1. libvirt	211
2. JeOS and vmbuilder	216

List of Tables

2.1. Recommended Minimum Requirements	4
14.1. Access Methods	171

Chapter 1. Introduction

Welcome to the *Ubuntu Server Guide*!

Here you can find information on how to install and configure various server applications. It is a step-by-step, task-oriented guide for configuring and customizing your system.

This guide assumes you have a basic understanding of your Ubuntu system. Some installation details are covered in *Chapter 2, Installation [p. 3]*, but if you need detailed instructions installing Ubuntu please refer to the *Ubuntu Installation Guide*¹.

A HTML version of the manual is available online at *the Ubuntu Documentation website*². The HTML files are also available in the `ubuntu-serverguide` package. See *Chapter 3, Package Management [p. 14]* for details on installing packages.

If you choose to install the `ubuntu-serverguide` you can view this document from a console by:

```
w3m /usr/share/ubuntu-serverguide/html/en_GB/index.html
```



Replace `en_GB` with your language localization.

¹ <https://help.ubuntu.com/8.10/installation-guide/>

² <http://help.ubuntu.com>

1. Support

There are a couple of different ways that Ubuntu Server Edition is supported, commercial support and community support. The main commercial support (and development funding) is available from Canonical Ltd. They supply reasonably priced support contracts on a per desktop or per server basis. For more information see the *Canonical Services*³ page.

Community support is also provided by dedicated individuals, and companies, that wish to make Ubuntu the best distribution possible. Support is provided through multiple mailing lists, IRC channels, forums, blogs, wikis, etc. The large amount of information available can be overwhelming, but a good search engine query can usually provide an answer to your questions. See the *Ubuntu Support*⁴ page for more information.

³ <http://www.canonical.com/services/support>

⁴ <http://www.ubuntu.com/support>

Chapter 2. Installation

This chapter provides a quick overview of installing Ubuntu 8.10 Server Edition. For more detailed instructions, please refer to the *Ubuntu Installation Guide*¹.

¹ <https://help.ubuntu.com/8.10/installation-guide/>

1. Preparing to Install

This section explains various aspects to consider before starting the installation.

1.1. System Requirements

Ubuntu 8.10 Server Edition supports two (2) major architectures: Intel x86 and AMD64. The table below lists recommended hardware specifications. Depending on your needs, you might manage with less than this. However, most users risk being frustrated if they ignore these suggestions.

Table 2.1. Recommended Minimum Requirements

Install Type	RAM	Hard Drive Space
		Base System
Server	128 megabytes	50 gigabyte megabytes

The Server Edition provides a common base for all sorts of server applications. It is a minimalist design providing a platform for the desired services, such as file/print services, web hosting, email hosting, etc.

1.2. Server and Desktop Differences

There are a few differences between the *Ubuntu Server Edition* and the *Ubuntu Desktop Edition*. It should be noted that both editions use the same apt repositories. Making it just as easy to install a *server* application on the Desktop Edition as it is on the Server Edition.

The differences between the two editions are the lack of an X window environment in the Server Edition, the installation process, and different Kernel options.

1.2.1. Kernel Differences:

- The Server Edition uses the *Deadline* I/O scheduler instead of the *CFQ* scheduler used by the Desktop Edition.
- *Preemption* is turned off in the Server Edition.
- The timer interrupt is 100 Hz in the Server Edition and 250 Hz in the Desktop Edition.



When running a 64-bit version of Ubuntu on 64-bit processors you are not limited by memory addressing space.

To see all kernel configuration options you can look through `/boot/config-2.6.27-server`. Also, *Linux Kernel in a Nutshell*² is a great resource on the options available.

² <http://www.kroah.com/lkn/>

1.3. Backing Up

- Before installing Ubuntu Server Edition you should make sure all data on the system is backed up. See *Chapter 16, Backups [p. 197]* for backup options.

If this is not the first time an operating system has been installed on your computer, it is likely you will need to re-partition your disk to make room for Ubuntu.

Any time you partition your disk, you should be prepared to lose everything on the disk should you make a mistake or something goes wrong during partitioning. The programs used in installation are quite reliable, most have seen years of use, but they also perform destructive actions.

2. Installing from CD

The basic steps to install Ubuntu Server Edition from CD are the same for installing any operating system from CD. Unlike the *Desktop Edition* the *Server Edition* does not include a graphical installation program. Instead the Server Edition uses a console menu based process.

- First, download and burn the appropriate ISO file from the *Ubuntu web site*³.
- Boot the system from the CD-ROM drive.
- At the boot prompt you will be asked to select the language. Afterwards the installation process begins by asking for your keyboard layout.
- The installer then discovers your hardware configuration, and configures the network settings using DHCP.
- Next, the installer asks for the system's hostname and Time Zone.
- You can then choose from several options to configure the hard drive layout. For advanced disk options see *Section 4, "Advanced Installation" [p. 10]*.
- The Ubuntu base system is then installed.
- A new user is setup, this user will have *root* access through the *sudo* utility.
- After the user is setup, you will be asked to setup an encrypted `private` directory. If you choose to setup the directory you will then be prompted for an encryption password.
- The next step in the installation process is to decide how you want to update the system. There are three options:
 - *No automatic updates*: this requires an administrator to log into the machine and manually install updates.
 - *Install security updates Automatically*: will install the unattended-upgrades package, which will install security updates without the intervention of an administrator. For more details see *Section 5, "Automatic Updates" [p. 21]*.
 - *Manage the system with Landscape*: Landscape is a paid service provided by Canonical to help manager your Ubuntu machines. See the *Landscape*⁴ site for details.
- You now have the option to install, or not install, several package tasks. See *Section 2.1, "Package Tasks" [p. 7]* for details.
- Finally, the last step before rebooting is to set the clock to UTC.



If at any point during installation you are not satisfied by the default setting, use the "Go Back" function at any prompt to be brought to a detailed installation menu that will allow you to modify the default settings.

At some point during the installation process you may want to read the help screen provided by the installation system. To do this, press F1.

Once again, for detailed instructions see the *Ubuntu Installation Guide*⁵.

⁵ <https://help.ubuntu.com/8.10/installation-guide/>

2.1. Package Tasks

During the Server Edition installation you have the option of installing additional packages from the CD. The packages are grouped by the type of service they provide.

- DNS server: Selects the BIND DNS server and its documentation.
- LAMP server: Selects a ready-made Linux/Apache/MySQL/PHP server.
- Mail server: This task selects a variety of package useful for a general purpose mail server system.
- OpenSSH server: Selects packages needed for an OpenSSH server.
- PostgreSQL database: This task selects client and server packages for the PostgreSQL database.
- Print server: This task sets up your system to be a print server.
- Samba File server: This task sets up your system to be a Samba file server, which is especially suitable in networks with both Windows and Linux systems.
- Tomcat server: Installs the Apache Tomcat and needed dependencies Java, gcj, etc.

Installing the package groups is accomplished using the `tasksel` utility. One of the important difference between Ubuntu (or Debian) and other GNU/Linux distribution is that, when installed, a package is also configured to reasonable defaults, eventually prompting you for additional required information. Likewise, when installing a task, the packages are not only installed, but also configured to provided a fully integrated service.

Once the installation process has finished you can view a list of available tasks by entering the following from a terminal prompt:

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



The output will list tasks from other Ubuntu based distributions such as Kubuntu and Edubuntu. Note that you can also invoke the `tasksel` command by itself, which will bring up a menu of the different tasks available.

You can view a list of which packages are installed with each task using the `--task-packages` option. For example, to list the packages installed with the *DNS Server* task enter the following:

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

The output of the command should list:

```
bind9-doc  
bind9
```

Also, if you did not install one of the tasks during the installation process, but for example you decide to make your new LAMP server a DNS server as well. Simply insert the installation CD and from a terminal:

```
sudo taskset install dns-server
```

3. Upgrading

There are several ways to upgrade from one Ubuntu release to another. This section gives an overview of the recommended upgrade method.

3.1. `do-release-upgrade`

The recommended way to upgrade a Server Edition installation is to use the `do-release-upgrade` utility. Part of the `update-manager-core` package, it does not have any graphical dependencies and is installed by default.

Debian based systems can also be upgraded by using **`apt-get dist-upgrade`**. However, using `do-release-upgrade` is recommended because it has the ability to handle system configuration changes sometimes needed between releases.

To upgrade to a newer release, from a terminal prompt enter:

```
do-release-upgrade
```

It is also possible to use `do-release-upgrade` to upgrade to a development version of Ubuntu. To accomplish this use the `-d` switch:

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



Upgrading to a development release is *not* recommended for production environments.

4. Advanced Installation

4.1. Software RAID

RAID is a method of configuring multiple hard drives to act as one, reducing the probability of catastrophic data loss in case of drive failure. RAID is implemented in either software (where the operating system knows about both drives and actively maintains both of them) or hardware (where a special controller makes the OS think there's only one drive and maintains the drives 'invisibly').

The RAID software included with current versions of Linux (and Ubuntu) is based on the 'mdadm' driver and works very well, better even than many so-called 'hardware' RAID controllers.

4.1.1. Partitioning

Follow the installation steps until you get to the *Partition disks* step, then:

1. Select *Manual* as the partition method.
2. Select the first hard drive, and agree to "*Create a new empty partition table on this device?*".

Repeat this step for each drive you wish to be part of the RAID array.

3. Select the "*FREE SPACE*" on the first drive then select "*Create a new partition*".
4. Next, select the *Size* of the partition, then choose *Primary*, then *Beginning*.
5. Select the "*Use as:*" line at the top. By default this is "*Ext3 journaling file system*", change that to "*physical volume for RAID*".
6. Repeat steps three through five for the other disks and partitions.

4.1.2. RAID Configuration

With the partitions setup the array is ready to be configured:

1. Back in the main "Partition Disks" page, select "*Configure Software RAID*" at the top.
2. Select "*yes*" to write the changes to disk.
3. Choose "*Create new MD drive*".
4. Select "*RAID1*", or the type of RAID you want (RAID0 RAID1 RAID5).



In order to use *RAID5* you need at least *three* drives. Using RAID0 or RAID1 only *two* drives are required.

5. Enter the number of active devices "*2*", or the amount of hard drives you have, for the array. Then select "*Continue*".
6. Next, enter the number of spare devices "*0*" by default, then choose "*Continue*".
7. Choose which partitions to use. Generally they will be sda1, sdb1, sdc1, etc. The numbers will usually match and the different letters correspond to different hard drives.

Select "*Continue*" to go to the next step.

- Repeat steps *three* through *seven* with each pair of partitions you have created (you may only have one pair).
- Once done select "*Finish*".

4.1.3. Formatting

There should now be a list of hard drives and RAID devices. The next step is to format and set the mount point for the RAID devices. Treat the RAID device as a local hard drive, format and mount accordingly.

- Select first RAID device partition.
- Choose "*Use as:*". Then select "*Ext3 journaling file system*", or whichever filesystem you prefer.
- If you selected Ext3, then select your mount point. You can also create multiple partitions on one RAID device or use multiple RAID devices for different partitions. As an example, if you only have one partition for choose "/" as the mount point.
- Repeat for any additional RAID devices.
- Finally, select "*Finish partitioning and write changes to disk*".

If you choose to place the root partition on a RAID array, the installer will then ask if you would like to boot in a *degraded* state. See *Section 4.1.4, "Degraded RAID" [p. 11]* for further details.

The installation process will then continue normally.

4.1.4. Degraded RAID

At some point in the life of the computer a disk failure event may occur. When this happens, using Software RAID, the operating system will place the array into what is known as a *degraded* state.

If the array has become degraded, due to the chance of data corruption, by default Ubuntu Server Edition will boot to *initramfs* after thirty seconds. Once the *initramfs* has booted there is a fifteen second prompt giving you the option to go ahead and boot the system, or attempt manual recover. Booting to the *initramfs* prompt may or may not be the desired behavior, especially if the machine is in a remote location. Booting to a degraded array can be configured several ways:

- The `dpkg-reconfigure` utility can be used to configure the default behavior, and during the process you will be queried about additional settings related to the array. Such as monitoring, email alerts, etc. To reconfigure `mdadm` enter the following:

```
sudo dpkg-reconfigure mdadm
```

- The `dpkg-reconfigure mdadm` process will change the `/etc/initramfs-tools/conf.d/mdadm` configuration file. The file has the advantage of being able to pre-configure the system's behavior, and can also be manually edited:

BOOT_DEGRADED=true



The configuration file can be overridden by using a Kernel argument.

- Using a Kernel argument will allow the system to boot to a degraded array as well:
 - When the server is booting press *ESC* to open the Grub menu.
 - Press "*e*" to edit your Kernel command options.
 - Press the *DOWN* arrow to highlight the kernel line.
 - Press the "*e*" key again to edit the kernel line.
 - Add "*bootdegraded=true*" (without the quotes) to the end of the line.
 - Press "*ENTER*".
 - Finally, press "*b*" to boot the system.

Once the system has booted you can either repair the array see *Section 4.1.5, "RAID Maintenance" [p. 12]* for details, or copy important data to another machine due to major hardware failure.

4.1.5. RAID Maintenance

The `mdadm` utility can be used to view the status of an array, add disks to an array, remove disks, etc:

- To view the status of an array, from a terminal prompt enter:

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

The `-D` tells `mdadm` to display *detailed* information about the `/dev/md0` device. Replace `/dev/md0` with the appropriate RAID device.

- To view the status of a disk in an array:

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

The output is very similar to the `mdadm -D` command, adjust `/dev/sda1` for each disk.

- If a disk fails and needs to be removed from an array enter:

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

Change `/dev/md0` and `/dev/sda1` to the appropriate RAID device and disk.

- Similarly, to add a new disk:

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

Sometimes a disk can change to a *faulty* state even though there is nothing physically wrong with the drive. It is usually worthwhile to remove the drive from the array then re-add it. This will cause

the drive to re-sync with the array. If the drive will not sync with the array, it is a good indication of hardware failure.

The `/proc/mdstat` file also contains useful information about the system's RAID devices:

```
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: <none>
```

The following command is great for watching the status of a syncing drive:

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

Press `Ctrl+c` to stop the watch command.

If you do need to replace a faulty drive, after the drive has been replaced and synced, grub will need to be installed. To install grub on the new drive, enter the following:

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

Replace `/dev/md0` with the appropriate array device name.

4.1.6. Resources

The topic of RAID arrays is a complex one due to the plethora of ways RAID can be configured. Please see the following links for more information:

- *Software RAID HOWTO*⁶
- *Managing RAID on Linux*⁷

Chapter 3. Package Management

Ubuntu features a comprehensive package management system for the installation, upgrade, configuration, and removal of software. In addition to providing access to an organized base of over 24,000 software packages for your Ubuntu computer, the package management facilities also feature dependency resolution capabilities and software update checking.

Several tools are available for interacting with Ubuntu's package management system, from simple command-line utilities which may be easily automated by system administrators, to a simple graphical interface which is easy to use by those new to Ubuntu.

1. Introduction

Ubuntu's package management system is derived from the same system used by the Debian GNU/Linux distribution. The package files contain all of the necessary files, meta-data, and instructions to implement a particular functionality or software application on your Ubuntu computer.

Debian package files typically have the extension '.deb', and typically exist in *repositories* which are collections of packages found on various media, such as CD-ROM discs, or online. Packages are normally of the pre-compiled binary format; thus installation is quick and requires no compiling of software.

Many complex packages use the concept of *dependencies*. Dependencies are additional packages required by the principal package in order to function properly. For example, the speech synthesis package Festival depends upon the package libasound2, which is a package supplying the ALSA sound library needed for audio playback. In order for Festival to function, it and all of its dependencies must be installed. The software management tools in Ubuntu will do this automatically.

2. dpkg

dpkg is a package manager for *Debian* based systems. It can install, remove, and build packages, but unlike other package management system's it can not automatically download and install packages and their dependencies. This section covers using dpkg to manage locally installed packages:

- To list all packages installed on the system, from a terminal prompt enter:

```
dpkg -l
```

- Depending on the amount of packages on your system, this can generate a large amount of output. Pipe the output through grep to see if a specific package is installed:

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

Replace *apache2* with any package name, part of a package name, or other regular expression.

- To list the files installed by a package, in this case the ufw package, enter:

```
dpkg -L ufw
```

- If you are not sure which package installed a file, dpkg -S may be able to tell you. For example:

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

The output shows that the */etc/host.conf* belongs to the base-files package.



Many files are automatically generated during the package install process, and even though they are on the filesystem **dpkg -S** may not know which package they belong to.

- You can install a local *.deb* file by entering:

```
sudo dpkg -i zip_2.32-1_i386.deb
```

Change *zip_2.32-1_i386.deb* to the actual file name of the local *.deb* file.

- Uninstalling a package can be accomplished by:

```
sudo dpkg -r zip
```



Uninstalling packages using dpkg, in most cases, is *NOT* recommended. It is better to use a package manager that handles dependencies, to ensure that the system is in a consistent state. For example using **dpkg -r** you can remove the zip package, but any packages that depend on it will still be installed and may no longer function correctly.

For more dpkg options see the man page: **man dpkg**.

3. Apt-Get

The `apt-get` command is a powerful command-line tool used to work with Ubuntu's *Advanced Packaging Tool* (APT) performing such functions as installation of new software packages, upgrade of existing software packages, updating of the package list index, and even upgrading the entire Ubuntu system.

Being a simple command-line tool, `apt-get` has numerous advantages over other package management tools available in Ubuntu for server administrators. Some of these advantages include ease of use over simple terminal connections (SSH) and the ability to be used in system administration scripts, which can in turn be automated by the cron scheduling utility.

Some examples of popular uses for the `apt-get` utility:

- **Install a Package:** Installation of packages using the `apt-get` tool is quite simple. For example, to install the network scanner `nmap`, type the following:

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

- **Remove a Package:** Removal of a package or packages is also a straightforward and simple process. To remove the `nmap` package installed in the previous example, type the following:

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



Multiple Packages: You may specify multiple packages to be installed or removed, separated by spaces.

Also, adding the `--purge` options to **`apt-get remove`** will remove the package configuration files as well. This may or may not be the desired effect so use with caution.

- **Update the Package Index:** The APT package index is essentially a database of available packages from the repositories defined in the `/etc/apt/sources.list` file. To update the local package index with the latest changes made in repositories, type the following:

```
sudo apt-get update
```

- **Upgrade Packages:** Over time, updated versions of packages currently installed on your computer may become available from the package repositories (for example security updates). To upgrade your system, first update your package index as outlined above, and then type:

```
sudo apt-get upgrade
```

For information on upgrading to a new Ubuntu release see *Section 3, “Upgrading” [p. 9]*.

Actions of the `apt-get` command, such as installation and removal of packages, are logged in the `/var/log/dpkg.log` log file.

For further information about the use of APT, read the comprehensive *Debian APT User Manual*¹ or type:

```
apt-get help
```

¹ <http://www.debian.org/doc/user-manuals#apt-howto>

4. Aptitude

Aptitude is a menu-driven, text-based front-end to the *Advanced Packaging Tool* (APT) system. Many of the common package management functions, such as installation, removal, and upgrade, are performed in Aptitude with single-key commands, which are typically lowercase letters.

Aptitude is best suited for use in a non-graphical terminal environment to ensure proper functioning of the command keys. You may start Aptitude as a normal user with the following command at a terminal prompt:

```
sudo aptitude
```

When Aptitude starts, you will see a menu bar at the top of the screen and two panes below the menu bar. The top pane contains package categories, such as *New Packages* and *Not Installed Packages*. The bottom pane contains information related to the packages and package categories.

Using Aptitude for package management is relatively straightforward, and the user interface makes common tasks simple to perform. The following are examples of common package management functions as performed in Aptitude:

- **Install Packages:** To install a package, locate the package via the Not Installed Packages package category, for example, by using the keyboard arrow keys and the **ENTER** key, and highlight the package you wish to install. After highlighting the package you wish to install, press the + key, and the package entry should turn *green*, indicating it has been marked for installation. Now press **g** to be presented with a summary of package actions. Press **g** again, and you will be prompted to become root to complete the installation. Press **ENTER** which will result in a Password: prompt. Enter your user password to become root. Finally, press **g** once more and you'll be prompted to download the package. Press **ENTER** on the *Continue* prompt, and downloading and installation of the package will commence.
- **Remove Packages:** To remove a package, locate the package via the Installed Packages package category, for example, by using the keyboard arrow keys and the **ENTER** key, and highlight the package you wish to remove. After highlighting the package you wish to install, press the - key, and the package entry should turn *pink*, indicating it has been marked for removal. Now press **g** to be presented with a summary of package actions. Press **g** again, and you will be prompted to become root to complete the installation. Press **ENTER** which will result in a Password: prompt. Enter your user password to become root. Finally, press **g** once more, and you'll be prompted to download the package. Press **ENTER** on the *Continue* prompt, and removal of the package will commence.
- **Update Package Index:** To update the package index, simply press the **u** key and you will be prompted to become root to complete the update. Press **ENTER** which will result in a Password: prompt. Enter your user password to become root. Updating of the package index will commence. Press **ENTER** on the OK prompt when the download dialog is presented to complete the process.
- **Upgrade Packages:** To upgrade packages, perform the update of the package index as detailed above, and then press the **U** key to mark all packages with updates. Now press **g** whereby you'll be

presented with a summary of package actions. Press **g** again, and you will be prompted to become root to complete the installation. Press **ENTER** which will result in a Password: prompt. Enter your user password to become root. Finally, press **g** once more, and you'll be prompted to download the packages. Press **ENTER** on the *Continue* prompt, and upgrade of the packages will commence.

The first column of information displayed in the package list in the top pane, when actually viewing packages lists the current state of the package, and uses the following key to describe the state of the package:

- **i**: Installed package
- **c**: Package not installed, but package configuration remains on system
- **p**: Purged from system
- **v**: Virtual package
- **B**: Broken package
- **u**: Unpacked files, but package not yet configured
- **C**: Half-configured - Configuration failed and requires fix
- **H**: Half-installed - Removal failed and requires fix

To exit Aptitude, simply press the **q** key and confirm you wish to exit. Many other functions are available from the Aptitude menu by pressing the **F10** key.

5. Automatic Updates

The `unattended-upgrades` package can be used to automatically install updated packages, and can be configured to update all packages or just install security updates. First, install the package by entering the following in a terminal:

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

To configure `unattended-upgrades`, edit `/etc/apt/apt.conf.d/50unattended-upgrades` and adjust the following to fit your needs:

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

Certain packages can also be *blacklisted* and therefore will not be automatically updated. To blacklist a package, add it to the list:

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



The double `“//”` serve as comments, so whatever follows `“//”` will not be evaluated.

The results of `unattended-upgrades` will be logged to `/var/log/unattended-upgrades`.

5.1. Notifications

Configuring `Unattended-Upgrade::Mail` in `/etc/apt/apt.conf.d/50unattended-upgrades` will enable `unattended-upgrades` to email an administrator detailing any packages that need upgrading or have problems.

Another useful package is `apticron`. `apticron` will configure a cron job to email an administrator information about any packages on the system that need updated as well as a summary of changes in each package.

To install the `apticron` package, in a terminal enter:

```
sudo apt-get install apticron
```

Once the package is installed edit `/etc/apticron/apticron.conf`, to set the email address and other options:

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

6. Configuration

Configuration of the *Advanced Packaging Tool* (APT) system repositories is stored in the `/etc/apt/sources.list` configuration file. An example of this file is referenced here, along with information on adding or removing repository references from the file.

*Here*² is a simple example of a typical `/etc/apt/sources.list` file.

You may edit the file to enable repositories or disable them. For example, to disable the requirement of inserting the Ubuntu CD-ROM whenever package operations occur, simply comment out the appropriate line for the CD-ROM, which appears at the top of the file:

```
# no more prompting for CD-ROM please
# deb cdrom:[Ubuntu 8.10_Intrepid_Ibex - Release i386 (20070419.1)]/ intrepid main restricted
```

6.1. Extra Repositories

In addition to the officially supported package repositories available for Ubuntu, there exist additional community-maintained repositories which add thousands more potential packages for installation. Two of the most popular are the *Universe* and *Multiverse* repositories. These repositories are not officially supported by Ubuntu, but because they are maintained by the community they generally provide packages which are safe for use with your Ubuntu computer.



Packages in the *Multiverse* repository often have licensing issues that prevent them from being distributed with a free operating system, and they may be illegal in your locality.



Be advised that neither the *Universe* or *Multiverse* repositories contain officially supported packages. In particular, there may not be security updates for these packages.

Many other package sources are available, sometimes even offering only one package, as in the case of package sources provided by the developer of a single application. You should always be very careful and cautious when using non-standard package sources, however. Research the source and packages carefully before performing any installation, as some package sources and their packages could render your system unstable or non-functional in some respects.

By default, the *Universe* and *Multiverse* repositories are enabled but if you would like to disable them edit `/etc/apt/sources.list` and comment the following lines:

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

deb http://us.archive.ubuntu.com/ubuntu/ intrepid universe
deb-src http://us.archive.ubuntu.com/ubuntu/ intrepid universe
```

² `../sample/sources.list`

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

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

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

6.1.1. References

*Adding Repositories HOWTO (Ubuntu Wiki)*³

³ <https://help.ubuntu.com/community/Repositories/Ubuntu>

Chapter 4. Networking

Networks consist of two or more devices, such as computer systems, printers, and related equipment which are connected by either physical cabling or wireless links for the purpose of sharing and distributing information among the connected devices.

This section provides general and specific information pertaining to networking, including an overview of network concepts and detailed discussion of popular network protocols.

1. Network Configuration

Ubuntu ships with a number of graphical utilities to configure your network devices. This document is geared toward server administrators and will focus on managing your network on the command line.

1.1. Ethernet

Most Ethernet configuration is centralized in a single file, `/etc/network/interfaces`. If you have no Ethernet devices, only the loopback interface will appear in this file, and it will look something like this:

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

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

If you have only one Ethernet device, `eth0`, and it gets its configuration from a DHCP server, and it should come up automatically at boot, only two additional lines are required:

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

The first line specifies that the `eth0` device should come up automatically when you boot. The second line means that interface (“iface”) `eth0` should have an IPv4 address space (replace “inet” with “inet6” for an IPv6 device) and that it should get its configuration automatically from DHCP. Assuming your network and DHCP server are properly configured, this machine's network should need no further configuration to operate properly. The DHCP server will provide the default gateway (implemented via the `route` command), the device's IP address (implemented via the `ifconfig` command), and DNS servers used on the network (implemented in the `/etc/resolv.conf` file.)

To configure your Ethernet device with a static IP address and custom configuration, some more information will be required. Suppose you want to assign the IP address `192.168.0.2` to the device `eth1`, with the typical netmask of `255.255.255.0`. Your default gateway's IP address is `192.168.0.1`. You would enter something like this into `/etc/network/interfaces`:

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

In this case, you will need to specify your DNS servers manually in `/etc/resolv.conf`, which should look something like this:

```
search mydomain.example
nameserver 192.168.0.1
nameserver 4.2.2.2
```

The *search* directive will append mydomain.example to hostname queries in an attempt to resolve names to your network. For example, if your network's domain is mydomain.example and you try to ping the host “mybox”, the DNS query will be modified to “mybox.mydomain.example” for resolution. The *nameserver* directives specify DNS servers to be used to resolve hostnames to IP addresses. If you use your own nameserver, enter it here. Otherwise, ask your Internet Service Provider for the primary and secondary DNS servers to use, and enter them into `/etc/resolv.conf` as shown above.

Many more configurations are possible, including dialup PPP interfaces, IPv6 networking, VPN devices, etc. Refer to `man 5 interfaces` for more information and supported options. Remember that `/etc/network/interfaces` is used by the `ifup/ifdown` scripts as a higher level configuration scheme than may be used in some other Linux distributions, and that the traditional, lower level utilities such as `ifconfig`, `route`, and `dhclient` are still available to you for ad hoc configurations.

1.2. Managing DNS Entries

This section explains how to configure which nameserver to use when resolving IP addresses to hostnames and vice versa. It does not explain how to configure the system as a name server.

To manage DNS entries, you can add, edit, or remove DNS names from the `/etc/resolv.conf` file. A sample file is given below:

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

The `search` key specifies the string which will be appended to an incomplete hostname. Here, we have configured it to `com`. So, when we run: **ping ubuntu** it would be interpreted as **ping ubuntu.com**.

The `nameserver` key specifies the nameserver IP address. It will be used to resolve a given IP address or hostname. This file can have multiple `nameserver` entries. The nameservers will be used by the network query in the same order.



If the DNS server names are retrieved dynamically from DHCP or PPPoE (retrieved from your ISP), do not add `nameserver` entries in this file. It will be overwritten.

1.3. Managing Hosts

To manage hosts, you can add, edit, or remove hosts from `/etc/hosts` file. The file contains IP addresses and their corresponding hostnames. When your system tries to resolve a hostname to an IP

address or determine the hostname for an IP address, it refers to the `/etc/hosts` file before using the name servers. If the IP address is listed in the `/etc/hosts` file, the name servers are not used. This behavior can be modified by editing `/etc/nsswitch.conf` at your peril.

If your network contains computers whose IP addresses are not listed in DNS, it is recommended that you add them to the `/etc/hosts` file.

1.4. Bridging

Bridging multiple interfaces is a more advanced configuration, but is very useful in multiple scenarios. One scenario is setting up a bridge with multiple network interfaces, then using a firewall to filter traffic between two network segments. Another scenario is using bridge on a system with one interface to allow virtual machines direct access to the outside network. The following example covers the latter scenario.

Before configuring a bridge you will need to install the `bridge-utils` package. To install the package, in a terminal enter:

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

Next, configure the bridge by editing `/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
```



Enter the appropriate values for your physical interface and network.

Now restart networking to enable the bridge interface:

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

If setting up a bridge interface using Ubuntu Desktop Edition, or if `dhcdd` is installed, the `dhcdd` daemon will need to be stopped and disabled.

After configuring the bridge in `/etc/network/interfaces`, shutdown `dhcdbd` by:

```
sudo /etc/init.d/dhcdbd stop
```

Now to disable it from starting on boot enter:

```
sudo update-rc.d -f dhcdbd remove
```

The new bridge interface should now be up and running. The `brctl` provides useful information about the state of the bridge, controls which interfaces are part of the bridge, etc. See **man brctl** for more information.

2. TCP/IP

The Transmission Control Protocol and Internet Protocol (TCP/IP) is a standard set of protocols developed in the late 1970s by the Defense Advanced Research Projects Agency (DARPA) as a means of communication between different types of computers and computer networks. TCP/IP is the driving force of the Internet, and thus it is the most popular set of network protocols on Earth.

2.1. TCP/IP Introduction

The two protocol components of TCP/IP deal with different aspects of computer networking. *Internet Protocol*, the "IP" of TCP/IP is a connectionless protocol which deals only with network packet routing using the *IP Datagram* as the basic unit of networking information. The IP Datagram consists of a header followed by a message. The *Transmission Control Protocol* is the "TCP" of TCP/IP and enables network hosts to establish connections which may be used to exchange data streams. TCP also guarantees that the data between connections is delivered and that it arrives at one network host in the same order as sent from another network host.

2.2. TCP/IP Configuration

The TCP/IP protocol configuration consists of several elements which must be set by editing the appropriate configuration files, or deploying solutions such as the Dynamic Host Configuration Protocol (DHCP) server which in turn, can be configured to provide the proper TCP/IP configuration settings to network clients automatically. These configuration values must be set correctly in order to facilitate the proper network operation of your Ubuntu system.

The common configuration elements of TCP/IP and their purposes are as follows:

- **IP address** The IP address is a unique identifying string expressed as four decimal numbers ranging from zero (0) to two-hundred and fifty-five (255), separated by periods, with each of the four numbers representing eight (8) bits of the address for a total length of thirty-two (32) bits for the whole address. This format is called *dotted quad notation*.
- **Netmask** The Subnet Mask (or simply, *netmask*) is a local bit mask, or set of flags which separate the portions of an IP address significant to the network from the bits significant to the *subnetwork*. For example, in a Class C network, the standard netmask is 255.255.255.0 which masks the first three bytes of the IP address and allows the last byte of the IP address to remain available for specifying hosts on the subnetwork.
- **Network Address** The Network Address represents the bytes comprising the network portion of an IP address. For example, the host 12.128.1.2 in a Class A network would use 12.0.0.0 as the network address, where twelve (12) represents the first byte of the IP address, (the network part) and zeroes (0) in all of the remaining three bytes to represent the potential host values. A network host using the private IP address 192.168.1.100 would in turn use a Network Address of 192.168.1.0, which specifies the first three bytes of the Class C 192.168.1 network and a zero (0) for all the possible hosts on the network.

- **Broadcast Address** The Broadcast Address is an IP address which allows network data to be sent simultaneously to all hosts on a given subnetwork rather than specifying a particular host. The standard general broadcast address for IP networks is 255.255.255.255, but this broadcast address cannot be used to send a broadcast message to every host on the Internet because routers block it. A more appropriate broadcast address is set to match a specific subnetwork. For example, on the private Class C IP network, 192.168.1.0, the broadcast address is 192.168.1.255. Broadcast messages are typically produced by network protocols such as the Address Resolution Protocol (ARP) and the Routing Information Protocol (RIP).
- **Gateway Address** A Gateway Address is the IP address through which a particular network, or host on a network, may be reached. If one network host wishes to communicate with another network host, and that host is not located on the same network, then a *gateway* must be used. In many cases, the Gateway Address will be that of a router on the same network, which will in turn pass traffic on to other networks or hosts, such as Internet hosts. The value of the Gateway Address setting must be correct, or your system will not be able to reach any hosts beyond those on the same network.
- **Nameserver Address** Nameserver Addresses represent the IP addresses of Domain Name Service (DNS) systems, which resolve network hostnames into IP addresses. There are three levels of Nameserver Addresses, which may be specified in order of precedence: The *Primary* Nameserver, the *Secondary* Nameserver, and the *Tertiary* Nameserver. In order for your system to be able to resolve network hostnames into their corresponding IP addresses, you must specify valid Nameserver Addresses which you are authorized to use in your system's TCP/IP configuration. In many cases these addresses can and will be provided by your network service provider, but many free and publicly accessible nameservers are available for use, such as the Level3 (Verizon) servers with IP addresses from 4.2.2.1 to 4.2.2.6.



The IP address, Netmask, Network Address, Broadcast Address, and Gateway Address are typically specified via the appropriate directives in the file `/etc/network/interfaces`. The Nameserver Addresses are typically specified via `nameserver` directives in the file `/etc/resolv.conf`. For more information, view the system manual page for `interfaces` or `resolv.conf` respectively, with the following commands typed at a terminal prompt:

Access the system manual page for `interfaces` with the following command:

```
man interfaces
```

Access the system manual page for `resolv.conf` with the following command:

```
man resolv.conf
```

2.3. IP Routing

IP routing is a means of specifying and discovering paths in a TCP/IP network along which network data may be sent. Routing uses a set of *routing tables* to direct the forwarding of network data packets from their source to the destination, often via many intermediary network nodes known as *routers*. There are two primary forms of IP routing: *Static Routing* and *Dynamic Routing*.

Static routing involves manually adding IP routes to the system's routing table, and this is usually done by manipulating the routing table with the route command. Static routing enjoys many advantages over dynamic routing, such as simplicity of implementation on smaller networks, predictability (the routing table is always computed in advance, and thus the route is precisely the same each time it is used), and low overhead on other routers and network links due to the lack of a dynamic routing protocol. However, static routing does present some disadvantages as well. For example, static routing is limited to small networks and does not scale well. Static routing also fails completely to adapt to network outages and failures along the route due to the fixed nature of the route.

Dynamic routing depends on large networks with multiple possible IP routes from a source to a destination and makes use of special routing protocols, such as the Router Information Protocol (RIP), which handle the automatic adjustments in routing tables that make dynamic routing possible. Dynamic routing has several advantages over static routing, such as superior scalability and the ability to adapt to failures and outages along network routes. Additionally, there is less manual configuration of the routing tables, since routers learn from one another about their existence and available routes. This trait also eliminates the possibility of introducing mistakes in the routing tables via human error. Dynamic routing is not perfect, however, and presents disadvantages such as heightened complexity and additional network overhead from router communications, which does not immediately benefit the end users, but still consumes network bandwidth.

2.4. TCP and UDP

TCP is a connection-based protocol, offering error correction and guaranteed delivery of data via what is known as *flow control*. Flow control determines when the flow of a data stream needs to be stopped, and previously sent data packets should to be re-sent due to problems such as *collisions*, for example, thus ensuring complete and accurate delivery of the data. TCP is typically used in the exchange of important information such as database transactions.

The User Datagram Protocol (UDP), on the other hand, is a *connectionless* protocol which seldom deals with the transmission of important data because it lacks flow control or any other method to ensure reliable delivery of the data. UDP is commonly used in such applications as audio and video streaming, where it is considerably faster than TCP due to the lack of error correction and flow control, and where the loss of a few packets is not generally catastrophic.

2.5. ICMP

The Internet Control Messaging Protocol (ICMP) is an extension to the Internet Protocol (IP) as defined in the Request For Comments (RFC) #792 and supports network packets containing control, error, and informational messages. ICMP is used by such network applications as the ping utility, which can determine the availability of a network host or device. Examples of some error messages returned by ICMP which are useful to both network hosts and devices such as routers, include *Destination Unreachable* and *Time Exceeded*.

2.6. Daemons

Daemons are special system applications which typically execute continuously in the background and await requests for the functions they provide from other applications. Many daemons are network-centric; that is, a large number of daemons executing in the background on an Ubuntu system may provide network-related functionality. Some examples of such network daemons include the *Hyper Text Transport Protocol Daemon* (httpd), which provides web server functionality; the *Secure SHell Daemon* (sshd), which provides secure remote login shell and file transfer capabilities; and the *Internet Message Access Protocol Daemon* (imapd), which provides E-Mail services.

3. Dynamic Host Configuration Protocol (DHCP)

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

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

- IP-Address and Netmask
- DNS
- WINS

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

- Host Name
- Domain Name
- Default Gateway
- Time Server
- Print Server

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

A DHCP server can provide configuration settings using two methods:

MAC Address

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

Address Pool

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

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

3.1. Installation

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

```
sudo apt-get install dhcp3-server
```

You will probably need to change the default configuration by editing `/etc/dhcp3/dhcpd.conf` to suit your needs and particular configuration.

You also need to edit `/etc/default/dhcp3-server` to specify the interfaces `dhcpd` should listen to. By default it listens to `eth0`.

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

3.2. Configuration

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

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

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

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

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

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

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

Dhcpd configuration settings are taken from the DHCP mini-HOWTO, which can be found *here*¹.

¹ <http://www.tldp.org/HOWTO/DHCP/index.html>

3.3. References

*DHCP FAQ*²

² http://www.dhcp-handbook.com/dhcp_faq.html

4. Time Synchronisation with NTP

This page describes methods for keeping your computer's time accurate. This is useful for servers, but is not necessary (or desirable) for desktop machines.

NTP is a TCP/IP protocol for synchronising time over a network. Basically a client requests the current time from a server, and uses it to set its own clock.

Behind this simple description, there is a lot of complexity - there are tiers of NTP servers, with the tier one NTP servers connected to atomic clocks (often via GPS), and tier two and three servers spreading the load of actually handling requests across the Internet. Also the client software is a lot more complex than you might think - it has to factor out communication delays, and adjust the time in a way that does not upset all the other processes that run on the server. But luckily all that complexity is hidden from you!

Ubuntu has two ways of automatically setting your time: `ntpdate` and `ntpd`.

4.1. ntpdate

Ubuntu comes with `ntpdate` as standard, and will run it once at boot time to set up your time according to Ubuntu's NTP server. However, a server's clock is likely to drift considerably between reboots, so it makes sense to correct the time occasionally. The easiest way to do this is to get cron to run `ntpdate` every day. With your favourite editor, as root, create a file `/etc/cron.daily/ntpdate` containing:

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

The file `/etc/cron.daily/ntpdate` must also be executable.

```
sudo chmod 755 /etc/cron.daily/ntpdate
```

4.2. ntpd

`ntpdate` is a bit of a blunt instrument - it can only adjust the time once a day, in one big correction.

The `ntp` daemon `ntpd` is far more subtle. It calculates the drift of your system clock and continuously adjusts it, so there are no large corrections that could lead to inconsistent logs for instance. The cost is a little processing power and memory, but for a modern server this is negligible.

To set up `ntpd`:

```
sudo apt-get install ntp
```

4.3. Changing Time Servers

In both cases above, your system will use Ubuntu's NTP server at `ntp.ubuntu.com` by default. This is OK, but you might want to use several servers to increase accuracy and resilience, and you may want to use time servers that are geographically closer to you. to do this for `ntpdate`, change the contents of `/etc/cron.daily/ntpdate` to:

```
ntpdate ntp.ubuntu.com pool.ntp.org
```

And for ntpd edit `/etc/ntp.conf` to include additional server lines:

```
server ntp.ubuntu.com
server pool.ntp.org
```

You may notice `pool.ntp.org` in the examples above. This is a really good idea which uses round-robin DNS to return an NTP server from a pool, spreading the load between several different servers. Even better, they have pools for different regions - for instance, if you are in New Zealand, so you could use `nz.pool.ntp.org` instead of `pool.ntp.org`. Look at <http://www.pool.ntp.org/> for more details.

You can also Google for NTP servers in your region, and add these to your configuration. To test that a server works, just type `sudo ntpdate ntp.server.name` and see what happens.

4.4. Related Pages

- *NTP Support*³
- *The NTP FAQ and HOWTO*⁴

Chapter 5. Remote Administration

There are many ways to remotely administer a Linux server. This chapter will cover one of the most popular SSH as well as eBox, a web based administration framework.

1. OpenSSH Server

1.1. Introduction

This section of the Ubuntu Server Guide introduces a powerful collection of tools for the remote control of networked computers and transfer of data between networked computers, called *OpenSSH*. You will also learn about some of the configuration settings possible with the OpenSSH server application and how to change them on your Ubuntu system.

OpenSSH is a freely available version of the Secure Shell (SSH) protocol family of tools for remotely controlling a computer or transferring files between computers. Traditional tools used to accomplish these functions, such as telnet or rcp, are insecure and transmit the user's password in cleartext when used. OpenSSH provides a server daemon and client tools to facilitate secure, encrypted remote control and file transfer operations, effectively replacing the legacy tools.

The OpenSSH server component, `sshd`, listens continuously for client connections from any of the client tools. When a connection request occurs, `sshd` sets up the correct connection depending on the type of client tool connecting. For example, if the remote computer is connecting with the `ssh` client application, the OpenSSH server sets up a remote control session after authentication. If a remote user connects to an OpenSSH server with `scp`, the OpenSSH server daemon initiates a secure copy of files between the server and client after authentication. OpenSSH can use many authentication methods, including plain password, public key, and Kerberos tickets.

1.2. Installation

Installation of the OpenSSH client and server applications is simple. To install the OpenSSH client applications on your Ubuntu system, use this command at a terminal prompt:

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

To install the OpenSSH server application, and related support files, use this command at a terminal prompt:

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

The `openssh-server` package can also be selected to install during the Server Edition installation process.

1.3. Configuration

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

```
man sshd_config
```

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



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

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

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

The following are examples of configuration directives you may change:

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

Port 2222

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

PubkeyAuthentication yes

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

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

Banner /etc/issue.net

In the `/etc/ssh/sshd_config` file.

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

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



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

1.4. SSH Keys

SSH *keys* allow authentication between two hosts without the need of a password. SSH key authentication uses two keys a *private* key and a *public* key.

To generate the keys, from a terminal prompt enter:

```
ssh-keygen -t dsa
```

This will generate the keys using a *DSA* authentication identity of the user. During the process you will be prompted for a password. Simply hit *Enter* when prompted to create the key.

By default the *public* key is saved in the file `~/.ssh/id_dsa.pub`, while `~/.ssh/id_dsa` is the *private* key. Now copy the `id_dsa.pub` file to the remote host and appended it to `~/.ssh/authorized_keys2`:

```
cat id_dsa.pub >> .ssh/authorized_keys2
```

Finally, double check the permissions on the `authorized_keys2` file, only the authenticated user should have read and write permissions. If the permissions are not correct change them by:

```
chmod 644 .ssh/authorized_keys2
```

You should now be able to SSH to the host without being prompted for a password.

1.5. References

*OpenSSH Website*¹

*Advanced OpenSSH Wiki Page*²

¹ <http://www.openssh.org/>

² <https://wiki.ubuntu.com/AdvancedOpenSSH>

2. eBox

eBox is a web framework used to manager server application configuration. The modular design of eBox allows you to pick and choose which services you want to configure using eBox.

2.1. Installation

The different eBox modules are split into different packages, allowing you to only install those necessary. One way to view the available packages is to enter the following from a terminal:

```
apt-cache rdepends ebox | uniq
```

To install the ebox package, which contains the default modules, enter the following:

```
sudo apt-get install ebox
```

If you want to install all the available modules, the ebox-all meta package will install all the modules.

During the installation you will be asked to supply a password for the ebox user. After installing eBox the web interface can be accessed from: <https://yourserver/ebox>.

2.2. Configuration

An important thing to remember when using eBox is that when configuring most modules there is a *Change* button that implements the new configuration. After clicking the Change button most, but not all, modules will then need to be *Saved*. To save the new configuration click on the “Save changes” link in the top right hand corner.



Once you make a change that requires a Save, the link will change from green to red.

2.3. eBox Modules

By default all eBox *Modules* are not enabled, and when a new module is installed it will not be automatically enabled.

To enable a disabled module click on the *Module status* link in the left hand menu. Then *check* which modules you would like to enable and click the “Save” link.

2.3.1. Default Modules

This section provides a quick summary of the default eBox modules.

- *System*: contains options allowing configuration of general eBox items.
 - *General*: allows you to set the language, port number, and contains a change password form.
 - *Disk Usage*: displays a graph detailing information about disk usage.

- *Backup*: is used to backup eBox configuration information, and the *Full Backup* option allows you to save all eBox information not included in the *Configuration* option such as log files.
- *Halt/Reboot*: will shutdown the system or reboot it.
- *Bug Report*: creates a file containing details helpful when reporting bugs to the eBox developers.
- *Logs*: allows eBox logs to be queried depending on the purge time configured.
- *Events*: this module has the ability to send alerts through rss, jabber, and log file.
 - *Available Events*:
 - *Free Storage Space*: will send alert if free disk space drops below a configured percentage, 10% by default.
 - *Log Observer*: unfortunately this event does not work with the eBox version shipped with Ubuntu 7.10.
 - *RAID*: will monitor the RAID system and send alerts if any issues arise.
 - *Service*: sends alerts if a service restarts multiple times in a short time period.
 - *State*: alerts on the state of eBox, either up or down.
 - *Dispatchers*:
 - *Log*: this dispatcher will send event messages to the eBox log file `/var/log/ebox/ebox.log`.
 - *Jabber*: before enabling this dispatcher you must first configure it by clicking on the “Configure” icon.
 - *RSS*: once this dispatcher is configured you can subscribe to the link in order to view event alerts.

2.4. Additional Modules

Here is a quick description of other available eBox modules:

- *Network*: allows configuration of the server's network options through eBox.
- *Firewall*: configures firewall options for the eBox host.
- *UsersandGroups*: this module will manage users and groups contained in an OpenLDAP LDAP directory.
- *DHCP*: provides an interface for configuring a DHCP server.
- *DNS*: provides BIND9 DNS server configuration options.
- *Objects*: allow configuration of eBox *Network Objects*, which allow you to assign a name to an IP address or group of IPs.
- *Services*: displays configuration information for services that are available to the network.
- *Squid*: configuration options for the Squid proxy server.
- *CA*: configures a Certificate Authority for the server.
- *NTP*: set Network Time Protocol options.
- *Printers*: allows the configuration of printers.

- *Samba*: configuration options for Samba.
- *OpenVPN*: setup options for OpenVPN Virtual Private Network application.

2.5. Resources

- For more information see the *eBox Home Page*³.

Chapter 6. Network Authentication

This section explains various Network Authentication protocols.

1. OpenLDAP Server

LDAP is an acronym for Lightweight Directory Access Protocol, it is a simplified version of the X.500 protocol. The directory setup in this section will be used for authentication. Nevertheless, LDAP can be used in numerous ways: authentication, shared directory (for mail clients), address book, etc.

To describe LDAP quickly, all information is stored in a tree structure. With OpenLDAP you have freedom to determine the directory arborescence (the Directory Information Tree: the DIT) yourself. We will begin with a basic tree containing two nodes below the root:

- "People" node where your users will be stored
- "Groups" node where your groups will be stored

Before beginning, you should determine what the root of your LDAP directory will be. By default, your tree will be determined by your Fully Qualified Domain Name (FQDN). If your domain is example.com (which we will use in this example), your root node will be dc=example,dc=com.

1.1. Installation

First, install the OpenLDAP server daemon slapd and ldap-utils, a package containing LDAP management utilities:

```
sudo apt-get install slapd ldap-utils
```

The installation process will prompt you for the LDAP directory admin password and confirmation.

By default the directory suffix will match the domain name of the server. For example, if the machine's Fully Qualified Domain Name (FQDN) is ldap.example.com, the default suffix will be *dc=example,dc=com*. If you require a different suffix, the directory can be reconfigured using dpkg-reconfigure. Enter the following in a terminal prompt:

```
sudo dpkg-reconfigure slapd
```

You will then be taken through a menu based configuration dialog, allowing you to configure various slapd options.

1.2. Configuration

OpenLDAP uses a separate database which contains the *cn=config* Directory Information Tree (DIT). The *cn=config* DIT is used to dynamically configure the slapd daemon, allowing the modification of schema definitions, indexes, ACLs, etc without stopping the service.

The *cn=config* tree can be manipulated using the utilities in the ldap-utils package. For example:

- Use ldapsearch to view the tree, entering the admin password set during installation or reconfiguration:

```
ldapsearch -xLLL -b cn=config -D cn=admin,cn=config -W olcDatabase={1}hdb
```

Enter LDAP Password:

```
dn: olcDatabase={1}hdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcHdbConfig
olcDatabase: {1}hdb
olcDbDirectory: /var/lib/ldap
olcSuffix: dc=example,dc=com
olcAccess: {0}to attrs=userPassword,shadowLastChange by dn="cn=admin,dc=exampl
e,dc=com" write by anonymous auth by self write by * none
olcAccess: {1}to dn.base="" by * read
olcAccess: {2}to * by dn="cn=admin,dc=example,dc=com" write by * read
olcLastMod: TRUE
olcDbCheckpoint: 512 30
olcDbConfig: {0}set_cachesize 0 2097152 0
olcDbConfig: {1}set_lik_max_objects 1500
olcDbConfig: {2}set_lik_max_locks 1500
olcDbConfig: {3}set_lik_max_lockers 1500
olcDbIndex: objectClass eq
```

The output above is the current configuration options for the *hdb* backend database. Which in this case contains the *dc=example,dc=com* suffix.

- Refine the search by supplying a *filter*, in this case only show which attributes are indexed:

```
ldapsearch -xLLL -b cn=config -D cn=admin,cn=config -W olcDatabase={1}hdb olcDbIndex
```

Enter LDAP Password:

```
dn: olcDatabase={1}hdb,cn=config
olcDbIndex: objectClass eq
```

- As an example of modifying the *cn=config* tree, add another attribute to the index list using `ldapmodify`:

```
ldapmodify -x -D cn=admin,cn=config -W
```

Enter LDAP Password:

```
dn: olcDatabase={1}hdb,cn=config
add: olcDbIndex
olcDbIndex: cn eq,pres,sub
```

```
modifying entry "olcDatabase={1}hdb,cn=config"
```

Once the modification has completed, press *Ctrl+D* to exit the utility.

- `ldapmodify` can also read the changes from a file. Copy and paste the following into a file named `uid_index.ldif`:

```
dn: olcDatabase={1}hdb,cn=config
add: olcDbIndex
olcDbIndex: uid eq,pres,sub
```

Then execute `ldapmodify`:

```
ldapmodify -x -D cn=admin,cn=config -W -f uid_index.ldif
```

```
Enter LDAP Password:
modifying entry "olcDatabase={1}hdb,cn=config"
```

The file method is very useful for large changes.

- Adding additional *schemas* to `slapd` requires the schema to be converted to LDIF format. Fortunately, the `slapd` program can be used to automate the conversion. The following example will add the *misc.schema*:

1. First, create a conversion `schema_convert.conf` file containing the following lines:

```
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
```

2. Next, create a temporary directory to hold the output:

```
mkdir /tmp/ldif_output
```

3. Now using `slaptest` convert the schema files to LDIF:

```
slaptest -f schema_convert.conf -F /tmp/ldif_output
```

Adjust the configuration file name and temporary directory names if yours are different. Also, it may be worthwhile to keep the `ldif_output` directory around in case you want to add additional schemas in the future.

4. Edit the `/tmp/ldif_output/cn=config/cn=schema/cn={8}misc.ldif` file, changing the following attributes:

```
dn: cn=misc,cn=schema,cn=config
...
cn: misc
```

And remove the following lines from the bottom of the file:

```
structuralObjectClass: olcSchemaConfig
entryUUID: 10dae0ea-0760-102d-80d3-f9366b7f7757
creatorsName: cn=config
createTimestamp: 20080826021140Z
entryCSN: 20080826021140.791425Z#000000#000#000000
modifiersName: cn=config
modifyTimestamp: 20080826021140Z
```



The attribute values will vary, just be sure the attributes are removed.

5. Finally, using the `ldapadd` utility, add the new schema to the directory:

```
ldapadd -x -D cn=admin,cn=config -f /tmp/ldif_output/cn=config/cn=schema/cn=\{8\}misc.ldif
```

There should now be a `dn: cn={4}misc,cn=schema,cn=config` entry in the `cn=config` tree.

1.3. Populating LDAP

The directory has been created during installation and reconfiguration, and now it is time to populate it. It will be populated with a "classical" scheme that will be compatible with address book applications and with Unix Posix accounts. Posix accounts will allow authentication to various applications, such as web applications, email Mail Transfer Agent (MTA) applications, etc.



For external applications to authenticate using LDAP they will each need to be specifically configured to do so. Refer to the individual application documentation for details.

LDAP directories can be populated with LDIF (LDAP Directory Interchange Format) files. Copy the following example LDIF file, naming it `example.com.ldif`, somewhere on your system:

```
dn: ou=people,dc=example,dc=com
objectClass: organizationalUnit
ou: people
```

```
dn: ou=groups,dc=example,dc=com
objectClass: organizationalUnit
ou: groups
```

```
dn: uid=john,ou=people,dc=example,dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: john
sn: Doe
givenName: John
cn: John Doe
displayName: John Doe
uidNumber: 1000
gidNumber: 10000
userPassword: password
gecos: John Doe
loginShell: /bin/bash
homeDirectory: /home/john
shadowExpire: -1
shadowFlag: 0
shadowWarning: 7
shadowMin: 8
shadowMax: 999999
shadowLastChange: 10877
mail: john.doe@example.com
postalCode: 31000
l: Toulouse
o: Example
mobile: +33 (0)6 xx xx xx xx
homePhone: +33 (0)5 xx xx xx xx
title: System Administrator
postalAddress:
initials: JD
```

```
dn: cn=example,ou=groups,dc=example,dc=com
objectClass: posixGroup
cn: example
gidNumber: 10000
```

In this example the directory structure, a user, and a group have been setup. In other examples you might see the *objectClass: top* added in every entry, but that is the default behaviour so you do not have to add it explicitly.

To add the entries to the LDAP directory use the `ldapadd` utility:

```
ldapadd -x -D cn=admin,dc=example,dc=com -W -f example.com.ldif
```

We can check that the content has been correctly added with the tools from the `ldap-utils` package. In order to execute a search of the LDAP directory:

```
ldapsearch -xLLL -b "dc=example,dc=com" uid=john sn givenName cn
```

```
dn: uid=john,ou=people,dc=example,dc=com
cn: John Doe
```

```
sn: Doe
givenName: John
```

Just a quick explanation:

- `-x`: will not use SASL authentication method, which is the default.
- `-LLL`: disable printing LDIF schema information.

1.4. LDAP replication

LDAP often quickly becomes a highly critical service to the network. Multiple systems will come to depend on LDAP for authentication, authorization, configuration, etc. It is a good idea to setup a redundant system through replication.

Replication is achieved using the *Syncrepl* engine. Syncrepl allows the directory to be synced using either a *push* or *pull* based system. In a push based configuration a “primary” server will push directory updates to “secondary” servers, while a pull based approach allows replication servers to sync on a time based interval.

The following is an example of a *Multi-Master* configuration. In this configuration each OpenLDAP server is configured for both *push* and *pull* replication.

1. First, configure the server to sync the `cn=config` database. Copy the following to a file named `syncrepl_cn-config.ldif`:

```
dn: cn=module{0},cn=config
changetype: modify
add: olcModuleLoad
olcModuleLoad: syncprov

dn: cn=config
changetype: modify
replace: olcServerID
olcServerID: 1 ldap://ldap01.example.com
olcServerID: 2 ldap://ldap02.example.com

dn: olcOverlay=syncprov,olcDatabase={0}config,cn=config
changetype: add
objectClass: olcOverlayConfig
objectClass: olcSyncProvConfig
olcOverlay: syncprov

dn: olcDatabase={0}config,cn=config
changetype: modify
add: olcSyncRepl
olcSyncRepl: rid=001 provider=ldap://ldap01.example.com binddn="cn=admin,cn=config" bindmethod=
  credentials=secret searchbase="cn=config" type=refreshAndPersist
  retry="5 5 300 5" timeout=1
olcSyncRepl: rid=002 provider=ldap://ldap02.example.com binddn="cn=admin,cn=config" bindmethod=
```

```
credentials=secret searchbase="cn=config" type=refreshAndPersist
retry="5 5 300 5" timeout=1
```

```
-
add: olcMirrorMode
olcMirrorMode: TRUE
```

2. Edit the file changing:

- `ldap://ldap01.example.com` and `ldap://ldap02.example.com` to the hostnames of your LDAP servers.



You can have more than two LDAP servers, and when a change is made to one of them it will be synced to the rest. Be sure to increment the `olcServerID` for each server, and the `rid` for each `olcSyncRepl` entry.

- And adjust `credentials=secret` to match your admin password.

3. Next, add the LDIF file using the `ldapmodify` utility:

```
ldapmodify -x -D cn=admin,cn=config -W -f syncrepl_cn-config.ldif
```

4. Copy the `syncrepl_cn-config.ldif` file to the next LDAP server and repeat the `ldapmodify` command above.

5. Because a new module has been added, the `slapd` daemon, on all replicated servers, needs to be restarted:

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

6. Now that the configuration database is synced between servers, the `backend` database needs to be synced as well. Copy and paste the following into another LDIF file named `syncrepl_backend.ldif`:

```
dn: olcDatabase={1}hdb,cn=config
changetype: modify
add: olcRootDN
olcRootDN: cn=admin,dc=example,dc=edu
-
add: olcSyncRepl
olcSyncRepl: rid=003 provider=ldap://ldap01.example.com binddn="cn=admin,dc=example,dc=com"
bindmethod=simple credentials=secret searchbase="dc=example,dc=com" type=refreshOnly
interval=00:00:00:10 retry="5 5 300 5" timeout=1
olcSyncRepl: rid=004 provider=ldap://ldap02.example.com binddn="cn=admin,dc=example,dc=com"
bindmethod=simple credentials=secret searchbase="dc=example,dc=com" type=refreshOnly
interval=00:00:00:10 retry="5 5 300 5" timeout=1
-
add: olcMirrorMode
olcMirrorMode: TRUE

dn: olcOverlay=syncprov,olcDatabase={1}hdb,cn=config
changetype: add
objectClass: olcOverlayConfig
```

```
objectClass: olcSyncProvConfig
olcOverlay: syncprov
```

7. Like the previous LDIF file, edit this one changing:

- `searchbase="dc=example,dc=com"` to your directory's searchbase.
- If you use a different admin user, change `binddn="cn=admin,dc=example,dc=com"`.
- Also, replace `credentials=secret` with your admin password.

8. Add the LDIF file:

```
ldapmodify -x -D cn=admin,cn=config -W -f syncrepl_backend.ldif
```

Because the servers' configuration is already synced there is no need to copy this LDIF file to the other servers.

The configuration and backend databases should now sync to the other servers. You can add additional servers using the `ldapmodify` utility as the need arises. See *Section 1.2, "Configuration" [p. 47]* for details.



The `slapd` daemon will send log information to `/var/log/syslog` by default. So if all does *not* go well check there for errors and other troubleshooting information.

1.5. Setting up ACL

Authentication requires access to the password field, that should be not accessible by default. Also, in order for users to change their own password, using `passwd` or other utilities, `shadowLastChange` needs to be accessible once a user has authenticated.

To view the Access Control List (ACL), use the `ldapsearch` utility:

```
ldapsearch -xLLL -b cn=config -D cn=admin,cn=config -W olcDatabase=hdb olcAccess
```

```
Enter LDAP Password:
dn: olcDatabase={1}hdb,cn=config
olcAccess: {0}to attrs=userPassword,shadowLastChange by dn="cn=admin,dc=example,dc=com" write by anonymous auth by self write by * none
olcAccess: {1}to dn.base="" by * read
olcAccess: {2}to * by dn="cn=admin,dc=example,dc=com" write by * read
```

1.6. TLS and SSL

When authenticating to an OpenLDAP server it is best to do so using an encrypted session. This can be accomplished using Transport Layer Security (TLS) and/or Secure Sockets Layer (SSL).

The first step in the process is to obtain or create a *certificate*. See *Section 5, "Certificates" [p. 105]* and *Section 5.5, "Certification Authority" [p. 107]* for details.

Once you have a certificate, key, and CA cert installed, use `ldapmodify` to add the new configuration options:

```
ldapmodify -x -D cn=admin,cn=config -W
```

```
Enter LDAP Password:
dn: cn=config
add: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/ssl/certs/cacert.pem
-
add: olcTLSCertificateFile
olcTLSCertificateFile: /etc/ssl/certs/server.crt
-
add: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/ssl/private/server.key

modifying entry "cn=config"
```



Adjust the `server.crt`, `server.key`, and `cacert.pem` names if yours are different.

Next, edit `/etc/default/slapd` uncomment the `SLAPD_SERVICES` option:

```
SLAPD_SERVICES="ldap://127.0.0.1:389/ ldaps:/// ldapi://"
```

Now the *openldap* user needs access to the certificate:

```
sudo adduser openldap ssl-cert
sudo chgrp ssl-cert /etc/ssl/private/server.key
```



If the `/etc/ssl/private` and `/etc/ssl/private/server.key` have different permissions, adjust the commands appropriately.

Finally, restart `slapd`:

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

The `slapd` daemon should now be listening for LDAPS connections and be able to use STARTTLS during authentication.

1.6.1. TLS Replication

If you have setup Syncrepl between servers, it is prudent to encrypt the replication traffic using *Transport Layer Security (TLS)*. For details on setting up replication see *Section 1.4, "LDAP replication" [p. 52]*.

After setting up replication, and following the instructions in *Section 1.6, “TLS and SSL” [p. 54]*, there are a couple of consequences that should be kept in mind:

- The configuration only needs to be modified on *one* server.
- The path names for the *certificate* and *key* must be the same on all servers.

So on each replicated server: install a certificate, edit `/etc/default/slapd`, and restart slapd.

Once *TLS* has been setup on each server, modify the `cn=config` replication by entering the following in a terminal:

```
ldapmodify -x -D cn=admin,cn=config -W
```

```
Enter LDAP Password:
dn: olcDatabase={0}config,cn=config
replace: olcSyncrepl
olcSyncrepl: {0}rid=001 provider=ldap://ldap01.example.com binddn="cn=admin,cn
=config" bindmethod=simple credentials=secret searchbase="cn=config" type=refre
shAndPersist retry="5 5 300 5" timeout=1 starttls=yes
olcSyncrepl: {1}rid=002 provider=ldap://ldap02.example.com binddn="cn=admin,cn
=config" bindmethod=simple credentials=secret searchbase="cn=config" type=refre
shAndPersist retry="5 5 300 5" timeout=1 starttls=yes

modifying entry "olcDatabase={0}config,cn=config"
```

Now adjust the *backend* database replication:

```
ldapmodify -x -D cn=admin,cn=config -W
```

```
Enter LDAP Password:
dn: olcDatabase={1}hdb,cn=config
replace: olcSyncrepl
olcSyncrepl: {0}rid=003 provider=ldap://ldap01.example.com binddn="cn=admin,dc=example,dc=
com" bindmethod=simple credentials=secret searchbase="dc=example,dc=com" type=r
efreshOnly interval=00:00:00:10 retry="5 5 300 5" timeout=1 starttls=yes
olcSyncrepl: {1}rid=004 provider=ldap://ldap02.example.com binddn="cn=admin,dc=example,dc=
com" bindmethod=simple credentials=secret searchbase="dc=example,dc=com" type=r
efreshOnly interval=00:00:00:10 retry="5 5 300 5" timeout=1 starttls=yes

modifying entry "olcDatabase={1}hdb,cn=config"
```

If the LDAP server hostname does not match the Fully Qualified Domain Name (FQDN) in the certificate, you may have to edit `/etc/ldap/ldap.conf` and add the following TLS options:

```
TLS_CERT /etc/ssl/certs/server.crt
TLS_KEY /etc/ssl/private/server.key
TLS_CACERT /etc/ssl/certs/cacert.pem
```

Finally, restart slapd on each of the servers:

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

1.7. LDAP Authentication

Once you have a working LDAP server, the auth-client-config and libnss-ldap packages take the pain out of configuring an Ubuntu client to authenticate using LDAP. To install the packages from, a terminal prompt enter:

```
sudo apt-get install libnss-ldap
```

During the install a menu dialog will ask you connection details about your LDAP server.

If you make a mistake when entering your information you can execute the dialog again using:

```
sudo dpkg-reconfigure ldap-auth-config
```

The results of the dialog can be seen in `/etc/ldap.conf`. If your server requires options not covered in the menu edit this file accordingly.

Now that libnss-ldap is configured enable the auth-client-config LDAP profile by entering:

```
sudo auth-client-config -a -p lac_ldap
```

- *-a*: applies the specified profile.
- *-p*: name of the profile to enable, disable, etc.
- *lac_ldap*: the auth-client-config profile that is part of the ldap-auth-config package.

You should now be able to login using user credentials stored in the LDAP directory.

1.8. User and Group Management

The ldap-utils package comes with multiple utilities to manage the directory, but the long string of options needed, can make them a burden to use. The ldapscripts package contains configurable scripts to easily manage LDAP users and groups.

To install the package, from a terminal enter:

```
sudo apt-get install ldapscripts
```

Next, edit the config file `/etc/ldapscripts/ldapscripts.conf` uncommenting and changing the following to match your environment:

```
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
```

Now, create the `ldapscripts.passwd` file to allow authenticated access to the directory:

```
sudo sh -c "echo -n 'secret' > /etc/ldapscripts/ldapscripts.passwd"
sudo chmod 400 /etc/ldapscripts/ldapscripts.passwd
```



Replace “secret” with the actual password for your LDAP admin user.

The `ldapscripts` are now ready to help manage your directory. The following are some examples of how to use the scripts:

- Create a new user:

```
sudo ldapadduser george example
```

This will create a user with uid `george` and set the user's primary group (gid) to `example`

- Change a user's password:

```
sudo ldapsetpasswd george
Changing password for user uid=george,ou=People,dc=example,dc=com
New Password:
New Password (verify):
```

- Delete a user:

```
sudo ldapdeleteuser george
```

- Add a group:

```
sudo ldapaddgroup qa
```

- Delete a group:

```
sudo ldapdeletegroup qa
```

- Add a user to a group:

```
sudo ldapaddusertogroup george qa
```

You should now see a *memberUid* attribute for the *qa* group with a value of *george*.

- Remove a user from a group:

```
sudo ldapdeleteuserfromgroup george qa
```

The *memberUid* attribute should now be removed from the *qa* group.

- The *ldapmodifyuser* script allows you to add, remove, or replace a user's attributes. The script uses the same syntax as the *ldapmodify* utility. For example:

```
sudo ldapmodifyuser george
# About to modify the following entry :
dn: uid=george,ou=People,dc=example,dc=com
objectClass: account
objectClass: posixAccount
cn: george
uid: george
uidNumber: 1001
gidNumber: 1001
homeDirectory: /home/george
loginShell: /bin/bash
gecos: george
description: User account
userPassword:: e1NTSEF9eXFstFcyWlhwWkFleGUybVdFWHZKRzJVMjFTSG9vcHk=

# Enter your modifications here, end with CTRL-D.
dn: uid=george,ou=People,dc=example,dc=com
replace: geccos
gecos: George Carlin
```

The user's *gecos* should now be “George Carlin”.

- Another great feature of *ldapscripts*, is the template system. Templates allow you to customize the attributes of user, group, and machine objects. For example, to enable the *user* template edit */etc/ldapscripts/ldapscripts.conf* changing:

```
UTEMPLATE="/etc/ldapscripts/ldapadduser.template"
```

There are *sample* templates in the */etc/ldapscripts* directory. Copy or rename the *ldapadduser.template.sample* file to */etc/ldapscripts/ldapadduser.template*:

```
sudo cp /etc/ldapscripts/ldapadduser.template.sample /etc/ldapscripts/ldapadduser.template
```

Edit the new template to add the desired attributes. The following will create new user's as with an *objectClass* of *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
```

Notice the `<ask>` option used for the `cn` value. Using `<ask>` will configure `ldapadduser` to prompt you for the attribute value during user creation.

There are more useful scripts in the package, to see a full list enter: **`dpkg -L ldapscripts | grep bin`**

1.9. Resources

- For more information see *OpenLDAP Home Page*¹
- Though starting to show it's age, a great source for in depth LDAP information is O'Reilly's *LDAP System Administration*²
- Packt's *Mastering OpenLDAP*³ is a great reference covering newer versions of OpenLDAP.
- For more information on `auth-client-config` see the man page: **`man auth-client-config`**.
- For more details regarding the `ldapscripts` package see the man pages: **`man ldapscripts`, `man ldapadduser`, `man ldapaddgroup`**, etc.

2. Samba and LDAP

This section covers configuring Samba to use LDAP for user, group, and machine account information and authentication. The assumption is, you already have a working OpenLDAP directory installed and the server is configured to use it for authentication. See *Section 1, “OpenLDAP Server”* [p. 47] and *Section 1.7, “LDAP Authentication”* [p. 57] for details on setting up OpenLDAP.

2.1. Installation

There are three packages needed when integrating Samba with LDAP. `samba`, `samba-doc`, and `smbldap-tools` packages. To install the packages, from a terminal enter:

```
sudo apt-get install samba samba-doc smbldap-tools
```

Strictly speaking the `smbldap-tools` package isn't needed, but unless you have another package or custom scripts, a method of managing users, groups, and computer accounts is needed.

2.2. OpenLDAP Configuration

In order for Samba to use OpenLDAP as a *passwd backend*, the user objects in the directory will need additional attributes. This section assumes you want Samba to be configured as a Windows NT domain controller, and will add the necessary LDAP objects and attributes.

- The Samba attributes are defined in the `samba.schema` file which is part of the `samba-doc` package. The schema file needs to be unzipped and copied to `/etc/ldap/schema`. From a terminal prompt enter:

```
sudo cp /usr/share/doc/samba-doc/examples/LDAP/samba.schema.gz /etc/ldap/schema/  
sudo gzip -d /etc/ldap/schema/samba.schema.gz
```

- The `samba` schema needs to be added to the `cn=config` tree. The procedure to add a new schema to `slapd` is also detailed in *Section 1.2, “Configuration”* [p. 47].

1. First, create a configuration file named `schema_convert.conf`, or a similar descriptive name, containing the following lines:

```
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/samba.schema
```

2. Next, create a temporary directory to hold the output:

```
mkdir /tmp/ldif_output
```

3. Now use slaptest to convert the schema files:

```
slaptest -f schema_convert.conf -F /tmp/ldif_output
```

Change the above file and path names to match your own if they are different.

4. Edit the generated `/tmp/ldif_output/cn=config/cn=schema/cn={12}samba.ldif` file, changing the following attributes:

```
dn: cn=samba,cn=schema,cn=config
...
cn: samba
```

And remove the following lines from the bottom of the file:

```
structuralObjectClass: olcSchemaConfig
entryUUID: b53b75ca-083f-102d-9fff-2f64fd123c95
creatorsName: cn=config
createTimestamp: 20080827045234Z
entryCSN: 20080827045234.341425Z#000000#000#000000
modifiersName: cn=config
modifyTimestamp: 20080827045234Z
```



The attribute values will vary, just be sure the attributes are removed.

5. Finally, using the `ldapadd` utility, add the new schema to the directory:

```
ldapadd -x -D cn=admin,cn=config -f /tmp/ldif_output/cn=config/cn=schema/cn=\{12\}misc.ldif
```

There should now be a `dn: cn={X}misc,cn=schema,cn=config`, where "X" is the next sequential schema, entry in the `cn=config` tree.

- Copy and paste the following into a file named `samba_indexes.ldif`:

```
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
```

Using the `ldapmodify` utility load the new indexes:

```
ldapmodify -x -D cn=admin,cn=config -W -f samba_indexes.ldif
```

If all went well you should see the new indexes using `ldapsearch`:

```
ldapsearch -xLLL -D cn=admin,cn=config -x -b cn=config -W olcDatabase={1}hdb
```

- Next, configure the `smbldap-tools` package to match your environment. The package comes with a configuration script that will ask questions about the needed options. To run the script enter:

```
sudo gzip -d /usr/share/doc/smbldap-tools/configure.pl.gz
sudo perl /usr/share/doc/smbldap-tools/configure.pl
```

Once you have answered the questions, there should be `/etc/smbldap-tools/smbldap.conf` and `/etc/smbldap-tools/smbldap_bind.conf` files. These files are generated by the configure script, so if you made any mistakes while executing the script it may be simpler to edit the file appropriately.

- The `smbldap-populate` script will add the necessary users, groups, and LDAP objects required for Samba. It is a good idea to make a backup LDAP Data Interchange Format (LDIF) file with `slapcat` before executing the command:

```
sudo slapcat -l backup.ldif
```

- Once you have a current backup execute `smbldap-populate` by entering:

```
sudo smbldap-populate
```



You can create an LDIF file containing the new Samba objects by executing **sudo smbldap-populate -e samba.ldif**. This allows you to look over the changes making sure everything is correct.

Your LDAP directory now has the necessary domain information to authenticate Samba users.

2.3. Samba Configuration

There are multiple ways to configure Samba for details on some common configurations see *Chapter 15, Windows Networking [p. 178]*. To configure Samba to use LDAP, edit the main Samba configuration file `/etc/samba/smb.conf` commenting the *passdb backend* option and adding the following:

```
# 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 = dc=example,dc=com
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"
```

Restart samba to enable the new settings:

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

Now Samba needs to know the LDAP admin password. From a terminal prompt enter:

```
sudo smbpasswd -w secret
```



Replacing *secret* with your LDAP admin password.

If you currently have users in LDAP, and you want them to authenticate using Samba, they will need some Samba attributes defined in the `samba.schema` file. Add the Samba attributes to existing users using the `smbpasswd` utility, replacing *username* with an actual user:

```
sudo smbpasswd -a username
```

You will then be asked to enter the user's password.

To add new user, group, and machine accounts use the utilities from the `smbldap-tools` package. Here are some examples:

- To add a new user to LDAP with Samba attributes enter the following, replacing *username* with an actual username:

```
sudo smbldap-useradd -a -P username
```

The `-a` option adds the Samba attributes, and the `-P` options calls the `smbldap-passwd` utility after the user is created allowing you to enter a password for the user.

- To remove a user from the directory enter:

```
sudo smbldap-userdel username
```

The smbldap-userdel utility also has a *-r* option to remove the user's home directory.

- Use smbldap-groupadd to add a group, replacing groupname with an appropriate group:

```
sudo smbldap-groupadd -a groupname
```

Similar to smbldap-useradd, the *-a* adds the Samba attributes.

- To add a user to a group use smbldap-groupmod:

```
sudo smbldap-groupmod -m username groupname
```

Be sure to replace *username* with a real user. Also, the *-m* option can add more than one user at a time by listing them in *comma separated* format.

- smbldap-groupmod can also be used to remove a user from a group:

```
sudo smbldap-groupmod -x username groupname
```

- Additionally, the smbldap-useradd utility can add Samba machine accounts:

```
sudo smbldap-useradd -t 0 -w username
```

Replace *username* with the name of the workstation. The *-t 0* option creates the machine account without a delay, while the *-w* option specifies the user as a machine account. Also, note the *add machine script* option in `/etc/samba/smb.conf` was changed to use smbldap-useradd.

There are more useful utilities and options in the smbldap-tools package. The man page for each utility provides more details.

2.4. Resources

- There are multiple places where LDAP and Samba is documented in the *Samba HOWTO Collection*⁴.
- Specifically see the *passwd* section⁵.
- Another good site is *Samba OpenLDAP HOWTO*⁶.
- Again, for more information on smbldap-tools see the man pages: **man smbldap-useradd**, **man smbldap-groupadd**, **man smbldap-populate**, etc.

3. Kerberos

Kerberos is a network authentication system based on the principal of a trusted third party. The other two parties being the user and the service the user wishes to authenticate to. Not all services and applications can use Kerberos, but for those that can, it brings the network environment one step closer to being Single Sign On (SSO).

This section covers installation and configuration of a Kerberos server, and some example client configurations.

3.1. Overview

If you are new to Kerberos there are a few terms that are good to understand before setting up a Kerberos server. Most of the terms will relate to things you may be familiar with in other environments:

- *Principal*: any users, computers, and services provided by servers need to be defined as Kerberos Principals.
- *Instances*: are used for service principals and special administrative principals.
- *Realms*: the unique realm of control provided by the Kerberos installation. Usually the DNS domain converted to uppercase (EXAMPLE.COM).
- *Key Distribution Center*: (KDC) consist of three parts, a database of all principals, the authentication server, and the ticket granting server. For each realm there must be at least one KDC.
- *Ticket Granting Ticket*: issued by the Authentication Server (AS), the Ticket Granting Ticket (TGT) is encrypted in the user's password which is known only to the user and the KDC.
- *Ticket Granting Server*: (TGS) issues service tickets to clients upon request.
- *Tickets*: confirm the identity of the two principals. One principal being a user and the other a service requested by the user. Tickets establish an encryption key used for secure communication during the authenticated session.
- *Keytab Files*: are files extracted from the KDC principal database and contain the encryption key for a service or host.

To put the pieces together, a Realm has at least one KDC, preferably two for redundancy, which contains a database of Principals. When a user principal logs into a workstation, configured for Kerberos authentication, the KDC issues a Ticket Granting Ticket (TGT). If the user supplied credentials match, the user is authenticated and can then request tickets for Kerberized services from the Ticket Granting Server (TGS). The service tickets allow the user to authenticate to the service without entering another username and password.

3.2. Kerberos Server

3.2.1. Installation

Before installing the Kerberos server a properly configured DNS server is needed for your domain. Since the Kerberos Realm by convention matches the domain name, this section uses the *example.com* domain configured in *Section 2.3, "Primary Master" [p. 76]*.

Also, Kerberos is a time sensitive protocol. So if the local system time between a client machine and the server differs by more than five minutes (by default), the workstation will not be able to authenticate. To correct the problem all hosts should have their time synchronized using the *Network Time Protocol (NTP)*. For details on setting up NTP see *Section 4, "Time Synchronisation with NTP" [p. 37]*.

The first step in installing a Kerberos Realm is to install the `krb5-kdc` and `krb5-admin-server` packages. From a terminal enter:

```
sudo apt-get install krb5-kdc krb5-admin-server
```

You will be asked at the end of the install to supply a name for the Kerberos and Admin servers, which may or may not be the same server, for the realm.

Next, create the new realm with the `kdb5_newrealm` utility:

```
sudo krb5_newrealm
```

3.2.2. Configuration

The questions asked during installation are used to configure the `/etc/krb5.conf` file. If you need to adjust the Key Distribution Center (KDC) settings simply edit the file and restart the `krb5-kdc` daemon.

1. Now that the KDC running an admin user is needed. It is recommended to use a different username from your everyday username. Using the `kadmin.local` utility in a terminal prompt enter:

```
sudo kadmin.local
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
```

In the the above example *steve* is the *Principal*, */admin* is an *Instance*, and *@EXAMPLE.COM* signifies the realm. The "*every day*" Principal would be *steve@EXAMPLE.COM*, and should have only normal user rights.



Replace *EXAMPLE.COM* and *steve* with your Realm and admin username.

- Next, the new admin user needs to have the appropriate Access Control List (ACL) permissions. The permissions are configured in the `/etc/krb5kdc/kadm5.ac1` file:

```
steve/admin@EXAMPLE.COM *
```

This entry grants *steve/admin* the ability to perform any operation on all principals in the realm.

- Now restart the `krb5-admin-server` for the new ACL to take affect:

```
sudo /etc/init.d/krb5-admin-server restart
```

- The new user principal can be tested using the `kinit` utility:

```
kinit steve/admin
steve/admin@EXAMPLE.COM's Password:
```

After entering the password, use the `klist` utility to view information about the Ticket Granting Ticket (TGT):

```
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
```

You may need to add an entry into the `/etc/hosts` for the KDC. For example:

```
192.168.0.1    kdc01.example.com    kdc01
```

Replacing *192.168.0.1* with the IP address of your KDC.

- In order for clients to determine the KDC for the Realm some DNS SRV records are needed. Add the following to `/etc/named/db.example.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.
```



Replace *EXAMPLE.COM*, *kdc01*, and *kdc02* with your domain name, primary KDC, and secondary KDC.

See *Chapter 7, Domain Name Service (DNS) [p. 73]* for detailed instructions on setting up DNS.

Your new Kerberos Realm is now ready to authenticate clients.

3.3. Secondary KDC

Once you have one Key Distribution Center (KDC) on your network, it is good practice to have a Secondary KDC in case the primary becomes unavailable.

1. First, install the packages, and when asked for the Kerberos and Admin server names enter the name of the Primary KDC:

```
sudo apt-get install krb5-kdc krb5-admin-server
```

2. Once you have the packages installed, create the Secondary KDC's host principal. From a terminal prompt, enter:

```
kadmin -q "addprinc -randkey host/kdc02.example.com"
```



After, issuing any `kadmin` commands you will be prompted for your *username/admin@EXAMPLE.COM* principal password.

3. Extract the *keytab* file:

```
kadmin -q "ktadd -k keytab.kdc02 host/kdc02.example.com"
```

4. There should now be a `keytab.kdc02` in the current directory, move the file to `/etc/krb5.keytab`:

```
sudo mv keytab.kdc02 /etc/krb5.keytab
```



If the path to the `keytab.kdc02` file is different adjust accordingly.

Also, you can list the principals in a Keytab file, which can be useful when troubleshooting, using the `klist` utility:

```
sudo klist -k /etc/krb5.keytab
```

5. Next, there needs to be a `kpropd.ac1` file on each KDC that lists all KDCs for the Realm. For example, on both primary and secondary KDC, create `/etc/krb5kdc/kpropd.ac1`:

```
host/kdc01.example.com@EXAMPLE.COM  
host/kdc02.example.com@EXAMPLE.COM
```

6. Create an empty database on the *Secondary KDC*:

```
sudo kdb5_util -s create
```

7. Now start the kpropd daemon, which listens for connections from the kprop utility. kprop is used to transfer dump files:

```
sudo kpropd -s
```

8. From a terminal on the *Primary KDC*, create a dump file of the principal database:

```
sudo kdb5_util dump /var/lib/krb5kdc/dump
```

9. Extract the Primary KDC's *keytab* file and copy it to `/etc/krb5.keytab`:

```
kadmin -q "ktadd -k keytab.kdc01 host/kdc01.example.com"  
sudo mv keytab.kdc01 /etc/kr5b.keytab
```



Make sure there is a *host* for `kdc01.example.com` before extracting the Keytab.

10. Using the kprop utility push the database to the Secondary KDC:

```
sudo kprop -r EXAMPLE.COM -f /var/lib/krb5kdc/dump kdc02.example.com
```



There should be a *SUCCEEDED* message if the propagation worked. If there is an error message check `/var/log/syslog` on the secondary KDC for more information.

You may also want to create a cron job to periodically update the database on the Secondary KDC. For example, the following will push the database every hour:

```
# m h dom mon dow    command  
0 * * * * /usr/sbin/kdb5_util dump /var/lib/krb5kdc/dump && /usr/sbin/kprop -r EXAMPLE.COM -f /
```

11. Back on the *Secondary KDC*, create a *stash* file to hold the Kerberos master key:

```
sudo kdb5_util stash
```

12. Finally, start the `krb5-kdc` daemon on the Secondary KDC:

```
sudo /etc/init.d/krb5-kdc start
```

The *Secondary KDC* should now be able to issue tickets for the Realm. You can test this by stopping the `krb5-kdc` daemon on the Primary KDC, then use `kinit` to request a ticket. If all goes well you should receive a ticket from the Secondary KDC.

3.4. Kerberos Linux Client

This section covers configuring a Linux system as a Kerberos client. This will allow access to any kerberized services once a user has successfully logged into the system.

3.4.1. Installation

In order to authenticate to a Kerberos Realm, the `krb5-user` and `libpam-krb5` packages are needed, along with a few others that are not strictly necessary but make life easier. To install the packages enter the following in a terminal prompt:

```
sudo apt-get install krb5-user libpam-krb5 libpam-ccreds auth-client-config
```

The `auth-client-config` package allows simple configuration of PAM for authentication from multiple sources, and the `libpam-ccreds` will cache authentication credentials allowing you to login in case the Key Distribution Center (KDC) is unavailable. This package is also useful for laptops that may authenticate using Kerberos while on the corporate network, but will need to be accessed off the network as well.

3.4.2. Configuration

To configure the client in a terminal enter:

```
sudo dpkg-reconfigure krb5-config
```

You will then be prompted to enter the name of the Kerberos Realm. Also, if you don't have DNS configured with Kerberos *SRV* records, the menu will prompt you for the hostname of the Key Distribution Center (KDC) and Realm Administration server.

The `dpkg-reconfigure` adds entries to the `/etc/krb5.conf` file for your Realm. You should have entries similar to the following:

```
[libdefaults]
    default_realm = EXAMPLE.COM
...
[realms]
    EXAMPLE.COM = {
        kdc = 192.168.0.1
        admin_server = 192.168.0.1
    }
```

You can test the configuration by requesting a ticket using the `kinit` utility. For example:

```
kinit steve@EXAMPLE.COM
Password for steve@EXAMPLE.COM:
```

When a ticket has been granted, the details can be viewed using `klist`:

klist

```
Ticket cache: FILE:/tmp/krb5cc_1000
Default principal: steve@EXAMPLE.COM
```

```
Valid starting    Expires          Service principal
07/24/08 05:18:56  07/24/08 15:18:56  krbtgt/EXAMPLE.COM@EXAMPLE.COM
        renew until 07/25/08 05:18:57
```

```
Kerberos 4 ticket cache: /tmp/tkt1000
klist: You have no tickets cached
```

Next, use the `auth-client-config` to configure the `libpam-krb5` module to request a ticket during login:

```
sudo auth-client-config -a -p kerberos_example
```

You will should now receive a ticket upon successful login authentication.

3.5. Resources

- For more information on Kerberos see the *MIT Kerberos*⁷ site.
- O'Reilly's *Kerberos: The Definitive Guide*⁸ is a great reference when setting up Kerberos.
- Also, feel free to stop by the `#ubuntu-server` IRC channel on *Freenode*⁹ if you have Kerberos questions.

Chapter 7. Domain Name Service (DNS)

Domain Name Service (DNS) is an Internet service that maps IP addresses and fully qualified domain names (FQDN) to one another. In this way, DNS alleviates the need to remember IP addresses.

Computers that run DNS are called *name servers*. Ubuntu ships with BIND (Berkley Internet Naming Daemon), the most common program used for maintaining a name server on Linux.

1. Installation

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

```
sudo apt-get install bind9
```

A very useful package for testing and troubleshooting DNS issues is the dnsutils package. To install dnsutils enter the following:

```
sudo apt-get install dnsutils
```

2. Configuration

There are many ways to configure BIND9. Some of the most common configurations are as a caching nameserver, primary master, and as a secondary master.

- When configured as a caching nameserver BIND9 will find the answer to name queries and remember the answer when the domain is queried again.
- As a primary master server BIND9 reads the data for a zone from a file on its host and is authoritative for that zone.
- In a secondary master configuration BIND9 gets the zone data from another nameserver authoritative for the zone.

2.1. Overview

The DNS configuration files are stored in the `/etc/bind` directory. The primary configuration file is `/etc/bind/named.conf`.

The *include* line specifies the filename which contains the DNS options. The *directory* line in the `/etc/bind/named.conf.options` file tells DNS where to look for files. All files BIND uses will be relative to this directory.

The file named `/etc/bind/db.root` describes the root nameservers in the world. The servers change over time, so the `/etc/bind/db.root` file must be maintained now and then. This is usually done as updates to the bind9 package. The *zone* section defines a master server, and it is stored in a file mentioned in the *file* option.

It is possible to configure the same server to be a caching name server, primary master, and secondary master. A server can be the Start of Authority (SOA) for one zone, while providing secondary service for another zone. All the while providing caching services for hosts on the local LAN.

2.2. Caching Nameserver

The default configuration is setup to act as a caching server. All that is required is simply adding the IP Addresses of your ISP's DNS servers. Simply uncomment and edit the following in `/etc/bind/named.conf.options`:

```
forwarders {  
    1.2.3.4;  
    5.6.7.8;  
};
```



Replace *1.2.3.4* and *5.6.7.8* with the IP Addresses of actual nameservers.

Now restart the DNS server, to enable the new configuration. From a terminal prompt:

```
sudo /etc/init.d/bind9 restart
```

See Section 3.1.3, “dig” [p. 80] for information on testing a caching DNS server.

2.3. Primary Master

In this section BIND9 will be configured as the Primary Master for the domain *example.com*. Simply replace *example.com* with your FQDN (Fully Qualified Domain Name).

2.3.1. Forward Zone File

To add a DNS zone to BIND9, turning BIND9 into a Primary Master server, the first step is to edit `/etc/bind/named.conf.local`:

```
zone "example.com" {
    type master;
        file "/etc/bind/db.example.com";
};
```

Now use an existing zone file as a template to create the `/etc/bind/db.example.com` file:

```
sudo cp /etc/bind/db.local /etc/bind/db.example.com
```

Edit the new zone file `/etc/bind/db.example.com` change *localhost*. to the FQDN of your server, leaving the additional "." at the end. Change *127.0.0.1* to the nameserver's IP Address and *root.localhost* to a valid email address, but with a "." instead of the usual "@" symbol, again leaving the "." at the end.

Also, create an *A record* for *ns.example.com*. The name server in this example:

```

;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      ns.example.com. root.example.com. (
                        1          ; Serial
                        604800     ; Refresh
                        86400      ; Retry
                        2419200    ; Expire
                        604800 )   ; Negative Cache TTL
;
@         IN      NS       ns.example.com.
@         IN      A        192.168.1.10
ns        IN      A        192.168.1.10
```

You must increment the *Serial Number* every time you make changes to the zone file. If you make multiple changes before restarting BIND9, simply increment the Serial once.

Now, you can add DNS records to the bottom of the zone file. See *Section 4.1, “Common Record Types” [p. 84]* for details.



Many admins like to use the last date edited as the serial of a zone, such as *2007010100* which is *yyyymmddss* (where *ss* is the Serial Number)

Once you have made a change to the zone file BIND9 will need to be restarted for the changes to take affect:

```
sudo /etc/init.d/bind9 restart
```

2.3.2. Reverse Zone File

Now that the zone is setup and resolving names to IP Addresses a *Reverse zone* is also required. A Reverse zone allows DNS to resolve an address to a name.

Edit `/etc/bind/named.conf.local` and add the following:

```
zone "1.168.192.in-addr.arpa" {
    type master;
    notify no;
    file "/etc/bind/db.192";
};
```



Replace *1.168.192* with the first three octets of whatever network you are using. Also, name the zone file `/etc/bind/db.192` appropriately. It should match the first octet of your network.

Now create the `/etc/bind/db.192` file:

```
sudo cp /etc/bind/db.127 /etc/bind/db.192
```

Next edit `/etc/bind/db.192` changing the basically the same options as `/etc/bind/db.example.com`:

```
;  
; BIND reverse data file for local loopback interface  
;  
$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.
```

The *Serial Number* in the Reverse zone needs to be incremented on each changes as well. For each *A record* you configure in `/etc/bind/db.example.com` you need to create a *PTR record* in `/etc/bind/db.192`.

After creating the reverse zone file restart BIND9:

```
sudo /etc/init.d/bind9 restart
```

2.4. Secondary Master

Once a *Primary Master* has been configured a *Secondary Master* is needed in order to maintain the availability of the domain should the Primary become unavailable.

First, on the Primary Master server, the zone transfer needs to be allowed. Add the *allow-transfer* option to the example Forward and Reverse zone definitions in `/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;
    notify no;
    file "/etc/bind/db.192";
    allow-transfer { 192.168.1.11; };
};
```



Replace *192.168.1.11* with the IP Address of your Secondary nameserver.

Next, on the Secondary Master, install the `bind9` package the same way as on the Primary. Then edit the `/etc/bind/named.conf.local` and add the following declarations for the Forward and Reverse zones:

```
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; };
};
```



Replace *192.168.1.10* with the IP Address of your Primary nameserver.

Restart BIND9 on the Secondary Master:

```
sudo /etc/init.d/bind9 restart
```

In `/var/log/syslog` you should see something similar to:

```
slave zone "example.com" (IN) loaded (serial 6)
slave zone "100.18.172.in-addr.arpa" (IN) loaded (serial 3)
```



Note: A zone is only transferred if the *Serial Number* on the Primary is larger than the one on the Secondary.

3. Troubleshooting

This section covers ways to help determine the cause when problems happen with DNS and BIND9.

3.1. Testing

3.1.1. resolv.conf

The first step in testing BIND9 is to add the nameserver's IP Address to a hosts resolver. The Primary nameserver should be configured as well as another host to double check things. Simply edit `/etc/resolv.conf` and add the following:

```
nameserver 192.168.1.10
nameserver 192.168.1.11
```



You should also add the IP Address of the Secondary nameserver in case the Primary becomes unavailable.

3.1.2. ping

Once a host has been configured to use the new nameserver one of the simplest tests is the ping utility. From a terminal prompt enter:

```
ping example.com
```

This tests if the nameserver can resolve the name *example.com* to an IP Address. The command output should resemble:

```
PING example.com (192.168.1.10) 56(84) bytes of data.
64 bytes from ns (192.168.1.10): icmp_seq=1 ttl=64 time=0.800 ms
64 bytes from ns (192.168.1.10): icmp_seq=2 ttl=64 time=0.813 ms
```

3.1.3. dig

If you installed the `dnsutils` package you can test your setup using the DNS lookup utility `dig`:

- After installing BIND9 use `dig` against the loopback interface to make sure it is listening on port 53. From a terminal prompt:

```
dig -x 127.0.0.1
```

You should see lines similar to the following in the command output:

```
;; Query time: 1 msec
;; SERVER: 192.168.1.10#53(192.168.1.10)
```

- If you have configured BIND9 as a *Caching* nameserver "dig" an outside domain to check the query time:

```
dig ubuntu.com
```

Note the query time toward the end of the command output:

```
;; Query time: 49 msec
```

After a second dig there should be improvement:

```
;; Query time: 1 msec
```

3.1.4. named-checkzone

A great way to test your zone files is by using the named-checkzone utility installed with the bind9 package. This utility allows you to make sure the configuration is correct before restarting BIND9 and making the changes live.

- To test our example Forward zone file enter the following from a command prompt:

```
named-checkzone example.com /etc/bind/db.example.com
```

If everything is configured correctly you should see output similar to:

```
zone example.com/IN: loaded serial 6
OK
```

- Similarly, to test the Reverse zone file enter the following:

```
named-checkzone example.com /etc/bind/db.192
```

The output should be similar to:

```
zone example.com/IN: loaded serial 3
OK
```



The *Serial Number* of your zone file will probably be different.

3.2. Logging

BIND9 has a wide variety of logging configuration options available. There are two main options. The *channel* option configures where logs go, and the *category* option determines what information to log.

If no logging option is configured the default option is:

```
logging {
    category default { default_syslog; default_debug; };
    category unmatched { null; };
};
```

This section covers configuring BIND9 to send *debug* messages related to DNS queries to a separate file.

- First, we need to configure a channel to specify which file to send the messages to. Edit `/etc/bind/named.conf.local` and add the following:

```
logging {
    channel query.log {
        file "/var/log/query.log";
        severity debug 3;
    };
};
```

- Next, configure a category to send all DNS queries to the query file:

```
logging {
    channel query.log {
        file "/var/log/query.log";
        severity debug 3;
    };
    category queries { query.log; };
};
```



Note: the *debug* option can be set from 1 to 3. If a level isn't specified level 1 is the default.

- Since the *named daemon* runs as the *bind* user the `/var/log/query.log` file must be created and the ownership changed:

```
sudo touch /var/log/query.log
sudo chown bind /var/log/query.log
```

- Before *named daemon* can write to the new log file the AppArmor profile must be updated. First, edit `/etc/apparmor.d/usr.sbin.named` and add:

```
/var/log/query.log w,
```

Next, reload the profile:

```
cat /etc/apparmor.d/usr.sbin.named | sudo apparmor_parser -r
```

For more information on AppArmor see *Section 4, "AppArmor" [p. 101]*

- Now restart BIND9 for the changes to take affect:

```
sudo /etc/init.d/bind9 restart
```

You should see the file `/var/log/query.log` fill with query information. This is a simple example of the BIND9 logging options. For coverage of advanced options see *Section 4.2, “More Information”* [p. 84].

4. References

4.1. Common Record Types

This section covers some of the most common DNS record types.

- *A* record: This record maps an IP Address to a hostname.

```
www      IN      A        192.168.1.12
```

- *CNAME* record: Used to create an alias to an existing *A* record. You cannot create a *CNAME* record pointing to another *CNAME* record.

```
web      IN      CNAME    www
```

- *MX* record: Used to define where email should be sent to. Must point to an *A* record, not a *CNAME*.

```
          IN      MX        mail.example.com.
mail     IN      A         192.168.1.13
```

- *NS* record: Used to define which servers serve copies of a zone. It must point to an *A* record, not a *CNAME*. This is where Primary and Secondary servers are defined.

```
          IN      NS        ns.example.com.
          IN      NS        ns2.example.com.
ns       IN      A         192.168.1.10
ns2     IN      A         192.168.1.11
```

4.2. More Information

The *DNS HOWTO*¹ explains more advanced options for configuring BIND9.

For in depth coverage of *DNS* and BIND9 see *Bind9.net*².

*DNS and BIND*³ is a popular book now in it's fifth edition.

A great place to ask for BIND9 assistance, and get involved with the Ubuntu Server community, is the *#ubuntu-server* IRC channel on *freenode*⁴.

¹ <http://www.tldp.org/HOWTO/DNS-HOWTO.html>

² <http://www.bind9.net/>

³ <http://www.oreilly.com/catalog/dns5/index.html>

⁴ <http://freenode.net>

Chapter 8. Security

Security should always be considered when installing, deploying, and using any type of computer system. Although a fresh installation of Ubuntu is relatively safe for immediate use on the Internet, it is important to have a balanced understanding of your systems security posture based on how it will be used after deployment.

This chapter provides an overview of security related topics as they pertain to Ubuntu 8.10 Server Edition, and outlines simple measures you may use to protect your server and network from any number of potential security threats.

1. User Management

User management is a critical part of maintaining a secure system. Ineffective user and privilege management often lead many systems into being compromised. Therefore, it is important that you understand how you can protect your server through simple and effective user account management techniques.

1.1. Where is root?

Ubuntu developers made a conscientious decision to disable the administrative root account by default in all Ubuntu installations. This does not mean that the root account has been deleted or that it may not be accessed. It merely has been given a password which matches no possible encrypted value, therefore may not log in directly by itself.

Instead, users are encouraged to make use of a tool by the name of sudo to carry out system administrative duties. Sudo allows an authorized user to temporarily elevate their privileges using their own password instead of having to know the password belonging to the root account. This simple yet effective methodology provides accountability for all user actions, and gives the administrator granular control over which actions a user can perform with said privileges.

- If for some reason you wish to enable the root account, simply give it a password:

```
sudo passwd
```

Sudo will prompt you for your password, and then ask you to supply a new password for root as shown below:

```
[sudo] password for username: (enter your own password)
Enter new UNIX password: (enter a new password for root)
Retype new UNIX password: (repeat new password for root)
passwd: password updated successfully
```

- To disable the root account, use the following passwd syntax:

```
sudo passwd -l root
```

- You should read more on Sudo by checking out it's man page:

```
man sudo
```

By default, the initial user created by the Ubuntu installer is a member of the group "admin" which is added to the file `/etc/sudoers` as an authorized sudo user. If you wish to give any other account full root access through sudo, simply add them to the admin group.

1.2. Adding and Deleting Users

The process for managing local users and groups is straight forward and differs very little from most other GNU/Linux operating systems. Ubuntu and other Debian based distributions, encourage the use of the "adduser" package for account management.

- To add a user account, use the following syntax, and follow the prompts to give the account a password and identifiable characteristics such as a full name, phone number, etc.

```
sudo adduser username
```

- To delete a user account and its primary group, use the following syntax:

```
sudo deluser username
```

Deleting an account does not remove their respective home folder. It is up to you whether or not you wish to delete the folder manually or keep it according to your desired retention policies.

Remember, any user added later on with the same UID/GID as the previous owner will now have access to this folder if you have not taken the necessary precautions.

You may want to change these UID/GID values to something more appropriate, such as the root account, and perhaps even relocate the folder to avoid future conflicts:

```
sudo chown -R root:root /home/username/  
sudo mkdir /home/archived_users/  
sudo mv /home/username /home/archived_users/
```

- To temporarily lock or unlock a user account, use the following syntax, respectively:

```
sudo passwd -l username  
sudo passwd -u username
```

- To add or delete a personalized group, use the following syntax, respectively:

```
sudo addgroup groupname  
sudo delgroup groupname
```

- To add a user to a group, use the following syntax:

```
sudo adduser username groupname
```

1.3. User Profile Security

When a new user is created, the adduser utility creates a brand new home directory named `/home/username`, respectively. The default profile is modeled after the contents found in the directory of `/etc/skel`, which includes all profile basics.

If your server will be home to multiple users, you should pay close attention to the user home directory permissions to ensure confidentiality. By default, user home directories in Ubuntu are created with world read/execute permissions. This means that all users can browse and access the contents of other users home directories. This may not be suitable for your environment.

- To verify your current users home directory permissions, use the following syntax:

```
ls -ld /home/username
```

The following output shows that the directory `/home/username` has world readable permissions:

```
drwxr-xr-x  2 username username    4096 2007-10-02 20:03 username
```

- You can remove the world readable permissions using the following syntax:

```
sudo chmod 0750 /home/username
```



Some people tend to use the recursive option (-R) indiscriminately which modifies all child folders and files, but this is not necessary, and may yield other undesirable results. The parent directory alone is sufficient for preventing unauthorized access to anything below the parent.

A much more efficient approach to the matter would be to modify the `adduser` global default permissions when creating user home folders. Simply edit the file `/etc/adduser.conf` and modify the `DIR_MODE` variable to something appropriate, so that all new home directories will receive the correct permissions.

```
DIR_MODE=0750
```

- After correcting the directory permissions using any of the previously mentioned techniques, verify the results using the following syntax:

```
ls -ld /home/username
```

The results below show that world readable permissions have been removed:

```
drwxr-x---  2 username username    4096 2007-10-02 20:03 username
```

1.4. Password Policy

A strong password policy is one of the most important aspects of your security posture. Many successful security breaches involve simple brute force and dictionary attacks against weak passwords. If you intend to offer any form of remote access involving your local password system, make sure you adequately address minimum password complexity requirements, maximum password lifetimes, and frequent audits of your authentication systems.

1.4.1. Minimum Password Length

By default, Ubuntu requires a minimum password length of 4 characters, as well as some basic entropy checks. These values are controlled in the file `/etc/pam.d/common-password`, which is outlined below.

```
password    required    pam_unix.so nullok obscure min=4 max=8 md5
```

If you would like to adjust the minimum length to 6 characters, change the appropriate variable to `min=6`. The modification is outlined below.

```
password    required    pam_unix.so nullok obscure min=6 max=8 md5
```



The `max=8` variable does not represent the maximum length of a password. It only means that complexity requirements will not be checked on passwords over 8 characters. You may want to look at the `libpam-cracklib` package for additional password entropy assistance.

1.4.2. Password Expiration

When creating user accounts, you should make it a policy to have a minimum and maximum password age forcing users to change their passwords when they expire.

- To easily view the current status of a user account, use the following syntax:

```
sudo chage -l username
```

The output below shows interesting facts about the user account, namely that there are no policies applied:

```
Last password change           : Jan 20, 2008
Password expires               : never
Password inactive              : never
Account expires                : never
Minimum number of days between password change : 0
Maximum number of days between password change : 99999
Number of days of warning before password expires : 7
```

- To set any of these values, simply use the following syntax, and follow the interactive prompts:

```
sudo chage username
```

The following is also an example of how you can manually change the explicit expiration date (`-E`) to `01/31/2008`, minimum password age (`-m`) of 5 days, maximum password age (`-M`) of 90 days, inactivity period (`-I`) of 5 days after password expiration, and a warning time period (`-W`) of 14 days before password expiration.

```
sudo chage -E 01/31/2008 -m 5 -M 90 -I 30 -W 14 username
```

- To verify changes, use the same syntax as mentioned previously:

```
sudo chage -l username
```

The output below shows the new policies that have been established for the account:

```
Last password change           : Jan 20, 2008
Password expires                : Apr 19, 2008
Password inactive               : May 19, 2008
Account expires                 : Jan 31, 2008
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
```

1.5. Other Security Considerations

Many applications use alternate authentication mechanisms that can be easily overlooked by even experienced system administrators. Therefore, it is important to understand and control how users authenticate and gain access to services and applications on your server.

1.5.1. SSH Access by Disabled Users

Simply disabling/locking a user account will not prevent a user from logging into your server remotely if they have previously set up RSA public key authentication. They will still be able to gain shell access to the server, without the need for any password. Remember to check the users home directory for files that will allow for this type of authenticated SSH access. e.g. `/home/username/.ssh/authorized_keys`.

Remove or rename the directory `.ssh/` in the user's home folder to prevent further SSH authentication capabilities.

Be sure to check for any established SSH connections by the disabled user, as it is possible they may have existing inbound or outbound connections. Kill any that are found.

Restrict SSH access to only user accounts that should have it. For example, you may create a group called "sshlogin" and add the group name as the value associated with the `AllowGroups` variable located in the file `/etc/ssh/sshd_config`.

```
AllowGroups sshlogin
```

Then add your permitted SSH users to the group "sshlogin", and restart the SSH service.

```
sudo adduser username sshlogin
sudo /etc/init.d/ssh restart
```

1.5.2. External User Database Authentication

Most enterprise networks require centralized authentication and access controls for all system resources. If you have configured your server to authenticate users against external databases, be sure to disable the user accounts both externally and locally, this way you ensure that local fallback authentication is not possible.

2. Console Security

As with any other security barrier you put in place to protect your server, it is pretty tough to defend against untold damage caused by someone with physical access to your environment, for example, theft of hard drives, power or service disruption and so on. Therefore, console security should be addressed merely as one component of your overall physical security strategy. A locked "screen door" may deter a casual criminal, or at the very least slow down a determined one, so it is still advisable to perform basic precautions with regard to console security.

The following instructions will help defend your server against issues that could otherwise yield very serious consequences.

2.1. Disable Ctrl+Alt+Delete

First and foremost, anyone that has physical access to the keyboard can simply use the **Ctrl+Alt+Delete** key combination to reboot the server without having to log on. Sure, someone could simply unplug the power source, but you should still prevent the use of this key combination on a production server. This forces an attacker to take more drastic measures to reboot the server, and will prevent accidental reboots at the same time.

- To disable the reboot action taken by pressing the **Ctrl+Alt+Delete** key combination, comment out the following line in the file `/etc/event.d/control-alt-delete`.

```
#exec /sbin/shutdown -r now "Control-Alt-Delete pressed"
```

2.2. GRUB Password Security

Ubuntu installs GNU GRUB as its default boot loader, which allows for great flexibility and recovery options. For example, when you install additional kernel images, these are automatically added as available boot options in the grub menu. Also, by default, alternate boot options are available for each kernel entry that may be used for system recovery, aptly labeled (recovery mode). Recovery mode simply boots the corresponding kernel image into single user mode (init 1), which lands the administrator at a root prompt without the need for any password.

Therefore, it is important to control who may edit the grub menu items which, would otherwise allow for someone to perform the following dangerous actions:

- Pass kernel options at boot up.
- Boot the server into single user mode.

You can prevent these actions by adding a password to GRUB's configuration file of `/boot/grub/menu.lst`, which will be required to unlock GRUB's more advanced features prior to use.

- To add a password for use with grub, first you must generate an md5 password hash using the `grub-md5-crypt` utility:

`grub-md5-crypt`

The command will ask you to enter a password and offer a resulting hash value as shown below:

```
Password: (enter new password)
Retype password: (repeat password)
$1$s3YiK$M31xAbqA6JLm2FbDwnClQ0
```

- Add the resulting hash value to the file `/boot/grub/menu.lst` in the following format:

```
password --md5 $1$s3YiK$M31xAbqA6JLm2FbDwnClQ0
```

- To require use of the password for entering single user mode, change the value of the `lockalternative` variable in the file `/boot/grub/menu.lst` to `true`, as shown in the following example.

```
# lockalternative=true
```



This does not prevent someone from booting the server from alternate media. A determined attacker would simply boot into an alternate environment, overwrite your master boot record, mount or copy your physical volumes, destroy your data, or anything else they can imagine. Please explore other countermeasures that may help you with these types of attacks.

3. Firewall

3.1. Introduction

The Linux kernel includes the *Netfilter* subsystem, which is used to manipulate or decide the fate of network traffic headed into or through your server. All modern Linux firewall solutions use this system for packet filtering.

The kernel's packet filtering system would be of little use to administrators without a userspace interface to manage it. This is the purpose of iptables. When a packet reaches your server, it will be handed off to the Netfilter subsystem for acceptance, manipulation, or rejection based on the rules supplied to it from userspace via iptables. Thus, iptables is all you need to manage your firewall if you're familiar with it, but many frontends are available to simplify the task.

3.2. ufw - Uncomplicated Firewall

The default firewall configuration tool for Ubuntu is ufw. Developed to ease iptables firewall configuration, ufw provides a user friendly way to create an IPv4 or IPv6 host-based firewall.

ufw by default is initially disabled. From the ufw man page:

“ ufw is not intended to provide complete firewall functionality via its command interface, but instead provides an easy way to add or remove simple rules. It is currently mainly used for host-based firewalls. ”

The following are some examples of how to use ufw:

- First, ufw needs to be enabled. From a terminal prompt enter:

```
sudo ufw enable
```

- To open a port (ssh in this example):

```
sudo ufw allow 22
```

- Similarly, to close an opened port:

```
sudo ufw deny 22
```

- To remove a rule, use delete followed by the rule:

```
sudo ufw delete deny 22
```

- It is also possible to allow access from specific hosts or networks to a port. The following example allows ssh access from host 192.168.0.2 to any ip address on this host:

```
sudo ufw allow proto tcp from 192.168.0.2 to any port 22
```

Replace 192.168.0.2 with 192.168.0.0/24 to allow ssh access from the entire subnet.

- Adding the `--dry-run` option to a `ufw` command will output the resulting rules, but not apply them. For example, the following is what would be applied if opening the HTTP port:

```
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` can be disabled by:

```
sudo ufw disable
```

- To see the firewall status, enter:

```
sudo ufw status
```

- And for more verbose status information use:

```
sudo ufw status verbose
```



If the port you want to open or close is defined in `/etc/services`, you can use the port name instead of the number. In the above examples, replace 22 with `ssh`.

This is a quick introduction to using `ufw`. Please refer to the `ufw` man page for more information.

3.2.1. `ufw` Application Integration

Applications that open ports can include an `ufw` profile, which details the ports needed for the application to function properly. The profiles are kept in `/etc/ufw/applications.d`, and can be edited if the default ports have been changed.

- To view which applications have installed a profile, enter the following in a terminal:

```
sudo ufw app list
```

- Similar to allowing traffic to a port, using an application profile is accomplished by entering:

```
sudo ufw allow Samba
```

- An extended syntax is available as well:

```
ufw allow from 192.168.0.0/24 to any app Samba
```

Replace *Samba* and *192.168.0.0/24* with the application profile you are using and the IP range for your network.



There is no need to specify the *protocol* for the application, because that information is detailed in the profile. Also, note that the *app* name replaces the *port* number.

- To view details about which ports, protocols, etc are defined for an application, enter:

```
sudo ufw info Samba
```

Not all applications that require opening a network port come with ufw profiles, but if you have profiled an application and want the file to be included with the package, please file a bug against the package in *Launchpad*¹.

3.3. IP Masquerading

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

3.3.1. ufw Masquerading

IP Masquerading can be achieved using custom ufw rules. This is possible because the current backend for ufw is iptables-restore with the rules files located in `/etc/ufw/*.rules`. These files are a great place to add legacy iptables rules used without ufw, and rules that are more network gateway or bridge related.

¹ <https://launchpad.net/>

The rules are split into two different files, rules that should be executed before ufw command line rules, and rules that are executed after ufw command line rules.

- First, packet forwarding needs to be enabled in ufw. Two configuration files will need to be adjusted, in `/etc/default/ufw` change the `DEFAULT_FORWARD_POLICY` to “ACCEPT”:

```
DEFAULT_FORWARD_POLICY="ACCEPT"
```

Then edit `/etc/ufw/sysctl.conf` and uncomment:

```
net.ipv4.ip_forward=1
```

Similarly, for IPv6 forwarding uncomment:

```
net.ipv6.conf.default.forwarding=1
```

- Now we will add rules to the `/etc/ufw/before.rules` file. The default rules only configure the *filter* table, and to enable masquerading the *nat* table will need to be configured. Add the following to the top of the file just after the header comments:

```
# nat Table rules
*nat
:POSTROUTING ACCEPT [0:0]

# Forward traffic from eth1 through eth0.
-A POSTROUTING -s 192.168.0.0/24 -o eth0 -j MASQUERADE

# don't delete the 'COMMIT' line or these nat table rules won't be processed
COMMIT
```

The comments are not strictly necessary, but it is considered good practice to document your configuration. Also, when modifying any of the *rules* files in `/etc/ufw`, make sure these lines are the last line for each table modified:

```
# don't delete the 'COMMIT' line or these rules won't be processed
COMMIT
```

For each *Table* a corresponding *COMMIT* statement is required. In these examples only the *nat* and *filter* tables are shown, but you can also add rules for the *raw* and *mangle* tables.



In the above example replace `eth0`, `eth1`, and `192.168.0.0/24` with the appropriate interfaces and IP range for your network.

- Finally, disable and re-enable ufw to apply the changes:

```
sudo ufw disable && sudo ufw enable
```

IP Masquerading should now be enabled. You can also add any additional FORWARD rules to the `/etc/ufw/before.rules`. It is recommended that these additional rules be added to the `ufw-before-forward` chain.

3.3.2. iptables Masquerading

iptables can also be used to enable masquerading.

- Similar to ufw, the first step is to enable IPv4 packet forwarding by editing `/etc/sysctl.conf` and uncomment the following line

```
net.ipv4.ip_forward=1
```

If you wish to enable IPv6 forwarding also uncomment:

```
net.ipv6.conf.default.forwarding=1
```

- Next, execute the `sysctl` command to enable the new settings in the configuration file:

```
sudo sysctl -p
```

- IP Masquerading can now be accomplished with a single iptables rule, which may differ slightly based on your network configuration:

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

The above command assumes that your private address space is `192.168.0.0/16` and that your Internet-facing device is `ppp0`. The syntax is broken down as follows:

- `-t nat` -- the rule is to go into the nat table
- `-A POSTROUTING` -- the rule is to be appended (`-A`) to the POSTROUTING chain
- `-s 192.168.0.0/16` -- the rule applies to traffic originating from the specified address space
- `-o ppp0` -- the rule applies to traffic scheduled to be routed through the specified network device
- `-j MASQUERADE` -- traffic matching this rule is to "jump" (`-j`) to the MASQUERADE target to be manipulated as described above
- Also, each chain in the filter table (the default table, and where most or all packet filtering occurs) has a default *policy* of ACCEPT, but if you are creating a firewall in addition to a gateway device, you may have set the policies to DROP or REJECT, in which case your masqueraded traffic needs to be allowed through the FORWARD chain for the above rule to work:

```
sudo iptables -A FORWARD -s 192.168.0.0/16 -o ppp0 -j ACCEPT
```

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

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

- If you want masquerading to be enabled on reboot, which you probably do, edit `/etc/rc.local` and add any commands used above. For example add the first command with no filtering:

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

3.4. Logs

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

If you are using ufw, you can turn on logging by entering the following in a terminal:

```
sudo ufw logging on
```

To turn logging off in ufw, simply replace *on* with *off* in the above command.

If using iptables instead of ufw, enter:

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

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

```
[4304885.870000] NEW_HTTP_CONN: IN=lo OUT= MAC=00:00:00:00:00:00:00:00:00:00:00:00:00:00:08:00 SRC=127.0.
```

The above log will also appear in `/var/log/messages`, `/var/log/syslog`, and `/var/log/kern.log`.

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

3.5. Other Tools

There are many tools available to help you construct a complete firewall without intimate knowledge of iptables. For the GUI-inclined:

- *Firestarter*² is quite popular and easy to use.
- *fwbuilder*³ is very powerful and will look familiar to an administrator who has used a commercial firewall utility such as Checkpoint FireWall-1.

If you prefer a command-line tool with plain-text configuration files:

- *Shorewall*⁴ is a very powerful solution to help you configure an advanced firewall for any network.

- *ipkungfu*⁵ should give you a working firewall "out of the box" with zero configuration, and will allow you to easily set up a more advanced firewall by editing simple, well-documented configuration files.
- *fireflie*⁶ is designed to be a desktop firewall application. It is made up of a server (fireflie-server) and your choice of GUI clients (GTK or QT), and behaves like many popular interactive firewall applications for Windows.

3.6. References

- The *Ubuntu Firewall*⁷ wiki page contains information on the development of ufw.
- Also, the ufw manual page contains some very useful information: **man ufw**.
- See the *packet-filtering-HOWTO*⁸ for more information on using iptables.
- The *nat-HOWTO*⁹ contains further details on masquerading.

4. AppArmor

AppArmor is a Linux Security Module implementation of name-based mandatory access controls. AppArmor confines individual programs to a set of listed files and posix 1003.1e draft capabilities.

AppArmor is installed and loaded by default. It uses *profiles* of an application to determine what files and permissions the application requires. Some packages will install their own profiles, and additional profiles can be found in the `apparmor-profiles` package.

To install the `apparmor-profiles` package from a terminal prompt:

```
sudo apt-get install apparmor-profiles
```

AppArmor profiles have two modes of execution:

- **Complaining/Learning:** profile violations are permitted and logged. Useful for testing and developing new profiles.
- **Enforced/Confined:** enforces profile policy as well as logging the violation.

4.1. Using AppArmor

The `apparmor-utils` package contains command line utilities that you can use to change the AppArmor execution mode, find the status of a profile, create new profiles, etc.

- `apparmor_status` is used to view the current status of AppArmor profiles.

```
sudo apparmor_status
```

- `aa-complain` places a profile into *complain* mode.

```
sudo aa-complain /path/to/bin
```

- `aa-enforce` places a profile into *enforce* mode.

```
sudo aa-enforce /path/to/bin
```

- The `/etc/apparmor.d` directory is where the AppArmor profiles are located. It can be used to manipulate the *mode* of all profiles.

Enter the following to place all profiles into complain mode:

```
sudo aa-complain /etc/apparmor.d/*
```

To place all profiles in enforce mode:

```
sudo aa-enforce /etc/apparmor.d/*
```

- `apparmor_parser` is used to load a profile into the kernel. It can also be used to reload a currently loaded profile using the `-r` option. To load a profile:

```
cat /etc/apparmor.d/profile.name | sudo apparmor_parser -a
```

To reload a profile:

```
cat /etc/apparmor.d/profile.name | sudo apparmor_parser -r
```

- `/etc/init.d/apparmor` can be used to *reload* all profiles:

```
sudo /etc/init.d/apparmor reload
```

- The `/etc/apparmor.d/disable` directory can be used along with the `apparmor_parser -R` option to *disable* a profile.

```
sudo ln -s /etc/apparmor.d/profile.name /etc/apparmor.d/disable/  
sudo apparmor_parser -R /etc/apparmor.d/profile.name
```

To *re-enable* a disabled profile remove the symbolic link to the profile in `/etc/apparmor.d/disable/`. Then load the profile using the `-a` option.

```
sudo rm /etc/apparmor.d/disable/profile.name  
cat /etc/apparmor.d/profile.name | sudo apparmor_parser -a
```

- AppArmor can be disabled, and the kernel module unloaded by entering the following:

```
sudo /etc/init.d/apparmor stop  
sudo update-rc.d -f apparmor remove
```

- To re-enable AppArmor enter:

```
sudo /etc/init.d/apparmor start  
sudo update-rc.d apparmor defaults
```



Replace *profile.name* with the name of the profile you want to manipulate. Also, replace `/path/to/bin/` with the actual executable file path. For example for the ping command use `/bin/ping`

4.2. Profiles

AppArmor profiles are simple text files located in `/etc/apparmor.d/`. The files are named after the full path to the executable they profile replacing the `/` with `.`. For example `/etc/apparmor.d/bin.ping` is the AppArmor profile for the `/bin/ping` command.

There are two main type of rules used in profiles:

- *Path entries*: which detail which files an application can access in the file system.

- *Capability entries*: determine what privileges a confined process is allowed to use.

As an example take a look at `/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>*: include statements from other files. This allows statements pertaining to multiple applications to be placed in a common file.
- */bin/ping flags=(complain)*: path to the profiled program, also setting the mode to *complain*.
- *capability net_raw*,: allows the application access to the CAP_NET_RAW Posix.1e capability.
- */bin/ping mixr*,: allows the application read and execute access to the file.



After editing a profile file the profile must be reloaded. See *Section 4.1, “Using AppArmor” [p. 101]* for details.

4.2.1. Creating a Profile

- *Design a test plan*: Try to think about how the application should be exercised. The test plan should be divided into small test cases. Each test case should have a small description and list the steps to follow.

Some standard test cases are:

- Starting the program.
 - Stopping the program.
 - Reloading the program.
 - Testing all the commands supported by the init script.
- *Generate the new profile*: Use `aa-genprof` to generate a new profile. From a terminal:

```
sudo aa-genprof executable
```

For example:

```
sudo aa-genprof slapd
```

- To get your new profile included in the `apparmor-profiles` package, file a bug in *Launchpad* against the *AppArmor*¹⁰ package:
 - Include your test plan and test cases.
 - Attach your new profile to the bug.

4.2.2. Updating Profiles

When the program is misbehaving, audit messages are sent to the log files. The program `aa-logprof` can be used to scan log files for AppArmor audit messages, review them and update the profiles.

From a terminal:

```
sudo aa-logprof
```

4.3. References

- See the *AppArmor Administration Guide*¹¹ for advanced configuration options.
- For details using AppArmor with other Ubuntu releases see the *AppArmor Community Wiki*¹² page.
- The *OpenSUSE AppArmor*¹³ page is another introduction to AppArmor.
- A great place to ask for AppArmor assistance, and get involved with the Ubuntu Server community, is the `#ubuntu-server` IRC channel on *freenode*¹⁴.

5. Certificates

One of the most common forms of cryptography today is *public-key* cryptography. Public-key cryptography utilizes a *public key* and a *private key*. The system works by *encrypting* information using the public key. The information can then only be *decrypted* using the private key.

A common use for public-key cryptography is encrypting application traffic using a Secure Socket Layer (SSL) or Transport Layer Security (TLS) connection. For example, configuring Apache to provide *HTTPS*, the HTTP protocol over SSL. This allows a way to encrypt traffic using a protocol that does not itself provide encryption.

A *Certificate* is a method used to distribute a *public key* and other information about a server and the organization who is responsible for it. Certificates can be digitally signed by a *Certification Authority* or CA. A CA is a trusted third party that has confirmed that the information contained in the certificate is accurate.

5.1. Types of Certificates

To set up a secure server using public-key cryptography, in most cases, you send your certificate request (including your public key), proof of your company's identity, and payment to a CA. The CA verifies the certificate request and your identity, and then sends back a certificate for your secure server. Alternatively, you can create your own *self-signed* certificate.



Note, that self-signed certificates should not be used in most production environments.

Continuing the HTTPS example, a CA-signed certificate provides two important capabilities that a self-signed certificate does not:

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

Most Web browsers, and computers, that support SSL have a list of CAs whose certificates they automatically accept. If a browser encounters a certificate whose authorizing CA is not in the list, the browser asks the user to either accept or decline the connection. Also, other applications may generate an error message when using a self-signed certificate.

The process of getting a certificate from a CA is fairly easy. A quick overview is as follows:

1. Create a private and public encryption key pair.
2. Create a certificate request based on the public key. The certificate request contains information about your server and the company hosting it.

3. Send the certificate request, along with documents proving your identity, to a CA. We cannot tell you which certificate authority to choose. Your decision may be based on your past experiences, or on the experiences of your friends or colleagues, or purely on monetary factors.

Once you have decided upon a CA, you need to follow the instructions they provide on how to obtain a certificate from them.

4. When the CA is satisfied that you are indeed who you claim to be, they send you a digital certificate.
5. Install this certificate on your secure server, and configure the appropriate applications to use the certificate.

5.2. Generating a Certificate Signing Request (CSR)

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

To generate the *keys* for the Certificate Signing Request (CSR) run the following command from a terminal prompt:

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

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

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

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



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

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

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

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

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

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

It will prompt you enter the passphrase. If you enter the correct passphrase, it will prompt you to enter Company Name, Once you enter all these details, your CSR will be created and it will be stored in the `server.csr` file. Site Name, Email Id, etc.

You can now submit this CSR file to a CA for processing. The CA will use this CSR file and issue the certificate. On the other hand, you can create self-signed certificate using this CSR.

5.3. Creating a Self-Signed Certificate

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

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

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



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

5.4. Installing the Certificate

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

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

Now simply configure any applications, with the ability to use public-key cryptography, to use the *certificate* and *key* files. For example, Apache can provide HTTPS, Dovecot can provide IMAPS and POP3S, etc.

5.5. Certification Authority

If the services on your network require more than a few self-signed certificates it may be worth the additional effort to setup your own internal *Certification Authority (CA)*. Using certificates signed by your own CA, allows the various services using the certificates to easily trust other services using certificates issued from the same CA.

1. First, create the directories to hold the CA certificate and related files:

```
sudo mkdir /etc/ssl/CA
```

```
sudo mkdir /etc/ssl/newcerts
```

- The CA needs a few additional files to operate, one to keep track of the last serial number used by the CA, each certificate must have a unique serial number, and another file to record which certificates have been issued:

```
sudo sh -c "echo '01' > /etc/ssl/CA/serial"
sudo touch /etc/ssl/CA/index.txt
```

- The third file is a CA configuration file. Though not strictly necessary, it is very convenient when issuing multiple certificates. Edit `/etc/ssl/openssl.cnf`, and in the `[CA_default]` change:

```
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
```

- Next, create the self-signed root certificate:

```
openssl req -new -x509 -extensions v3_ca -keyout cakey.pem -out cacert.pem -days 3650
```

You will then be asked to enter the details about the certificate.

- Now install the root certificate and key:

```
sudo mv cakey.pem /etc/ssl/private/
sudo mv cacert.pem /etc/ssl/certs/
```

- You are now ready to start signing certificates. The first item needed is a Certificate Signing Request (CSR), see *Section 5.2, “Generating a Certificate Signing Request (CSR)” [p. 106]* for details. Once you have a CSR, enter the following to generate a certificate signed by the CA:

```
sudo openssl ca -in server.csr -config /etc/ssl/openssl.cnf
```

After entering the password for the CA key, you will be prompted to sign the certificate, and again to commit the new certificate. You should then see a somewhat large amount of output related to the certificate creation.

- There should now be a new file, `/etc/ssl/newcerts/01.pem`, containing the same output. Copy and paste everything between the `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` lines to a file named after the hostname of the server where the certificate will be installed. For example `mail.example.com.crt`, is a nice descriptive name.

Subsequent certificates will be named `02.pem`, `03.pem`, etc.



Replace `mail.example.com.crt` with your own descriptive name.

8. Finally, copy the new certificate to the host that needs it, and configure the appropriate applications to use it. The default location to install certificates is `/etc/ssl/certs`. This enables multiple services to use the same certificate without overly complicated file permissions.

For applications that can be configured to use a CA certificate, you should also copy the `/etc/ssl/certs/cacert.pem` file to the `/etc/ssl/certs/` directory on each server.

5.6. References

- For more detailed instructions on using cryptography see the *SSL Certificates HOWTO*¹⁵ by tlpd.org
- *The PKI Page*¹⁶ contains a list of Certificate Authorities.
- The Wikipedia *HTTPS*¹⁷ page has more information regarding HTTPS.
- For more information on *OpenSSL* see the *OpenSSL Home Page*¹⁸.
- Also, O'Reilly's *Network Security with OpenSSL*¹⁹ is a good in depth reference.

Chapter 9. Web Servers

A Web server is a software responsible for accepting HTTP requests from clients, which are known as Web browsers, and serving them HTTP responses along with optional data contents, which usually are Web pages such as HTML documents and linked objects (images, etc.).

1. HTTPD - Apache2 Web Server

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

Users enter a Uniform Resource Locator (URL) to point to a Web server by means of its Fully Qualified Domain Name (FQDN) and a path to the required resource. For example, to view the home page of the *Ubuntu Web site*¹ a user will enter only the FQDN. To request specific information about *paid support*², a user will enter the FQDN followed by a path.

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

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

1.1. Installation

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

- At a terminal prompt enter the following command:

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

1.2. Configuration

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

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

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

¹ <http://www.ubuntu.com>

² <http://www.ubuntu.com/support/paid>

1.2.1. Basic Settings

This section explains Apache2 server essential configuration parameters. Refer to the *Apache2 Documentation*³ for more details.

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



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

- The *DocumentRoot* directive specifies where Apache should look for the files that make up the site. The default value is `/var/www`. No site is configured there, but if you uncomment the *RedirectMatch* directive in `/etc/apache2/apache2.conf` requests will be redirected to `/var/www/`

³ <http://httpd.apache.org/docs/2.2/>

apache2-default where the default Apache2 site awaits. Change this value in your site's virtual host file, and remember to create that directory if necessary!



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

1.2.2. Default Settings

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

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

For example, when a user requests the page `http://www.example.com/this_directory/`, he or she will get either the *DirectoryIndex* page if it exists, a server-generated directory list if it does not and the *Indexes* option is specified, or a *Permission Denied* page if neither is true. The server will try to find one of the files listed in the *DirectoryIndex* directive and will return the first one it finds. If it does not find any of these files and if *Options Indexes* is set for that directory, the server will generate and return a list, in HTML format, of the subdirectories and files in the directory. The default value, found in `/etc/apache2/apache2.conf` is " `index.html index.cgi index.pl index.php index.xhtml`". Thus, if Apache2 finds a file in a requested directory matching any of these names, the first will be displayed.

- The *ErrorDocument* directive allows you to specify a file for Apache to use for specific error events. For example, if a user requests a resource that does not exist, a 404 error will occur, and per Apache2's default configuration, the file `/usr/share/apache2/error/HTTP_NOT_FOUND.html.var` will be displayed. That file is not in the server's *DocumentRoot*, but there is an *Alias* directive in `/etc/apache2/apache2.conf` that redirects requests to the `/error` directory to `/usr/share/apache2/error/`. To see a list of the default *ErrorDocument* directives, use this command: **`grep ErrorDocument /etc/apache2/apache2.conf`**
- By default, the server writes the transfer log to the file `/var/log/apache2/access.log`. You can change this on a per-site basis in your virtual host configuration files with the *CustomLog* directive, or omit it to accept the default, specified in `/etc/apache2/apache2.conf`. You may also specify the file to which errors are logged, via the *ErrorLog* directive, whose default is `/var/log/apache2/error.log`. These are kept separate from the transfer logs to aid in troubleshooting problems with your Apache2 server. You may also specify the *LogLevel* (the default value is "warn") and the *LogFormat* (see `/etc/apache2/apache2.conf` for the default value).
- Some options are specified on a per-directory basis rather than per-server. Option is one of these directives. A *Directory* stanza is enclosed in XML-like tags, like so:

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

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

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



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

- **Includes** - Allow server-side includes. Server-side includes allow an HTML file to *include* other files. This is not a common option. See *the Apache2 SSI HOWTO*⁴ for more information.
- **IncludesNOEXEC** - Allow server-side includes, but disable the #exec and #include commands in CGI scripts.
- **Indexes** - Display a formatted list of the directory's contents, if no *DirectoryIndex* (such as index.html) exists in the requested directory.



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

- **Multiview** - Support content-negotiated multiviews; this option is disabled by default for security reasons. See the *Apache2 documentation on this option*⁵.
- **SymLinksIfOwnerMatch** - Only follow symbolic links if the target file or directory has the same owner as the link.

1.2.3. Virtual Hosts Settings

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

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

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

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

1.2.4. Server Settings

This section explains how to configure basic server settings.

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

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

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



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

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

1.2.5. Apache Modules

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

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

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

1.3. HTTPS Configuration

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

The `mod_ssl` module is available in `apache2-common` package. Execute the following command from a terminal prompt to enable the `mod_ssl` module:

```
sudo a2enmod ssl
```

There is a default HTTPS configuration file in `/etc/apache2/sites-available/default-ssl`. In order for Apache to provide HTTPS, a *certificate* and *key* file are also needed. The default HTTPS configuration will use a certificate and key generated by the `ssl-cert` package. They are good for testing, but the auto-generated certificate and key should be replaced by a certificate specific to the site or server. For information on generating a key and obtaining a certificate see *Section 5, "Certificates" [p. 105]*

To configure Apache for HTTPS, enter the following:

```
sudo a2ensite default-ssl
```



The directories `/etc/ssl/certs` and `/etc/ssl/private` are the default locations. If you install the certificate and key in another directory make sure to change `SSLCertificateFile` and `SSLCertificateKeyFile` appropriately.

With Apache now configured for HTTPS, restart the service to enable the new settings:

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



Depending on how you obtained your certificate you may need to enter a passphrase when Apache starts.

You can access the secure server pages by typing `https://your_hostname/url/` in your browser address bar.

1.4. References

*Apache2 Documentation*⁶

*Mod SSL Documentation*⁷

⁶ <http://httpd.apache.org/docs/2.2/>

⁷ <http://www.modssl.org/docs/>

2. PHP5 - Scripting Language

PHP is a general-purpose scripting language suited for Web development. The PHP script can be embedded into HTML. This section explains how to install and configure PHP5 in Ubuntu System with Apache2 and MySQL.

This section assumes you have installed and configured Apache 2 Web Server and MySQL Database Server. You can refer to Apache 2 section and MySQL sections in this document to install and configure Apache 2 and MySQL respectively.

2.1. Installation

The PHP5 is available in Ubuntu Linux.

- To install PHP5 you can enter the following command in the terminal prompt:

```
sudo apt-get install php5 libapache2-mod-php5
```

You can run PHP5 scripts from command line. To run PHP5 scripts from command line you should install php5-cli package. To install php5-cli you can enter the following command in the terminal prompt:

```
sudo apt-get install php5-cli
```

You can also execute PHP5 scripts without installing PHP5 Apache module. To accomplish this, you should install php5-cgi package. You can run the following command in a terminal prompt to install php5-cgi package:

```
sudo apt-get install php5-cgi
```

To use MySQL with PHP5 you should install php5-mysql package. To install php5-mysql you can enter the following command in the terminal prompt:

```
sudo apt-get install php5-mysql
```

Similarly, to use PostgreSQL with PHP5 you should install php5-pgsql package. To install php5-pgsql you can enter the following command in the terminal prompt:

```
sudo apt-get install php5-pgsql
```

2.2. Configuration

Once you install PHP5, you can run PHP5 scripts from your web browser. If you have installed php5-cli package, you can run PHP5 scripts from your command prompt.

By default, the Apache 2 Web server is configured to run PHP5 scripts. In other words, the PHP5 module is enabled in Apache2 Web server automatically when you install the module. Please verify if the files `/etc/apache2/mods-enabled/php5.conf` and `/etc/apache2/mods-enabled/php5.load` exist. If they do not exist, you can enable the module using **a2enmod** command.

Once you install PHP5 related packages and enabled PHP5 Apache 2 module, you should restart Apache2 Web server to run PHP5 scripts. You can run the following command at a terminal prompt to restart your web server:

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

2.3. Testing

To verify your installation, you can run following PHP5 `phpinfo` script:

```
<?php
print_r (phpinfo());
?>
```

You can save the content in a file `phpinfo.php` and place it under **DocumentRoot** directory of Apache2 Web server. When point your browser to `http://hostname/phpinfo.php`, it would display values of various PHP5 configuration parameters.

3. Squid - Proxy Server

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

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

3.1. Installation

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

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

3.2. Configuration

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



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

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

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

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

```
http_port 8888
```

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

```
visible_hostname weezie
```

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

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

```
acl fortytwo_network src 192.168.42.0/24
```

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

```
http_access allow fortytwo_network
```

- Using the excellent access control features of Squid, you may configure use of Internet services proxied by Squid to be available only during normal business hours. For example, we'll illustrate access by employees of a business which is operating between 9:00AM and 5:00PM, Monday through Friday, and which uses the 10.1.42.0/24 subnetwork:

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

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

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

```
http_access allow biz_network biz_hours
```



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

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

3.3. References

*Squid Website*⁸

⁸ <http://www.squid-cache.org/>

4. Ruby on Rails

Ruby on Rails is an open source web framework for developing database backed web applications. It is optimized for sustainable productivity of the programmer since it lets the programmer to write code by favouring convention over configuration.

4.1. Installation

Before installing Rails you should install Apache and MySQL. To install the Apache package, please refer to *Section 1, "HTTPD - Apache2 Web Server" [p. 111]*. For instructions on installing MySQL refer to *Section 1, "MySQL" [p. 128]*.

Once you have Apache and MySQL packages installed, you are ready to install Ruby on Rails package.

To install the Ruby base packages and Ruby on Rails, you can enter the following command in the terminal prompt:

```
sudo apt-get install rails
```

4.2. Configuration

Modify the `/etc/apache2/sites-available/default` configuration file to setup your domains.

The first thing to change is the *DocumentRoot* directive:

```
DocumentRoot /path/to/rails/application/public
```

Next, change the `<Directory "/path/to/rails/application/public">` directive:

```
<Directory "/path/to/rails/application/public">
    Options Indexes FollowSymLinks MultiViews ExecCGI
    AllowOverride All
    Order allow,deny
    allow from all
    AddHandler cgi-script .cgi
</Directory>
```

You should also enable the `mod_rewrite` module for Apache. To enable `mod_rewrite` module, please enter the following command in a terminal prompt:

```
sudo a2enmod rewrite
```

Finally you will need to change the ownership of the `/path/to/rails/application/public` and `/path/to/rails/application/tmp` directories to the user used to run the Apache process:

```
sudo chown -R www-data:www-data /path/to/rails/application/public
sudo chown -R www-data:www-data /path/to/rails/application/tmp
```

That's it! Now you have your Server ready for your Ruby on Rails applications.

5. Apache Tomcat

Apache Tomcat is a web container that allows you to serve Java Servlets and JSP (Java Server Pages) web applications.

The Tomcat 6.0 packages in Ubuntu support two different ways of running Tomcat. You can install them as a classic unique system-wide instance, that will be started at boot time and will run as the tomcat6 unprivileged user. But you can also deploy private instances that will run with your own user rights, and that you should start and stop by yourself. This second way is particularly useful in a development server context where multiple users need to test on their own private Tomcat instances.

5.1. System-wide installation

To install the Tomcat server, you can enter the following command in the terminal prompt:

```
sudo apt-get install tomcat6
```

This will install a Tomcat server with just a default ROOT webapp that displays a minimal "It works" page by default.

5.2. Configuration

Tomcat configuration files can be found in `/etc/tomcat6`. Only a few common configuration tweaks will be described here, please see *Tomcat 6.0 documentation*⁹ for more.

5.2.1. Changing default ports

By default Tomcat 6.0 runs a HTTP connector on port 8080 and an AJP connector on port 8009. You might want to change those default ports to avoid conflict with another server on the system. This is done by changing the following lines in `/etc/tomcat6/server.xml`:

```
<Connector port="8080" protocol="HTTP/1.1"
           connectionTimeout="20000"
           redirectPort="8443" />
...
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
```

5.2.2. Changing JVM used

By default Tomcat will run preferably with OpenJDK-6, then try Sun's JVM, then try some other JVMs. If you have various JVMs installed, you can set which should be used by setting `JAVA_HOME` in `/etc/default/tomcat6`:

```
JAVA_HOME=/usr/lib/jvm/java-6-sun
```

⁹ <http://tomcat.apache.org/tomcat-6.0-doc/index.html>

5.2.3. Declaring users and roles

Username, passwords and roles (groups) can be defined centrally in a Servlet container. In Tomcat 6.0 this is done in the `/etc/tomcat6/tomcat-users.xml` file:

```
<role rolename="admin"/>
<user username="tomcat" password="s3cret" roles="admin"/>
```

5.3. Using Tomcat standard webapps

Tomcat is shipped with webapps that you can install for documentation, administration or demo purposes.

5.3.1. Tomcat documentation

The `tomcat6-docs` package contains Tomcat 6.0 documentation, packaged as a webapp that you can access by default at `http://yourserver:8080/docs`. You can install it by entering the following command in the terminal prompt:

```
sudo apt-get install tomcat6-docs
```

5.3.2. Tomcat administration webapps

The `tomcat6-admin` package contains two webapps that can be used to administer the Tomcat server using a web interface. You can install them by entering the following command in the terminal prompt:

```
sudo apt-get install tomcat6-admin
```

The first one is the *manager* webapp, which you can access by default at `http://yourserver:8080/manager/html`. It is primarily used to get server status and restart webapps.



Access to the *manager* application is protected by default: you need to define a user with the role "manager" in `/etc/tomcat6/tomcat-users.xml` before you can access it.

The second one is the *host-manager* webapp, which you can access by default at `http://yourserver:8080/host-manager/html`. It can be used to create virtual hosts dynamically.



Access to the *host-manager* application is also protected by default: you need to define a user with the role "admin" in `/etc/tomcat6/tomcat-users.xml` before you can access it.

For security reasons, the `tomcat6` user cannot write to the `/etc/tomcat6` directory by default. Some features in these admin webapps (application deployment, virtual host creation) need write access to that directory. If you want to use these features execute the following, to give users in the `tomcat6` group the necessary rights:

```
sudo chgrp -R tomcat6 /etc/tomcat6
sudo chmod -R g+w /etc/tomcat6
```

5.3.3. Tomcat examples webapps

The tomcat6-examples package contains two webapps that can be used to test or demonstrate Servlets and JSP features, which you can access them by default at <http://yourserver:8080/examples>. You can install them by entering the following command in the terminal prompt:

```
sudo apt-get install tomcat6-examples
```

5.4. Using private instances

Tomcat is heavily used in development and testing scenarios where using a single system-wide instance doesn't meet the requirements of multiple users on a single system. The Tomcat 6.0 packages in Ubuntu come with tools to help deploy your own user-oriented instances, allowing every user on a system to run (without root rights) separate private instances while still using the system-installed libraries.



It is possible to run the system-wide instance and the private instances in parallel, as long as they do not use the same TCP ports.

5.4.1. Installing private instance support

You can install everything necessary to run private instances by entering the following command in the terminal prompt:

```
sudo apt-get install tomcat6-user
```

5.4.2. Creating a private instance

You can create a private instance directory by entering the following command in the terminal prompt:

```
tomcat6-instance-create my-instance
```

This will create a new `my-instance` directory with all the necessary subdirectories and scripts. You can for example install your common libraries in the `lib/` subdirectory and deploy your webapps in the `webapps/` subdirectory. No webapps are deployed by default.

5.4.3. Configuring your private instance

You will find the classic Tomcat configuration files for your private instance in the `conf/` subdirectory. You should for example certainly edit the `conf/server.xml` file to change the default ports used by your private Tomcat instance to avoid conflict with other instances that might be running.

5.4.4. Starting/stopping your private instance

You can start your private instance by entering the following command in the terminal prompt (supposing your instance is located in the `my-instance` directory):

```
my-instance/bin/startup.sh
```



You should check the `logs/` subdirectory for any error. If you have a *java.net.BindException: Address already in use<null>:8080* error, it means that the port you're using is already taken and that you should change it.

You can stop your instance by entering the following command in the terminal prompt (supposing your instance is located in the `my-instance` directory):

```
my-instance/bin/shutdown.sh
```

Chapter 10. Databases

Ubuntu provides two popular database servers. They are:

- MySQL™
- PostgreSQL

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

1. MySQL

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

1.1. Installation

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

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

During the installation process you will be prompted to enter a password for the MySQL root user.

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

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

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

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

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

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

1.2. Configuration

You can edit the `/etc/mysql/my.cnf` file to configure the basic settings -- log file, port number, etc. For example, to configure MySQL to listen for connections from network hosts, change the `bind_address` directive to the server's IP address:

```
bind-address          = 192.168.0.5
```



Replace 192.168.0.5 with the appropriate address.

After making a change to `/etc/mysql/my.cnf` the `mysql` daemon will need to be restarted:

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

1.3. Resources

- See the *MySQL Home Page*¹ for more information.

- The *MySQL Handbook* is also available in the `mysql-doc-5.0` package. To install the package enter the following in a terminal:

```
sudo apt-get install mysql-doc-5.0
```

The documentation is in HTML format, to view them enter **`file:///usr/share/doc/mysql-doc-5.0/refman-5.0-en.html-chapter/index.html`** in your browser's address bar.

- For general SQL information see *Using SQL Special Edition*² by Rafe Colburn.

2. PostgreSQL

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

2.1. Installation

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

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

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

2.2. Configuration

By default, connection via TCP/IP is disabled. PostgreSQL supports multiple client authentication methods. By default, IDENT authentication method is used for postgres and local users. Please refer *the PostgreSQL Administrator's Guide*³.

The following discussion assumes that you wish to enable TCP/IP connections and use the MD5 method for client authentication. PostgreSQL configuration files are stored in the `/etc/postgresql/<version>/main` directory. For example, if you install PostgreSQL 8.3, the configuration files are stored in the `/etc/postgresql/8.3/main` directory.



To configure *ident* authentication, add entries to the `/etc/postgresql/8.3/main/pg_ident.conf` file.

To enable TCP/IP connections, edit the file `/etc/postgresql/8.3/main/postgresql.conf`

Locate the line `#listen_addresses = 'localhost'` and change it to:

```
listen_addresses = 'localhost'
```



To allow other computers to connect to your PostgreSQL server replace 'localhost' with the *IP Address* of your server.

You may also edit all other parameters, if you know what you are doing! For details, refer to the configuration file or to the PostgreSQL documentation.

Now that we can connect to our PostgreSQL server, the next step is to set a password for the *postgres* user. Run the following command at a terminal prompt to connect to the default PostgreSQL template database:

³ <http://www.postgresql.org/docs/8.3/static/admin.html>

```
sudo -u postgres psql template1
```

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

```
ALTER USER postgres with encrypted password 'your_password';
```

After configuring the password, edit the file `/etc/postgresql/8.3/main/pg_hba.conf` to use *MD5* authentication with the *postgres* user:

```
local    all             postgres                                md5     sameuser
```

Finally, you should restart the PostgreSQL service to initialize the new configuration. From a terminal prompt enter the following to restart PostgreSQL:

```
sudo /etc/init.d/postgresql-8.3 restart
```



The above configuration is not complete by any means. Please refer *the PostgreSQL Administrator's Guide*⁴ to configure more parameters.

2.3. Resources

- As mentioned above the *Administrator's Guide*⁵ is an excellent resource. The guide is also available in the `postgresql-doc-8.3` package. Execute the following in a terminal to install the package:

```
sudo apt-get install postgresql-doc-8.3
```

To view the guide enter `file:///usr/share/doc/postgresql-doc-8.3/html/index.html` into the address bar of your browser.

- For general SQL information see *Using SQL Special Edition*⁶ by Rafe Colburn.

Chapter 11. Wiki Applications

A Wiki is a website that allows the visitors to easily add, remove and modify available content easily. The ease of interaction and operation makes Wiki an effective tool for mass collaborative authoring. The term Wiki is also referred to the collaborative software.

In this section, we explain howto install and configure the Wiki applications, MoinMoin and MediaWiki on your Ubuntu system.

1. Moin Moin

MoinMoin is a Wiki engine implemented in Python, based on the PikiPiki Wiki engine, and licensed under the GNU GPL.

1.1. Installation

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

```
sudo apt-get install python-moinmoin
```

You should also install apache2 web server. For installing apache2 web server, please refer to *Section 1.1, "Installation" [p. 111]* sub-section in *Section 1, "HTTPD - Apache2 Web Server" [p. 111]* section.

1.2. Configuration

For configuring your first Wiki application, please run the following set of commands. Let us assume that you are creating a Wiki named *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
```

Now you should configure MoinMoin to find your new Wiki *mywiki*. To configure MoinMoin, open `/etc/moin/mywiki.py` file and change the following line:

```
data_dir = '/org/moin/mywiki/data'
```

to

```
data_dir = '/usr/share/moin/mywiki/data'
```



If the `/etc/moin/mywiki.py` file does not exist, you should copy `/etc/moin/moinmaster.py` file to `/etc/moin/mywiki.py` file and do the above mentioned change.



If you have named your Wiki as *my_wiki_name* you should insert a line `("my_wiki_name", r".*")` in `/etc/moin/farmconfig.py` file after the line `("mywiki", r".*")`.

Once you have configured MoinMoin to find your first Wiki application *mywiki*, you should configure apache2 and make it ready for your Wiki application.

You should add the following lines in `/etc/apache2/sites-available/default` file inside the “<VirtualHost *>” tag:

```
### moin
  ScriptAlias /mywiki "/usr/share/moin/mywiki/moin.cgi"
  alias /wiki "/usr/share/moin/htdocs"
  <Directory /usr/share/moin/htdocs>
    Order allow,deny
    allow from all
  </Directory>
### end moin
```

Once you configure the apache2 web server and make it ready for your Wiki application, you should restart it. You can run the following command to restart the apache2 web server:

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

1.3. Verification

You can verify the Wiki application and see if it works by pointing your web browser to the following URL:

```
http://localhost/mywiki
```

You can also run the test command by pointing your web browser to the following URL:

```
http://localhost/mywiki?action=test
```

For more details, please refer to the *MoinMoin*¹ web site.

¹ <http://moinmoin.wikiwikiweb.de/>

2. MediaWiki

MediaWiki is an web based Wiki software written in the PHP language. It can either use MySQL or PostgreSQL Database Management System.

2.1. Installation

Before installing MediaWiki you should also install Apache2, the PHP5 scripting language and Database a Management System. MySQL or PostgreSQL are the most common, choose one depending on your need. Please refer to those sections in this manual for installation instructions.

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

```
sudo apt-get install mediawiki php5-gd
```

2.2. Configuration

Run the following commands to configure MediaWiki:

```
sudo ln -s /var/lib/mediawiki /var/www/mediawiki
```

Point your web browser to the following URL for MediaWiki setup:

```
http://localhost/mediawiki/config/index.php
```



Please read the “Checking environment...” section in this page. You should be able to fix many issues by carefully reading this section.

For more details, please refer to the *MediaWiki*² web site.

² <http://www.mediawiki.org>

Chapter 12. File Servers

If you have more than one computer on a single network. At some point you will probably need to share files between them. In this section we cover installing and configuring FTP, NFS, and CUPS.

1. FTP Server

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

Access to an FTP server can be managed in two ways:

- Anonymous
- Authenticated

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

1.1. vsftpd - FTP Server Installation

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

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

1.2. vsftpd - FTP Server Configuration

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

```
anonymous_enable=YES
```

to

```
anonymous_enable=NO
```

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

```
#local_enable=YES
```

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

```
#write_enable=YES
```

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

```
#anon_upload_enable=YES
```

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

Once you configure vsftpd you can start the daemon. You can run following command to run the vsftpd daemon:

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



Please note that the defaults in the configuration file are set as they are for security reasons. Each of the above changes makes the system a little less secure, so make them only if you need them.

2. Network File System (NFS)

NFS allows a system to share directories and files with others over a network. By using NFS, users and programs can access files on remote systems almost as if they were local files.

Some of the most notable benefits that NFS can provide are:

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

2.1. Installation

At a terminal prompt enter the following command to install the NFS Server:

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

2.2. Configuration

You can configure the directories to be exported by adding them to the `/etc/exports` file. For example:

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

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

To start the NFS server, you can run the following command at a terminal prompt:

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

2.3. NFS Client Configuration

Use the `mount` command to mount a shared NFS directory from another machine, by typing a command line similar to the following at a terminal prompt:

```
sudo mount example.hostname.com:/ubuntu /local/ubuntu
```



The mount point directory `/local/ubuntu` must exist. There should be no files or subdirectories in the `/local/ubuntu` directory.

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

The general syntax for the line in `/etc/fstab` file is as follows:

```
example.hostname.com:/ubuntu /local/ubuntu nfs rsize=8192,wsiz=8192,timeo=14,intr
```

If you have trouble mounting an NFS share, make sure the `nfs-common` package is installed on your client. To install `nfs-common` enter the following command at the terminal prompt:

```
sudo apt-get install nfs-common
```

2.4. References

*Linux NFS faq*¹

¹ <http://nfs.sourceforge.net/>

3. CUPS - Print Server

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

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

3.1. Installation

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

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

Upon authenticating with your user password, the packages should be downloaded and installed without error. Upon the conclusion of installation, the CUPS server will be started automatically.

For troubleshooting purposes, you can access CUPS server errors via the error log file at: `/var/log/cups/error_log`. If the error log does not show enough information to troubleshoot any problems you encounter, the verbosity of the CUPS log can be increased by changing the **LogLevel** directive in the configuration file (discussed below) to "debug" or even "debug2", which logs everything, from the default of "info". If you make this change, remember to change it back once you've solved your problem, to prevent the log file from becoming overly large.

3.2. Configuration

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



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

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

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

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

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

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

```
man cupsd.conf
```



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

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

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

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

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

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

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

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

Port 631 # Listen on port 631 on all interfaces

3.3. References

*CUPS Website*²

² <http://www.cups.org/>

Chapter 13. Email Services

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

1. Postfix

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

1.1. Installation

To install postfix run the following command:

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

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

1.2. Basic Configuration

To configure postfix, run the following command:

```
sudo dpkg-reconfigure postfix
```

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

- Internet Site
- mail.example.com
- steve
- mail.example.com, localhost.localdomain, localhost
- No
- 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128 192.168.0/24
- 0
- +
- all



Replace mail.example.com with your mail server hostname, 192.168.0/24 with the actual network and class range of your mail server, and steve with the appropriate username.

Now is a good time to decide which mailbox format you want to use. By default Postfix will use **mbox** for the mailbox format. Rather than editing the configuration file directly, you can use the **postconf** command to configure all postfix parameters. The configuration parameters will be stored in `/etc/postfix/main.cf` file. Later if you wish to re-configure a particular parameter, you can either run the command or change it manually in the file.

To configure the mailbox format for **Maildir**:

```
sudo postconf -e 'home_mailbox = Maildir/'
```



This will place new mail in `/home/username/Maildir` so you will need to configure your Mail Delivery Agent (MDA) to use the same path.

1.3. SMTP Authentication

SMTP-AUTH allows a client to identify itself through an authentication mechanism (SASL). Transport Layer Security (TLS) should be used to encrypt the authentication process. Once authenticated the SMTP server will allow the client to relay mail.

1. Configure Postfix for SMTP-AUTH using SASL (Dovecot SASL):

```
sudo postconf -e 'smtpd_sasl_type = dovecot'
sudo postconf -e 'smtpd_sasl_path = private/auth-client'
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,relayed_client'
sudo postconf -e 'inet_interfaces = all'
```



The `smtpd_sasl_path` configuration is a path relative to the Postfix queue directory.

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

```
openssl genrsa -des3 -rand /etc/hosts -out smtpd.key 1024
chmod 600 smtpd.key
openssl req -new -key smtpd.key -out smtpd.csr
sudo openssl x509 -req -days 365 -in smtpd.csr -signkey smtpd.key -out smtpd.crt
openssl rsa -in smtpd.key -out smtpd.key.unencrypted
mv -f smtpd.key.unencrypted smtpd.key
openssl req -new -x509 -extensions v3_ca -keyout cakey.pem -out cacert.pem -days 3650
sudo mv smtpd.key /etc/ssl/private/
sudo mv smtpd.crt /etc/ssl/certs/
sudo mv cakey.pem /etc/ssl/private/
sudo mv cacert.pem /etc/ssl/certs/
```



You can get the digital certificate from a certificate authority. But unlike web clients, SMTP clients rarely complain about "self-signed certificates", so alternatively, you can create the certificate yourself. Refer to *Section 5.3, "Creating a Self-Signed Certificate"* [p. 107] for more details.

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

```
sudo postconf -e 'smtpd_tls_auth_only = no'
sudo postconf -e 'smtp_use_tls = yes'
```

```
sudo postconf -e 'smtpd_use_tls = yes'
sudo postconf -e 'smtp_tls_note_starttls_offer = yes'
sudo postconf -e 'smtpd_tls_key_file = /etc/ssl/private/smtpd.key'
sudo postconf -e 'smtpd_tls_cert_file = /etc/ssl/certs/smtpd.crt'
sudo postconf -e 'smtpd_tls_CAfile = /etc/ssl/certs/cacert.pem'
sudo postconf -e 'smtpd_tls_loglevel = 1'
sudo postconf -e 'smtpd_tls_received_header = yes'
sudo postconf -e 'smtpd_tls_session_cache_timeout = 3600s'
sudo postconf -e 'tls_random_source = dev:/dev/urandom'
sudo postconf -e 'myhostname = mail.example.com'
```



After running all the commands, Postfix is configured for SMTP-AUTH and a self-signed certificate has been created for TLS encryption.

Now, the file `/etc/postfix/main.cf` should look like *this*¹.

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

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

Postfix supports SMTP-AUTH as defined in *RFC2554*². It is based on *SASL*³. However it is still necessary to set up SASL authentication before you can use SMTP-AUTH.

1.4. Configuring SASL

Postfix supports two SASL implementations Cyrus SASL and Dovecot SASL. To enable Dovecot SASL the dovecot-common package will need to be installed. From a terminal prompt enter the following:

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

Next you will need to edit `/etc/dovecot/dovecot.conf`. In the *auth default* section uncomment the *socket listen* option and change the following:

```
socket listen {
  #master {
    # Master socket provides access to userdb information. It's typically
    # used to give Dovecot's local delivery agent access to userdb so it
    # can find mailbox locations.
    #path = /var/run/dovecot/auth-master
    #mode = 0600
    # Default user/group is the one who started dovecot-auth (root)
    #user =
    #group =
```

¹ ../sample/postfix_configuration

² ftp://ftp.isi.edu/in-notes/rfc2554.txt

³ ftp://ftp.isi.edu/in-notes/rfc2222.txt

```
#}
client {
    # The client socket is generally safe to export to everyone. Typical use
    # is to export it to your SMTP server so it can do SMTP AUTH lookups
    # using it.
    path = /var/spool/postfix/private/auth-client
    mode = 0660
    user = postfix
    group = postfix
}
}
```

Once you have Dovecot configured restart it with:

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

1.5. Testing

SMTP-AUTH configuration is complete. Now it is time to test the setup.

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

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

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

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

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

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

1.6. Troubleshooting

This section introduces some common ways to determine the cause if problems arise.

1.6.1. Escaping chroot

The Ubuntu postfix package will by default install into a *chroot* environment for security reasons. This can add greater complexity when troubleshooting problems.

To turn off the chroot operation locate for the following line in the `/etc/postfix/master.cf` configuration file:

```
smtp      inet  n       -       -       -       -       smtpd
```

and modify it as follows:

```
smtp      inet  n       -       n       -       -       smtpd
```

You will then need to restart Postfix to use the new configuration. From a terminal prompt enter:

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

1.6.2. Log Files

Postfix sends all log messages to `/var/log/mail.log`. However error and warning messages can sometimes get lost in the normal log output so they are also logged to `/var/log/mail.err` and `/var/log/mail.warn` respectively.

To see messages entered into the logs in real time you can use the `tail -f` command:

```
tail -f /var/log/mail.err
```

The amount of detail that is recorded in the logs can be increased. Below are some configuration options for increasing the log level for some of the areas covered above.

- To increase *TLS* activity logging set the `smtpd_tls_loglevel` option to a value from 1 to 4.

```
sudo postconf -e 'smtpd_tls_loglevel = 4'
```

- If you are having trouble sending or receiving mail from a specific domain you can add the domain to the `debug_peer_list` parameter.

```
sudo postconf -e 'debug_peer_list = problem.domain'
```

- You can increase the verbosity of any Postfix daemon process by editing the `/etc/postfix/master.cf` and adding a `-v` after the entry. For example edit the `smtp` entry:

```
smtp      unix  -       -       -       -       -       smtp -v
```



It is important to note that after making one of the logging changes above the Postfix process will need to be reloaded in order to recognize the new configuration: **sudo /etc/init.d/postfix reload**

- To increase the amount of information logged when troubleshooting *SASL* issues you can set the following options in `/etc/dovecot/dovecot.conf`

```
auth_debug=yes
auth_debug_passwords=yes
```



Just like Postfix if you change a Dovecot configuration the process will need to be reloaded: **sudo /etc/init.d/dovecot reload.**



Some of the options above can drastically increase the amount of information sent to the log files. Remember to return the log level back to normal after you have corrected the problem. Then reload the appropriate daemon for the new configuration to take affect.

1.6.3. References

Administering a Postfix server can be a very complicated task. At some point you may need to turn to the Ubuntu community for more experienced help.

A great place to ask for Postfix assistance, and get involved with the Ubuntu Server community, is the *#ubuntu-server* IRC channel on *freenode*⁴. You can also post a message to one of the *Web Forums*⁵.

For in depth Postfix information Ubuntu developers highly recommend: *The Book of Postfix*⁶.

Finally, the *Postfix*⁷ website also has great documentation on all the different configuration options available.

⁴ <http://freenode.net>

⁵ <http://www.ubuntu.com/support/community/webforums>

⁶ <http://www.postfix-book.com/>

⁷ <http://www.postfix.org/documentation.html>

2. Exim4

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

2.1. Installation

To install exim4, run the following command:

```
sudo apt-get install exim4
```

2.2. Configuration

To configure Exim4, run the following command:

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

The user interface will be displayed. The user interface lets you configure many parameters. For example, In Exim4 the configuration files are split among multiple files. If you wish to have them in one file you can configure accordingly in this user interface.

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

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

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



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

You can run the following command to start Exim4 daemon.

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

2.3. SMTP Authentication

This section covers configuring Exim4 to use SMTP-AUTH with TLS and SASL.

The first step is to create a certificate for use with TLS. Enter the following into a terminal prompt:

```
sudo /usr/share/doc/exim4-base/examples/exim-gencert
```

Now Exim4 needs to be configured for TLS by editing `/etc/exim4/conf.d/main/03_exim4-config_tlsoptions` add the following:

```
MAIN_TLS_ENABLE = yes
```

Next you need to configure Exim4 to use the `saslauthd` for authentication. Edit `/etc/exim4/conf.d/auth/30_exim4-config_examples` and uncomment the `plain_saslauthd_server` and `login_saslauthd_server` sections:

```
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
```

Finally, update the Exim4 configuration and restart the service:

```
sudo update-exim4.conf
sudo /etc/init.d/exim4 restart
```

2.4. Configuring SASL

This section provides details on configuring the `saslauthd` to provide authentication for Exim4.

The first step is to install the `sasl2-bin` package. From a terminal prompt enter the following:

```
sudo apt-get install sasl2-bin
```

To configure `saslauthd` edit the `/etc/default/saslauthd` configuration file and set `START=no` to:

```
START=yes
```

Next the *Debian-exim* user needs to be part of the *sasl* group in order for Exim4 to use the `saslauthd` service:

```
sudo adduser Debian-exim sasl
```

Now start the `saslauthd` service:

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

Exim4 is now configured with SMTP-AUTH using TLS and SASL authentication.

3. Dovecot Server

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

3.1. Installation

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

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

3.2. Configuration

To configure dovecot, you can edit the file `/etc/dovecot/dovecot.conf`. You can choose the protocol you use. It could be pop3, pop3s (pop3 secure), imap and imaps (imap secure). A description of these protocols is beyond the scope of this guide. For further information, refer to the Wikipedia articles on *POP3*⁸ and *IMAP*⁹.

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

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

Next, choose the mailbox you would like to use. Dovecot supports **maildir** and **mbox** formats. These are the most commonly used mailbox formats. They both have their own benefits and are discussed on *the Dovecot web site*¹⁰.

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

```
mail_location = maildir:~/Maildir # (for maildir)
or
mail_location = mbox:~/mail:INBOX=/var/spool/mail/%u # (for mbox)
```



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

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

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

⁸ <http://en.wikipedia.org/wiki/POP3>

⁹ http://en.wikipedia.org/wiki/Internet_Message_Access_Protocol

¹⁰ <http://wiki.dovecot.org/MailboxFormat>

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

```
bhuvan@rainbow:~$ telnet localhost pop3
Trying 127.0.0.1...
Connected to localhost.localdomain.
Escape character is '^]'.
+OK Dovecot ready.
```

3.3. Dovecot SSL Configuration

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

```
ssl_cert_file = /etc/ssl/certs/ssl-cert-snakeoil.pem
ssl_key_file = /etc/ssl/private/ssl-cert-snakeoil.key
ssl_disable = no
disable_plaintext_auth = no
```

You can get the SSL certificate from a Certificate Issuing Authority or you can create self signed SSL certificate. The latter is a good option for email, because SMTP clients rarely complain about "self-signed certificates". Please refer to *Section 5, "Certificates" [p. 105]* for details about how to create self signed SSL certificate. Once you create the certificate, you will have a key file and a certificate file. Please copy them to the location pointed in the `/etc/dovecot/dovecot.conf` configuration file.

3.4. Firewall Configuration for an Email Server

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

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

4. Mailman

Mailman is an open source program for managing electronic mail discussions and e-newsletter lists. Many open source mailing lists (including all the *Ubuntu mailing lists*¹¹) use Mailman as their mailing list software. It is powerful and easy to install and maintain.

4.1. Installation

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

- Postfix
- Exim
- Sendmail
- Qmail

We will see how to install and configure Mailman with, the Apache web server, and either the Postfix or Exim mail server. If you wish to install Mailman with a different mail server, please refer to the references section.



You only need to install one mail server and Postfix is the default Ubuntu Mail Transfer Agent.

4.1.1. Apache2

To install apache2 you refer to *HTTPD Installation*¹² section for details.

4.1.2. Postfix

For instructions on installing and configuring Postfix refer to *Section 1, “Postfix” [p. 145]*

4.1.3. Exim4

To install Exim4 refer to *Section 2, “Exim4” [p. 151]*.

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

- `dc_use_split_config='true'`

4.1.4. Mailman

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

¹¹ <http://lists.ubuntu.com>

¹² [./web-servers.xml#http-installation](#)

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

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

4.2. Configuration

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

4.2.1. Apache2

An example Apache configuration file comes with Mailman and is placed in `/etc/mailman/apache.conf`. In order for Apache to use the config file it needs to be copied to `/etc/apache2/sites-available:`

```
sudo cp /etc/mailman/apache.conf /etc/apache2/sites-available/mailman.conf
```

This will setup a new Apache *VirtualHost* for the Mailman administration site. Now enable the new configuration and restart Apache:

```
sudo a2ensite mailman.conf
sudo /etc/init.d/apache2 restart
```

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

4.2.2. Postfix

For Postfix integration, we will associate the domain `lists.example.com` with the mailing lists. Please replace `lists.example.com` with the domain of your choosing.

You can use the `postconf` command to add the necessary configuration to `/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'
```

In `/etc/postfix/master.cf` double check that you have the following transport:

```
mailman  unix  -      n      n      -      -      pipe
         flags=FR user=list argv=/usr/lib/mailman/bin/postfix-to-mailman.py
```

```
{nexthop} {user}
```

It calls the *postfix-to-mailman.py* script when a mail is delivered to a list.

Associate the domain lists.example.com to the Mailman transport with the transport map. Edit the file `/etc/postfix/transport`:

```
lists.example.com      mailman:
```

Now have Postfix build the transport map by entering the following from a terminal prompt:

```
sudo postmap -v /etc/postfix/transport
```

Then restart Postfix to enable the new configurations:

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

4.2.3. Exim4

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

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

In order to make mailman work with Exim4, you need to configure Exim4. As mentioned earlier, by default, Exim4 uses multiple configuration files of different types. For details, please refer to the *Exim*¹³ web site. To run mailman, we should add new a configuration file to the following configuration types:

- Main
- Transport
- Router

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

4.2.4. Main

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

```
# start
# Home dir for your Mailman installation -- aka Mailman's prefix
# directory.
# On Ubuntu this should be "/var/lib/mailman"
```

¹³ <http://www.exim.org>

```
# 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
```

4.2.5. Transport

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

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

4.2.6. Router

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

```
mailman_router:
  driver = accept
```

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



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

4.2.7. Mailman

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

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

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

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

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

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

```
Hit enter to notify mailman owner...
```

```
#
```

We have configured either Postfix or Exim4 to recognize all emails from mailman. So, it is not mandatory to make any new entries in `/etc/aliases`. If you have made any changes to the configuration files, please ensure that you restart those services before continuing to next section.

4.3. Administration

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

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

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

4.4. Users

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

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

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

4.5. References

*GNU Mailman - Installation Manual*¹⁴

*HOWTO - Using Exim 4 and Mailman 2.1 together*¹⁵

¹⁴ <http://www.list.org/mailman-install/index.html>

¹⁵ <http://www.exim.org/howto/mailman21.html>

5. Mail Filtering

One of the largest issues with email today is the problem of Unsolicited Bulk Email (UBE). Also known as SPAM, such messages may also carry viruses and other forms of malware. According to some reports these messages make up the bulk of all email traffic on the Internet.

This section will cover integrating Amavisd-new, Spamassassin, and ClamAV with the Postfix Mail Transport Agent (MTA). Postfix can also check email validity by passing it through external content filters. These filters can sometimes determine if a message is spam without needing to process it with more resource intensive applications. Two common filters are dkim-filter and python-policyd-spf.

- Amavisd-new is a wrapper program that can call any number of content filtering programs for spam detection, antivirus, etc.
- Spamassassin uses a variety of mechanisms to filter email based on the message content.
- ClamAV is an open source antivirus application.
- dkim-filter implements a Sendmail Mail Filter (Milter) for the DomainKeys Identified Mail (DKIM) standard.
- python-policyd-spf enables Sender Policy Framework (SPF) checking with Postfix.

This is how the pieces fit together:

- An email message is accepted by Postfix.
- The message is passed through any external filters dkim-filter and python-policyd-spf in this case.
- Amavisd-new then processes the message.
- ClamAV is used to scan the message. If the message contains a virus Postfix will reject the message.
- Clean messages will then be analyzed by Spamassassin to find out if the message is spam. Spamassassin will then add X-Header lines allowing Amavisd-new to further manipulate the message.

For example, if a message has a Spam score of over fifty the message could be automatically dropped from the queue without the recipient ever having to be bothered. Another, way to handle flagged messages is to deliver them to the Mail User Agent (MUA) allowing the user to deal with the message as they see fit.

5.1. Installation

See *Section 1, "Postfix" [p. 145]* for instructions on installing and configuring Postfix.

To install the rest of the applications enter the following from a terminal prompt:

```
sudo apt-get install amavisd-new spamassassin clamav-daemon
sudo apt-get install dkim-filter python-policyd-spf
```

There are some optional packages that integrate with Spamassassin for better spam detection:

```
sudo apt-get install pyzor razor
```

Along with the main filtering applications compression utilities are needed to process some email attachments:

```
sudo apt-get install arj cabextract cpio lha nomarch pax rar unrar unzip unzoo zip zoo
```

5.2. Configuration

Now configure everything to work together and filter email.

5.2.1. ClamAV

The default behaviour of ClamAV will fit our needs. For more ClamAV configuration options, check the configuration files in `/etc/clamav`.

Add the `clamav` user to the `amavis` group in order for Amavisd-new to have the appropriate access to scan files:

```
sudo adduser clamav amavis
```

5.2.2. Spamassassin

Spamassassin automatically detects optional components and will use them if they are present. This means that there is no need to configure pyzor and razor.

Edit `/etc/default/spamassassin` to activate the Spamassassin daemon. Change `ENABLED=0` to:

```
ENABLED=1
```

Now start the daemon:

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

5.2.3. Amavisd-new

First activate spam and antivirus detection in Amavisd-new by editing `/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
```

Bouncing spam can be a bad idea as the return address is often faked. Consider editing `/etc/amavis/conf.d/20-debian_defaults` to set `$final_spam_destiny` to `D_DISCARD` rather than `D_BOUNCE`, as follows:

```
$final_spam_destiny      = D_DISCARD;
```

If the server's `hostname` is different from the domain's MX record you may need to manually set the `$myhostname` option. Also, if the server receives mail for multiple domains the `@local_domains_acl` option will need to be customized. Edit the `/etc/amavis/conf.d/50-user` file:

```
$myhostname = 'mail.example.com';
@local_domains_acl = ( "example.com", "example.org" );
```

After configuration Amavisd-new needs to be restarted:

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

5.2.3.1. DKIM Whitelist

Amavisd-new can be configured to automatically *Whitelist* addresses from domains with valid Domain Keys. There are some pre-configured domains in the `/etc/amavis/conf.d/40-policy_banks`.

There are multiple ways to configure the Whitelist for a domain:

- `'example.com' => 'WHITELIST'`; will whitelist any address from the "example.com" domain.
- `'example.com' => 'WHITELIST'`; will whitelist any address from any *subdomains* of "example.com" that have a valid signature.
- `'example.com/@example.com' => 'WHITELIST'`; will whitelist subdomains of "example.com" that use the signature of *example.com* the parent domain.

- `'./@example.com'` => `'WHITELIST'`; adds addresses that have a valid signature from "example.com". This is usually used for discussion groups that sign their messages.

A domain can also have multiple Whitelist configurations. After, editing the file restart amavisd-new:

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



In this context, once a domain has been added to the Whitelist the message will not receive any anti-virus or spam filtering. This may or may not be the intended behavior you wish for a domain.

5.2.4. Postfix

For Postfix integration, enter the following from a terminal prompt:

```
sudo postconf -e 'content_filter = smtp-amavis:[127.0.0.1]:10024'
```

Next edit `/etc/postfix/master.cf` and add the following to the end of the file:

```
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
```

Also add the following two lines immediately below the *"pickup"* transport service:

```
-o content_filter=
-o receive_override_options=no_header_body_checks
```

This will prevent messages that are generated to report on spam from being classified as spam.

Now restart Postfix:

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

Content filtering with spam and virus detection is now enabled.

5.3. Testing

First, test that the Amavisd-new SMTP is listening:

```
telnet localhost 10024
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 [127.0.0.1] ESMTTP amavisd-new service ready
^]
```

In the Header of messages that go through the content filter you should see:

```
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:
```



Your output will vary, but the important thing is that there are *X-Virus-Scanned* and *X-Spam-Status* entries.

5.4. Troubleshooting

The best way to figure out why something is going wrong is to check the log files.

- For instructions on Postfix logging see the *Section 1.6, “Troubleshooting” [p. 148]* section.
- Amavisd-new uses Syslog to send messages to `/var/log/mail.log`. The amount of detail can be increased by adding the `$log_level` option to `/etc/amavis/conf.d/50-user`, and setting the value from 1 to 5.

```
$log_level = 2;
```



When the Amavisd-new log output is increased Spamassassin log output is also increased.

- The ClamAV log level can be increased by editing `/etc/clamav/clamd.conf` and setting the following option:

```
LogVerbose true
```

By default ClamAV will send log messages to `/var/log/clamav/clamav.log`.



After changing an applications log settings remember to restart the service for the new settings to take affect. Also, once the issue you are troubleshooting is resolved it is a good idea to change the log settings back to normal.

5.5. References

For more information on filtering mail see the following links:

- *Amavisd-new Documentation*¹⁶
- *ClamAV Documentation*¹⁷ and *ClamAV Wiki*¹⁸
- *Spamassassin Wiki*¹⁹
- *Pyzor Homepage*²⁰
- *Razor Homepage*²¹
- *DKIM.org*²²

Also, feel free to ask questions in the `#ubuntu-server` IRC channel on *freenode*²³.

²³ <http://freenode.net>

Chapter 14. Version Control System

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

1. Bazaar

Bazaar is a new version control system sponsored by Canonical, the commercial company behind Ubuntu. Unlike Subversion and CVS that only support a central repository model, Bazaar also supports *distributed version control*, giving people the ability to collaborate more efficiently. In particular, Bazaar is designed to maximize the level of community participation in open source projects.

1.1. Installation

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

```
sudo apt-get install bzz
```

1.2. Configuration

To introduce yourself to bzz, use the *whoami* command like this:

```
$ bzz whoami 'Joe Doe <joe.doe@gmail.com>'
```

1.3. Learning Bazaar

Bazaar comes with bundled documentation installed into `/usr/share/doc/bzz/html` by default. The tutorial is a good place to start. The bzz command also comes with built-in help:

```
$ bzz help
```

To learn more about the *foo* command:

```
$ bzz help foo
```

1.4. Launchpad Integration

While highly useful as a stand-alone system, Bazaar has good, optional integration with *Launchpad*¹, the collaborative development system used by Canonical and the broader open source community to manage and extend Ubuntu itself. For information on how Bazaar can be used with Launchpad to collaborate on open source projects, see <http://bazaar-vcs.org/LaunchpadIntegration>².

¹ <https://launchpad.net/>

² <http://bazaar-vcs.org/LaunchpadIntegration/>

2. Subversion

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

2.1. Installation

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

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

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

2.2. Server Configuration

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

2.2.1. Create Subversion Repository

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

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

2.2.2. Importing Files

Once you create the repository you can *import* files into the repository. To import a directory, enter the following from a terminal prompt:

```
svn import /path/to/import/directory file:///path/to/repos/project
```

2.3. Access Methods

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

Table 14.1. Access Methods

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

In this section, we will see how to configure Subversion for all these access methods. Here, we cover the basics. For more advanced usage details, refer to the *svn book*³.

2.3.1. Direct repository access (file://)

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

```
svn co file:///path/to/repos/project
```

or

```
svn co file://localhost/path/to/repos/project
```



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

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

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

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

```
<Location /svn>
  DAV svn
  SVNParentPath /home/svn
  AuthType Basic
  AuthName "Your repository name"
  AuthUserFile /etc/subversion/passwd
  <LimitExcept GET PROPFIND OPTIONS REPORT>
```

³ <http://svnbook.red-bean.com/>

```
Require valid-user
</LimitExcept>
</Location>
```



The above configuration snippet assumes that Subversion repositories are created under `/home/svn/` directory using **svnadmin** command. They can be accessible using **http://hostname/svn/repos_name** url.

To import or commit files to your Subversion repository over HTTP, the repository should be owned by the HTTP user. In Ubuntu systems, normally the HTTP user is **www-data**. To change the ownership of the repository files enter the following command from terminal prompt:

```
sudo chown -R www-data:www-data /path/to/repos
```



By changing the ownership of repository as **www-data** you will not be able to import or commit files into the repository by running **svn import file:///** command as any user other than **www-data**.

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

```
sudo htpasswd -c /etc/subversion/passwd user_name
```

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

```
svn co http://servername/svn
```



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

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

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

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

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

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

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

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

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

```
username = password
```

For more details, please refer to the file.

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

```
$ svnserv -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:

```
$ svnserv --help
```

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

```
svn co svn://hostname/project project --username user_name
```

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

```
cd project_dir ; svn update
```

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

```
svn co help
```

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

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

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

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

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



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

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

3. CVS Server

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

3.1. Installation

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

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

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

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

3.2. Configuration

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

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

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

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



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

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

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

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

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

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

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

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



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

3.3. Add Projects

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

```
cd your/project
```

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



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

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



When you add a new project, the CVS user you use must have write access to the CVS repository (/var/lib/cvs). By default, the src group has write access to the CVS repository. So, you can add the user to this group, and he can then add and manage projects in the CVS repository.

4. References

*Bazaar Home Page*⁴

*Launchpad*⁵

*Subversion Home Page*⁶

*Subversion Book*⁷

*CVS Manual*⁸

⁴ <http://bazaar-vcs.org/>

⁵ <https://launchpad.net/>

⁶ <http://subversion.tigris.org/>

⁷ <http://svnbook.red-bean.com/>

⁸ http://ximbiot.com/cvs/manual/cvs-1.11.21/cvs_toc.html

Chapter 15. Windows Networking

Computer networks are often comprised of diverse systems, and while operating a network made up entirely of Ubuntu desktop and server computers would certainly be fun, some network environments must consist of both Ubuntu and Microsoft® Windows® systems working together in harmony. This section of the Ubuntu Server Guide introduces principles and tools used in configuring your Ubuntu Server for sharing network resources with Windows computers.

1. Introduction

Successfully networking your Ubuntu system with Windows clients involves providing and integrating with services common to Windows environments. Such services assist the sharing of data and information about the computers and users involved in the network, and may be classified under three major categories of functionality:

- **File and Printer Sharing Services.** Using the Server Message Block (SMB) protocol to facilitate the sharing of files, folders, volumes, and the sharing of printers throughout the network.
- **Directory Services.** Sharing vital information about the computers and users of the network with such technologies as the Lightweight Directory Access Protocol (LDAP) and Microsoft Active Directory®.
- **Authentication and Access.** Establishing the identity of a computer or user of the network and determining the information the computer or user is authorized to access using such principles and technologies as file permissions, group policies, and the Kerberos authentication service.

Fortunately, your Ubuntu system may provide all such facilities to Windows clients and share network resources among them. One of the principal pieces of software your Ubuntu system includes for Windows networking is the Samba suite of SMB server applications and tools.

This section of the Ubuntu Server Guide will introduce some of the common Samba use cases, and how to install and configure the necessary packages. Additional detailed documentation and information on Samba can be found on the *Samba website*¹.

¹ <http://www.samba.org>

2. Samba File Server

One of the most common ways to network Ubuntu and Windows computers is to configure Samba as a File Server. This section covers setting up a Samba server to share files with Windows clients.

The server will be configured to share files with any client on the network without prompting for a password. If your environment requires stricter Access Controls see *Section 4, “Securing a Samba File and Print Server” [p. 183]*

2.1. Installation

The first step is to install the samba package. From a terminal prompt enter:

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

That's all there is to it; you are now ready to configure Samba to share files.

2.2. Configuration

The main Samba configuration file is located in `/etc/samba/smb.conf`. The default configuration file has a significant amount of comments in order to document various configuration directives.



Not all the available options are included in the default configuration file. See the `smb.conf` man page or the *Samba HOWTO Collection*² for more details.

1. First, edit the following key/value pairs in the `[global]` section of `/etc/samba/smb.conf`:

```
workgroup = EXAMPLE
...
security = user
```

The `security` parameter is farther down in the `[global]` section, and is commented by default. Also, change `EXAMPLE` to better match your environment.

2. Create a new section at the bottom of the file, or uncomment one of the examples, for the directory to be shared:

```
[share]
comment = Ubuntu File Server Share
path = /srv/samba/share
browsable = yes
guest ok = yes
read only = no
create mask = 0755
```

- *comment*: a short description of the share. Adjust to fit your needs.
- *path*: the path to the directory to share.

This example uses `/srv/samba/sharename` because, according to the *Filesystem Hierarchy Standard (FHS)*, `/srv`³ is where site-specific data should be served. Technically Samba shares can be placed anywhere on the filesystem as long as the permissions are correct, but adhering to standards is recommended.

- *browsable*: enables Windows clients to browse the shared directory using Windows Explorer.
 - *guest ok*: allows clients to connect to the share without supplying a password.
 - *read only*: gives write access to the shared directory.
 - *create mask*: determines the permissions new files will have when created.
3. Now that Samba is configured, the directory needs to be created and the permissions changed. From a terminal enter:

```
sudo mkdir -p /srv/samba/share
sudo chown nobody.nogroup /srv/samba/share/
```



The `-p` switch tells `mkdir` to create the entire directory tree if it doesn't exist. Change the share name to fit your environment.

4. Finally, restart the samba services to enable the new configuration:

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



Once again, the above configuration gives all access to any client on the local network. For a more secure configuration see *Section 4*, “*Securing a Samba File and Print Server*” [p. 183].

From a Windows client you should now be able to browse to the Ubuntu file server and see the shared directory. To check that everything is working try creating a directory from Windows.

To create additional shares simply create new `[dir]` sections in `/etc/samba/smb.conf`, and restart *Samba*. Just make sure that the directory you want to share actually exists and the permissions are correct.

2.3. Resources

- For in depth Samba configurations see the *Samba HOWTO Collection*⁴
- The guide is also available in *printed format*⁵.
- O'Reilly's *Using Samba*⁶ is another good reference.

3. Samba Print Server

Another common use of Samba is to configure it to share printers installed, either locally or over the network, on an Ubuntu server. Similar to *Section 2, “Samba File Server” [p. 180]* this section will configure Samba to allow any client on the local network to use the installed printers without prompting for a username and password.

For a more secure configuration see *Section 4, “Securing a Samba File and Print Server” [p. 183]*.

3.1. Installation

Before installing and configuring Samba it is best to already have a working CUPS installation. See *Section 3, “CUPS - Print Server” [p. 141]* for details.

To install the samba package, from a terminal enter:

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

3.2. Configuration

After installing samba edit `/etc/samba/smb.conf`. Change the *workgroup* attribute to what is appropriate for your network, and change *security* to *share*:

```
workgroup = EXAMPLE
...
security = user
```

In the *[printers]* section change the *guest ok* option to *yes*:

```
browsable = yes
guest ok = yes
```

After editing `smb.conf` restart the Samaba:

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

The default Samba configuration will automatically share any printers installed. Simply install the printer locally on your Windows clients.

3.3. Resources

- For in depth Samba configurations see the *Samba HOWTO Collection*⁷
- The guide is also available in *printed format*⁸.
- O'Reilly's *Using Samba*⁹ is another good reference.
- Also, see the *CUPS Website*¹⁰ for more information on configuring CUPS.

4. Securing a Samba File and Print Server

4.1. Samba Security Modes

There are two security levels available to the Common Internet Filesystem (CIFS) network protocol *user-level* and *share-level*. Samba's *security mode* implementation allows more flexibility, providing four ways of implementing user-level security and one way to implement share-level:

- *security = user*: requires clients to supply a username and password to connect to shares. Samba user accounts are separate from system accounts, but the `libpam-smbpass` package will sync system users and passwords with the Samba user database.
- *security = domain*: this mode allows the Samba server to appear to Windows clients as a Primary Domain Controller (PDC), Backup Domain Controller (BDC), or a Domain Member Server (DMS). See *Section 5, “Samba as a Domain Controller” [p. 187]* for further information.
- *security = ADS*: allows the Samba server to join an Active Directory domain as a native member. See *Section 6, “Samba Active Directory Integration” [p. 191]* for details.
- *security = server*: this mode is left over from before Samba could become a member server, and due to some security issues should not be used. See the *Server Security*¹¹ section of the Samba guide for more details.
- *security = share*: allows clients to connect to shares without supplying a username and password.

The security mode you choose will depend on your environment and what you need the Samba server to accomplish.

4.2. Security = User

This section will reconfigure the Samba file and print server, from *Section 2, “Samba File Server” [p. 180]* and *Section 3, “Samba Print Server” [p. 182]*, to require authentication.

First, install the `libpam-smbpass` package which will sync the system users to the Samba user database:

```
sudo apt-get install libpam-smbpass
```



If you chose the *Samba Server* task during installation `libpam-smbpass` is already installed.

Edit `/etc/samba/smb.conf`, and in the `[share]` section change:

```
guest ok = no
```

Finally, restart Samba for the new settings to take effect:

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

Now when connecting to the shared directories or printers you should be prompted for a username and password.



If you choose to map a network drive to the share you can check the “Reconnect at Logon” check box, which will require you to only enter the username and password once, at least until the password changes.

4.3. Share Security

There are several options available to increase the security for each individual shared directory. Using the *[share]* example, this section will cover some common options.

4.3.1. Groups

Groups define a collection of computers or users which have a common level of access to particular network resources and offer a level of granularity in controlling access to such resources. For example, if a group *qa* is defined and contains the users *freda*, *danika*, and *rob* and a second group *support* is defined and consists of users *danika*, *jeremy*, and *vincent* then certain network resources configured to allow access by the *qa* group will subsequently enable access by *freda*, *danika*, and *rob*, but not *jeremy* or *vincent*. Since the user *danika* belongs to both the *qa* and *support* groups, she will be able to access resources configured for access by both groups, whereas all other users will have only access to resources explicitly allowing the group they are part of.

By default Samba looks for the local system groups defined in */etc/group* to determine which users belong to which groups. For more information on adding and removing users from groups see *Section 1.2, “Adding and Deleting Users” [p. 87]*.

When defining groups in the Samba configuration file, */etc/samba/smb.conf*, the recognized syntax is to preface the group name with an "@" symbol. For example, if you wished to define a group named *sysadmin* in a certain section of the */etc/samba/smb.conf*, you would do so by entering the group name as **@sysadmin**.

4.3.2. File Permissions

File Permissions define the explicit rights a computer or user has to a particular directory, file, or set of files. Such permissions may be defined by editing the */etc/samba/smb.conf* file and specifying the explicit permissions of a defined file share.

For example, if you have defined a Samba share called *share* and wish to give *read-only* permissions to the group of users known as *qa*, but wanted to allow writing to the share by the group called *sysadmin* and the user named *vincent*, then you could edit the */etc/samba/smb.conf* file, and add the following entries under the *[share]* entry:

```
read list = @qa
write list = @sysadmin, vincent
```

Another possible Samba permission is to declare *administrative* permissions to a particular shared resource. Users having administrative permissions may read, write, or modify any information contained in the resource the user has been given explicit administrative permissions to.

For example, if you wanted to give the user *melissa* administrative permissions to the *share* example, you would edit the `/etc/samba/smb.conf` file, and add the following line under the `[share]` entry:

```
admin users = melissa
```

After editing `/etc/samba/smb.conf`, restart Samba for the changes to take effect:

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



For the *read list* and *write list* to work the Samba security mode must *not* be set to `security = share`

Now that Samba has been configured to limit which groups have access to the shared directory, the filesystem permissions need to be updated.

Traditional Linux file permissions do not map well to Windows NT Access Control Lists (ACLs). Fortunately POSIX ACLs are available on Ubuntu servers providing more fine grained control. For example, to enable ACLs on `/srv` an EXT3 filesystem, edit `/etc/fstab` adding the *acl* option:

```
UUID=66bcdd2e-8861-4fb0-b7e4-e61c569fe17d /srv ext3 noatime,relatime,acl 0 1
```

Then remount the partition:

```
sudo mount -v -o remount /srv
```



The above example assumes `/srv` on a separate partition. If `/srv`, or wherever you have configured your share path, is part of the `/` partition a reboot may be required.

To match the Samba configuration above the *sysadmin* group will be given read, write, and execute permissions to `/srv/samba/share`, the *qa* group will be given read and execute permissions, and the files will be owned by the username *melissa*. Enter the following in a 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/
```



The `setfacl` command above gives *execute* permissions to all files in the `/srv/samba/share` directory, which you may or may not want.

Now from a Windows client you should notice the new file permissions are implemented. See the `acl` and `setfacl` man pages for more information on POSIX ACLs.

4.4. Samba AppArmor Profile

Ubuntu comes with the AppArmor security module, which provides mandatory access controls. The default AppArmor profile for Samba will need to be adapted to your configuration. For more details on using AppArmor see *Section 4, “AppArmor” [p. 101]*.

There are default AppArmor profiles for `/usr/sbin/smbd` and `/usr/sbin/nmbd`, the Samba daemon binaries, as part of the `apparmor-profiles` packages. To install the package, from a terminal prompt enter:

```
sudo apt-get install apparmor-profiles
```



This package contains profiles for several other binaries.

By default the profiles for `smbd` and `nmbd` are in *complain* mode allowing Samba to work without modifying the profile, and only logging errors. To place the `smbd` profile into *enforce* mode, and have Samba work as expected, the profile will need to be modified to reflect any directories that are shared.

Edit `/etc/apparmor.d/usr.sbin.smbd` adding information for *[share]* from the file server example:

```
/srv/samba/share/ r,  
/srv/samba/share/** rwkix,
```

Now place the profile into *enforce* and reload it:

```
sudo aa-enforce /usr/sbin/smbd  
cat /etc/apparmor.d/usr.sbin.smbd | sudo apparmor_parser -r
```

You should now be able to read, write, and execute files in the shared directory as normal, and the `smbd` binary will have access to only the configured files and directories. Be sure to add entries for each directory you configure Samba to share. Also, any errors will be logged to `/var/log/syslog`.

4.5. Resources

- For in depth Samba configurations see the *Samba HOWTO Collection*¹²
- The guide is also available in *printed format*¹³.
- O'Reilly's *Using Samba*¹⁴ is also a good reference.
- *Chapter 18*¹⁵ of the Samba HOWTO Collection is devoted to security.
- For more information on Samba and ACLs see the *Samba ACLs page*¹⁶.

5. Samba as a Domain Controller

Although it cannot act as an Active Directory Primary Domain Controller (PDC), a Samba server can be configured to appear as a Windows NT4-style domain controller. A major advantage of this configuration is the ability to centralize user and machine credentials. Samba can also use multiple backends to store the user information.

5.1. Primary Domain Controller

This section covers configuring Samba as a Primary Domain Controller (PDC) using the default `smbpasswd` backend.

1. First, install Samba, and `libpam-smbpass` to sync the user accounts, by entering the following in a terminal prompt:

```
sudo apt-get install samba libpam-smbpass
```

2. Next, configure Samba by editing `/etc/samba/smb.conf`. The *security* mode should be set to *user*, and the *workgroup* should relate to your organization:

```
workgroup = EXAMPLE
...
security = user
```

3. In the commented “Domains” section add or uncomment the following:

```
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 /
```

- *domain logons*: provides the netlogon service causing Samba to act as a domain controller.
- *logon path*: places the user's Windows profile into their home directory. It is also possible to configure a *[profiles]* share placing all profiles under a single directory.
- *logon drive*: specifies the home directory local path.
- *logon home*: specifies the home directory location.
- *logon script*: determines the script to be run locally once a user has logged in. The script needs to be placed in the *[netlogon]* share.
- *add machine script*: a script that will automatically create the *Machine Trust Account* needed for a workstation to join the domain.

In this example the *machines* group will need to be created using the `addgroup` utility see *Section 1.2, “Adding and Deleting Users”* [p. 87] for details.



If you wish to not use *Roaming Profiles* leave the *logon home* and *logon path* options commented.

4. Uncomment the `[homes]` share to allow the *logon home* to be mapped:

```
[homes]
comment = Home Directories
browseable = no
read only = no
create mask = 0700
directory mask = 0700
valid users = %S
```

5. When configured as a domain controller a `[netlogon]` share needs to be configured. To enable the share, uncomment:

```
[netlogon]
comment = Network Logon Service
path = /srv/samba/netlogon
guest ok = yes
read only = yes
share modes = no
```



The original *netlogon* share path is `/home/samba/netlogon`, but according to the Filesystem Hierarchy Standard (FHS), `/srv`¹⁷ is the correct location for site-specific data provided by the system.

6. Now create the `netlogon` directory, and an empty (for now) `logon.cmd` script file:

```
sudo mkdir -p /srv/samba/netlogon
sudo touch /srv/samba/netlogon/logon.cmd
```

You can enter any normal Windows logon script commands in `logon.cmd` to customize the client's environment.

7. With *root* being disabled by default, in order to join a workstation to the domain, a system group needs to be mapped to the Windows *Domain Admins* group. Using the `net` utility, from a terminal enter:

```
sudo net groupmap add ntgroup="Domain Admins" unixgroup=sysadmin rid=512 type=d
```



Change *sysadmin* to whichever group you prefer. Also, the user used to join the domain needs to be a member of the *sysadmin* group, as well as a member of the system *admin* group. The *admin* group allows `sudo` use.

8. Finally, restart Samba to enable the new domain controller:

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

9. You should now be able to join Windows clients to the Domain in the same manner as joining them to an NT4 domain running on a Windows server.

5.2. Backup Domain Controller

With a Primary Domain Controller (PDC) on the network it is best to have a Backup Domain Controller (BDC) as well. This will allow clients to authenticate in case the PDC becomes unavailable.

When configuring Samba as a BDC you need a way to sync account information with the PDC. There are multiple ways of accomplishing this `scp`, `rsync`, or by using LDAP as the *passwd backend*.

Using LDAP is the most robust way to sync account information, because both domain controllers can use the same information in real time. However, setting up a LDAP server may be overly complicated for a small number of user and computer accounts. See *Section 2, "Samba and LDAP" [p. 61]* for details.

1. First, install `samba` and `libpam-smbpass`. From a terminal enter:

```
sudo apt-get install samba libpam-smbpass
```

2. Now, edit `/etc/samba/smb.conf` and uncomment the following in the *[global]*:

```
workgroup = EXAMPLE
...
security = user
```

3. In the commented *Domains* uncomment or add:

```
domain logons = yes
domain master = no
```

4. Make sure a user has rights to read the files in `/var/lib/samba`. For example, to allow users in the *admin* group to `scp` the files, enter:

```
sudo chgrp -R admin /var/lib/samba
```

5. Next, sync the user accounts, using `scp` to copy the `/var/lib/samba` directory from the PDC:

```
sudo scp -r username@pdc:/var/lib/samba /var/lib
```



Replace *username* with a valid username and *pdc* with the hostname or IP Address of your actual PDC.

6. Finally, restart `samba`:

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

You can test that your Backup Domain controller is working by stopping the Samba daemon on the PDC, then trying to login to a Windows client joined to the domain.

Another thing to keep in mind is if you have configured the *logon home* option as a directory on the PDC, and the PDC becomes unavailable, access to the user's *Home* drive will also be unavailable. For this reason it is best to configure the *logon home* to reside on a separate file server from the PDC and BDC.

5.3. Resources

- For in depth Samba configurations see the *Samba HOWTO Collection*¹⁸
- The guide is also available in *printed format*¹⁹.
- O'Reilly's *Using Samba*²⁰ is also a good reference.
- *Chapter 4*²¹ of the Samba HOWTO Collection explains setting up a Primary Domain Controller.
- *Chapter 5*²² of the Samba HOWTO Collection explains setting up a Backup Domain Controller.

6. Samba Active Directory Integration

6.1. Accessing a Samba Share

Another use for Samba is to integrate into an existing Windows network. Once part of an Active Directory domain, Samba can provide file and print services to AD users.

The simplest way to join an AD domain is to use Likewise-open. For detailed instructions see *Section 7, “Likewise Open” [p. 193]*.

Once part of the domain, install the following packages:

```
sudo apt-get install samba smbfs smbclient
```

Since the likewise-open and samba packages use separate `secrets.tdb` files, a symlink will need to be created in `/var/lib/samba`:

```
sudo mv /var/lib/samba/secrets.tdb /var/lib/samba/secrets.tdb.orig
sudo ln -s /etc/samba/secrets.tdb /var/lib/samba
```

Next, edit `/etc/samba/smb.conf` changing:

```
workgroup = EXAMPLE
...
security = ads
realm = EXAMPLE.COM
...
idmap backend = lwopen
idmap uid = 50-9999999999
idmap gid = 50-9999999999
```

Restart samba for the new settings to take effect:

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

You should now be able to access any Samba shares from a Windows client. However, be sure to give the appropriate AD users or groups access to the share directory. See *Section 4, “Securing a Samba File and Print Server” [p. 183]* for more details.

6.2. Accessing a Windows Share

Now that the Samba server is part of the Active Directory domain you can access any Windows server shares:

- To mount a Windows file share enter the following in a terminal prompt:

```
mount.cifs //fs01.example.com/share mount_point
```

It is also possible to access shares on computers not part of an AD domain, but a username and password will need to be provided.

- To mount the share during boot place an entry in `/etc/fstab`, for example:

```
//192.168.0.5/share /mnt/windows cifs auto,username=steve,password=secret,rw 0 0
```

- Another way to copy files from a Windows server is to use the `smbclient` utility. To list the files in a Windows share:

```
smbclient //fs01.example.com/share -k -c "ls"
```

- To copy a file from the share, enter:

```
smbclient //fs01.example.com/share -k -c "get file.txt"
```

This will copy the `file.txt` into the current directory.

- And to copy a file to the share:

```
smbclient //fs01.example.com/share -k -c "put /etc/hosts hosts"
```

This will copy the `/etc/hosts` to `//fs01.example.com/share/hosts`.

- The `-c` option used above allows you to execute the `smbclient` command all at once. This is useful for scripting and minor file operations. To enter the `smb: \>` prompt, a FTP like prompt where you can execute normal file and directory commands, simply execute:

```
smbclient //fs01.example.com/share -k
```



Replace all instances of `fs01.example.com/share`, `//192.168.0.5/share`, `username=steve,password=secret`, and `file.txt` with your server's IP, hostname, share name, file name, and an actual username and password with rights to the share.

For more `smbclient` options see the man page: **man smbclient**

7. Likewise Open

Likewise Open simplifies the necessary configuration needed to authenticate a Linux machine to an Active Directory domain. Based on winbind, the likewise-open package takes the pain out of integrating Ubuntu authentication into an existing Windows network.

7.1. Installation

There are two ways to use Likewise Open, likewise-open the command line utility and likewise-open-gui. This section focuses on the command line utility.

To install the likewise-open package, open a terminal prompt and enter:

```
sudo apt-get install likewise-open
```

7.2. Joining a Domain

The main executable file of the likewise-open package is `/usr/bin/domainjoin-cli`, which is used to join your computer to the domain. Before you join a domain you will need to make sure and have:

- Access to an Active Directory user with appropriate rights to join the domain.
- The *Fully Qualified Domain Name* (FQDN) of the domain you want to join. If your AD domain does not match a valid domain such as *example.com*, it is likely that it has the form of *domainname.local*.
- DNS for the domain setup properly. In a production AD environment this should be the case. Proper Microsoft DNS is needed so that client workstations can determine the Active Directory domain is available.

If you don't have a Windows DNS server on your network, see *Section 7.5, "Microsoft DNS" [p. 195]* for details.

To join a domain, from a terminal prompt enter:

```
sudo domainjoin-cli join example.com Administrator
```



Replace *example.com* with your domain name, and *Administrator* with the appropriate user name.

You will then be prompted for the user's password. If all goes well a *SUCCESS* message should be printed to the console.

After successfully joining an Ubuntu machine to an Active Directory domain you can authenticate using any valid AD user. To login you will need to enter the user name as 'domain\username'. For example to ssh to a server joined to the domain enter:

```
ssh 'example\steve'@hostname
```



If configuring a Desktop the user name will need to be prefixed with *domain* in the graphical logon as well.

To make likewise-open use a default domain, you can add the following statement to `/etc/samba/lwiauthd.conf`:

```
winbind use default domain = yes
```

Then restart the likewise-open daemons:

```
sudo /etc/init.d/likewise-open restart
```



Once configured for a *default domain* the '*domain*' is no longer required, users can login using only their username.

The `domainjoin-cli` utility can also be used to leave the domain. From a terminal:

```
sudo domainjoin-cli leave
```

7.3. Other Utilities

The likewise-open package comes with a few other utilities that may be useful for gathering information about the Active Directory environment. These utilities are used to join the machine to the domain, and are the same as those available in the `samba-common` and `winbind` packages:

- `lwinet`: Returns information about the network and the domain.
- `lwimsg`: Allows interaction with the `likewise-winbindd` daemon.
- `lwiinfo`: Displays information about various parts of the Domain.

Please refer to each utility's man page specific for details.

7.4. Troubleshooting

- If the client has trouble joining the domain, double check that the Microsoft DNS is listed first in `/etc/resolv.conf`. For example:

```
nameserver 192.168.0.1
```

- For more information when joining a domain, use the `--loglevel verbose` or `--advanced` option of the `domainjoin-cli` utility:

```
sudo domainjoin-cli --loglevel verbose join example.com Administrator
```

- If an Active Directory user has trouble logging in, check the `/var/log/auth.log` for details.
- When joining an Ubuntu Desktop workstation to a domain, you may need to edit `/etc/nsswitch.conf` if your AD domain uses the `.local` syntax. In order to join the domain the `"mdns4"` entry from the `hosts` option. For example:

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

Change the above to:

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

Then restart networking by entering:

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

You should now be able to join the Active Directory domain.

7.5. Microsoft DNS

The following are instructions for installing DNS on an Active Directory domain controller running Windows Server 2003, but the instructions should be similar for other versions:

- Click Start → Administrative Tools → Manager Your Server. This will open the Server Role Management utility.
 1. Click Add or remove a role
 2. Click Next
 3. Select "DNS Server"
 4. Click Next
 5. Next
 6. Select "Create a forward lookup zone" if it is not selected.
 7. Click Next
 8. Make sure "This server maintains the zone" is selected and click Next.
 9. Enter your domain name and click Next
 10. Click Next to "Allow only secure dynamic updates"
 11. Click Next to "Allow only secure dynamic updates"
 12. Enter the IP for DNS servers to forward queries to, or Select "No, it should not forward queries" and click Next.
 13. Click Finish
 14. Click Finish

DNS is now installed and can be further configured using the Microsoft Management Console DNS snap-in.

- Next, configure the Server to use itself for DNS queries:
 1. Click Start
 2. Control Panel

3. Network Connections
4. Right Click "Local Area Connection"
5. Click Properties
6. Double click "Internet Protocol (TCP/IP)"
7. Enter the Server's IP Address as the "Preferred DNS server"
8. Click Ok
9. Click Ok again to save the settings

7.6. References

Please refer to the *Likewise*²³ home page for further information.

For more domainjoin-cli options see the man page: **man domainjoin-cli**.

²³ <http://www.likewissoftware.com/>

Chapter 16. Backups

There are many ways to backup a Ubuntu installation. The most import thing about backups is to develop a *backup plan* consisting of what to backup, where to backup it up to, and how to restore it.

The following sections discuss various ways of accomplishing these tasks.

1. Shell Scripts

One of the simplest ways to backup a system is using a *shell script*. For example, a script can be used to configure which directories to backup, and use those directories as arguments to the tar utility creating an archive file. The archive file can then be moved or copied to another location. The archive can also be created on a remote file system such as an *NFS* mount.

The tar utility creates one archive file out of many files or directories. tar can also filter the files through compression utilities reducing the size of the archive file.

1.1. Simple Shell Script

The following shell script uses tar to create an archive file on a remotely mounted NFS file system. The archive filename is determined using additional command line utilities.

```
#!/bin/sh
#####
#
# Backup to NFS mount script.
#
#####

# What to backup.
backup_files="/home /var/spool/mail /etc /root /boot /opt"

# Where to backup to.
dest="/mnt/backup"

# Create archive filename.
day=$(date +%A)
hostname=$(hostname -s)
archive_file="$hostname-$day.tgz"

# Print start status message.
echo "Backing up $backup_files to $dest/$archive_file"
date
echo

# Backup the files using tar.
tar czf $dest/$archive_file $backup_files

# Print end status message.
echo
echo "Backup finished"
date

# Long listing of files in $dest to check file sizes.
ls -lh $dest
```

- *\$backup_files*: a variable listing which directories you would like to backup. The list should be customized to fit your needs.
- *\$day*: a variable holding the day of the week (Monday, Tuesday, Wednesday, etc). This is used to create an archive file for each day of the week, giving a backup history of seven days. There are other ways to accomplish this including other ways using the date utility.
- *\$hostname*: variable containing the *short* hostname of the system. Using the hostname in the archive filename gives you the option of placing daily archive files from multiple systems in the same directory.
- *\$archive_file*: the full archive filename.
- *\$dest*: destination of the archive file. The directory needs to be created and in this case *mounted* before executing the backup script. See *Section 2, “Network File System (NFS)” [p. 139]* for details using *NFS*.
- *status messages*: optional messages printed to the console using the echo utility.
- *tar czf \$dest/\$archive_file \$backup_files*: the tar command used to create the archive file.
 - *c*: creates an archive.
 - *z*: filter the archive through the gzip utility compressing the archive.
 - *f*: use archive file. Otherwise the tar output will be sent to STDOUT.
- *ls -lh \$dest*: optional statement prints a *-l* long listing in *-h* human readable format of the destination directory. This is useful for a quick file size check of the archive file. This check should not replace testing the archive file.

This is a simple example of a backup shell script. There are large amount of options that can be included in a backup script. See *Section 1.4, “References” [p. 201]* for links to resources providing more in depth shell scripting information.

1.2. Executing the Script

1.2.1. Executing from a Terminal

The simplest way of executing the above backup script is to copy and paste the contents into a file. `backup.sh` for example. Then from a terminal prompt:

```
sudo bash backup.sh
```

This is a great way to test the script to make sure everything works as expected.

1.2.2. Executing with cron

The cron utility can be used to automate the script execution. The cron daemon allows the execution of scripts, or commands, at a specified time and date.

cron is configured through entries in a `crontab` file. `crontab` files are separated into fields:

```
# m h dom mon dow  command
```

- *m*: minute the command executes on between 0 and 59.
- *h*: hour the command executes on between 0 and 23.
- *dom*: day of month the command executes on.
- *mon*: the month the command executes on between 1 and 12.
- *dow*: the day of the week the command executes on between 0 and 7. Sunday may be specified by using 0 or 7, both values are valid.
- *command*: the command to execute.

To add or change entries in a `crontab` file the `crontab -e` command should be used. Also, the contents of a `crontab` file can be viewed using the `crontab -l` command.

To execute the `backup.sh` script listed above using cron. Enter the following from a terminal prompt:

```
sudo crontab -e
```



Using `sudo` with the `crontab -e` command edits the `root` user's crontab. This is necessary if you are backing up directories only the root user has access to.

Add the following entry to the `crontab` file:

```
# m h dom mon dow  command
0 0 * * * bash /usr/local/bin/backup.sh
```

The `backup.sh` script will now be executed every day at 12:00 am.



The `backup.sh` script will need to be copied to the `/usr/local/bin/` directory in order for this entry to execute properly. The script can reside anywhere on the file system simply change the script path appropriately.

For more in depth crontab options see *Section 1.4, "References" [p. 201]*.

1.3. Restoring from the Archive

Once an archive has been created it is important to test the archive. The archive can be tested by listing the files it contains, but the best test is to *restore* a file from the archive.

- To see a listing of the archive contents. From a terminal prompt:

```
tar -tzvf /mnt/backup/host-Monday.tgz
```

- To restore a file from the archive to a different directory enter:

```
tar -xzvf /mnt/backup/host-Monday.tgz -C /tmp etc/hosts
```

The `-C` option to `tar` redirects the extracted files to the specified directory. The above example will extract the `/etc/hosts` file to `/tmp/etc/hosts`. `tar` recreates the directory structure that it contains.

Also, notice the leading `"/` is left off the path of the file to restore.

- To restore all files in the archive enter the following:

```
cd /  
sudo tar -xzvf /mnt/backup/host-Monday.tgz
```



This will overwrite the files currently on the file system.

1.4. References

- For more information on shell scripting see the *Advanced Bash-Scripting Guide*¹
- The book *Teach Yourself Shell Programming in 24 Hours*² is available online and a great resource for shell scripting.
- The *CronHowto Wiki Page*³ contains details on advanced cron options.
- See the *GNU tar Manual*⁴ for more tar options.
- The Wikipedia *Backup Rotation Scheme*⁵ article contains information on other backup rotation schemes.
- The shell script uses `tar` to create the archive, but there many other command line utilities that can be used. For example:
 - `cpio`⁶: used to copy files to and from archives.
 - `dd`⁷: part of the `coreutils` package. A low level utility that can copy data from one format to another
 - `rsnapshot`⁸: a file system snap shot utility used to create copies of an entire file system.

2. Archive Rotation

The shell script in section *Section 1, "Shell Scripts" [p. 198]* only allows for seven different archives. For a server whose data doesn't change often this may be enough. If the server has a large amount of data a more robust rotation scheme should be used.

2.1. Rotating NFS Archives

In this section the shell script will be slightly modified to implement a grandfather-father-son rotation scheme (monthly-weekly-daily):

- The rotation will do a *daily* backup Sunday through Friday.
- On Saturday a *weekly* backup is done giving you four weekly backups a month.
- The *monthly* backup is done on the first of the month rotating two monthly backups based on if the month is odd or even.

Here is the new script:

```
#!/bin/bash
#####
#
# Backup to NFS mount script with
# grandfather-father-son rotation.
#
#####

# What to backup.
backup_files="/home /var/spool/mail /etc /root /boot /opt"

# Where to backup to.
dest="/mnt/backup"

# Setup variables for the archive filename.
day=$(date +%A)
hostname=$(hostname -s)

# Find which week of the month 1-4 it is.
day_num=$(date +%d)
if (( $day_num <= 7 )); then
    week_file="$hostname-week1.tgz"
elif (( $day_num > 7 && $day_num <= 14 )); then
    week_file="$hostname-week2.tgz"
elif (( $day_num > 14 && $day_num <= 21 )); then
    week_file="$hostname-week3.tgz"
elif (( $day_num > 21 && $day_num < 32 )); then
    week_file="$hostname-week4.tgz"
fi
```

```
# Find if the Month is odd or even.
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

# Create archive filename.
if [ $day_num == 1 ]; then
    archive_file=$month_file
elif [ $day != "Saturday" ]; then
    archive_file="$hostname-$day.tgz"
else
    archive_file=$week_file
fi

# Print start status message.
echo "Backing up $backup_files to $dest/$archive_file"
date
echo

# Backup the files using tar.
tar czf $dest/$archive_file $backup_files

# Print end status message.
echo
echo "Backup finished"
date

# Long listing of files in $dest to check file sizes.
ls -lh $dest/
```

The script can be executed using the same methods as in *Section 1.2, "Executing the Script"* [p. 199].

It is good practice to take backup media off site in case of a disaster. In the shell script example the backup media is another server providing an NFS share. In all likelihood taking the NFS server to another location would not be practical. Depending upon connection speeds it may be an option to copy the archive file over a WAN link to a server in another location.

Another option is to copy the archive file to an external hard drive which can then be taken off site. Since the price of external hard drives continue to decrease it may be cost affective to use two drives for each archive level. This would allow you to have one external drive attached to the backup server and one in another location.

2.2. Tape Drives

A tape drive attached to the server can be used instead of a NFS share. Using a tape drive simplifies archive rotation, and taking the media off site as well.

When using a tape drive the filename portions of the script aren't needed because the date is sent directly to the tape device. Some commands to manipulate the tape are needed. This is accomplished using `mt`, a magnetic tape control utility part of the `cpio` package.

Here is the shell script modified to use a tape drive:

```
#!/bin/bash
#####
#
# Backup to tape drive script.
#
#####

# What to backup.
backup_files="/home /var/spool/mail /etc /root /boot /opt"

# Where to backup to.
dest="/dev/st0"

# Print start status message.
echo "Backing up $backup_files to $dest"
date
echo

# Make sure the tape is rewound.
mt -f $dest rewind

# Backup the files using tar.
tar czf $dest $backup_files

# Rewind and eject the tape.
mt -f $dest rewoffl

# Print end status message.
echo
echo "Backup finished"
date
```



The default device name for a SCSI tape drive is `/dev/st0`. Use the appropriate device path for your system.

Restoring from a tape drive is basically the same as restoring from a file. Simply rewind the tape and use the device path instead of a file path. For example to restore the `/etc/hosts` file to `/tmp/etc/hosts`:

```
mt -f /dev/st0 rewind
tar -xzf /dev/st0 -C /tmp etc/hosts
```

3. Bacula

Bacula is a backup program enabling you to backup, restore, and verify data across your network. There are Bacula clients for Linux, Windows, and Mac OSX. Making it a cross platform network wide solution.

3.1. Overview

Bacula is made up of several components and services used to manage which files to backup and where to back them up to:

- Bacula Director: a service that controls all backup, restore, verify, and archive operations.
- Bacula Console: an application allowing communication with the Director. There are three versions of the Console:
 - Text based command line version.
 - Gnome based GTK+ Graphical User Interface (GUI) interface.
 - wxWidgets GUI interface.
- Bacula File: also known as the Bacula Client program. This application is installed on machines to be backed up, and is responsible for the data requested by the Director.
- Bacula Storage: the programs that perform the storage and recovery of data to the physical media.
- Bacula Catalog: is responsible for maintaining the file indexes and volume databases for all files backed up, enabling quick location and restoration of archived files. The Catalog supports three different databases MySQL, PostgreSQL, and SQLite.
- Bacula Monitor: allows the monitoring of the Director, File daemons, and Storage daemons. Currently the Monitor is only available as a GTK+ GUI application.

These services and applications can be run on multiple servers and clients, or they can be installed on one machine if backing up a single disk or volume.

3.2. Installation

There are multiple packages containing the different Bacula components. To install Bacula, from a terminal prompt enter:

```
sudo apt-get install bacula
```

By default installing the bacula package will use a MySQL database for the Catalog. If you want to use SQLite or PostgreSQL, for the Catalog, install bacula-director-sqlite3 or bacula-director-pgsql respectively.

During the install process you will be asked to supply credentials for the database *administrator* and the *bacula* database *owner*. The database administrator will need to have the appropriate rights to create a database, see *Section 1, "MySQL" [p. 128]* for more information.

3.3. Configuration

Bacula configuration files are formatted based on *resources* comprising of *directives* surrounded by “{}” braces. Each Bacula component has an individual file in the `/etc/bacula` directory.

The various Bacula components must authorize themselves to each other. This is accomplished using the *password* directive. For example, the *Storage* resource password in the `/etc/bacula/bacula-dir.conf` file must match the *Director* resource password in `/etc/bacula/bacula-sd.conf`.

By default the backup job named *Client1* is configured to archive the Bacula Catalog. If you plan on using the server to backup more than one client you should change the name of this job to something more descriptive. To change the name edit `/etc/bacula/bacula-dir.conf`:

```
#
# Define the main nightly save backup job
# By default, this job will back up to disk in
Job {
    Name = "BackupServer"
    JobDefs = "DefaultJob"
    Write Bootstrap = "/var/lib/bacula/Client1.bsr"
}
```



The example above changes the job name to *BackupServer* matching the machine's host name. Replace “BackupServer” with your appropriate hostname, or other descriptive name.

The *Console* can be used to query the *Director* about jobs, but to use the Console with a *non-root* user, the user needs to be in the *bacula* group. To add a user to the bacula group enter the following from a terminal:

```
sudo adduser $username bacula
```



Replace *\$username* with the actual username. Also, if you are adding the current user to the group you should log out and back in for the new permissions to take effect.

3.4. Localhost Backup

This section describes how to backup specified directories on a single host to a local tape drive.

- First, the *Storage* device needs to be configured. Edit `/etc/bacula/bacula-sd.conf` add:

```
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'"
}
```

The example is for a *DDS-4* tape drive. Adjust the Media Type and Archive Device to match your hardware.

You could also uncomment one of the other examples in the file.

- After editing `/etc/bacula/bacula-sd.conf` the Storage daemon will need to be restarted:

```
sudo /etc/init.d/bacula-sd restart
```

- Now add a *Storage* resource in `/etc/bacula/bacula-dir.conf` to use the new Device:

```
# Definition of "Tape Drive" storage device
Storage {
    Name = TapeDrive
    # Do not use "localhost" here
    Address = backupserver          # N.B. Use a fully qualified name here
    SDPort = 9103
    Password = "Cv70F6pflt6pBopT4vQOnigDrR0v3LT3Cgkiyj"
    Device = "Tape Drive"
    Media Type = tape
}
```

The *Address* directive needs to be the Fully Qualified Domain Name (FQDN) of the server. Change *backupserver* to the actual host name.

Also, make sure the *Password* directive matches the password string in `/etc/bacula/bacula-sd.conf`.

- Create a new *FileSet*, which will determine what directories to backup, by adding:

```
# LocalhostBacup FileSet.
FileSet {
    Name = "LocalhostFiles"
    Include {
        Options {
            signature = MD5
            compression=GZIP
        }
        File = /etc
        File = /home
    }
}
```

This *FileSet* will backup the `/etc` and `/home` directories. The *Options* resource directives configure the *FileSet* to create a MD5 signature for each file backed up, and to compress the files using GZIP.

- Next, create a new *Schedule* for the backup job:

```
# LocalhostBackup Schedule -- Daily.
Schedule {
    Name = "LocalhostDaily"
    Run = Full daily at 00:01
}
```

The job will run every day at 00:01 or 12:01 am. There are many other scheduling options available.

- Finally create the *Job*:

```
# Localhost backup.
Job {
    Name = "LocalhostBackup"
    JobDefs = "DefaultJob"
    Enabled = yes
    Level = Full
    FileSet = "LocalhostFiles"
    Schedule = "LocalhostDaily"
    Storage = TapeDrive
    Write Bootstrap = "/var/lib/bacula/LocalhostBackup.bsr"
}
```

The job will do a *Full* backup every day to the tape drive.

- Each tape used will need to have a *Label*. If the current tape does not have a label Bacula will send an email letting you know. To label a tape using the Console enter the following from a terminal:

```
bconsole
```

- At the Bacula Console prompt enter:

```
label
```

- You will then be prompted for the *Storage* resource:

```
Automatically selected Catalog: MyCatalog
Using Catalog "MyCatalog"
The defined Storage resources are:
    1: File
    2: TapeDrive
Select Storage resource (1-2):2
```

- Enter the new *Volume* name:

```
Enter new Volume name: sunday
```

```
Defined Pools:
```

```
1: Default
```

```
2: Scratch
```

Replace *Sunday* with the desired label.

- Now, select the *Pool*:

```
Select the Pool (1-2): 1
```

```
Connecting to Storage daemon TapeDrive at backupserver:9103 ...
```

```
Sending label command for Volume "Sunday" Slot 0 ...
```

Congratulations, you have now configured *Bacula* to backup the localhost to an attached tape drive.

3.5. Resources

- For more *Bacula* configuration options refer to the *Bacula User's Manual*⁹
- The *Bacula Home Page*¹⁰ contains the latest *Bacula* news and developments.

Chapter 17. Virtualization

Virtualization is being adopted in many different environments and situations. If you are a developer, virtualization can provide you with a contained environment where you can safely do almost any sort of development safe from messing up your main working environment. If you are a systems administrator, you can use virtualization to more easily separate your services and move them around based on demand.

The default virtualization technology supported in Ubuntu is KVM, a technology that takes advantage of virtualization extensions built into Intel and AMD hardware. For hardware without virtualization extensions Xen and Qemu are popular solutions.

1. libvirt

The libvirt library is used to interface with different virtualization technologies. Before getting started with libvirt it is best to make sure your hardware supports the necessary virtualization extensions for KVM. Enter the following from a terminal prompt:

```
egrep '(vmx|svm)' /proc/cpuinfo
```

If nothing is printed, it means that your cpu does *not* support hardware virtualization.



On most computer whose processor supports virtualization, it is necessary to activate an option in the bios to enable it. The method described above does not show the status of it's activation.

1.1. Virtual Networking

There are a few different ways to allow a virtual machine access to the external network. The default virtual network configuration is *usermode* networking, which uses the SLIRP protocol and traffic is NATed through the host interface to the outside network.

To enable external hosts to directly access services on virtual machines a *bridge* needs to be configured. This allows the virtual interfaces to connect to the outside network through the physical interface, making them appear as normal hosts to the rest of the network. For information on setting up a bridge see *Section 1.4, "Bridging" [p. 28]*.

1.2. Installation

To install the necessary packages, from a terminal prompt enter:

```
sudo apt-get install kvm libvirt-bin
```

After installing libvirt-bin, the user used to manage virtual machines will need to be added to the *libvirtd* group. Doing so will grant the user access to the advanced networking options.

In a terminal enter:

```
sudo adduser $USERNAME libvirtd
```



If the user chosen is the current user, you will need to log out and back in for the new group membership to take effect.

You are now ready to install a *Guest* operating system. Installing a virtual machine follows the same process as installing the operating system directly on the hardware. You either need a way to automate the installation, or a keyboard and monitor will need to be attached to the physical machine.

In the case of virtual machines a Graphical User Interface (GUI) is analogous to using a physical keyboard and mouse. Instead of installing a GUI the virt-viewer application can be used to connect

to a virtual machine's console using VNC. See *Section 1.6, “Virtual Machine Viewer”* [p. 214] for more information.

There are several ways to automate the Ubuntu installation process, for example using preseeds, kickstart, etc. Refer to the *Ubuntu Installation Guide*¹ for details.

Yet another way to install an Ubuntu virtual machine is to use `ubuntu-vm-builder`. `ubuntu-vm-builder` allows you to setup advanced partitions, execute custom post-install scripts, etc. For details see *Section 2, “JeOS and vmbuilder”* [p. 216]

1.3. virt-install

`virt-install` is part of the `python-virtinst` package. To install it, from a terminal prompt enter:

```
sudo apt-get install python-virtinst
```

There are several options available when using `virt-install`. For example:

```
sudo virt-install -n web_devel -r 256 -f web_devel.img -s 4 -c jeos.iso --accelerate --connect=qemu
```

- `-n web_devel`: the name of the new virtual machine will be `web_devel` in this example.
- `-r 256`: specifies the amount of memory the virtual machine will use.
- `-f web_devel.img`: indicates the path to the virtual disk which can be a file, partition, or logical volume. In this example a file named `web_devel.img`.
- `-s 4`: the size of the virtual disk.
- `-c jeos.iso`: file to be used as a virtual CDROM. The file can be either an ISO file or the path to the host's CDROM device.
- `--accelerate`: enables the kernel's acceleration technologies.
- `--vnc`: exports the guest's virtual console using VNC.
- `--noautoconsole`: will not automatically connect to the virtual machine's console.

After launching `virt-install` you can connect to the virtual machine's console either locally using a GUI or with the `virt-viewer` utility.

1.4. virt-clone

The `virt-clone` application can be used to copy one virtual machine to another. For example:

```
sudo virt-clone -o web_devel -n database_devel -f /path/to/database_devel.img --connect=qemu:///sys
```

- `-o`: original virtual machine.
- `-n`: name of the new virtual machine.

¹ <https://help.ubuntu.com/8.10/installation-guide/>

- *-f*: path to the file, logical volume, or partition to be used by the new virtual machine.
- *--connect*: specifies which hypervisor to connect to.

Also, use *-d* or *--debug* option to help troubleshoot problems with *virt-clone*.



Replace *web_devel* and *database_devel* with appropriate virtual machine names.

1.5. Virtual Machine Management

1.5.1. virsh

There are several utilities available to manage virtual machines and libvirt. The *virsh* utility can be used from the command line. Some examples:

- To list running virtual machines:

```
virsh -c qemu:///system list
```

- To start a virtual machine:

```
virsh -c qemu:///system start web_devel
```

- Similarly, to start a virtual machine at boot:

```
virsh -c qemu:///system autostart web_devel
```

- Reboot a virtual machine with:

```
virsh -c qemu:///system reboot web_devel
```

- The *state* of virtual machines can be saved to a file in order to be restored later. The following will save the virtual machine state into a file named according to the date:

```
virsh -c qemu:///system save web_devel web_devel-022708.state
```

Once saved the virtual machine will no longer be running.

- A saved virtual machine can be restored using:

```
virsh -c qemu:///system restore web_devel-022708.state
```

- To shutdown a virtual machine do:

```
virsh -c qemu:///system shutdown web_devel
```

- A CDROM device can be mounted in a virtual machine by entering:

```
virsh -c qemu:///system attach-disk web_devel /dev/cdrom /media/cdrom
```



In the above examples replace *web_devel* with the appropriate virtual machine name, and `web_devel-022708.state` with a descriptive file name.

1.5.2. Virtual Machine Manager

The `virt-manager` package contains a graphical utility to manage local and remote virtual machines. To install `virt-manager` enter:

```
sudo apt-get install virt-manager
```

Since `virt-manager` requires a Graphical User Interface (GUI) environment it is recommended to be installed on a workstation or test machine instead of a production server. To connect to the local `libvirt` service enter:

```
virt-manager -c qemu:///system
```

You can connect to the `libvirt` service running on another host by entering the following in a terminal prompt:

```
virt-manager -c qemu+ssh://virtnode1.mydomain.com/system
```



The above example assumes that SSH connectivity between the management system and `virtnode1.mydomain.com` has already been configured, and uses SSH keys for authentication. SSH keys are needed because `libvirt` sends the password prompt to another process. For details on configuring SSH see *Section 1, "OpenSSH Server" [p. 40]*

1.6. Virtual Machine Viewer

The `virt-viewer` application allows you to connect to a virtual machine's console. `virt-viewer` does require a Graphical User Interface (GUI) to interface with the virtual machine.

To install `virt-viewer` from a terminal enter:

```
sudo apt-get install virt-viewer
```

Once a virtual machine is installed and running you can connect to the virtual machine's console by using:

```
virt-viewer qemu:///system web_devel
```

Similar to `virt-manager`, `virt-viewer` can connect to a remote host using *SSH* with key authentication, as well:

```
virt-viewer -c qemu+ssh://virtnode1.mydomain.com/system web_devel
```

Be sure to replace *web_devel* with the appropriate virtual machine name.

If configured to use a *bridged* network interface you can also setup SSH access to the virtual machine. See *Section 1, “OpenSSH Server” [p. 40]* and *Section 1.4, “Bridging” [p. 28]* for more details.

1.7. Resources

- See the *KVM*² home page for more details.
- For more information on libvirt see the *libvirt home page*³
- The *Virtual Machine Manager*⁴ site has more information on virt-manager development.
- Also, stop by the *#ubuntu-virt* IRC channel on *freenode*⁵ to discuss virtualization technology in Ubuntu.

2. JeOS and vmbuilder

2.1. Introduction

2.1.1. What is JeOS

Ubuntu *JeOS* (pronounced "Juice") is an efficient variant of the Ubuntu Server operating system, configured specifically for virtual appliances. No longer available as a CD-ROM ISO for download, but only as an option either:

- While installing from the Server Edition ISO (pressing *F4* on the first screen will allow you to pick "Minimal installation", which is the package selection equivalent to JeOS).
- Or to be built using Ubuntu's vmbuilder, which is described here.

JeOS is a specialized installation of Ubuntu Server Edition with a tuned kernel that only contains the base elements needed to run within a virtualized environment.

Ubuntu JeOS has been tuned to take advantage of key performance technologies in the latest virtualization products from VMware. This combination of reduced size and optimized performance ensures that Ubuntu JeOS Edition delivers a highly efficient use of server resources in large virtual deployments.

Without unnecessary drivers, and only the minimal required packages, ISVs can configure their supporting OS exactly as they require. They have the peace of mind that updates, whether for security or enhancement reasons, will be limited to the bare minimum of what is required in their specific environment. In turn, users deploying virtual appliances built on top of JeOS will have to go through fewer updates and therefore less maintenance than they would have had to with a standard full installation of a server.

2.1.2. What is vmbuilder

With vmbuilder, there is no need to download a JeOS ISO anymore. vmbuilder will fetch the various package and build a virtual machine tailored for our need in about a minute for us. Vmbuilder is a Script that automates the process of creating a ready to use Linux based VM. The currently supported hypervisors are KVM and Xen.

You can pass command line options to add extra packages, remove packages, choose which version of Ubuntu, which mirror etc. On recent hardware with plenty of RAM, tmpdir in `/dev/shm` or using a tmpfs, and a local mirror, you can bootstrap a VM in less than a minute.

First introduced as a shell script in Ubuntu 8.04LTS, ubuntu-vm-builder started with little emphasis as a hack to help developers test their new code in a virtual machine without having to restart from scratch each time. As a few Ubuntu administrators started to notice this script, a few of them went on improving it and adapting it for so many use case that Soren Hansen (the author of the script and Ubuntu virtualization specialist, not the golf player) decided to rewrite it from scratch for Intrepid as a python script with a few new design goals:

- Develop it so that it can be reused by other distributions.
- Use a plugin mechanisms for all virtualization interactions so that others can easily add logic for other virtualization environments.
- Provide an easy to maintain web interface as an option to the command line interface.

But the general principles and commands remain the same.

2.2. Initial Setup

It is assumed that you have installed and configured libvirt and KVM locally on the machine you are using. For details on how to perform this, please refer to:

- *Section 1, “libvirt” [p. 211]*
- The *KVM*⁶ Wiki page.

We also assume that you know how to use a text based text editor such as nano or vi. If you have not used any of them before, you can get an overview of the various text editors available by reading the *PowerUsersTextEditors*⁷ page. This tutorial has been done on KVM, but the general principle should remain on other virtualization technologies.

2.2.1. Install vmbuilder

The name of the package that we need to install is python-vm-builder. In a terminal prompt enter:

```
sudo apt-get install python-vm-builder
```



If you are running Hardy, you can still perform most of this using the older version of the package named ubuntu-vm-builder, there are only a few changes to the syntax of the tool.

2.3. Defining Your Virtual Machine

Defining a virtual machine with Ubuntu's vmbuilder is quite simple, but here are a few thing to consider:

- If you plan on shipping a virtual appliance, do not assume that the end-user will know how to extend disk size to fit their need, so either plan for a large virtual disk to allow for your appliance to grow, or explain fairly well in your documentation how to allocate more space. It might actually be a good idea to store data on some separate external storage.
- Given that RAM is much easier to allocate in a VM, RAM size should be set to whatever you think is a safe minimum for your appliance.

The vmbuilder command has 2 main parameters: the *virtualization technology (hypervisor)* and the targeted *distribution*. Optional parameters are quite numerous and can be found using the following command:

⁷ <https://help.ubuntu.com/community/PowerUsersTextEditors>

```
vmbuilder --help
```

2.3.1. Base Parameters

As this example is based on KVM and Ubuntu 8.10 (Intrepid Ibex), and we are likely to rebuild the same virtual machine multiple time, we'll invoke vmbuilder with the following first parameters:

```
sudo vmbuilder kvm ubuntu --suite intrepid --flavour virtual --arch i386 -o --libvirt qemu:///system
```

The `--suite` defines the Ubuntu release, the `--flavour` specifies that we want to use the virtual kernel (that's the one used to build a JeOS image), the `--arch` tells that we want to use a 32 bit machine, the `-o` tells vmbuilder to overwrite the previous version of the VM and the `--libvirt` tells to inform the local virtualization environment to add the resulting VM to the list of available machines.

Notes:

- Because of the nature of operations performed by vmbuilder, it needs to have root privilege, hence the use of `sudo`.
- If your virtual machine needs to use more than 3Gb of ram, you should build a 64 bit machine (`--arch amd64`).
- Until Ubuntu 8.10, the virtual kernel was only built for 32 bit architecture, so if you want to define an amd64 machine on Hardy, you should use `--flavour server` instead.

2.3.2. JeOS Installation Parameters

2.3.2.1. JeOS Networking

2.3.2.1.1. Assigning a fixed IP address

As a virtual appliance that may be deployed on various very different networks, it is very difficult to know what the actual network will look like. In order to simplify configuration, it is a good idea to take an approach similar to what network hardware vendors usually do, namely assigning an initial fixed IP address to the appliance in a private class network that you will provide in your documentation. An address in the range 192.168.0.0/255 is usually a good choice.

To do this we'll use the following parameters:

- `--ip ADDRESS`: IP address in dotted form (defaults to dhcp if not specified)
- `--mask VALUE`: IP mask in dotted form (default: 255.255.255.0)
- `--net VALUE`: IP net address (default: X.X.X.0)
- `--bcast VALUE`: IP broadcast (default: X.X.X.255)
- `--gw ADDRESS`: Gateway address (default: X.X.X.1)
- `--dns ADDRESS`: Name server address (default: X.X.X.1)

We assume for now that default values are good enough, so the resulting invocation becomes:

```
sudo vmbuilder kvm ubuntu --suite intrepid --flavour virtual --arch i386 -o --libvirt qemu:///system
```

2.3.2.1.2. Modifying the libvirt Template to use Bridging

Because our appliance will be likely to need to be accessed by remote hosts, we need to configure libvirt so that the appliance uses bridge networking. To do this we use vmbuilder template mechanism to modify the default one.

In our working directory we create the template hierarchy and copy the default template:

```
mkdir -p VMBuilder/plugins/libvirt/templates
cp /etc/vmbuilder/libvirt/* VMBuilder/plugins/libvirt/templates/
```

We can then edit `VMBuilder/plugins/libvirt/templates/libvirtxml.tmpl` to change:

```
<interface type='network'>
  <source network='default' />
</interface>
```

To:

```
<interface type='bridge'>
  <source bridge='br0' />
</interface>
```

2.3.2.2. Partitioning

Partitioning of the virtual appliance will have to take into consideration what you are planning to do with it. Because most appliances want to have a separate storage for data, having a separate `/var` would make sense.

In order to do this vmbuilder provides us with `--part`:

```
--part PATH
Allows to specify a partition table in partfile each line of partfile should specify
(root first):
  mountpoint size
where size is in megabytes. You can have up to 4 virtual disks, a new disk starts on a
line with '---'. ie :
  root 1000
  /opt 1000
  swap 256
  ---
  /var 2000
  /log 1500
```

In our case we will define a text file name `vmbuilder.partition` which will contain the following:

```
root 8000
swap 4000
---
/var 20000
```



Note that as we are using virtual disk images, the actual sizes that we put here are maximum sizes for these volumes.

Our command line now looks like:

```
sudo vmbuilder kvm ubuntu --suite intrepid --flavour virtual --arch i386 \
-o --libvirt qemu:///system --ip 192.168.0.100 --part vmbuilder.partition
```



Using a "\" in a command will allow long command strings to wrap to the next line.

2.3.2.3. User and Password

Again setting up a virtual appliance, you will need to provide a default user and password that is generic so that you can include it in your documentation. We will see later on in this tutorial how we will provide some security by defining a script that will be run the first time a user actually logs in the appliance, that will, among other things, ask him to change his password. In this example I will use *'user'* as my user name, and *'default'* as the password.

To do this we use the following optional parameters:

- `--user USERNAME`: Sets the name of the user to be added. Default: ubuntu.
- `--name FULLNAME`: Sets the full name of the user to be added. Default: Ubuntu.
- `--pass PASSWORD`: Sets the password for the user. Default: ubuntu.

Our resulting command line becomes:

```
sudo vmbuilder kvm ubuntu --suite intrepid --flavour virtual --arch i386 \
-o --libvirt qemu:///system --ip 192.168.0.100 --part vmbuilder.partition \
--user user --name user --pass default
```

2.3.3. Installing Required Packages

In this example we will be installing a package (Limesurvey) that accesses a MySQL database and has a web interface. We will therefore require our OS to provide us with:

- Apache
- PHP
- MySQL
- OpenSSH Server
- Limesurvey (as an example application that we have packaged)

This is done using `vmbuilder` by specifying the `--addpkg` command multiple times:

```
--addpkg PKG
    Install PKG into the guest (can be specified multiple times)
```

However, due to the way `vmbuilder` operates, packages that have to ask questions to the user during the post install phase are not supported and should instead be installed while interactivity can occur. This is the case of `Limesurvey`, which we will have to install later, once the user logs in.

Other packages that ask simple `debconf` question, such as `mysql-server` asking to set a password, the package can be installed immediately, but we will have to reconfigure it the first time the user logs in.

If some packages that we need to install are not in `main`, we need to enable the additional repositories using `--comp` and `--ppa`:

```
--components COMP1,COMP2,...,COMPn
    A comma separated list of distro components to include (e.g. main,universe). This default
    to "main"
--ppa=PPA Add ppa belonging to PPA to the vm's sources.list.
```

`Limesurvey` not being part of the archive at the moment, we'll specify it's PPA (personal package archive) address so that it is added to the VM `/etc/apt/source.list`, so we add the following options to the command line:

```
--addpkg apache2 --addpkg apache2-mpm-prefork --addpkg apache2-utils --addpkg apache2.2-common \
--addpkg dbconfig-common --addpkg libapache2-mod-php5 --addpkg mysql-client --addpkg php5-
--addpkg php5-gd --addpkg php5-ldap --addpkg php5-mysql --addpkg wwwconfig-common \
--addpkg mysql-server --ppa nijaba
```

2.3.3.1. *OpenSSH*

Another convenient tool that we want to have on our appliance is `OpenSSH`, as it will provide our admins to access to access the appliance remotely. However, pushing in the wild an appliance with a pre-installed `OpenSSH` server is a big security risk as all these server will share the same secret key, making it very easy for hackers to target our appliance with all the tools they need to crack it open in a breeze. As for the user password, we will instead rely on a script that will install `OpenSSH` the first time a user logs in so that the key generated will be different for each appliance. For this we'll use a `--firstboot` script, as it does not need any user interaction.

2.3.4. Speed Considerations

2.3.4.1. *Package Caching*

When `vmbuilder` creates builds your system, it has to go fetch each one of the packages that composes it over the network to one of the official repositories, which, depending on your internet connection speed and the load of the mirror, can have a big impact on the actual build time. In order to reduce

this, it is recommended to either have a local repository (which can be created using `apt-mirror`) or using a caching proxy such as `apt-cache`. The later option being much simpler to implement and requiring less disk space, it is the one we will pick in this tutorial. To install it, simply type:

```
sudo apt-get install apt-proxy
```

Once this is complete, your (empty) proxy is ready for use on `http://mirroraddress:9999` and will find ubuntu repository under `/ubuntu`. For `vmbuilder` to use it, we'll have to use the `--mirror` option:

```
--mirror=URL Use Ubuntu mirror at URL instead of the default, which
             is http://archive.ubuntu.com/ubuntu for official
             arches and http://ports.ubuntu.com/ubuntu-ports
             otherwise
```

So we add to the command line:

```
--mirror http://mirroraddress:9999/ubuntu
```



The mirror address specified here will also be used in the `/etc/apt/source.list` of the newly created guest, so it is useful to specify here an address that can be resolved by the guest or to plan on resetting this address later on, such as in a `--firstboot` script.

2.3.4.2. Install a Local Mirror

If we are in a larger environment, it may make sense to setup a local mirror of the Ubuntu repositories. The package `apt-mirror` provides you with a script that will handle the mirroring for you. You should plan on having about 20 gigabyte of free space per supported release and architecture.

By default, `apt-mirror` uses the configuration file in `/etc/apt/mirror.list`. As it is set up, it will replicate only the architecture of the local machine. If you would like to support other architectures on your mirror, simply duplicate the lines starting with “deb”, replacing the deb keyword by `/deb-{arch}` where arch can be `i386`, `amd64`, etc... For example, on an `amd64` machine, to have the `i386` archives as well, you will have:

```
deb http://archive.ubuntu.com/ubuntu intrepid main restricted universe multiverse
/deb-i386 http://archive.ubuntu.com/ubuntu intrepid main restricted universe multiverse

deb http://archive.ubuntu.com/ubuntu intrepid-updates main restricted universe multiverse
/deb-i386 http://archive.ubuntu.com/ubuntu intrepid-updates main restricted universe multiverse

deb http://archive.ubuntu.com/ubuntu/ intrepid-backports main restricted universe multiverse
/deb-i386 http://archive.ubuntu.com/ubuntu intrepid-backports main restricted universe multiverse

deb http://security.ubuntu.com/ubuntu intrepid-security main restricted universe multiverse
/deb-i386 http://security.ubuntu.com/ubuntu intrepid-security main restricted universe multiverse

deb http://archive.ubuntu.com/ubuntu intrepid main/debian-installer restricted/debian-installer uni
```

```
/deb-i386 http://archive.ubuntu.com/ubuntu intrepid main/debian-installer restricted/debian-installer
```

Notice that the source packages are not mirrored as they are seldom used compared to the binaries and they do take a lot more space, but they can be easily added to the list.

Once the mirror has finished replicating (and this can be quite long), you need to configure Apache so that your mirror files (in `/var/spool/apt-mirror` if you did not change the default), are published by your Apache server. For more information on Apache see *Section 1, "HTTPD - Apache2 Web Server" [p. 111]*.

2.3.5. Installing in a RAM Disk

As you can easily imagine, writing to RAM is a *LOT* faster than writing to disk. If you have some free memory, letting `vmbuilder` perform its operation in a RAMdisk will help a lot and the option `--tmpfs` will help you do just that:

```
--tmpfs OPTS Use a tmpfs as the working directory, specifying its
              size or "-" to use tmpfs default (suid,dev,size=1G).
```

So adding `--tmpfs` - sounds like a very good idea if you have 1G of free ram.

2.4. Package the Application

Two options are available to us:

- The recommended method to do so is to make a *Debian* package. Since this is outside of the scope of this tutorial, we will not perform this here and invite the reader to read the documentation on how to do this in the *Ubuntu Packaging Guide*⁸. In this case it is also a good idea to setup a repository for your package so that updates can be conveniently pulled from it. See the *Debian Administration*⁹ article for a tutorial on this.
- Manually install the application under `/opt` as recommended by the *FHS guidelines*¹⁰.

In our case we'll use Limesurvey as example web application for which we wish to provide a virtual appliance. As noted before, we've made a version of the package available in a PPA (Personal Package Archive).

2.5. Finishing Install

2.5.1. First Boot

As we mentioned earlier, the first time the machine boots we'll need to install `openssh-server` so that the key generated for it is unique for each machine. To do this, we'll write a script called `boot.sh` as follows:

```
# This script will run the first time the virtual machine boots
# It is ran as root.
```

```
apt-get update
apt-get install -qqy --force-yes openssh-server
```

And we add the **--firstboot boot.sh** option to our command line.

2.5.2. First Login

Mysql and Limesurvey needing some user interaction during their setup, we'll set them up the first time a user logs in using a script named login.sh. We'll also use this script to let the user specify:

- His own password
- Define the keyboard and other locale info he wants to use

So we'll define login.sh as follows:

```
# This script is ran the first time a user logs in

echo "Your appliance is about to be finished to be set up."
echo "In order to do it, we'll need to ask you a few questions,"
echo "starting by changing your user password."

passwd

#give the opportunity to change the keyboard
sudo dpkg-reconfigure console-setup

#configure the mysql server root password
sudo dpkg-reconfigure mysql-server-5.0

#install limesurvey
sudo apt-get install -qqy --force-yes limesurvey

echo "Your appliance is now configured. To use it point your"
echo "browser to http://serverip/limesurvey/admin"
```

And we add the **--firstlogin login.sh** option to our command line.

2.6. Useful Additions

2.6.1. Configuring Automatic Updates

To have your system be configured to update itself on a regular basis, we will just install unattended-upgrades, so we add the following option to our command line:

```
--addpkg unattended-upgrades
```

As we have put our application package in a PPA, the process will update not only the system, but also the application each time we update the version in the PPA.

2.6.2. ACPI Event Handling

For your virtual machine to be able to handle restart and shutdown events it is being sent, it is a good idea to install the acpid package as well. To do this we just add the following option:

```
--addpkg acpid
```

2.7. Final Command

Here is what the command with all the options discussed above:

```
sudo vmbuilder kvm ubuntu --suite intrepid --flavour virtual --arch i386 -o \  
  --libvirt qemu:///system --ip 192.168.0.100 --part vmbuilder.partition --user user \  
  --name user --pass default --addpkg apache2 --addpkg apache2-mpm-prefork \  
  --addpkg apache2-utils --addpkg apache2.2-common --addpkg dbconfig-common \  
  --addpkg libapache2-mod-php5 --addpkg mysql-client --addpkg php5-cli \  
  --addpkg php5-gd --addpkg php5-ldap --addpkg php5-mysql --addpkg wwwconfig-common \  
  --addpkg mysql-server --addpkg unattended-upgrades --addpkg acpid --ppa nijaba \  
  --mirror http://mirroraddress:9999/ubuntu --tmpfs - --firstboot boot.sh \  
  --firstlogin login.sh es
```

2.8. Resources

If you are interested in learning more, have questions or suggestions, please contact the Ubuntu Server Team at:

- IRC: #ubuntu-server on freenode
- Mailing list: *ubuntu-server at lists.ubuntu.com*¹¹